République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la recherche Scientifique
Université Abou Bekr Belkaid - Tlemcen
Faculté des sciences de l'Ingénieur
Département d'Informatique

Laboratoire de Recherche
«Systèmes, Technologies de l'Information et de la Communication »

Thèse de Doctorat
Spécialité: Informatique

Présentée par
KADRI Benamar

Thème:

Mobile Ad hoc Networks Management:

Routing and Security

Soutenue devant le jury :

Président du Jury : M.A. CHIKH, Maître de Conférences, Université ABB- Tlemcen

Directeur de Thèse : M. FEHAM, Professeur, Université ABB- Tlemcen

Examinateurs :
A. BENYETTOU, Professeur, Université des Sciences et de la Technologie d'Oran
M. ABDALLAH, Maître de Conférences, Telecom & Management Sud-Paris
H.LABIOD, Maître de Conférences, Télécom Paris Tech Sud-Paris
M.A. ABDERRAHIM, Maître de Conférences, Université ABB- Tlemcen

Invité : M. LEHSAINI, Maître de Conférences, Université ABB- Tlemcen

Dedication

To the memory of my brother,

My parents,

My brother,

My sister.

Benamar

Acknowledgements

First and foremost I thank Allah,

My dept thanks to Pr Feham Mohamed the director of this thesis for his patience and encouragement in order to achieve this work. I would also appreciate his characters in managing and directing the STIC lab,

I would also thank Mr M'hamed Abdellah from the national institute of telecommunication in France for his guidance, support and help especially during the publications of my papers,

I would also thank the members of jury:

Mr M.A. CHIKH et Mr M.A. ABDERRAHIM de Université ABB à Tlemcen, Mr A. BENYETTOU de Université des Sciences et de la Technologie d'Oran, ainsi que Mm H.LABIOD de Télécom Paris Tech Sud-Paris, for accepting to judge this work and for their patient when reading it.

ملخص

عرفت العشريات الأخيرة تطورا كبيرا لتقنيات الاتصالات، خاصة منها اللاسلكية و التي خلال أعوام استطاعت أن تستحوذ على نطاق واسع من حياتنا اليومية عبر شبكات لاسلكية عوضت السلكية منها التي لم يعد لها وجود إلا في بعض المجالات المحدودة. و نظرا لسهولة الاستخدام و بناء الشبكات اللاسلكية عرفت هذه الأخيرة تطورا و استخدامات لا تعد و لا تحصى في مجالات عدة مثل العسكرية، الطبية، الصناعية والمدنية.

هذه الشبكات مكونة في مجملها من مجموعة من الهواتف النقالة أو الحواسب المحمولة أو أي جهاز الكتروني يستطيع الاتصال لا سلكيا مع جهاز أخر يكون ضمن نطاق بضع سنتمترات لتشكيل شبكة جسمية أو عشرة أمتار في شبكة شخصية أو اكتر من مائة مترفي شبكة محلية.

و مواكبة لهذا التطور عرفت الساحة العلمية تطوير مجموعة من البروتوكولات و الميكانيزمات من اجل مسايرة خصائص هذه الشبكات مثل النقص في الطاقة و الحركة المستمرة للأجهزة. و لكن تبقى هذه البروتوكولات غير قادرة على ضمان الحد الأدنى من الخدمة في ظروف معينة للشبكة، و عليه فان هذه الأطروحة تتناول هذه الإشكالية بتقديم مجموعة من الحلول و الاقتراحات العملية لحلها أخدين بعين الاعتبار الخصائص و العوائق في هذه الشبكات، مقدمين بذلك حلول لإشكاليات كلاسيكية مثل routing, secuirty, QoS.

Abstract

Last decades have known a great development of telecommunication technologies especially the wireless ones, which have known a great use in our quotidian life, by the emergence of small wireless networks which have replaced the wired ones, which day after day become useless, compared to the wireless ones which are more efficient and flexible.

A wireless ad hoc network is essentially composed of small mobile phones, PDA, laptops or any device having the capacity to communicate with another device in the range of few centimeters for sensor or body networks, to ten miters for personnel networks or more than hundred of miters in a local area network.

For managing the diversity of these networks lot of protocols and algorithms have been developed in order to ensure the data forwarding and security. However due to the network characteristics such as device and medium constraints theses protocols are not efficient for some configurations and states of the network.

Therefore in this thesis we have developed a set of techniques and algorithms in order to manage the complexity and the constraints of these networks such as energy constraints, mobility, bandwidth…etc. The developed algorithms in this thesis are more efficient and have given best results compared to the existed ones regarding the end to end delay as well as the system lifetime, giving solution to classical problematic of ad hoc networks such as QoS, routing, security.

Résumé

Les dernières décennies ont connu un très grand essor des techniques de communication et spécialement les technologies sans fils, ces technologies qui ont pu dans quelques années gagner une très grande part de notre vie quotidienne, par l'émergence de petits réseaux sans fil qui ont remplacé ses prédécesseurs filaires, de plus en plus moins utilisés.

Un réseau ad hoc sans fil est essentiellement composé de petits téléphones portables, PC, PDA et n'importe quel appareil qui a la possibilité de communiquer sans fil avec un autre appareil dans le périmètre de quelques centimètres pour composer un réseau de capteurs, ou bien d'une dizaine de mètres pour composer un réseau personnel, ou aller jusqu'à cent mètres pour composer un réseau local sans fil.

Pour gérer la diversité de ces réseaux, plusieurs protocoles et algorithmes ont été développés pour assurer le routage et la sécurité des échanges de données à travers un réseau sans fil. Cependant ces protocoles se voient incapables de gérer toutes les contraintes des réseaux ad hoc telle que la mobilité et les capacités des nœuds qui sont très limitées par rapport aux nœuds des réseaux conventionnels.

Dans le même contexte cette thèse a été développée pour faire face aux problèmes rencontrés dans ces réseaux et gérer leurs inconvénients en analysant en détail ces réseaux et leurs problématiques, en développant des algorithmes de sécurité et de routage tenant compte des contraintes de ces réseaux telles que les contraintes d'énergie, de la mobilité, de la bande passante…etc, et proposant ainsi des solutions efficaces pour des problèmes classiques tels que la QoS, la sécurité et le routage.

Table of contents

Chapter I

Introduction to mobile ad hoc networks

Chapter II

Enhancing reactive routing protocols in MANETs

Chapter III

Swarm intelligence based routing in MANETs

Chapter IV

Securing reactive routing protocols in MANETs using PKI (PKI-SR)

Chapter V

Lightweight PKI for WSN μPKI

Chapter VI

Power control issues in sensor and ad hoc networks

List of figures

List of tables

General introduction

The first use of the wireless technology was by Marconi in 1901 in order to connect the European continent with the American one. Since this date the wireless technology has become a priority in the world of telecommunications given birth to new applications such as the radio, television, mobile phone and satellite which has considerably improved the human life.

Last years have known a great development of wireless networks, a technology developed specially to wirelessly connect handled devices such as laptops, mobile phone, PDAs…etc which have recently taken the great part of our lives.

Regarding their characteristics such as flexibility, scalability, mobility and costless, the wireless networks have known numerous classes of use, ranging from the personal ones to connect digital devices in our houses to the sensor ones used for surveillance in battlefields.

In the other hands, the wireless networks have lot of shortcomings and unsolved problematic such as routing, security, energy saving…etc, which constitute the biggest challenges for the impressive success of these networks.

Thus, in this thesis we are going to study the wireless networks especially the mobile ad hoc (MANETS) ones which are the most promising ones regarding their advantages and the large domains of application in the nearer future, our study gives a set of solutions and improvement of the existed ones for the most crucial problematic of ad hoc network which are routing, security and energy saving.

The manuscript of this thesis is composed of two parts:

The first part is composed of four chapters and devoted to security and routing in ad hoc network:

The first chapter gives a brief introduction to wireless ad hoc networks, their characteristics, applications and challenges. In the first half of this chapter we give a general definition of the terminology of ad hoc network. However the second half of this chapter is dedicated to the exposition of the most crucial problems of ad hoc networks which are security and routing by giving a state of the art of the existed routing algorithms and their strategy as well as the envisaged strategies taking place in recent years such cross-layering and swarm intelligence. Then in the rest of this chapter we give a brief introduction to security in ad hoc networks and the existed solution of implementing Public Key Infrastructure which is the most powerful tool for securing wired and wireless networks.

The second chapter treats the aspect of routing in ad hoc network, especially the reactive ones which are more suitable for ad hoc network since they react according to the state of the network and give solutions accordingly. In literature there is lot of relative protocols however

they do not include all the aspects of ad hoc network such as QoS, energy and mobility in the process of route establishment, which makes them not suitable for lot of configurations of ad hoc networks. Our proposed improvements for reactive routing makes use of cross-layer design and gives birth to new methods of routing based on more then one criterion which was the number of hops between the source and the destination nodes in the conventional networks. The application of our proposed strategies, on the Dynamic Source Routing called QoS based DSR includes the aspect of bandwidth in route selection and the Weight based DSR which includes the aspect of mobility and energy in route selection, have given best result regarding the end to end delay and the system lifetime.

The third chapter presents a new method of routing in ad hoc networks known in literature as swarm intelligence based routing. This category of routing is inspired from biological behavior of great communities of insects. The strategy used by ants or bees for finding the shortest path in the large nature can be used in ad hoc networks to find the best path between each communicating nodes over the network. This chapter is divided in two parts, the first part gives a brief definition and a state of the art of the swarm intelligence based routing for ad hoc networks, however the second part is dedicated to our proposed contribution in this domain which makes use of more parameters in the process of route establishment reflecting best the state of the network.

Chapter four is completely devoted to securing reactive routing protocols in ad hoc networks. Regarding the advantages of both reactive and PKI infrastructure for ad hoc network we tried in this chapter to implement a PKI infrastructure over reactive routing, by using the existed mechanisms of the underlying protocols such as route discovery and reply to publish, renew and revoke certificate in a PKI. Our proposed solution gives a set of procedures and mechanisms to secure end to end communication using symmetric cryptography and ensure authentication, integrity and intrusion detection using digital signature. Regarding the strategy of our proposed security scheme, it does not add any overhead to the network and does not affect the network performance.

The second part of this thesis is devoted to sensor networks; which have known great development recently gaining a vast range of applications. This part is composed of the two chapters five and six, which treat the aspect of security and energy saving in sensor networks:

The chapter five is dedicated for security in ad hoc networks, which is one of the most important and crucial problematic of these networks regarding their limited capacities in term of computing and battery power as well as the environment of deployment which is usually hostile. Our proposed solution for security is based on the PKI infrastructure called μPKI using a subset of specifications of the conventional PKI in order to secure sensor to sensor links as well as sensor to base station links using both symmetric and asymmetric encryption.

Compared to existed solution in literature μPKI gives best threshold of security with the minimum of energy consuming.

The chapter six treats the aspect of energy in sensor networks by exposing a set of criteria and aspects of energy saving in sensor networks. This chapter is divided into two parts; the first part briefly presents the aspect of power control in wireless network and its effect on the network lifetime as well as the performance of the network. The second part of this chapter is dedicated to our implementation of an energy control mechanism on the MAC layer and the simulation results which exhibits the advantages of the implementation of our method for power control regarding the system lifetime.

Chapter I

Introduction to mobile ad hoc networks

Mobile Ad hoc Networks are deployed in many new domestic and public applications, due to their costless and facility of use rising to new requirements in terms of performance and efficiency. However due to their nature, some usual network services as routing and security are not carried out as well as expected. Therefore, in this chapter we give a brief introduction to mobile ad hoc networks, their characteristics and challenges as well as their problematic such as security and routing which are the most challenging tasks to be carried out by future networks. We also provide the necessary issues to be handled by the future designed protocols for ad hoc network.

1. Introduction to MANETs

1.1 Definition

A Mobile ad hoc network is defined as a collection of mobile nodes (Figure I.1), which can vary from notebooks, PDAs, cellular phones, laptops to any electronic devices using as transmission medium radio waves [1]. Mobility, variety of devices and no-infrastructure form the basis of this network type [2].

Unlike infrastructure based wireless networks and other conventional ones, MANETs don't need any infrastructure or pre-configuration to create and maintain communication between nodes. Mobile nodes collaborate between themselves for creating and maintaining the connectivity in the networks. Thus, mobile nodes communicate with each other through multi-hop wireless links, without the existence of any infrastructure or administrative authority for routing or security [3]. This property provides the ability to quickly create a network in very unexpected and urgent situations without any extra cost or additional installation or infrastructures [4].

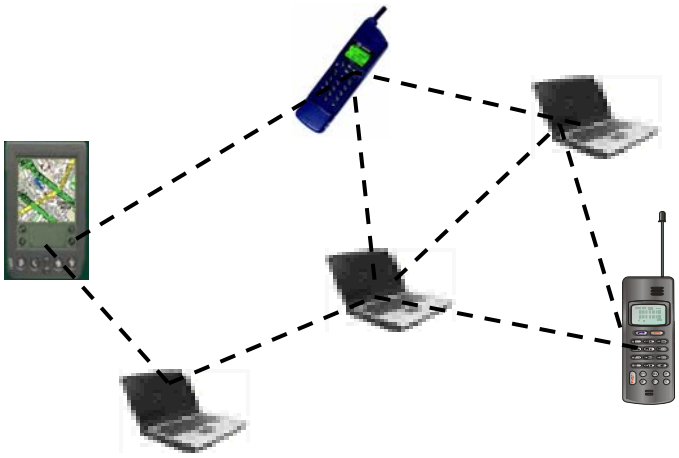


Figure I.1 Mobile Ad hoc network

The used spectre for wireless transmissions is the spectre situated around the 2.4 GHz ISM (Industrial, Scientific and Medical), and around the 5 GHz U-NII (Unlicensed-National Information Infrastructure). The transmission range and the emission power are regulated by laws in each country depending on the location where the network is deployed (indoor or outdoor), ranging from 10 m for Personal Area Networks to 100-200 m for Local Area Networks [5].

Typically MANETs are costless, too easy for use and deployment, which gives them lot of fields of use every day ranging from military applications for connecting soldier in battlefields to civilian or commercial applications such as Public and Personal Area Networks as well as sensor networks for monitoring or surveillance [6].

1.2 Existed standards

To handle the specificity of these networks and the nature of the used medium numerous standards are developed for each kind of ad hoc networks:

- **IEEE 802.11:** this standard is designed for WLANs (Wireless Local Area Networks). From the point of view of the physical layer, it defines three techniques: IEEE 802.11 FHSS (Frequency Hopping Spread Spectrum) and IEEE 802.11 DSSS (Direct Sequence Spread Spectrum), which use both the radio medium at 2.4 GHZ [7] and 5 GHZ [8], and IEEE 802.11 IR (InfraRed) [9]. IEEE 802.11 has modified the link layer of IEEE 802.2 (Ethernet) by changing the mechanism of accessing the physical layer which is the radio waves and keeps the LLC (*Logical Link Control*) the same as in IEEE 802.2 which gives it the possibility to operate with Ethernet network which is the most used standard in conventional network [10]. These specifications have given birth to a family of other standards: IEEE 802.11a [11], IEEE 802.11b [12], IEEE 802.11g [13], IEEE 802.11e [14], IEEE 802.11f [15], IEEE 802.11h [16], IEEE 802.1X [17] and IEEE 802.11i [18].
- **IEEE 802.15**: IEEE 802.15 also known as Bluetooth [19] is a standard designed by a consortium of private companies such as Ericsson, IBM, Intel, Microsoft, Motorola, Nokia and Toshiba for WPANs (Wireless Personal Area Networks). Bluetooth operates in the 2.4 GHz band using FHSS and has a short range of action of about 10 meters [20]. For such characteristics and its low cost, Bluetooth is fit for small WPANs and is also employed to connect peripherals such as keyboards, printers, or mobile phone headsets. Bluetooth radio technology works in a master-slave fashion, and each device can operate as master or as slave.
- **IEEE 802.16:** This standard is currently under tests [21] (marketed as WiMAX), is designed for WMANs (Wireless Metropolitan Area Networks) to overcome the range limitations of IEEE 802.11. It operates on frequencies from 10 to 66 GHz, and should ensure network coverage for several square Kilometres.
- **IEEE 802.20:** Also known as Wi-Mobile [22] it operates at the same level as UMTS [23] or CDMA2000 [24]. It is designed for WWANs (Wireless Wide Area Networks), it is considered as a concurrent of these two techniques. It may be largely used since it has low cost compared to UMTS, because it use existed techniques already developed like IP and Ethernet.

The table I.1 gives a list of existed wireless technologies with their transmission range, frequency, bandwidth and medium access technology:

	Max data rate	Frequency	Number of RF channels	Access technology	Transmission range
Bluetooth	1 Mbs	2,4 Ghz	79	FHSS	10 m
UWB	110 Mbs	3,1-10,6 Ghz	1-15	OFDM	10-15 m
IEEE 802.11b	11 Mbs	2,4-2,497 Ghz	3	DSSS	50-80 m
EEE 802.11a	54 Mbs	5 Ghz	4-12	OFDM	40-60 m
GPRS	171 Mbs	800-900 Ghz 1800 Ghz	-	TDMA with FDD	1-5 Km
UMTS	2 Mbs	1920-1980 Ghz 2210-2170 Ghz	-	DSSS	1-3 Km

Table I.4 Characteristics of wireless networks

1.3 Benefits of ad hoc networks

Wireless ad hoc networks offer four primary benefits:

- **User Mobility:** although, an ad hoc network is a collection of small devices connected to each other via wireless links giving them the possibility to be mobile and attached to the network in the same time to benefit from the network services such as files sharing, network resources, and the Internet without having to physically being connected to the network with wires [25].
- **Rapid Installation:** The time required for the installation of an ad hoc network is insignificant; since no wires or extra components are added to ensure devices connection. Because the elaboration of an ad hoc network needs a set of nodes having only wireless NIC (Network Interface Controller) and sharing the same network stack [26].
- **Flexibility:** Ad hoc networks are also flexible; since it can easily be configured to meet specific application and installation needs in addition it can be deployed in different environment, ranging from battlefields to conferences, trade show, or standards meeting [27].
- **Scalability:** an Ad hoc network can scales easily from a small peer to peer network to a very large network composed of thousands of devices, because no additive installation is needed for the increasing number of nodes and each new coming node is automatically attached to the network if it has the necessary hardware and the network stack [28].

1.4 Applications of ad hoc networks

Regarding their effectiveness, costless and facility of deployment, ad hoc networks gain every day new applications ranging form military to civilian ones. This section will cover some famous applications where ad hoc networks are used but the list isn't exhaustive and other applications may exist everywhere when a deployment of an infrastructure network is costly or difficult:

- **Military Tactical Networks:** in the military domain ad hoc networks are essentially used to connect vehicles and soldier in battlefields as well as collecting information about the enemy, where the installation of wires is not possible [29].
- **Personal Area Networks:** in personal networks only one person connects his digital devices such as his PDA, cellular phone, laptop etc, as well as connecting his house digital devices such as his television, PC, refrigerator, alarm system…etc. these kind of network are more and more promising due to the revolution of digital component in our houses [30].
- **Sensor Networks:** Sensor networks are a set of hundreds or thousands of sensors scattered in a given area in order to collect chemical, nuclear, pressure…etc parameters where the presence of humans is not possible. Sensor network know a great success in scientific domain such as environment and habitat monitoring [31].
- **Disaster Area Networks:** in catastrophic environment ad hoc network are the most adequate networks regarding the rapidity and facility of deployment which is much needed in such situation. In addition the infrastructure is very often destroyed by natural disasters or other events. Thus such networks could be used to improve the communication among rescue workers and other personnel and thereby support the relief efforts [32].
- **Public Area Networks:** This kind of network is deployed in public area like air port markets or in hotspots. Wireless network allows people to be connected to the existed local area network and profit from the services of the existed network, which allows the presentation of other services like publicity or the e-buy in this area [33].

2. Characteristics of ad hoc networks

In this section we are going to name some of the most important characteristics of wireless ad hoc networks; these characteristics can be seen as advantages of ad hoc networks and motivations for using this kind of networks. However, in some conditions these characteristics are also disadvantages and cause the most challenging problematic of ad hoc network such as security and routing:

- **Dynamic Topologies:** typically nodes in an Ad hoc network move unpredictably and cause topology changing. Thus, links between nodes can be broken at any time due to nodes' movement. This salient feature of ad hoc networks makes it difficult to establish secure key distribution and routing protocols for mobile ad hoc networks because there is no stable topology used to build an effective security or routing protocol [34].

- **Limited Bandwidth:** nodes in ad hoc networks rely on wireless links for communication with each other. However, due to some criteria of the radio waves such as the fading, noises and interferences, the wireless links have less bandwidth compared to the traditional wired networks. Thus, the usual services such as routing are hardly carried out and the existed methods for routing have to be optimized to be bandwidth saving [35].
- **Energy Constrained Devices:** Most of the nodes participating in ad hoc networks are small portable devices, relying for their energy consumption on batteries, in general the lifetime of the majority of batteries do not surpass few ours. In some kind of networks such as sensor networks, nodes rely on some light cell and vibration based generators to generate power, however relying on such means of energy can not be effective under some conditions. For this reason, the habitual routing and security protocols are not effective and sometime cryptographic operations that require complex mathematical calculations become difficult with energy constrained devices [36].
- **Limited Physical Security:** an ad hoc network is usually part of hostile environment such as in battlefields, otherwise it is part of unpredictable environment such as in catastrophe. Therefore, the network's nodes are exposed more than any other kind of network to physical attacks trying to compromise the network. In the other hands the transmission range of the network may exceed the area of the network which exposes it to several attacks [37].
- **Decentralized administration:** an ad hoc network is defined as a set of mobile nodes composing a network on relying on each other for data forwarding or security establishment, and therefore there is no real concept of administrative authority responsible of ensuring security or routing. Thus nodes in the network must collaborate in order to accomplish some task like key and authorization right distribution, or rely on an off-line administrative authority to distribute administrative information before the elaboration of the network [38].

3. Introduction to routing in MANETs

3.1 Conventional routing

Routing is the method of finding a path (route) between two communicating hosts in a given network.

A path is defined as, the sequence of intermediate hosts over which the packet is forwarded to its destination. These intermediate nodes are called routers; they play the most important role in any network for data forwarding [39].

In conventional network, the routers are preconfigured by the administrator to perform the task of routing, and each packet is forwarded according to its IP address. In the way, that each router controls a subnet of the whole network and according to the address of the destined subnet a packet is forwarded to a given router.

The routing may by static or dynamic according to the size and the nature of the network, for example in a small network routes are fixed during the installation of the network, conversely in a big size or congested network routes are dynamically defined according to the state of the link between routers [40].

In conventional networks, routers use routing tables to compute the next hop for a packet. Routing tables may take many forms regarding the nature of the routing algorithm; however they can be viewed as a sequence of destined subnet and the next hop to reach the desired subnet, or a default router if no information is found in the routing tables [41].

3.2 Routing in ad hoc networks

As described previously an ad hoc network consists of a number of handled devices which communicate to each other over wireless channel without any centralized control, or infrastructure. Thus, the network topology may change rapidly and unpredictably, therefore no dedicated node can be defined to perform routing in MANETs. Hence, mobile nodes must collaborate between themselves to perform routing and dynamically establish routes. Thus, any mobile node in an ad hoc network plays two roles, the first one as an ordinary node and the second one as a router in order to participate in the routing process by executing routing algorithms [42].

Therefore, the conventional routing protocols can not be used for MANETs [43]. Consequently, new protocols and extensions of the existed protocols must be defined for ad hoc routing taking into account the following characteristics:

- Limited bandwidth, since nodes share the same frequency.
- Topology changing, due to nodes mobility.

- The hostile environment where the network is deployed as in battlefields.
- Device constraint, since the mobile nodes are self powered with limited computing power.

Due to all these constraints, lot of routing protocols were defined for ad hoc networks, according to the strategy and the method of routing we can differentiate four categories:

- Proactive (table-driven) protocols.
- Reactive (on-demand) protocols.
- Hierarchical protocols.
- Geographical protocols.

3.2.1 Reactive protocols

Also called on demand routing protocols, it was known in conventional networks as source routing which means that the route is found only when needed by injecting in the network a route request containing the destination IP address, this packet is forwarded from router to another. Each router when receives this source packet it adds its address to the header of the packet [44]. Whenever this packet arrives to its destination, this last reverses the path contained in the header and sends a reply over the reversed path. Whenever the source node receives this route reply, it begins immediately using the established route for its farther transmission.

Although, any reactive protocol works as follow:

- When a mobile node needs to establish a route, it first launches the mechanism of route discovery. So, the source node floods the network with a route request RREQ (IP_{dest}) containing the IP address of the destination node, this route request is approximately treated by each node in the network.
- Each node when receiving this RREQ verifies if it has already treated this request or not by verifying its sequence number, because each route request is identified by a unique sequence number used to avoid routing loops. If this request was not already treated, the mobile node adds its address IP to the header and broadcast the request over the network.
- Whenever the request arrives to its destination, the corresponding node adds its IP address to the header, reverses the path, caches the path in his cache for future use and constructs a route reply packet and sends it over the established route.
- At the side of the source node, it caches the received routes and uses the shortest one for data forwarding.

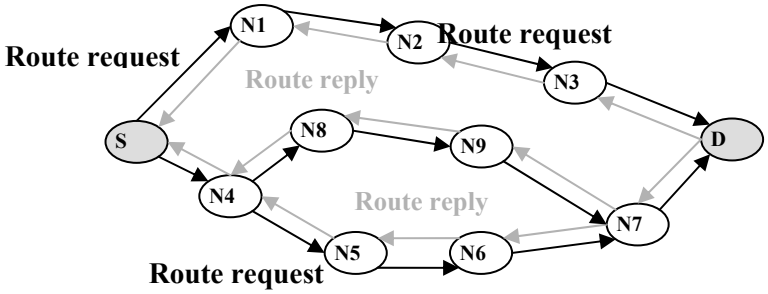


Figure I.2 Reactive routing

As we can observe (Figure I.2), the reactive protocol is simple and does not need extra treatment or resource reservation beyond the moment of route establishment. However, the mechanism of route discovery is the black hole of this routing protocol, because it can cause the blockage of the network if there is a great number of nodes in a limited area, in addition it consumes the great part of the network resources during that moment, nevertheless this kind of protocols are the most popular and the most efficient compared to other protocols.

The much known reactive protocol is DSR (Dynamic Source Routing) [45], however there exist other protocols such as AODV (Ad hoc On-demand Distance Vector routing)[46], TORA (Temporally-Ordered Routing Algorithm routing protocol) [47], ARA (Ant-based Routing Algorithm for Mobile Ad-Hoc Networks) [48].

3.2.2 Proactive protocols

Proactive protocols or table driven protocols are inherited from the conventional ones without lot of modifications, in the way that each node keeps the network topology in its routing tables, and routes are found when needed without waiting for route reply such as in reactive routing. Routing tables are maintained using periodic messages exchange, thus each node broadcast periodically its routing table to its neighbours [49].

In order to handle the specificity of ad hoc network such as bandwidth constraint proactive routing is modified by optimizing the mechanism of routing table update, in the way that the update of the routing tables are not periodically broadcasted as in conventional routing, since in ad hoc network broadcasting a message may overhead the network, thus only important changes on the network topology are broadcasted which minimizes the bandwidth consumption due to the tables maintenance [50].

Routes are immediately available and there is no additive overhead to find routes at each time a path is needed, a mechanism to find route as shortest path or link state is used to find the best route, typically every node is connected to another via a predefined path contained in its routing table (Figure I.3).

Destination	Next hop	Number of hops
D	**N1**	**4**
D	**N4**	**3**
D	**N6**	**4**
……		

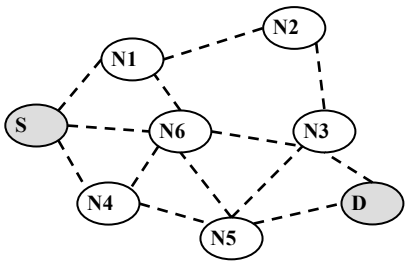


Figure I.3 Proactive routing

Theses protocols keep the network traffic within an acceptable threshold due to the maintain of routing tables; however when the topology changing is very frequent the maintenance of routing table causes a great overhead due to the number of exchanged data.

A mechanism is defined to limit the impact of routing tables maintenance is by broadcasting routing tables maintenance in a limited area, in the way that whenever a link between two nodes is broken the notification is sent only for two or three hops neighbors, or by fixing the period of update according to the number of hops for example doubling the period of update for every hop. FSR (Fisheye State Routing) [51] is one of the proactive protocols which implement this technique.

Compared to reactive routing, control traffic is more dense but constant, and routes are instantly available, in opposite reactive routing congests the network during the route discovery mechanism otherwise the network is stable which make them suitable for large network since the demand of routes is not frequent, however for small network proactive protocols are the most suitable due to the small number of links..

Some examples of this kind of routing protocols are: OLSR (Optimized Link State Routing) [52], WRP (Wireless Routing Protocol) [53] and DSDV (Dynamic Destination-Sequenced Distance Vector routing protocol) [54].

3.2.3 Hybrid protocols

As presented above each of the categories of the two algorithms have its advantages and disadvantages. For example reactive protocols are most desired for large networks however proactive ones are suitable for small networks [55].

Therefore, hybrid or Hierarchical protocols try to solve the problem of routing in ad hoc networks by designing protocols having the advantages of both reactive and proactive protocols; by dividing the whole networks into regions called clusters (Figure I.4). Hierarchical protocols deal with the network widening by creating new clusters which maintain the overhead of topology changing within an acceptable threshold.

Typically, hierarchical protocols employs two protocols the first one is a proactive protocol for routing inside its region and the second one is reactive protocol used for routing outside this region.

To manage this kind of routing for each cluster a mobile node is chosen to manage the network architecture called cluster-head, in general the cluster-head maintain the routing table for routing inside the cluster and finds routes outside the cluster using reactive strategy.

Conceptually these protocols are more efficient compared to reactive or proactive ones; however there is no real implementation which uses this technique. In the other hands, these protocols have an additional overhead due to the maintenance of the hierarchical architecture.

Examples of hybrid routing protocols are ZRP (Zone Routing Protocol) [56], CBRP (Cluster Based Routing Protocol) [57], GSR (Global State Routing protocol) [58] and HARP (Hybrid Ad Hoc Routing Protocol) [59].

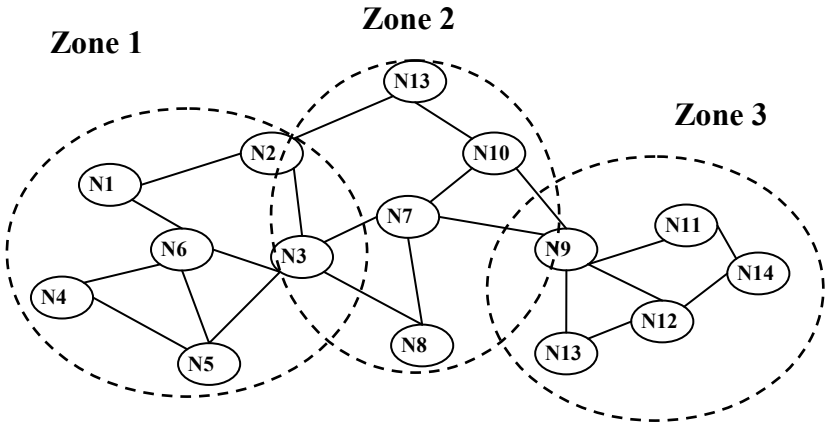


Figure I.4 Hierarchical protocols

3.2.4 Geographical protocols

Geographical routing protocols use nodes' position for routing, in order to minimize the overhead due to broadcasting used in all the routing protocols, by sending request and topology information only in the desired direction [60].

Thus, routing table maintains in addition to the number of hops the location of each node, thus each route is chosen according to the direction of the destination as well as the distance separating the source and the destination.

Research shows that geographical location information can improve routing performance in ad hoc networks. However, all the protocols assume that the nodes know their position.

In order to provide the position information of each node in the network a mechanism such as Global position System GPS must be implemented by each node. In some kind of networks such as the military networks this is possible however in other network implementing a GPS receptor is not possible and the majority of existed devices have not this opportunity, therefore these routing protocols are not practical for all ad hoc networks [61].

Example of these protocols are DREAM (Distance Routing Effect Algorithm for Mobility) [62], GLS (Grid) (Geographic Location Service) [63], LAR (Location-Aided Routing protocol) [64] and GPSAL (GPS Ant-Like Routing Algorithm) [65].

3.2.5 Other protocols

Research in the domain of ad hoc routing gives every day birth to new protocols and lot of extensions of the existed protocols trying to implement new methods to qualify the network characteristics to be used in routing, a list of these protocols exist in the annex.

Theses protocols are essentially based on devices' energy, mobility or resources, giving birth for example to power aware protocols such as PARO (Power-Aware Routing Optimization Protocol) [66], PAMAS (PAMAS-Power Aware Multi Access Protocol with Signaling Ad Hoc Networks) [67] and WBDSR (weight based DSR) [68].

3.3 Routing metrics in MANETs

Inherited from the conventional networks the used metrics for route selection is usually the number of hops, in the way that the chosen route is the shortest one. In the conventional network where the administrator controls the state of the network, this metric is sufficient, however in an ad hoc network minimizing the number of hops between the communicating parties is not enough to improve the network performance [69].

In [70], the authors use experimental results from two wireless test beds to show that using minimum hop counts as metric does not give the best results and very often it leads to less capacity than the existing best paths [71,72], because:

- The link quality is spread out and varies over time, due to battery draining and node movement.
- Nodes' resources decrease over time.

- Some links are asymmetric.
- A shortest path may contain some insecure or powerless nodes which may affect the performance of data forwarding.

To overcome this, new metrics must be defined for ad hoc routing taking into consideration the characteristics of ad hoc networks and device constraint as energy and topology changing. This metrics must include for route selection the maximum of theses characteristics [73].

3.4 Routing challenges in MANETs

Regarding the characteristics of ad hoc networks as topology changing and the nature of devices and the used medium, it seems that routing is not easily carried out and the most simple tasks as routing table maintenance are hardly achieved, in addition to other traditional problematic, thus any new developed protocol must take into consideration the following aspects:

3.4.1 Quality of service

One of the most delicate problematic of ad hoc routing is the quality of service QoS, since there is no clear idea of a QoS implementation for ad hoc network such as in conventional networks, and the extensions given in literature tries to apply the conventional methods for ad hoc networks, however these extensions do not give the same results as in conventional networks due to the characteristics of ad hoc networks as topology changing. Therefore, the best way to implement the QoS is to improve the existed routing protocol by adding some QoS criteria such as link bandwidth or signal strength for route selection which may improve the network performance [73, 74].

3.4.2 Security

In opposition of conventional network where a centralized authority is dedicated to ensure security services as certificate distribution or key establishment, in ad hoc network there is no centralised authority to accomplish this task, in addition to the nature of the environment which is usually hostile as in battlefield. Almost, only some extensions are added to the existed routing protocol to implement security since security is not natively implemented for ad hoc routing [75].

3.4.3 Energy

Typically an ad hoc network is composed of self powered handled devices such as cellular phones and laptops. Consequently, conserving battery power is more important in ad hoc network, and the only way to do this is to define new algorithms and metric taking into consideration the aspect of energy [76].

3.4.4 Mobility

Node mobility of ad hoc networks poses the great party of the known problems of routing in ad hoc networks. Thus, any new developed protocol must take this aspect during its conception, by defining a method for route selection which takes node stability and movement in route selection in order to choose the most stable route, since the disappearance of one node in the route my stop the process of data forwarding, therefore minimizing the number of unstable node in any route ensure more efficiency [77].

3.5 Proposed Solutions to these challenges

As presented in the previous sections, most of the existed routing protocols do not include all the aspects of ad hoc network such as mobility, energy constraints and security, thus the new developed protocols must include in their design these characteristics by developing new metrics and strategies of routing.

Cross-layering is one of the solutions given for routing improvement in ad hoc networks:

3.6 Cross-layer design

The existed routing protocols use the OSI (Open System Interconnection) [40] or layered model defined for conventional network where each layer receives data from the upper layer and executes its protocols independently and gives predefined services to the lower layer through predefined contact points [78].

However, improving the existed routing protocols by adding new criteria in the route selection process need more cooperation between layers and new services must be given by the lower layers to the network layer to perform an efficient routing.

Although, this new services are given form a layer to an other using cross-layer which means that an information is given from a layer to an other without any respect to the traditional OSI model.

A cross-layer design (Figure I.5) adapts the OSI model to the wireless context by sharing data between the entire layers used after by each one to the improvement of performances of

other layers. Several cross-layer techniques have been proposed in literature and they have improved the performance of lot of services in ad hoc networks [79, 80, 81, 82].

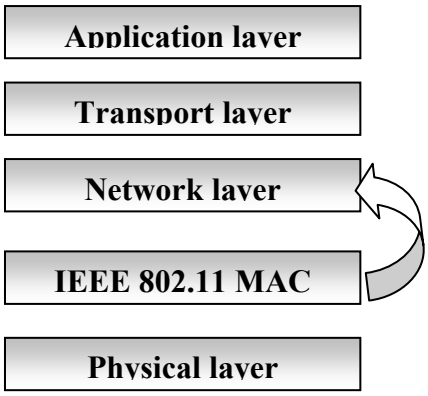


Figure I.5 Cross-layer design between MAC and network layers

4. Security in MANETs

Ad hoc networks are by nature very open to anyone, due to the used medium which is radio waves, basically anyone with the proper hardware and knowledge of the network topology and protocols can connect to the network. This allows potential attackers to infiltrate into the network and carry out attacks on its participants with the purpose of stealing or altering information.

Another problem is the no existence of centralized authority, responsible for the distribution of cryptographic keys, or to manage security mechanism like in wired networks. Thus, the network nodes collaborate between themselves to achieve security services which make the conventional security mechanisms not applicable for ad hoc networks [83].

Also, depending on the application, certain nodes or network components may be exposed to physical attacks which can disrupt the functionality of security or routing over the network. In the other hands, ad hoc network hosts are more often part of an environment that is not maintained professionally.

Another specificity of ad hoc networks is their heavy reliance on inter-node communication, to ensure routing which gives large area of attacks on the routing protocols.

In the other hands, the nature of devices which are usually constrained with limited battery and computing power, makes some cryptographic methods and robust conventional security mechanisms hard and effective less [84].

4.1 Security challenges in ad hoc networks

The principle of ad hoc networks is a dynamic connection between devices that can be used from anywhere and offers limitless business, recreational and educational opportunities. However, their biggest advantages which is the wireless medium and the mobility is also their biggest vulnerability, since the transmission range of the network typically exceeds the area where the network is deployed, giving great opportunities to attackers to infiltrate into the network and perform all kind of existed attack as well as the ones developed specially for theses networks [85].

Generally attacks against networks are divided into three categories:

4.1.1 Passive attacks

In this attacks an unauthorized party gains access to the network medium and eavesdrops passively the exchanged traffic over the network without any attempt to modify the exchanged data. Typically passive attacks may be the first step to perform active attacks, allowing the attacker to gain some interesting information about the system security, example of these attacks are traffic analysis, eavesdropping and impersonate attacks [86].

4.1.2 Active attacks

After have gathering the necessary information about security and routing mechanisms used in the network, the attackers performs active attacks against the routing protocols in order to block this service in the network or against the network users and modify the exchanged data. Examples of these attacks are denial of service attacks which is the most dangerous ones as well as black hole attack against routing, data modification, man in the meddle…etc [87].

4.1.3 Physical attacks

This kind of attacks focuses the equipment used in the network, in order to gain access to the network by using information stored in this device such as the cryptographic keys or the network stack. After stealing this information the attacker gains access to the network and become party of this network then performs any activity against the network without difficulties. These attacks are very often executed against sensor networks [87].

In order to ensure security in ad hoc network lot of security mechanisms have been developed in literature for both intrusion detection and the network protection. The majority of the mechanisms developed for ad hoc network are based on cryptographic methods, trying to protect the exchanged traffic over the network using both symmetric and asymmetric

encryption. Typically, security schemes developed for ad hoc networks are key management protocols, trying to handle key agreement between the network nodes such as key generation, distribution, renewal and update.

The most promising key management schemes given in literature are those inherited for the conventional Public Key Infrastructure (PKI). However, developing a PKI infrastructure for ad hoc network still a delicate task with the existed devices and topology of the network.

4.2 PKI for MANETs

A Public Key Infrastructure PKI is an infrastructure for managing digital certificates; PKI is the most powerful tool providing network security in conventional network. PKI relies on the public key cryptography to ensure authentication and non-repudiation over the network based on a trusted party called Certificate Authority (CA) which certifies, verifies and signs certificates over the network.

To ensure authentication, PKI uses asymmetric encryption which use two keys for both encryption and decryption, thus each entity over PKI based network have to get a pair of keys generated by the CA used to sign digital documents as well as the public key of the CA in order to verify the validity of certificates.

A PKI is essentially based on digital signature, which can be defined as the process of encrypting a message or its hash value using the public key of a given node, consequently, only this node can decrypt this document using the corresponding private key and verify its integrity, which also ensure the authenticity of messages over the network [88].

The public key of each node and other information such as name, serial number, expiration dates…etc are embedded in an electronic document called digital certificate which is digitally signed by the CA which certifies both pieces of information.

The most important component of PKI is the Certificate Authority, the trusted entity in the system that vouches for the validity of digital certificates. The CA is also responsible of publishing and revoking certificate over the networks. Thus, the success of PKI depends on the security, and availability of CA for the network users.

PKI has been deployed for wired networks and some infrastructure-based wireless networks, since good connectivity can be assumed in these networks. However, it is unclear if such approaches can be extended to ad hoc networks due to the infrastructure-less nature of ad hoc networks. Another serious problem present in ad hoc networks is the increased physical vulnerability of mobile nodes which exposes the certificate to physical attack and therefore impersonates attack which is the most dangerous attack against PKI, because the possibility of the nodes being captured or compromised in a hostile environment is higher than in wired networks with stationary hosts [89].

In literature there is lot of implementation of PKI, in which each author tries to simplify and adapt the PKI service for the constrained network using different mechanism some of these implementations are:

4.2.1 Partially Distributed Certificate Authority

This solution proposed by Zhou and Hass [90] uses a (k, n) threshold scheme to distribute the services of the certificate authority among a set of specialized nodes. the authors propose to choose K nodes to be servers and share the CA services, in the way that the CA's signing key is divided into K sub shares using Shamir's secret sharing mechanism, therefore the valid certificate can only be obtained by combining sub shares of the K servers in order to ensure the CA's services such as signature, publishing, revocation and verification of certificate over the network. This solution assumes that there are at least k server nodes in the neighborhood of each node to accomplish the availability of CA, which is also defined by giving an appropriate value to k.

In this scheme the security is ensured by dividing the CA's services among more than one server in order to make it difficult for an attacker to compromise the CA, since the compromising of the CA must pass by the compromising of both K servers which is not easy.

4.2.2 Fully Distributed Certificate Authority

This solution described by H. Luo and S. Lu in [91] and analyzed in [92] and [93], uses a (k, n) threshold scheme to distribute an RSA certificate signing key to all nodes in the network in order to overcome the limitation of scalability in the solution of partially distributed certificate, by making k=n. Although this solution is similar to the previous one, it also uses verifiable and proactive secret sharing mechanisms to protect against denial of service attacks and compromise of the certificate signing key. This solution isn't desired for networks where the nodes are joining and leaving network frequently, and routing security because any operation needs lot of messages to be achieved.

4.2.3 Self Issued Certificates

This solution is proposed by Hubaux [94]. It provides a public key management solution similar to PGP (Pretty Good Privacy) in the sense that certificates are issued by the users themselves without the involvement of any certification authority. Unlike the previous public key based solutions, this one is intended to function in spontaneous ad hoc networks where the nodes don't have any prior relationship. However, due to this it requires an initial phase during which its effectiveness is limited and therefore it is unsuitable for short-term networks.

4.2.4 Cluster based PKI

The authors in [95] propose a cluster based scheme to implements the PKI for ad hoc networks. This solution is based on partially distributed certificate authority, in order to divide the CA's signing key among cluster-heads, which means that any CA operation is achieved by the coalition of all cluster-heads in the network. However the use of threshold cryptography may add an over head due to the number of exchanged messages during any operation (verification, renewal…etc), it may also encounter other problems to ensure scalability when adding new cluster-head or whenever a cluster-head leaves the network.

In recent work we also proposed a simplified implementation of PKI for ad hoc networks, employing clustering architecture (Figure I.6) in order to simplify and distribute CA services over the network. The proposed scheme divides the whole network into clusters and chooses the most powerful node among cluster member to ensure the CA services for the corresponding cluster. The cluster-head or the CA of its cluster collaborates with other CAs over the network to ensure inter-cluster PKI services using a mechanism of multi-signature [96].

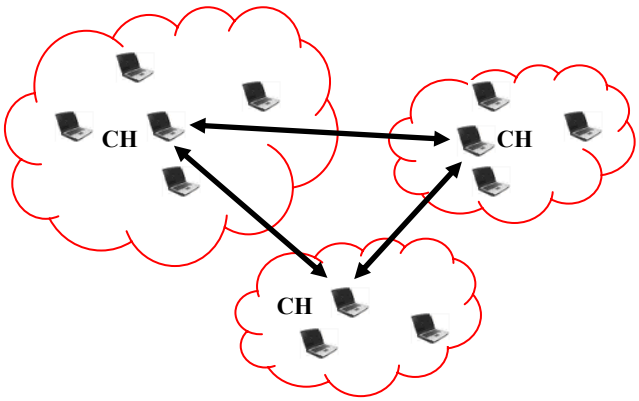


Figure I.6 Clustering architecture

As we have seen lot of implementation exist for PKI, however the majority of these implementations are not efficient because they do not take into consideration all the characteristics of ad hoc networks. Thus, any implementation of a PKI for ad hoc network must minimize the message exchange and rely on other underlying protocols such as routing to be more effective. In the next chapter we are going to propose a light weight implementation of PKI relying on reactive routing protocols to ensure certificate publishing.

5. Conclusion

In this chapter we have given an introduction to wireless ad hoc network, by exposing the most important advantages and problematic of these networks. As we have seen, wireless ad

hoc networks are more and more promising and gain every day new applications in our lives. However, some problematic such as security and routing still being the most delicate issues for ad hoc networks.

Security is the most challenging one due to the nature of these networks and the environment of deployment, and the used solution inherited from the conventional ones are not efficient such as the implementation given for PKI otherwise the security schemes are vulnerable against a large variety of attacks.

In the other hands, regardless the number of developed protocols for routing which are more than one hundred protocols, routing is always the black hole of ad hoc networks until an efficient routing protocol is developed tacking into consideration all the characteristics of ad hoc networks such as security, QoS, mobility and energy …etc.

In the next chapters we will present our contributions in the domain of routing and security in ad hoc network by proposing some new extended protocols trying to handle the specificity of MANETs.

Chapter II

Enhancing reactive routing protocols in MANETs

Routing in mobile ad hoc network is one of the most crucial problematic, since a good routing protocol must ensure fast and efficient packet forwarding, which isn't evident in ad hoc networks, due to the characteristics of these networks. In literature there exists lot of routing protocols however they don't include all the aspects of ad hoc networks such as mobility, device and medium constraints which make them not efficient for some configurations and categories of ad hoc networks. Thus in this chapter we propose an improvement to reactive routing protocols in order to include some of the aspects of ad hoc networks such as QoS, mobility and energy by proposing a new metric to evaluate routes based on intermediate nodes weight computed by combining the stability an the battery power of nodes to choose the most stable and powered nodes for packet forwarding. We also give a proposition to include in the metric the bandwidth of intermediate nodes.

1. REACTIVE ROUTING IN MANETS

As we have presented in the previous chapter, in reactive routing protocols routes are found only when needed, which makes them the preferred protocols for mobile ad hoc networks, since it is unnecessary to save the whole topology of the network on each node, because at a given moment only a limited number of nodes participate in the communication over the network [97].

In the other hands reactive protocols treat the mobility of nodes by launching new route discovery, which reflect the state of the network at that moment which save greatly the network resources as energy and memory.

Generally, reactive protocols manage the routing process over a mobile ad hoc network by two principle mechanisms, which are route discovery and route reply:

1.1 Route discovery

This mechanism is launched whenever a node wishes to send or contact any other node over the network out of its transmission range; therefore it must obtain a route to that node by launching a Route discovery mechanism as follow:

- It verifies its cache to find if there is any cached route to be used; otherwise it continues the process of route discovery.
- It creates a route request packets containing its address and the address of the destination node; then it broadcast this packet to all its neighbors using flooding (Figure II.1).

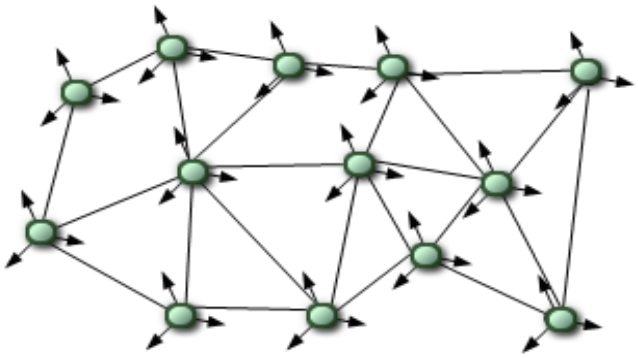


Figure II.1 Flooding in MANETs

- Each neighbour when receiving this request consults its cache to find an eventual route to this destination to be returned back to the sender; otherwise it rebroadcast the same route request to all its neighbors after adding its address to the header of the route

request and learns from this request any routing information to be added to its cache. If the node has already treated this route request it ignores the new received request by verifying its sequence number since each route request is identified by a unique sequence number in order to avoid routing loops.

- The same procedure is executed by each neighboring node until the route request arrives to its destination which adds its address at the end of the header and sends back a route reply.

1.2 Route reply

This procedure (Figure II.2) is executed by the destination node after receiving a route request destined to him, thus this node executes the following actions:

- Adds it address at the end of the path contained in the header of the route discovery.
- Reverses the path contained in the route discovery and adds this new route to its cache for future use.
- Replies to this request using unicast along the reversed path.

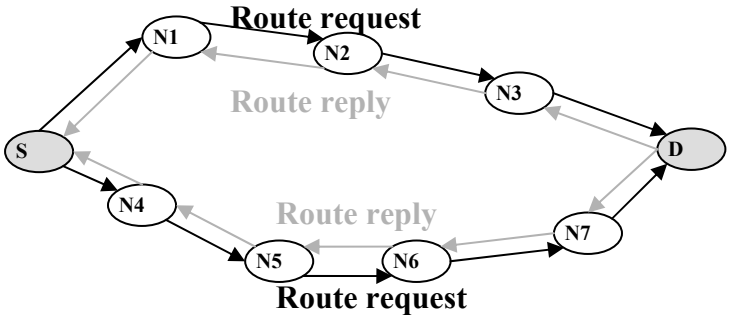


Figure II.2 Route discovery mechanism

The mechanisms described above are the two principle mechanisms specified for source routing in conventional networks [98]. But, for other reasons due to the characteristics of ad hoc networks, the source routing of ad hoc networks adds other mechanism to improve and manage the challenges of ad hoc networks which are:

1.3 Route maintenance

When forwarding a packet each intermediate node is responsible for confirming that the packet is correctly received by the next node, however due to the dynamic topology and the constraints of the wireless medium it may occur some situations where a node doesn't receive the acknowledgement of reception from the link layer, therefore it resends the same packet

until it reaches a predefined value of attempts [7]. Whenever this number of attempts is reached this node consider this link as broken then it deletes each route containing this link from its cache, and generates a route error packet to inform the source node and all intermediate nodes about this link failure. When receiving this route error each intermediate node deletes all routes containing the broken link until the route error packet arrives to its destination, which chooses to launch a new route request or to find a new route in its route cache.

1.4 Route cache

In order to improve the performance of DSR and other routing protocols to avoid new route requests for each packet, they use a cache in which they save all the established routes for future use.

The route cache is updated after treating each route request or reply by learning routing information from these requests. The cache is also updated whenever a node receives a route error by deleting each entry containing this node.

1.5 Metric

The metric used to evaluate (choose route) in reactive routing is usually the number of hops between a source node and a destination, which is the metric used for most of conventional routing protocols, however this mechanism isn't desired for ad hoc networks regarding their characteristics (mobility, devices constraints) [99]. Because it may exist a route with the minimum of hops however it contains some less powered or unstable nodes which may cause lot of link failures. Therefore using the number of hops as metric is not sufficient due to the characteristics of MANETs; consequently any new metric for MANETs must include other ad hoc networks' parameters for route evaluation such as mobility, bandwidth and devices constraints.

2. LIMITATIONS OF REACTIVE ROUTING PROTOCOLS

As we've said previously reactive protocols are the most promising ones and they have proven their efficiency for lot of configurations and sizes of the networks. However reactive routing still having lot of shortcomings such as:

- The network is occasionally overhead by the route discovery which can bloc the traffic over the network during the period of route discovery.
- Another problem is the metric used for route selection which is the same as conventional (wired) networks which is the number of hops between a source and a given destination

node, without taking into account any other parameters such as bandwidth of the chosen route [100].

- Reactive protocols suppose that nodes participate in the routing process without any malicious attention, which is not the case in the majority of deployed networks where any node can execute lot of routing attacks [101].
- No concern is given to the quality of service; the protocol forwards data without any concern to the priority of traffic and use the best effort for all packets [102].
- No consideration is given to the capacity of each node such as power computing, because nodes with less computing power may slow the forwarding of data flows [103].
- Reactive routing doesn't take into consideration the battery power of the intermediate nodes, because a node can't forward packets if it hasn't the sufficient energy power which causes link failures [104].
- Reactive routing doesn't include the aspect of stability of nodes in order to choose the most stable nodes as intermediate nodes, because unstable nodes causes topology changing which launches lot of route errors and therefore new route requests which greatly consumes energy [105].

To overcome some of these limitations in the remainder of this chapter we are going to propose an improvement to reactive routing protocol applied to DSR, in order to include in the process of route selection new parameters by which we try to defeat the encountered limitations of reactive protocols.

Two improvements are given in the rest of this chapter in order to include the aspect of QoS, mobility and energy. These improvement are applied to DSR, the first one is called Quality of service based DSR [106] in which we include the aspect of QoS and the second one is called weight based DSR [107]which chooses route according to route weight which is computed by summing a set of parameters.

3. QUALITY OF SERVICE BASED DSR

Quality of service (QoS) is the most challenging task to be performed by routing in both wired and wireless networks, since the QoS tries to use efficiently the existed bandwidth for different traffics and gives the best bandwidth for each node over the network [108].

In the conventional networks the task of implementing QoS was not very hard, and some mechanisms as Diffserv [109] and the reservation of resources give good results, but all these mechanisms was defined under the assumption that the router are already known and fixed by

the administrator with the sufficient resources as memory and bandwidth to accomplish the requirements of QoS.

Nevertheless, in ad hoc network the environment is not the same and the predefined routers do not exist. In the way that routing is done by the cooperation of a set of ordinary nodes with limited computing power [110], in the other hands the mobility of nodes make the mechanism of resources reservation inapplicable for ad hoc networks.

Therefore, new mechanisms and protocols must be defined for ad hoc networks to implement the QoS [111]. In our work, we have tried to implement one parameter of QoS which is the bandwidth by improving the reactive routing protocols in order to support the QoS in the route selection process, in the way that the chosen route must have the maximum bandwidth which may improve the delay of data forwarding.

In order to include the QoS into reactive routing protocol we have chosen a method based on bandwidth estimation, in which each node estimates the available bandwidth with each neighbor in a given neighborhood and uses the estimated bandwidth as a parameter for route selection combined with the number of hops.

Therefore each node always has an estimated value of its available bandwidth which is injected in the header of route discovery request. Hence a route is selected according to two parameters rather then one as in conventional routing which are the available bandwidth and the second one is the number of hops.

3.1 Bandwidth measurement in ad hoc networks

The bandwidth is defined as the number of bits transmitted over a given link per second; the bandwidth differs from a kind of network to and other according to link characteristics and the environment of deployment [112].

The network bandwidth can be measured using two approaches, end to end bandwidth measurement and per hop bandwidth measurement [113]. In each one the objective is to get the capacity (available bandwidth) of the link between two nodes.

In the other hand, the bandwidth can be measured using two modes, active mode in which the bandwidth is measured by injecting packets into a given route and measure the time taken by these packets to reach the destination, this method gives best results however it adds a great overhead to the network. The second method is the passive mode in which the bandwidth is measured without injecting extra packets, in the way that the bandwidth is measured using signaling packets such as routing packets [114,115].

3.1.1 End to end bandwidth measurement

In this method the estimated bandwidth defines the capacity of a given path between two nodes.

The estimation of the bandwidth is given by measuring the time taken by an extra packet exchanged between the two nodes this means that this method uses the active mode which is not suitable for ad hoc networks because it adds an additional overhead to the networks.

In the other hands, this method can not be used for route selection in our case, because we need to choose a route which contains the best sequence of nodes, therefore we need to know the available bandwidth between each two nodes in the network and choose as route the one having the greatest available bandwidth between each pair of nodes.

3.1.2 Per hop bandwidth measurement

In this method the bandwidth is estimated by measuring the link layer capacity of each two neighboring nodes. This method uses the passive mode to estimate the link capacity using signaling message of the 802.11 MAC layer as request to send and clear to send RTS/CTS packets used for medium reservation

We prefer this method for implementing our protocol, because it reflects the state of the network at each moment especially for reactive routing protocols, in the way that the information is collected during the route discovery period and used during the route reply period for route selection by maximizing the bandwidth between each pair of nodes.

3.2 Available bandwidth estimation

The Basic medium access mechanism specified by IEEE 802.11 standard for ad hoc networks is the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with binary exponential Backoff [7]. The node is not allowed to transmit until the medium becomes free, because the wireless medium is shared between the entire nodes in a given area which means that additional mechanism must be defined to detect and treat collisions.

The 802.11 MAC layer functioning (Figure II.3) can be explained in the following steps:

1- Whenever the MAC layer of a source node receive a packet from the upper layer it launches the medium access procedure:
   a. The source node senses if the medium is occupied or not by another transmission, if the medium is free it execute operation two.
   b. If the medium is not free the source node falls into exponential backoff with the initial size of the backoff window until the medium becomes free with a new size of the backoff window at each time.

2- Whenever the medium becomes free the source node sends a request to send RTS packets to the destination node in order to reserve the medium for transmission.
3- Whenever this request is received by the destination node it responses by sending a clear to send request CTS, this request is received by all nodes within the same neighbourhood and reserve immediately the medium for these two nodes.
4- Whenever the CTS packet is received, the source node begins the transmission of its queued data, an acknowledgement is sent for each correctly received packet.

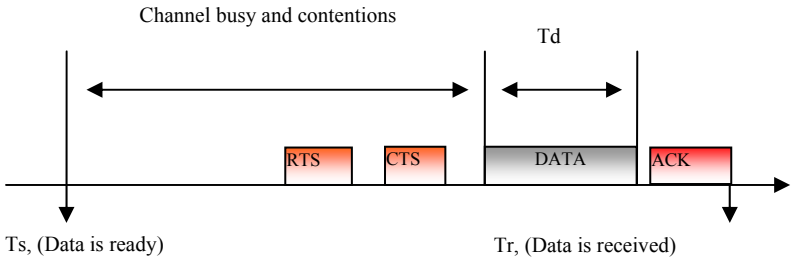


Figure II.3 Packet transmission stages in 802.11 MAC layer

Taking into account the described data delivery framework the time required for the transmission of a single data packet using CSMA/CA [7] in addition to the time of packet transmission over the wireless link, includes data queuing delay corresponding to the time the node was waiting for the medium to become free, as well as channel to channel access delay using random backoff and optional RTS/CTS exchange and the delay due to the reception of the acknowledgement.

Therefore the estimated available bandwidth (BW) for transmitting a packet of size S as described above is defined as:

$$BW = S/(T_r - T_s)$$

Where:

- T_r: the time when the data is sent to the MAC layer by the upper layer.
- T_s: the time of the achievement of the transmission by receiving the acknowledgement.

3.3 Implementation of QBDSR

In order to implement the parameter of link capacity in route selection over reactive routing protocols, we have chosen DSR as routing protocol for applying our specifications.

The major modifications are done on the route discovery, route reply and the cache of the original DSR in order to insert the parameter of QoS to be used for route selection.

3.3.1 Route discovery

The most important modifications made on the route discovery mechanism are done on the structure of the original header of DSR.

Thus, we have added a new field in which each intermediate node inserts the estimated bandwidth taken from the MAC layer into the header of the route request.

3.3.2 Route reply

The route reply packet is generated by the destination node in response of a route request, in QBDSR the destination node doesn't response immediately to the first route request, however it waits a predefined delay *d* to receive more route requests in order to choose the best one by maximizing the value of the bandwidth, whenever this delay expires the destination node chooses only one route and sends it back to the source nodes, in opposite of the original DSR which responses immediately to each route request which may congests the network during this period, because lot of collision are expected due to the interferences between the route discovery and reply.

3.3.3 The route cache

The modifications done on the cache are on the selection algorithm by changing the route selection algorithm based on the number of hops by our proposed algorithm based on link capacity.

In addition a mechanism of cache refresh is used to periodically refresh the cache in the way that each route when exceeds this period is automatically dropped, in this way only fresh routes reflecting the network state (regarding the bandwidth) are used for packet forwarding.

In order to include the aspect of the number of hops in the route selection we have included the parameter of ε, in the way that if the bandwidth of two routes are nearby ε we choose the one with the minimum of hops.

3.4 Route selection algorithm

The route selection algorithm is executed by the destination node when receiving a route request (Figure II.4) to select the route having the greatest bandwidth. The selection algorithm uses a min-max strategy as follow

1. We compute the route bandwidth defined as the minimum value of link bandwidth

$$BW_r = Min(BW_i),\ i \in r$$

2. Choose as main route the one having the maximum route-bandwidth.

$$Mr = Max(BW_r)$$

$r \in R$ / R the set of routes

3. If two or more routes have the same route-bandwidth or whenever their route- bandwidths are nearby ε ($(BW_i - BW_j) < \varepsilon$) we choose as route the one with the minimum of hops, (ε is a predefined value).

1.***begin***
2.while d do
3.begin
4. route = receive_route_request( ); **//receives a route if there is any one.**
5. if route=NULL then goto 12;
6. min:= route[0].bandwidth;
7. for i=1 to route.length -1 do
8. if route[i].bandwidth<min then min:=route[i].bandwidth;
9.route.bandwidth =min;
10. received_routes[recieved_routes.length]=route;
11. recieved_routes.length:= recieved_routes.length+1;
12. end;
13. route_max = received_routes[0];
14. for i=1 to received_routes.length-1 do
15. if received_routes[i]. bandwidth > (route_max.bandwidth -ε) then route_max:= received_routes[i];
16. *send_reply(route_max);* **//only one route is sent**
17. ***end*;**

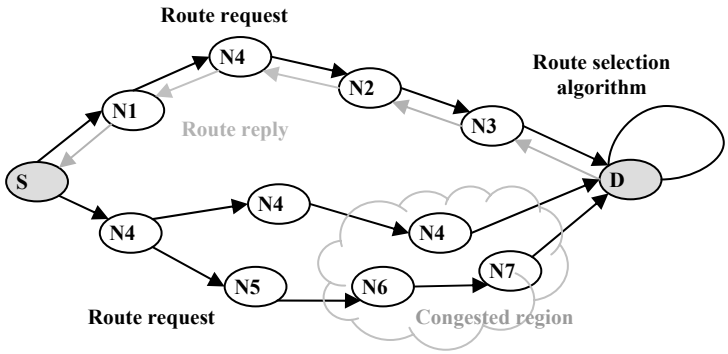


Figure II.4 Route discovery and reply in OBDSR

3.5 Simulation results

To test the performance of QBDSR we have used as tool the NS2 simulator [116], which is recognized as the most effective tool for ad hoc networks simulations. To make in practice the specifications described above we have performed modifications in different layer of the network stack.

The first modifications are done on the IEEE 802.11 MAC layer in order to implement our method to measure bandwidth.

The remainder of modifications are done on the network layer, especially on the DSR Route discovery mechanism, in which we have included a procedure to get the bandwidth size value from the MAC layer and insert it in the header of the route request

The topology of the network that was implemented to evaluate the performance of the QBDSR and compare it with the original DSR comprises 25 and 50 nodes dispersed on the area of 500 * 500 m^2. The Max speed of movement was set to 20 m/s. The type of traffic was CBR (Constant Bit Rate) with a packet length of 512 bytes.

Other parameters relative to QBDSR as the cache refresh period, which was set to 10 s, and the delay for route request is set to 0, 01 s.

The first simulations test the performance of QBDSR and compare it with the original DSR in two configurations the first one is with 25 nodes and the pause time is set to 0 s which means that the network nodes are always in movement and the second with 50 nodes and pause time is set to 100 s, for the two configurations we have used four CBR connections and we have measured the end to end delay of these connections.

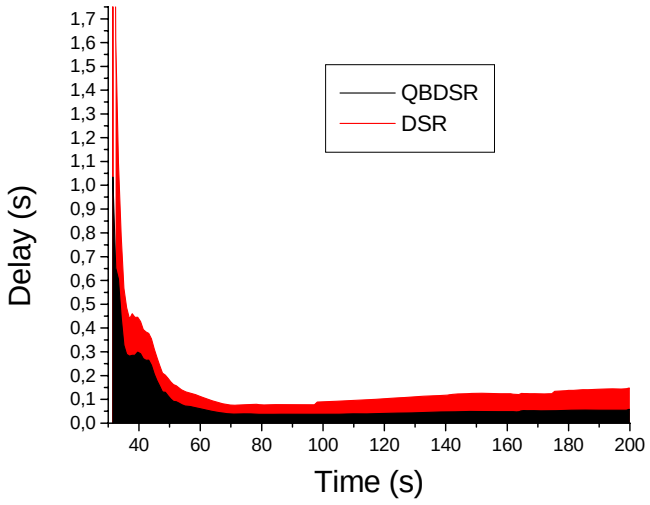


Figure II.5 End to End Delay with 25 nodes

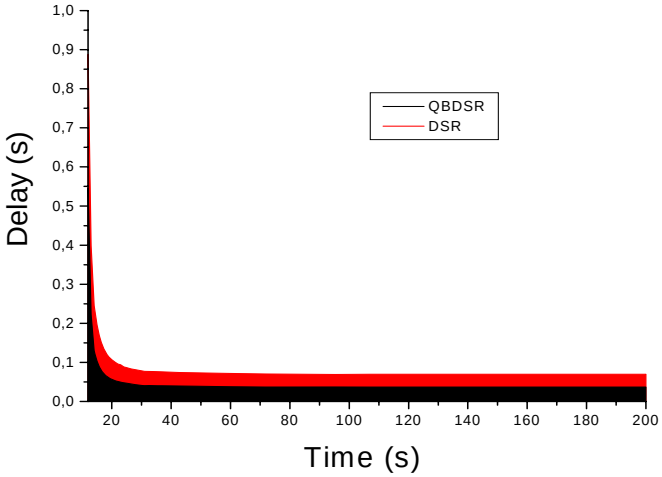


Figure II.6 End to End Delay with 50 nodes

The purpose of these simulations is to show the improvement given by QBDSR concerning end to end delay, as we can observe in both figures II.5 and II.6 QBDSR always gives the minimum delay compared to the original DSR this is due to the criterion used by QBDSR for route selection which is the bandwidth of each link.

This means that the packet forwarding was quicker compared to DSR, because the chosen route is the one having the greatest link bandwidth which is more efficient compared to the number of hops.

Figure II.7 shows the number of route errors according to the number of connections as we can observe QBDSR always generates less route errors. This is due to criterion of route selection and the mechanism of cache refresh which launches new route request instead of waiting until an error occurs.

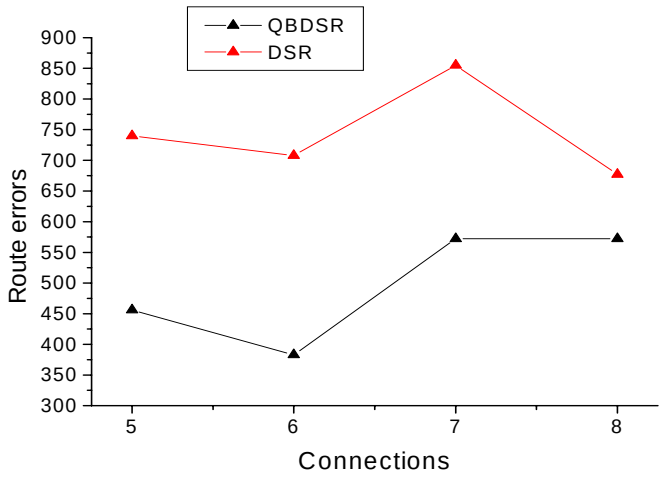


Figure II.7 Number of Route errors

In figure II.8 are shown the number of nodes still having a power in their battery at the end of simulation, as we can see QBDSR always have more powered nodes, because it equilibrates the use of network nodes as intermediate nodes. In the way that at each time the bandwidth of a route decreases we select another route which distributes the density of traffic between nodes, which increases the lifetime of the network.

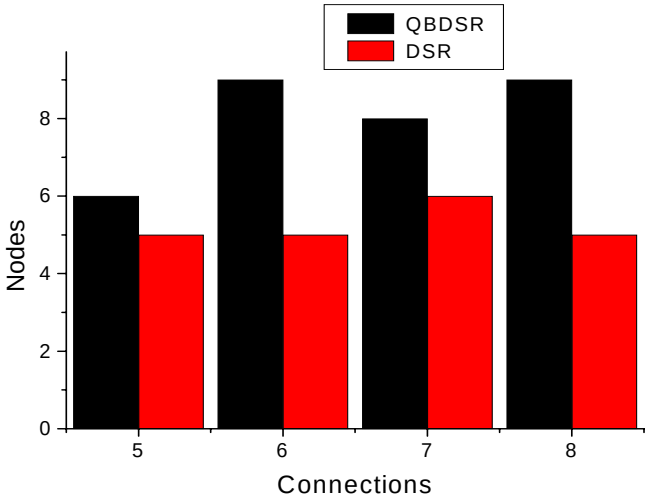


Figure II.8 The remainder of nodes with 25 nodes.

In figure II.9 we show the reaction of QBDSR in different configuration by varying the number of nodes between 10 and 100. As we can observe QBDSR always gives the minimum delay compared to DSR.

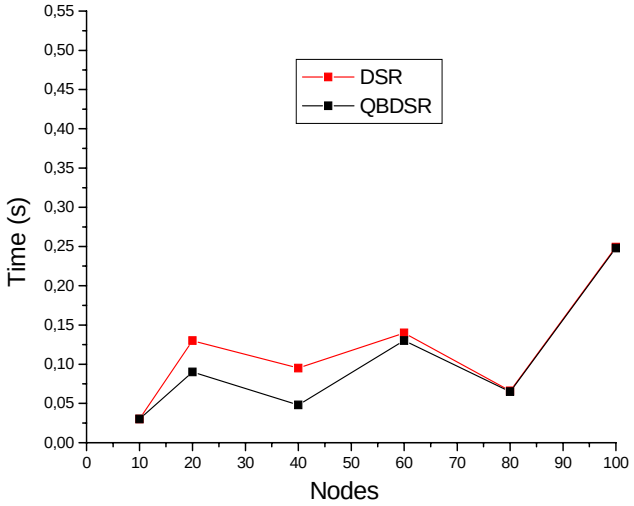


Figure II.9 The delay according to the number of nodes.

In figure II.10 is shown the delay according to the pause time. To perform these simulations we have fixed the number of nodes to 50 and varied the pause time from 50 to 200. As we can observe the QBDSR always gives the best delay.

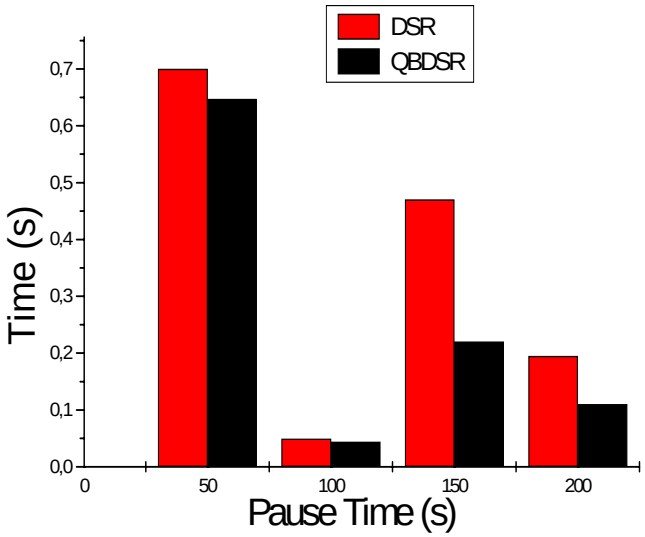


Figure II.10 The delay according to the pause time.

As we can observe from the previous simulations, QBDSR always gives best results compared to the original DSR, because it equilibrate the use of intermediate node since in the original DSR the traffic is concentrated over a limited routes until an error occurs or nodes become powerless, however in QBDSR at each time the bandwidth decreases a new sequence of node is used as route which saves the network resources and improve the delay and the network lifetime.

4. WEIGHT BASED DSR

As we have said reactive routing protocols suffer from lot of limitations presented above. In the previous sections we have implemented a method to include the QoS over reactive routing; however QoS is only one of the criteria that must be implemented for routing in ad hoc networks. Thus in the remainder of this chapter we are going to present a new method of route selection which includes more than one parameter in route selection. Our method is based on route weight computed by combining a set of system parameters reflecting the characteristics of ad hoc networks:

4.1 Weight based metric

Usually the metric used to evaluate routes is based on the number of hops (nodes) between the source and the destination as in conventional networks, in the previous section we have

presented an improvement to the reactive protocols in order to include the QoS in route selection, the results given by our implementation was good and the delay is improved, therefore in this section we are going to create a new metric more promising which includes more ad hoc network characteristics in route evaluation as battery power and node's mobility. Since it may exist a shortest route, however it includes a less powered node which can't forward efficiently packets, or unstable nodes causing quick link break down, this causes link failure and therefore new route discovery requests which overheads the network.

Thus, our proposed metric for mobile ad hoc routing is a combination of parameters which are node stability, battery power and the number of hops, in order to compute a route weight used after for route selection.

4.1.1 Stability

The most important advantages of MANETs is nodes' mobility, however in routing it is the most constraint because it causes topology changing which embarrasses the routing process [117]. Therefore, any routing protocol must confront this problematic.

However, the existed routing protocols do not give any consideration to mobility in route selection, in order to choose as intermediate node the most stable ones.

Thus, in the proposed metric we are going to include the aspect of nodes' mobility by computing the stability of nodes combined with other parameters to compute route weight.

We define the stability of nodes in ad hoc networks as the possibility of a given node to be as long as possible within the same neighbourhood (Figure II.11); this includes the case when the node moves within the same neighbourhood.

To compute stability, a mobile node must periodically scan its one or two hops neighborhood in order to define the number of nodes in this neighborhood, and controls if it stills having the same neighbors or not. If the majority of nodes stay unchanged this means that this node is always within the same neighborhood as a result it is marked stable otherwise it is marked as unstable to be avoided during routing.

To implements this we have made an improvement to the MAC layer [7] of each node, in order to periodically compute the number of neighbors, and define the number of absent node (nodes have left the neighborhood of the corresponding node). These operations are done using the routine MAC signal messages such as RTS, CTS and ACK messages.

Thus, a mobile node keeps a table where it saves the MAC addresses of all its one hop neighbors, the MAC address is obtained from the signaling messages. This table is scanned periodically to define the absent nodes, a node is marked as absent if we don't receive any

MAC layer packet from that node during a given period; used in the following equation to compute stability:

$$(\text{Stability})St = ((\text{total number of neighbors})t - (\text{number of absent nodes})t + \theta) / (\text{total number of neighbors})t$$

θ is the scan period.

A node is marked as stable if it has the greatest value of St, this means that this node is always within the same neighbourhood.

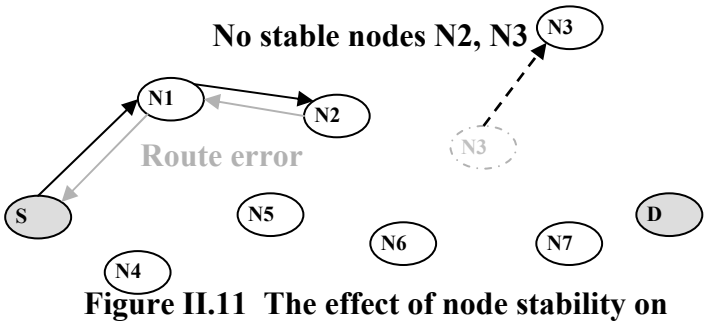


Figure II.11 The effect of node stability on packet forwarding

4.1.2 Battery power

Mobile nodes in an ad hoc network are usually handled devices; with limited battery power since the maximum life time of the best batteries does not exceeds some few hours, in the other hand we can not rely only on technology development in this domain because there is no new innovative technologies to develop new batteries with a long lifetime [118].

Thus, the single way to extend the network lifetime is to save the battery power rather than find new aspect to replace the existing one. Because the protocol stack on an ad hoc network there is no feature to save the battery power, this is due to the inheritance of this stack from the conventional one [119].

For example there is not any implementation of a MAC or IP layer special for ad hoc networks to save the battery power by limiting the number of unnecessary signaling packets.

Therefore, in this section we try to give an implementation of the aspect of battery power for reactive routing protocol (Figure II.12), which is added to node stability to define the weighted metric used for the evaluation of routes in ad hoc networks.

The aspect of battery power must be included at each layer to minimize the energy consumption and extend the network lifetime and improve the performance of the network, because powerless nodes in ad hoc networks cause lot of problems such as:

- They have small transmission range, which causes link failure.

- They cannot forward data for long time, which means that new routes must be found at each time an intermediate node is death.

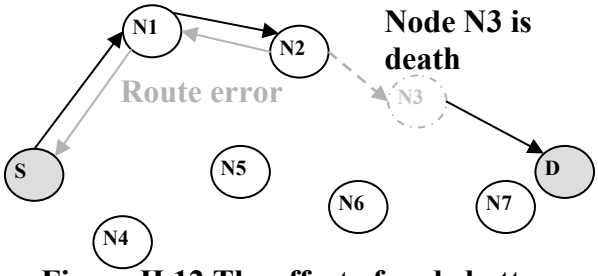


Figure II.12 The effect of node battery power on packet forwarding

Including the aspect of energy in route selection may minimize route error due to energy, in the way that the chosen route is the one containing the most powered nodes which can support dense traffic forwarding for long time, and whenever a new route is needed we choose always the most powered route which may differ from the fist ones which equilibrates the use of routes and the energy of intermediate nodes. This aspect may maximize the node lifetime and therefore the system lifetime and therefore minimize route errors due to nodes' death.

In order to include the aspect of energy in route selection we have used the battery level (Bl) of intermediate nodes as parameter, and we choose the route containing the most powered nodes which having the highest battery level.

The extraction of the battery level of nodes does not present a problem since in each mobile device there is a mechanism to extract the battery level.

4.1.3 Weight computing

As seen in the previous section we have defined two criteria to be considered when evaluating routes on which we add the number of hops, in order to choose as main route the one having the maximum power, the most stable nodes and the minimum of hops.

To accomplish this we propose to compute the weight of each route as the sum of all these criteria. Therefore when a route request is received by a destination the algorithm of route selection is launched in order to compute the route-weight of this route request and compares it with other route-weights and chooses as main route the one with the maximum weight (Figure II.13).

To do so we always use the min-max strategy to evaluate and choose routes, which tries to maximize the minimum of nodes' weights as follow:

1.Compute the node-weight (Nw_i) of each node i contained in each route which is the sum of the value of stability and the battery level of the corresponding node:

$$Nw_i = Bl_i + St_i$$

2.Compute the route-weight which is the minimum of all node-weights included in this route:

$$Rw_r = Min(Nw_i)\ ,\ i \in r$$

3.Choose as main route the one having the maximum route-weight.

$$Mr = Max(Rw_r)$$

$r \in R$ / R the set of routes

4.If two or more routes have the same route-weight or whenever their route-weights are nearby ε ($(Rw_i - Rw_j) < \varepsilon$) we choose as route the one with the minimum of hops, (ε is a predefined value).

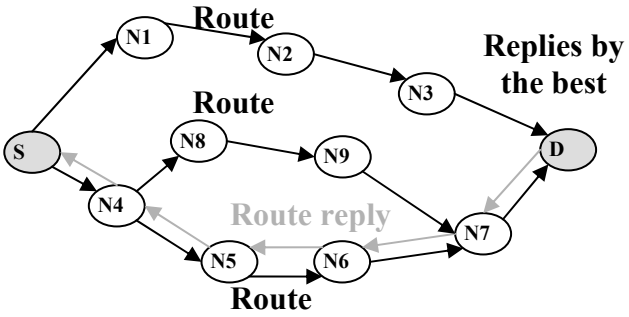


Figure II.13 Weight based reactive routing

4.2 Implementation

To make in practice the specifications defined above we applied them on the dynamic source routing DSR, our proposed version of DSR is called weight based dynamic source *routing WBDSR, and the most important modifications are done on:*

1. *MAC layer:* the modifications done on the MAC layer are intended to compute the stability, by implementing a mechanism for signaling packet capture in order to compute the neighboring nodes and define the absent ones for stability computing as defined in section 4.1.
2. *Route request:* the modification is done on the structure of the route request by including a new field to save node's weight, the second modification is done for route request treatment by which a node retrieve the stability from the MAC layer and get the battery level, sums them and inserts the obtained value in the header of the DSR's route request.
3. *Route reply:* the route reply differs from the original route one, in the way that the destination node doesn't response immediately to route request until it receives more route requests and computes for each one the route weight. After the expiration of the waiting delay it replies by the route having the maximum route-weight.

4. *The route cache*: we have used the same idea based on the maximization of route-weights to retrieve the best routes regarding weights from the cache. We have also added a mechanism to periodically refresh the cache in order to drop old routes which reflects best the state of the network (nodes battery power and stability).

4.3 Simulation results

We investigate the performance of WBDSR using the NS2 simulator [116]. We have compared the original version of DSR with our proposed version WBDSR to prove the utility of our improvement, the simulation parameters are given in the table II.1.

Parameters	Values
Network size	670*670 m^2
Number of CBR connections	4
Number of Nodes	25, 50
Max speed	20 m/s
Pause Time	0,60,120,300 s
Cache refresh	5 s
The value of ε	2
Wait time for route request *d*	0.25 s
Simulation time	200 s

Table 1: Simulation parameters

Table II.5 simulation parameters

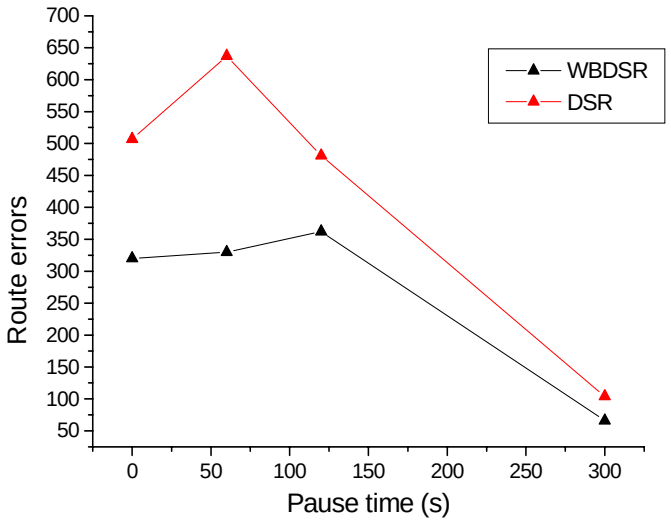


Figure II.14 Route errors with 25 nodes.

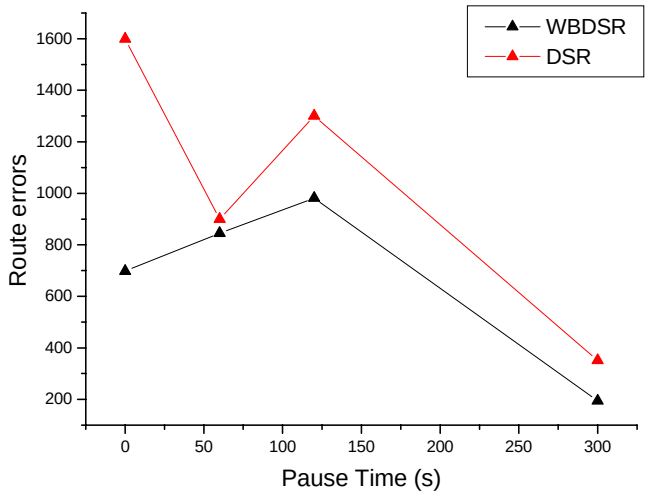


Figure II.15 Route errors with 50 nodes.

In Figures II.14 and II.15 we have tested the performance of WBDSR compared to the original DSR according to nodes pause time, as we can observe in the two scenarios (with 25 and 50 nodes), WBDSR gives less route errors which may improve the performance of the network because the maintenance using route errors needs to launch new route requests which causes a great overhead due to the flooding mechanism used to broadcast route requests over the entire network, which can block the network traffic in some situations and consume lot of energy from nodes' battery.

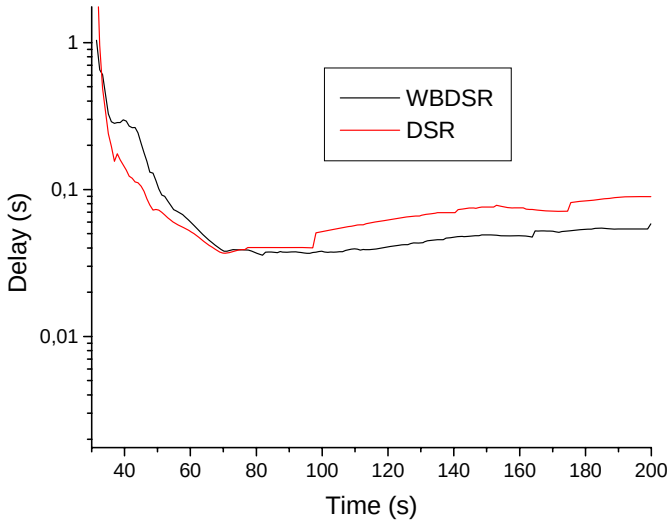


Figure II.16 End to End Delay with 25 nodes

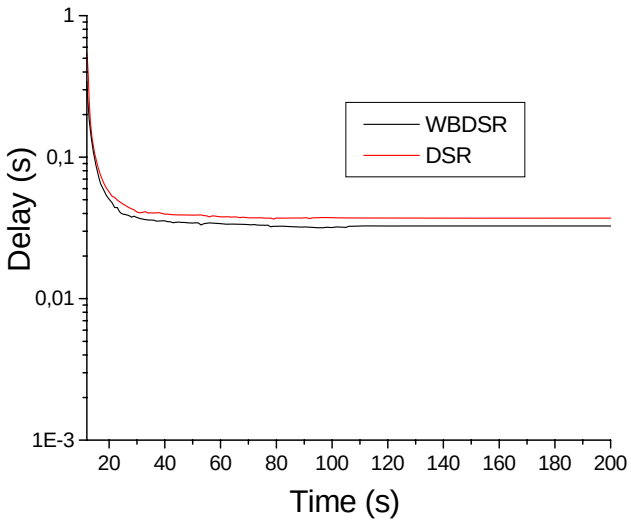


Figure II.17 End to End Delay with 50 nodes

As devoted in the previous simulations WBDSR may improve the network performance, which is proved in the two scenarios shown in Figure II.16 and Figure II.17 (with 25 and 50 nodes) in which WBDSR gives always best results compared to the original DSR concerning end to end delay. The performance improvement is clearer when the number of nodes gets high, since WBDSR gives always less delay for packet forwarding.

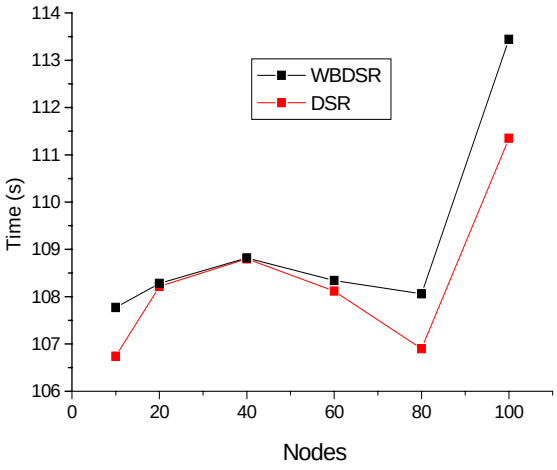


Figure II.18 system life time according to the number of nodes.

In Figure II.18 we have fixed all the parameters and we have varied the number of nodes from 10 nodes to 100 nodes and we have measured the system life time as we can observe the WBDSR always gives the longest system life time especially in dense network when the number of nodes gets high.

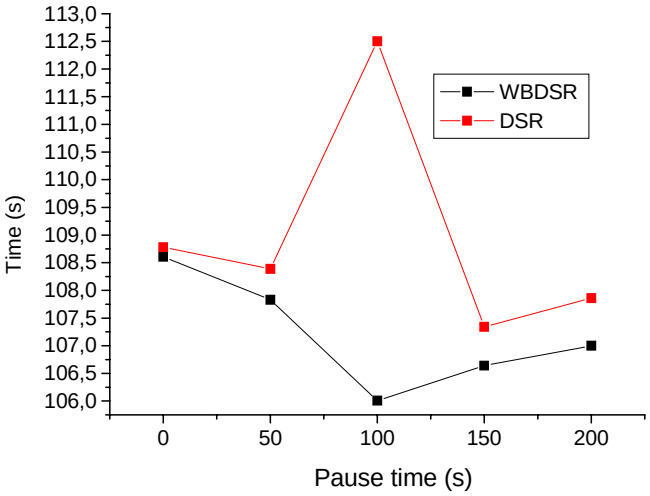


Figure II.19 End to End Delay with 50 nodes

In Figure II.19 we have fixed the number of nodes to 50 nodes and we have varied the pause time from 0 s to 200 s (static network), as it is shown WBDSR gives always the longest system life time in both high mobile networks and static network, because it periodically change the used route with another one which equilibrate the use of the nodes which increases the system life time.

5. CONCLUSION

In this chapter we have presented two possible improvements to reactive routing protocols for ad hoc networks in order to include some of the aspects of ad hoc networks as mobility, energy and QoS.

The first improvement tries to include the aspect of QoS in route selection using a mechanism of route selection which include the MAC link capacity in route selection, the application of our specification on DSR have given good results compared to the original DSR in term of energy saving, route errors and delay.

The second improvement is done in order to include the aspect of energy and nodes' mobility, by which we defined a method for stability computing in order to select the most stable nodes, the second aspect included in this second improvement is the battery power in order to choose as route the one having the most powered nodes.

These two parameters are used to define a new metric for routing which includes in addition to the number of hops the stability and the battery level of each node; these parameters are used to compute route-weight used for route selection.

To test the performance of our proposed metrics we have applied them on the most known routing protocol which is DSR, the simulation results given in this chapter prove the utility of our proposed metrics and always gives best results compared to the original DSR regarding end to end delay, system and nodes' lifetime and the number route errors.

In the next chapter we extend our work on reactive routing protocols, by studding a new method for routing based on swarm intelligence inspired from biological insects' swarm behaviour in which each insect with a little intelligence and capabilities define a smart global behaviour of the swarm. The same idea is used to define a new strategy of routing for MANETs.

Chapter 3

Swarm intelligence based routing in MANETs

In previous chapter we have investigated the problem of routing in MANETs. We have also developed new methods to improve reactive routing protocols in MANETs using cross-layer designs in order to exchange extra information between the networks layers used as parameter for route selection. Our proposed improvement for reactive routing protocols in the previous chapter was impressive, however it stills inherited from the classical routing. In this chapter we are going to present a new routing method for MANETs inspired from biological behavior of great communities of insects such as ant colony and bees, these communities achieve complex solutions with only a little intelligence and capacities at each individual, which can be emulated in ad hoc network usually composed of small nodes with limited capacities and moving randomly in a unpredictable environment.

1. INTRODUCTION

As described in previous chapter a mobile ad hoc network is a set of mobile nodes wirelessly connected to each other and use multi hop links to forward data and ensure nodes' connectivity when the distance between nodes exceeds their transmission range. This aspect makes the routing service one of the most crucial problematic of MANET, due to the nature of devices and the wireless medium.

In previous chapter we have tried to treat the routing problematic by using cross-layer design which consists of using information coming from several layers to improve routing regarding nodes' battery and system lifetime as well as end to end delay.

Using the cross-layers presented in the previous chapter we have treated the aspect of mobility, energy and bandwidth constraints in ad hoc networks which are the most challenging aspects of MANETs. These aspects were included in route selection giving birth to new metrics for routing which have considerably improved the network performances.

Solutions presented in the previous chapter as well as the ones presented in literature are based on classical routing which is inherited from the conventional routing developed for wired networks.

Classical routing finds routes according to some metrics or characteristics of links or devices and uses this route until an anomaly occurs such as link failures which launches a mechanism of route maintenance in order to solve the problem by finding a new route, it seems that this method of routing does not solve efficiently the problem of routing in MANETs due to the specificity of these networks.

Recently a new method is developed to handle the problem of routing in ad hoc network and overcomes the shortcomings of the classical methods, this methods are based on swarm intelligence inspired from biological swarms [120], such as ants or honeybees in order to solve some complex problems such as finding food or optimizing route to food in real insect swarms. These swarms, often containing thousands or tens of thousands of elements, routinely perform extraordinarily complex tasks of global optimization and resource allocation using only local information [121].

Therefore in the remainder of this chapter we are going to present the swam based routing for MANETs in order to improve and solve the problem of routing in ad hoc networks by projecting the swarm intelligence of ant colony for routing in MANETs.

2. SWARM INTELLIGENCE BASED ROUTING

2.1 Swarm Intelligence for optimization

Swarm Intelligence is an artificial intelligence technique based on the study of collective behaviour of great populations.

Swarm intelligent based systems are made up of a population of simple agents interacting locally with each other as well as with their environment. Typically there is no centralized control to show to these agents how to react, although local interactions between these agents often define the behaviour of the corresponding population or system [122].

Examples of such systems can be found in nature, including ant colonies, bird flocking, bee swarming, animal herding, bacteria molding and fish schooling [123].

In literature there exist lot of artificial optimization, since these optimizations give best solution to complex problems where the classical optimizations fail to deal with the complexity of the environment, however in our context there is two known swarm intelligence techniques:

- **Particle Swarm Optimization (PSO):** is a global minimization technique for dealing with problems in which a best solution can be represented as a point or surface in an n-dimensional space [124].
- **Ant Colony Optimization** (ACO): is a meta-heuristic optimization algorithm that can be used to find approximate solutions to complex problems in constrained environment. In ACO artificial ants build solutions by moving on the problem graph, deposing artificial pheromone on the graph in such a way that future artificial ants can build better solutions [125]. ACO has been recently applied successfully to lot of environment such as wireless networks and give best improvement compared to the classical techniques [126].

2.2 Ant Colony Optimization

In an ant colony for example, the swarm intelligence is achieved by using special form of communication between ants in order to find route to food or to the nest, since ants are very small insect in a big world however they always find their route [127]. Typically, this is done by deposing pheromone on the trail taken by each ant, a substance related to hormones produced by ants during movement, which other ants are able to sense. Ants are attracted by pheromone and therefore follow the exact trail to the nest or food [128].

Ants follow trails with higher pheromone concentration which often optimize their route to food and leads to follow the shortest trail and causes a self-accelerated reaction without any centralized intervention.

Figure III.1 shows a scenario where ants start from their nest and walk toward the food. When an ant reaches an intersection, it has to decide which branch to take next. The first ant randomly follows one of the two branches.

When coming back ants take another way to the nest and select one of the two branches, however after a while the concentration of pheromone will be more in the shortest branch and therefore ants follow the shortest path by mean of pheromone concentration.

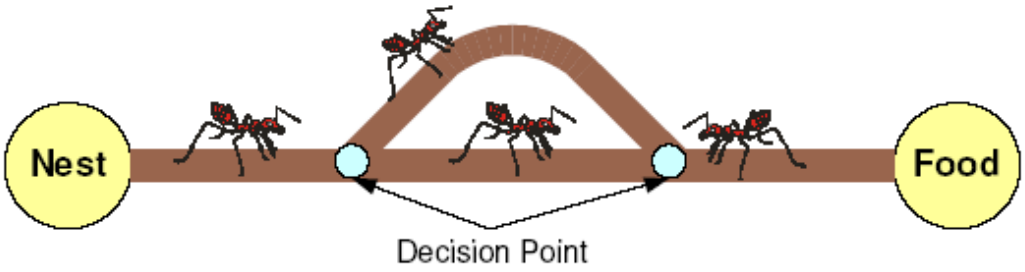


Figure III.1 Real ant colony path shortening

The behaviour of ants in order to find the shortest path from the nest to food can be used for routing optimization in MANETs, since an ant colony can be viewed as an ad hoc network composed of small devices and confronted to the same problem which is finding the shortest route in a decentralized fashion.

2.3 Swarm intelligence for routing in MANETs

Swarm intelligence routing algorithms are completely inspired from insect's communities; these communities have many desirable properties from the MANET perspective, since they are composed of simple, autonomous, and cooperative organisms that are interdependent and collaborate to achieve smart global objectives and define the global behaviour of the community, while such individual has relatively little intelligence incapable of understanding or modifying the community behaviour. Individuals of such community always execute simple actions and the methods of collaboration and communication between these individuals (agents) is simple, however very often generates best solutions compared to the capacity of each individual [129].

The characteristics of such communities is very suitable in the context of ad hoc networks, which are composed of simple mobile nodes with limited capacities working together to deliver services, in a constrained and unstable environment. An ad hoc environment may include any thing ranging from the nature of the environment itself to the nature of nodes and the used medium.

The ability of insects' communities to self organize can be used by ad hoc network to achieve complex and challenging services such as routing and security in ad hoc networks by using an analogy between these communities and ad hoc networking.

The reason behind choosing ACO for routing in MANETs is its distributed nature and the randomness of ant movement as well as the nature of the environment which is always constrained and unpredictable for ants. The algorithm used for optimization is a purely distributed executed by the collaboration of small agent with limited capacities and intelligent. This has lot of implications for MANET, since in a MANET's nodes are constrained by power, storage and processing power, a purely distributed algorithm like ACO reduce computation load and message exchange which may reduce the network overhead and improve the routing service over ad hoc network.

2.4 Motivation of swarm intelligence based routing

In swarm intelligence routing, the network nodes are supposed to be small agent collaborating with each other to perform routing over the network, by exchanging the minimum of messages, for example in ARA two kind of message are used forward and backward ants used to update pheromone table. According to the nature of a mobile ad hoc network the use of this category of routing is motivated by:

- **Dynamic topology:** This property is the most important advantages of MANETs, since it allows user mobility during his connection to the networks. However for routing it present the immense burden to be handled, it is also responsible for the poor performance of many classical routing algorithms, because the maintenance of link failures consumes the great part of the network resources. However, the ant algorithms are based on independent agents responsible of hop to hop data forwarding and the maintenance of per hop connection which allows high adaptation to the current topology of the network [130].
- **Local work:** In opposite to the classical routing, the ant algorithm is based only on local information gathered by each node about its neighbours and any decision about routing is taken locally according to the information stored at each node without needing to transmit routing tables or other information to other nodes of the network.
- **Multi criteria routing:** as described above the ant based routing is flexible and allows the integration of lot of parameters for route selection beyond the number of hops which allows us to include link state or distance into the computation of the pheromone concentration. This will improve the decision process with respect to lot of criteria according to the nature of the network and the state of nodes over the network, for example we can include security in hostile environments or energy in sensor networks.

- **Multi-path routing:** Each node over the network maintains a neighbour table containing pheromone corresponding to each neighbour used for route selection. The intermediate node can choose one of the neighbours for data forwarding according to this table, however for any reason (security, efficiency) the intermediate node can forward data to more than one neighbour in order to allow multi-path routing without any additional treatment or mechanism [131].
- **Decentralized decision about routing:** As devoted above each intermediate node is responsible of its link to all its neighbours and takes decision about route selection according to the pheromone table without the inclusion of the end users of the route. This allows a decentralized decision about routing in opposite of the classical routing in which the decision about route selection is taken by the source node according to the number of hops between the communicating nodes [132].
- **Limitation of flooding:** Usually classical routing uses flooding for route establishment, in reactive routing is used in order to broadcast the route discovery request over the entire network and for proactive routing it is used for routing table update which consumes lot of network resources. In ant based routing the decentralized nature of these algorithms minimizes the need of flooding to maintain and establish routes over the network [133].
- **Limited Overhead** : The expected overhead of ant based routing is very small, compared to other routing protocols because there are no routing tables to be updated or transmitted to neighbours, since ant based routing exchange only small routing packets which do not affect the network performance [134].

2.5 Ant colony optimization meta-heuristic for routing in MANETs

In this section we are going to present a simple example of using ant colony optimization meta-heuristic for routing in order to find the shortest path between two nodes in MANETs, the specifications given in this section are the basis of any ant colony based routing algorithm for MANETs [135].

The following assumptions and notation are used:

- We consider a connected graph $G = (V, E)$, where $|V| = n$, n is the number of nodes in the network.
- Each two neighbours i and j are connected by an edge $e(i, j) \in E$ if they are in the transmission range of each other.
- We denote N_i the set of one hop neighbours of i.
- $\varphi_{i,j}$ is the artificial pheromone deposed by ants corresponding to the edge $e(i, j)$ connecting i and j.

– Each ant when visiting an intermediate node in search of the shortest path deposits a constant amount of the artificial pheromone $\Delta\varphi_{i,j}$.

$$\varphi_{i,j} = \varphi_{i,j} + \Delta\varphi_{i,j}$$

– The artificial pheromone $\varphi_{i,j}$ is used by the ant on node i to compute the probability of using j as next hop for routing using the following equation

$$p_{i,j} = \begin{cases} \dfrac{\varphi_{i,j}}{\sum_{j \in N_i} \varphi_{i,j}} \; j \in N_i \\ 0 \; j \notin N_i \end{cases} \quad \ldots \text{(III.1)}$$

$$\sum_{j \in N_i} p_{i,j} = 1$$

– Artificial pheromone is decreased periodically using the following equation:

$$\varphi_{i,j}(t+\theta) = (1-q)\varphi_{i,j}(t), q \in (0,1] \ldots \text{(III.2)}$$

We suppose that a node s wants to find a path to a destination d using the ant colony algorithm described above:

- The source node s launches the operation of finding route to d by sending artificial ants over the whole network.
- Each ant travels over the network and deposit artificial pheromone on each used edge until it arrives to the destination node.
- Routes are selected according to the probability computed using the existed pheromone on each link using equation (III.1), by choosing the route having the best probability.

3. STATE OF THE ART

As described above, it seems that the use of swarm intelligence for routing in MANETs is efficient due to its decentralized nature which is very suitable for MANETs. Therefore, in the following sections we present an overview of the most known routing algorithms which are ARA and ABC:

3.1 The Ant Routing Algorithm for MANETs (ARA)

The method devoted in section 2.5 describes an abstraction of using swarm intelligence for routing in MANETs. Using the same idea and changing the manner of treating request and

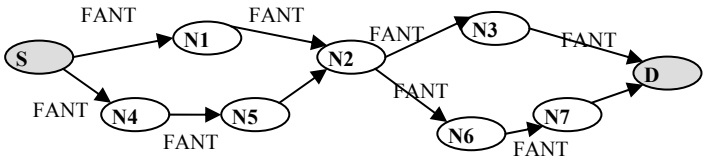
computing probability there are numerous swarm intelligence algorithms in literature, the most known between them is Ant Routing Algorithm (ARA), ARA uses specific method and mechanisms developed for ad hoc network in order to handle path establishment and maintenance [135].

Typically, ARA routing management is similar to DSR (dynamic source routing), in the way that the process of routing is composed of:

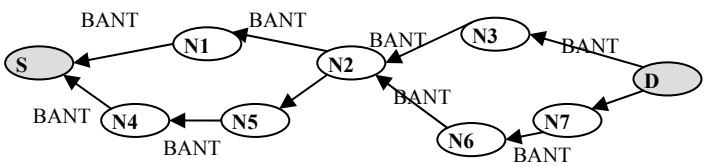
- Route discovery in which the route is established using forward and backward ants,
- Route maintenance phase in which the pheromone is updated according to equations (III.1) and (III.2) in section 2.5
- Finally an error handling phase in order to treat link failures.

5.1.1 Route discovery phase

The objective of this phase is finding a route between a source node s and a destination node d (Figure III.2). Two classes of ants exist for this purpose, the first one is called forward ant FANT which is defused over the whole network in order to find all possible routes to d. Thus FANT travel over the network and update pheromone on each visited node using equation (1) until it arrives to destination node d, at each time the FANT is received by an intermediate node, this last create a record in its pheromone table if it does not exist or increase the existed pheromone with $\Delta\varphi_{i,j}$. In the other hand the backward ants establish the final route to the source node s, similar to the biological system the pheromone is increased by both the FANT and BANT and decreased according to time.



Forward ant process



backward ant process

Figure III.2 Forward and backward ants in ARA

5.1.2 Pheromone table structure

The pheromone table is similar to the routing table in classical routing, except that for the pheromone table is stored information corresponding to only one hop neighbours. This table is updated using forward and backward ants

Whenever the forward ant visits an intermediate node for the first time an entry is created containing:

- The identifier of the source node which has initiated the route discovery.
- The identifier of the next hop used to reach the destination node.
- The initial value of the pheromone, which is the same for all new created entries.

The pheromone table is updated using two ways:

- The first way using forward and backward ants, since at each visit of these ants the pheromone is increased with a fixed amount such as in real systems.
- Periodically, the value of pheromone is decreased according to time in order to emulate the biological pheromone which loses concentration due to time.

5.1.3 Route maintenance and error handling

Route maintenance operation is responsible of maintaining routes during communication, by updating the pheromone tables as described above and handling link errors if they exist.

Link errors are caused by node mobility and detected by the MAC layer, the MAC layer decide that a link is lost if it does not receive acknowledgement for data packets after a predefined number of attempts. If this case appears this node is dropped from the pheromone table then the corresponding node tries to find an alternative route in his table to be used as next hop in place of the first one and continue the data forwarding, otherwise an error message is sent to the source node in order to launch new route discovery mechanism.

3.1 Ant based Control (ABC)

Ant based control is another implementation that uses swarm intelligence for searching the shortest path in communication networks. Contrary to ant routing algorithm ABC is designed for telephone networks however it shares lot of concepts with ARA [136,137].

ABC is composed of one class of ants which are responsible of establishing probability along various paths over the network. Thus, ants are launched at regular intervals to various destinations, these ants are responsible of updating pheromone table and computing probabilities, these probabilities are used by telephone traffic which follows the path of highest probability.

3.2 Other usage of swarm intelligence

The above described algorithms are only the most known and successful usage of swarm intelligence for routing and communication networks. However, in recent years swarm intelligence knows new fields of application in ad hoc networks regarding the possibilities given by this method to solve complex problems in distributed systems.

For example in [138] the author propose a method based on swarm intelligence in order to save energy in ad hoc network as well as in [139] for the network management.

Also swarm intelligence is used in security and intrusion detection system such as in [140], other applications exist using swarm intelligence to solve the increasing problematic for ad hoc network other than routing.

4. ANALYSIS OF ARA

As described above, ARA gives the simplest application of swarm intelligence for routing in ad hoc networks because it applies directly the concepts of ant colony to ad hoc networks without tacking into account all the characteristics of ad hoc networks such as mobility, bandwidth and energy constraints, thus we can differentiate the following shortcomings:

- In ARA the pheromone table is updated at regular intervals or whenever a forward or backward ants visit nodes over the networks which is not sufficient since the pheromone must be updated according to other parameters such as nodes mobility, battery power as well as the sate of links between neighbours which affect the routing in ad hoc networks.
- In ARA, the traffic is forwarded according to the concentration of pheromone over edges, therefore the same path may be used by several connections, which consumes the resources of intermediate nodes in this path, so a mechanism must be defined to avoid similar situations by distributing traffic according to the number of connections using the same route and choosing new paths whenever the number of connections over the same path reach its maximum.

5. LINK QUALITY BASED ARA

5.2 Introduction

As devoted above ARA suffers from some design limitations, since it do not gives the necessary consideration to the ad hoc networks characteristics in the process of pheromone update and route selection. Hence, in this section we are going to improve the Ant Routing Algorithm by defining a new mechanism of pheromone computing which includes some of

the most important characteristics of ad hoc network which are the link quality and the devices' constraints.

Link quality is the most promise parameters, since it define the ability of a given link and devices to support the density of the traffic for the period of connection. The link state between two neighbours can be affected by lot parameters such as distance, battery power and mobility [141].

Thus, in the next sections we are going to define a method for link state evaluation using cross-layer design between the physical layer and the network layer, used for pheromone update.

The second parameter used in route selection will be the number of connections over the same path, in order to choose paths with fewer connections (traffic) as route in order to save resources of intermediate nodes over this path by distributing the network traffic over other nodes of the network which increases the system lifetime as well as end to end delay.

5.3 Link quality evaluation

We define link quality between two neighbours as the ability of this link to be as long as possible stable, have less bit errors and reach its destination with the maximum signal strength [142].

In literature link quality is usually evaluated according to the received signal strength, because the transmission power of the wireless medium is proportional to the link quality, since a signal with high strength is more stable and has less bit errors.

Equation (III.3) gives the reception power P_r for a signal transmitted with power P_t at a distance d:

$$P_r = P_t \times G_r \times G_t \times \frac{\lambda^2}{(4 \times \pi \times d)^2} \quad \text{... (III.3)}$$

Where

P_r = received power,
P_t = transmitted power,
G_t =antenna gain of the transmitter,
G_r = antenna gain of the receiver,
λ = wavelength,
d = distance.

From the equation (III.3) evaluating the link quality according to the received signal strength can be descriptive for other network factors such as:

- The battery power of nodes, this factor is very important since a node with less energy in its battery have small transmission range which affects the quality of links with its neighbourhood; in the other hand it can not forward data for long time. From equation (III.3) whenever the battery level is low the transmission power is also low and therefore the reception power is low, thus this link has not high quality.
- The distance and obstacles (walls), from equation (III.3) links quality or the reception power is relative to the distance and obstacle between nodes since whenever the distance and the obstacles increase, the link quality decreases.
- The mobility of nodes, the link between two nodes is directly affected by nodes' mobility in the way that the link quality decreases whenever neighbours are going away from each other and increases whenever they go closer.

5.4 Implementation of link quality evaluation

As described above, we have chosen to evaluate the link quality according to the received signal strength, because the quality of links is proportional to the received power. In the other hand the received power can only be measured on the physical layer. Therefore, we need a cross-layer between the physical and the routing layers in order to transmit the value of the received signal strength from each neighbour to the routing layer.

The implementation of the cross layer can be described as follow:

Each node captures the entire packets exchanged within its neighbourhood in order to take information about all its neighbours regarding the link quality. Thus, at each time a new packet is received the corresponding node creates a record containing the *identifier of the sender* and *the received signal strength (*Figure III.3). This record is sent to the network layer and saved in pheromone table.

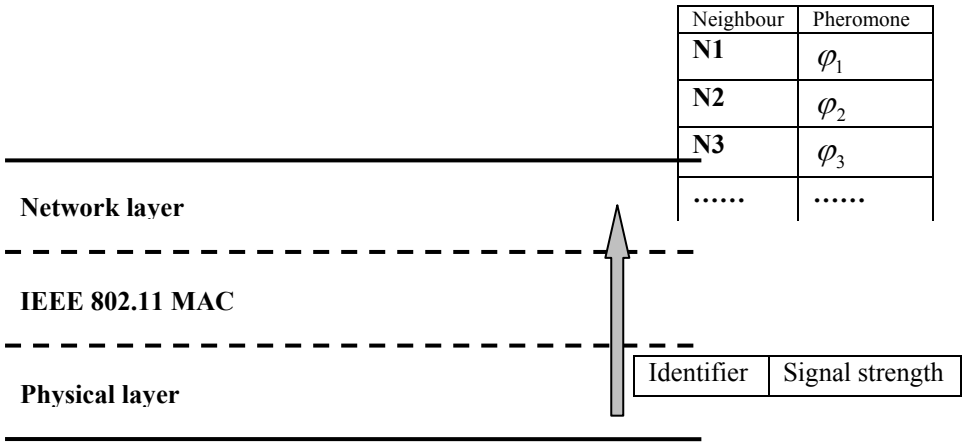


Figure III.3 Link quality evaluation Cross-layer

5.5 Pheromone and probability

As devoted previously the swarm intelligence routing is based on probability computing based on the amount pheromone on each link, the computation of pheromone in our proposed routing scheme is based on link state which is defined according to the receiving signal strength.

5.5.1 Pheromone computing

As said in previous sections, our proposed method to compute pheromone is based on the link state between neighbours, in the way that the greatest value is given to the best link. We have proposed in the previous section a method for link state evaluation based on the received signal strength, which gives us the possibility to implicitly evaluate other network parameters such as the battery power and the distance between nodes which can be concluded according to the signal strength.

Thus, the pheromone value is given using the following equation:

$$\varphi_{i,j} = \mathrm{Pr}_{i,j}$$

Where $\mathrm{Pr}_{i,j}$ is the power level of the received signal from the edge (i,j)

Using the value of $\varphi_{i,j}$ we can compute the probability of using this edge for routing according to the link quality factor using the following equation:

$$P_{lq(i,j)} = \frac{\varphi_{i,j}}{\sum_{j \in N_i} \varphi_{i,j}} \quad j \in N_i \qquad \text{(III.4)}$$

N_i is the set of all neighbors of node i.

As we have explained before, in classical or other algorithms the same path continues to be used until an error or an anomaly occurs, otherwise all the traffic will be forwarded over the same path which consumes intermediate nodes' resources. Thus, we have proposed to avoid such situation by including the connectivity factor to measure the number of connections forwarded by a link in pheromone computing. The connectivity factor is expressed by the probability of using the edge (i,j) according to the number of connection using the following equation :

$$Pcn_{(i,j)} = \frac{C_{i,j}}{\sum_{j \in N_i} C_{i,j}} \quad j \in N_i \qquad \text{(III.5)}$$

Where $C_{i,j}$ is the number of connection forwarded by the edge (i,j)

Routes will be chosen according to the link quality as well as the number of connections over the same edge, therefore the final value of probability to use the edge (i,j) for routing is given by:

$$p_{i,j} = \frac{Pcn_{(i,j)} + Plq_{(i,j)}}{2} \qquad \text{(III.6)}$$

$$\sum_{j \in N_i} p_{i,j} = 1$$

5.5.2 Pheromone update

The operation of pheromone update is intended to change the value of pheromone for each neighbour according to some criteria such as time or some system parameters such as in our case the link quality, since the link quality change during the system lifetime and therefore the pheromone must be accordingly changed.

In our proposed scheme the pheromone and similar to biological systems is decreased according to time, thus the amount of pheromone is decreased in regular intervals of time using the same equation given in literature:

$$\varphi_{i,j}(t+\theta) = (1-q)\varphi_{i,j}(t), q \in (0,1]$$

In addition to time factor, the pheromone is increased or decreased according to the link quality with each neighbour. Thus, the pheromone is increased whenever the received signal strength increases for example when the corresponding neighbours move close to each other, or decreased whenever the corresponding nodes go far from each other or if they move in an area where there are some obstacles such as walls.

5.6 Route discovery

Similar to ARA or DSR, the route discovery mechanism is intended to find routes over the network, as well as updating pheromone table such as in swarm intelligence based routing.

To accomplish the discovery and establishment of routes over the network, two classes of ants are defined which are forward and backward ants.

5.6.1 Forward ant (Packet structure)

Forward ants are intended to discover routes; it is launched by the source nodes and broadcasted over the entire network until it arrives to the destination node. During its trip over the network, the FANT causes pheromone update since the reception of FANT is the event which launches all kinds of pheromone update.

The structure of the forward ant can be described as follow (Figure III.4), where:

- *Packet Type:* This field is one byte size; its value describes the purpose of the packet, data, FANT or BANT, in this case it is fixed to FANT.
- *Source IP Address:* This field is four bytes and describes the IP address of the source node.
- *Destination IP Address:* This field is four bytes and describes the IP address of the destination node.
- *IP list:* This field is an array of four bytes and contains the list of IP addresses followed by the FANT during its broadcasting over the network.
- *Pheromone list:* This field is an array of four bytes and contains the amount of pheromone carried by each link traversed by the FANT.
- *Sequence number:* this field is four bytes and contains a unique sequence number used to avoid route loops, similar to DSR.
- *Time-To-Live (TTL):* This field is one byte and describes the remaining allowed hop-count for the FANT. It is fixed to 255 and decremented at each visited node.

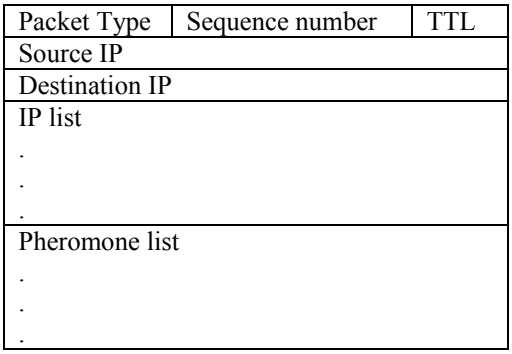


Figure III.4 Forward ant structure

5.6.2 Backward ant (Packet structure)

Backward ant is intended to establish the final route; it is launched by the destination and sent to the source node using unicast. Only, one BANT is sent to destination; across the route containing the greatest probability. Thus, whenever the destination node receives a set of FANTs it chooses the one having the greatest probability computed as described above and sends it back to the source node.

The structure of BANT packet is similar to the FANT except that it does not contain the list of pheromone (Figure III.5), because it is not used by the source node:

- *Packet Type:* is fixed to BANT.
- *Source IP Address:* contains the address of the destination node.
- *Destination IP Address* contains the address of the destination node.

- *Reversed IP list:* This field is an array of four bytes and contains the reversed list of the list retrieved from the FANT.
- *Time-To-Live (TTL):*is fixed to the length of the reversed list.

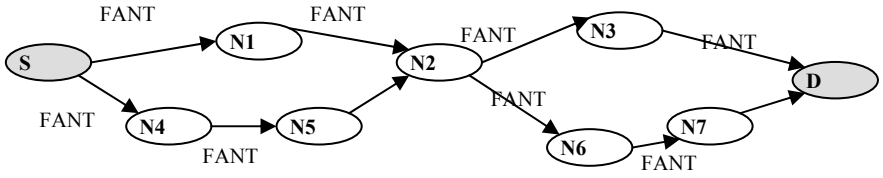
Packet Type	Sequence number	TTL
Source IP		
Destination IP		
IP list . . .		

Figure III.5 Backward ant structure

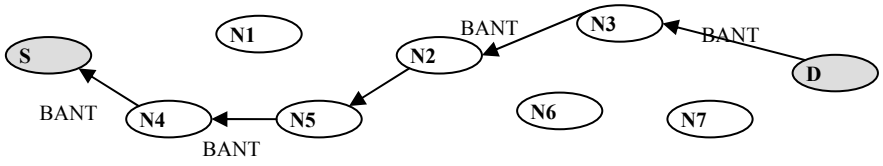
5.7 Link quality based ARA functioning (LQARA)

As it has been implicitly described, the functioning of LQARA is similar to the original ARA except that for our proposed algorithm the link quality is evaluated by the physical layer and transmitted to the network layer to be used for pheromone update.

In addition, the decision about route is done by the destination node by choosing node with best quality defined according to the probability computed using the list of pheromone joined to the list of IP addresses contained in the forward ant and collected during her trip over the network. Consequently, only one backward ant is sent to the source node in order to establish route which decreases the overhead due to this ants. Contrary to the original ARA which sends several backward ants used for pheromone update, because in our proposed enhancement the pheromone update is done using the cross layer design out of routing process which decreases the computing overhead during the route discovery process (Figure III.6).



Forward ant process



Backward ant process

Figure III.6 Routing process

5.8 Error handling and Route maintenance

The route maintenance is similar to the original ARA and no modifications are done. Hence, whenever a link between two neighbours fails included in the routing process, a route error packet is sent to the source node which launches a new route discovery as described above intended to establish a new path between the corresponding nodes.

The route error packet structure is similar to ARA:

- Error Source Address: The address of the node originating the Route Error (node has discovered the link failure).
- Error Destination Address: The address of the node to which the Route Error must be delivered For example
- Error Type field: in our proposed is always set to NODE_UNREACHABLE.

6 SIMULATION RESULTS

In order to test the performance of our proposed algorithm regarding the end to end delay and the system lifetime, we have compared LQARA to AODV using NS2 simulation tool. Simulations have been performed within the network area of 670*670 m^2 during 200s. Nodes move within this area with the speed of 20 m/s using four CBR connections. The pause time was set to 40 s and the number of nodes was varied from 10 nodes to 40 nodes.

As we have presented above the LQARA does not use the same procedure as ARA, it combines some of the mechanisms of ARA and DSR.

The simulation given in the following subsections does not use the parameter of the number of connections between each pair of nodes.

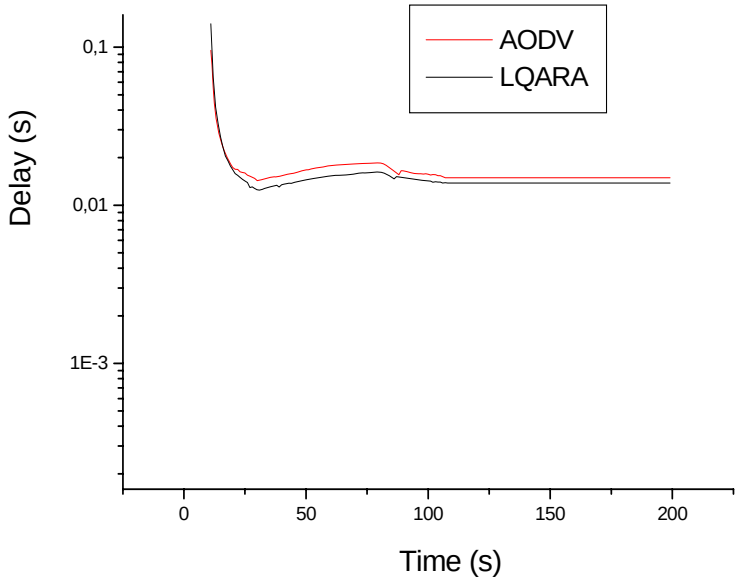


Figure III.7 end to end delay using 10 nodes

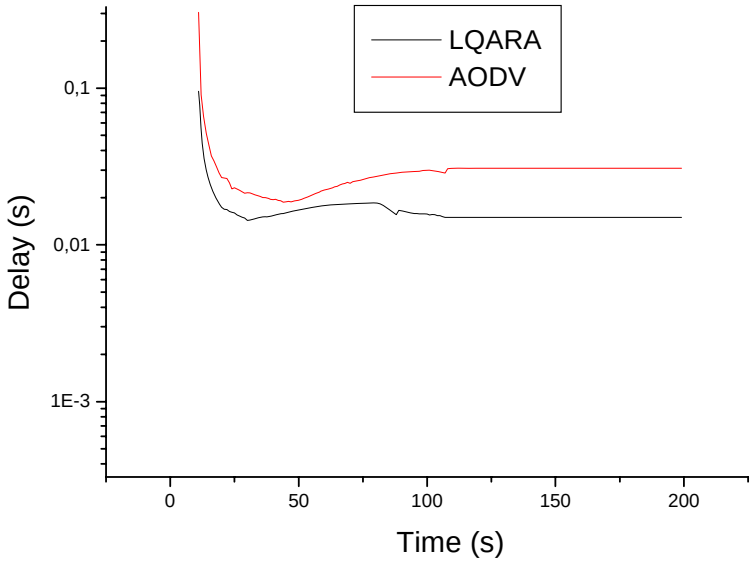


Figure III.8 end to end delay using 20 nodes

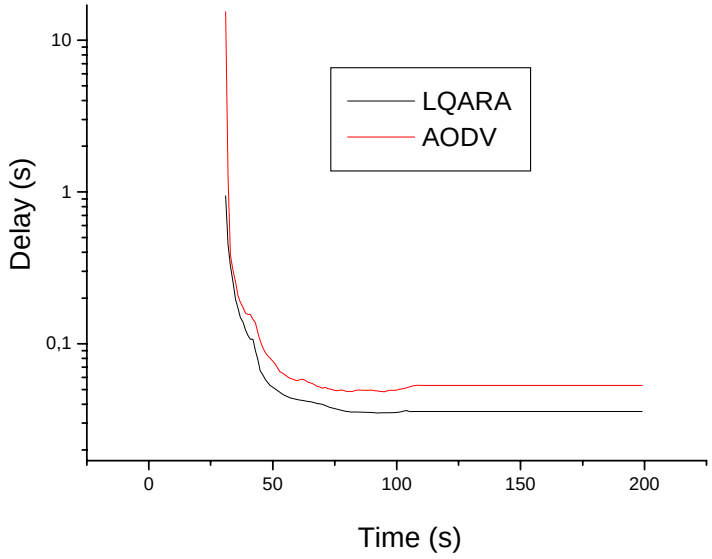


Figure III.9 end to end delay using 40 nodes

Figures III.7, III.8 and III.9 show the simulation results regarding end to end delay of respectively 10, 20 and 40 nodes. As we can observe the delay given by LQARA is always lower than the delay given by AODV this is due to the mechanism of pheromone update and route selection which distributes the network traffic over multiple paths and therefore decreases the end to end delay. In addition the link quality based routing decrease the number of route errors which saves the network's resources and decreases the network overhead due to link failures.

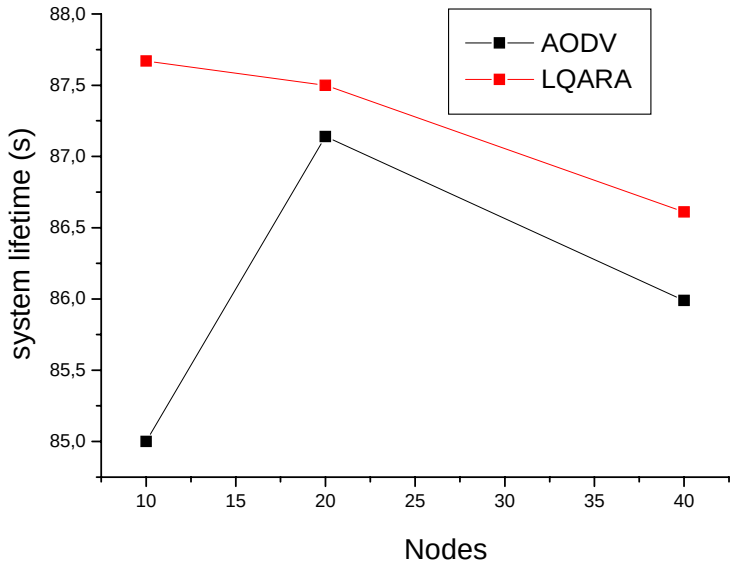


Figure III.10 system lifetime according to the number of nodes

Figure III.10 show the system lifetime according to the number of nodes which is set to 10, 20 and 40. As we can observe the system lifetime using LQARA is always higher compared

to AODV, since the network traffic using LQARA follows paths with the highest link quality which distribute the network traffic and save the system resources.

7 CONCLUSION

In this chapter we have investigated swarm intelligence based routing, this class of routing which is more promising in the nearer future by emerging new mechanisms and ideas. As devoted above, swarm intelligence is very suitable for ad hoc networks, regarding its distributed fashion to treat and resolve complex problems using analogy to biological swarm of insects.

We have also presented ant routing algorithm, one of the most known routing algorithm for MANETs, as described ARA suffers from some limitations in the pheromone computing since it has not taken the necessary consideration to the characteristics of MANETs such as mobility and the medium constraint.

Therefore, in our proposed enhancement to ARA called LQARA we have included the link quality in route selection and probability computing which have considerably improved the network performance and the system lifetime.

In the rest of this thesis we are going to treat the aspect of security in ad hoc and sensor networks by proposing a lightweight implementation of public key infrastructure PKI in order to secure communication over these networks, next chapter gives a set of specifications for implementing a PKI over reactive routing protocols for mobile ad hoc networks.

Chapter 4

Securing reactive routing protocols in MANETs using PKI (PKI-DSR)

In this chapter we are going to treat the aspect of routing security in MANETs, since security is not natively implemented in ad hoc routing and the extensions given in literature are complex and vulnerable against several attacks. Given that the Public Key Infrastructure (PKI) is the most promising solution for security in conventional networks, we will develop a new mechanism to secure reactive routing protocols and deploy Public Key Infrastructure (PKI). The proposed scheme uses the operations of reactive protocols such as route discovery and route reply to publish certificates over the network which are used after to secure the routing protocol by means of digital signatures and symmetric encryption giving for our design the possibility to detect lot of attacks, since there is no way for an attacker to infiltrate into the process of routing or data forwarding over the network.

1. Introduction

As devoted in previous chapter, Mobile Ad hoc networks knows a great success and large emerging in our lives, ranging from peace use for rescue in catastrophic environments such as in seism to sensor networks deployed in battlefields in order to collect information about the enemy army or to connect soldiers. This due to their facility of deployment and use since there is no need to administrate, to install or to manage any service over the network [143].

On the other hand, MANETs are by nature very open to basically anyone having the proper hardware and knowledge of the network stack, exposing the whole network to potential attackers willing to modify data or disrupt the network services.

Nevertheless, security is not carefully carried out and the majority of the mechanisms developed in literature are inherited from the conventional ones making them vulnerable to many attacks, otherwise they are subject of performance degradation of the network.

Therefore, new mechanisms must be developed to ensure security in MANETs, tacking into account their specificity as the topology changing and the used medium as well as the nature of the involved devices which are in general handled devices with limited capacities [144].

Another problem is the no existence of centralized authority, responsible of the distribution of cryptographic keys or the management of the Public Key Infrastructure, as in conventional networks [145]. Furthermore, their heavy reliance on inter-node communication to ensure routing, allows a big range of attacks against routing protocols by malicious intermediate nodes as well as data modification and denial of service attacks.

Therefore, any routing protocol developed for MANETs must natively implement security during design; although all the widely used routing protocols for MANETs do not consider security issues and suppose that all the network's nodes fairly participate in the routing operation without any malicious intention which is not always true in reality, in addition to outsider intruders can perform some attacks as Denial of Service attacks, data modification or simply eavesdropping the exchanged data [146].

2. Security risks in MANETs

MANETs have no boundaries and the transmission range of the network may exceed the area where the network is deployed exposing the network to numerous attacks executed from both interior and exterior attackers. In addition, the existed routing protocols do not implement any security mechanism to protect the exchanged data as well as the routing information.

On the other hands, each node in the network plays two roles the first one as an ordinary node and the second one as a router to forward data. This may create lot of problems because any node in the network forward a great amount of data as router and as ordinary node, in addition to data which can be passively eavesdropped.

Therefore, in this section we are going to give an idea using simulation about the risks to which the exchanged data are exposed over a MANET, by deploying a set of attackers over the network and computing the number of altered packets by each attacker over the network.

To do so, we have deployed 25 and 50 mobile nodes in the area of 670*670 m^2 and we have chosen 10% of mobile nodes to be attackers and perform data modification over the network, for simulation purposes we have implemented a mechanism to detect any modified packet.

To emulate traffic over the network we have also used some CBR (Constant Bit Rate) connections with packet length of 512 bytes to emulate traffic over the network; other simulation parameters are listed in table IV.1.

The simulation tool is always NS2 [116], which is recognized as one of the most powerful tool for wireless and wired networks simulations.

Parameters	Values
Network size	670*670 m^2
Number of Nodes	25, 50
Max speed	20 m/s
Wait Time	60 s
CBR connections	4,5,6,7,8
Routing protocol	DSR
Number of attackers	10%
Simulation time	600s

Table IV.1 Simulation parameters

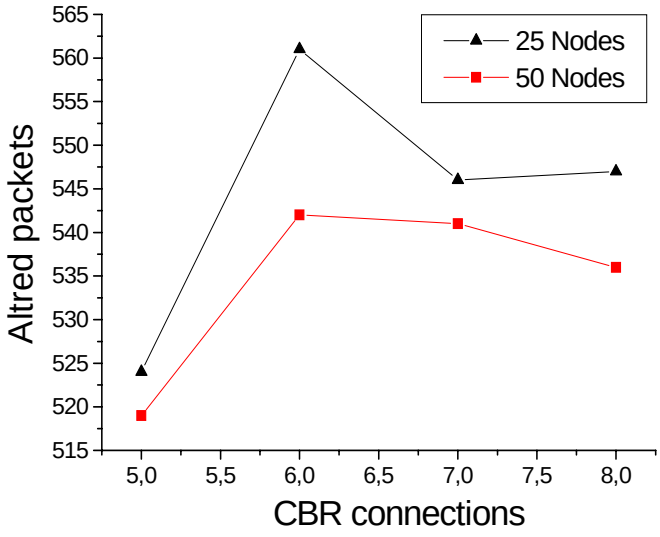


Figure IV.1 Number of altered packets forwarded by each node

In simulation of Figure IV.1 we give the average number of altered packets forwarded by each mobile node in the network with the absence of any security or intrusion detection mechanism.

As we can observe the number of altered packet is very high according to the number of CBR connections which is less than eight connections however in a real cases the number of connections is usually more than five.

We observe also that the number of altered packets gets high when the number of nodes is small this is because each node in a small network forward more data, which gives to the attacker more opportunity to alter and modify packets.

From these simulations we can predict the danger that makes any attacker in the network, since each node in the network forwards a great portion of data giving him the ability to control and eavesdrop the majority of the exchanged data over the network.

In the simulation the attacker does not perform any other attacks it only alter an eventual forwarded packet and do not try to attract traffic to over to alter more packet using for example black hole attack. This means that the results are more pessimists when the attackers collaborate between themselves to execute other routing attacks [147].

3. Routing attacks

As devoted above the open medium, the rely on intermediate nodes connections, gives the possibility to a large variety of attacks against MANETs and their routing protocols, hence in this section we try to present a no exhaustive list of routing attacks:

- **Black Hole:** This attack is usually executed against reactive protocols [148], by which an attacker tries to attract all or a subset of the network traffic over him, by injecting false route replies advertising the attacker as having the shortest path, which forces the data flow to pass by the attacker (Figure IV.2). After this, the attacker can perform other ordinary attacks against data as man in the middle, data modification or eavesdropping, replay, impersonate …etc

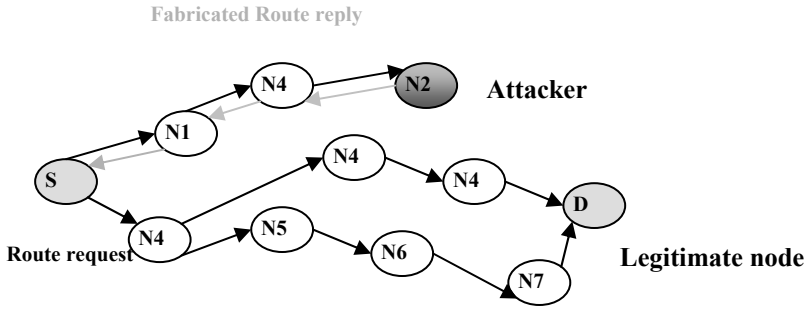


Figure IV.2 Black hole attack

- **Replay:** The attacker here injects into the network routing information that has been captured previously to perturb the functioning of routing in the network or to advertise the attacker as legitimate node and perform black hole attack [149]. This attack can only be executed against poorly designed protocols, since any additional security mechanism like digital signature can stop this attack.

- **Blackmail:** This attack is performed against routing protocols that are based on node behaviour to identify malicious nodes [150]. In this kind of security mechanisms, each node control its neighbour and sends eventual alerts against some presumed attackers, whenever the number of alerts gets high the corresponding node can be excluded from the routing process or from the network. These alerts are kept in a black list to be used for route selection; therefore the attacker usually fabricates false alerts against legitimate nodes in order to disturb the network.

- **Routing table poisoning:** in table driven routing protocols each node keeps a table where it saves the network topology used for routing, each entry in the table contains a route to a given node in the network. Thus, the attacker tries to trouble the routing process by fabricating false routing information or modify legitimate information coming from

legitimate nodes [151]; this attack may block the network process if it is not used to perform black hole attack.

- **Denial of service attacks:** this attack is one of the most important attacks since it can be executed against any routing protocol or mechanisms of security. This kind of attack is the last tentative of an attacker if all the above attacks do not success in which he tries to completely stop the routing process or other services over the network. Denial of services attacks are unavoidable however the attacker can quickly be detected [149].

- **Wormhole [150]:** This attack involves more than one attacker, in which the attackers colludes both the source and the destination nodes and construct a tunnel between the communicating nodes giving them the possibility to control all the traffic as well as any eventual mechanism of security. In other terms the legitimate node is colluded by attackers and can not do any thing without their control a mechanism of authentication can stop this kind of attacks.

4. Securing routing protocols

As we have presented above several routing attacks exist, some of them already exist against conventional routing however the rest are specially developed against ad hoc routing due to the nature of these networks. In the other hands, the existed routing protocols do not natively implement security which makes their treatment more difficult.

Although, in literature there are a lot of methods to secure routing protocols by adding new security issues over the existed routing methods. In this section we try to give an overview of some of these secured routing protocols:

- **The Secure Routing Protocol (SRP):** is a set of security extensions that can be applied to any ad hoc routing protocol that utilizes broadcasting as its route querying method [152]. The author in this proposition gives DSR as an example for the application of SRP. In SRP both the destination and the source nodes use a security association in order to share a secret key used to encrypt the traffic over the discovered route.

As shown in Figure IV.3, the SRP protocol appends the header of the original route discovery by adding the following parameters:

- A *query sequence* (QSEQ) number that is used by the destination in order to identify outdated requests.
- A random *query identifier* (QID) that is used to identify the specific request.

- The hash value of the IP header, the header of the basis protocol and the shared secret between the two nodes.

IP Header	
Routing protocol header	
Type	Reserved
Query identifier (QID)	
Query identifier (QSEQ)	
Message authentication code (MAC)	

Figure IV.3 SRP Header

The integrity of data is protected using the MAC function since the secret key is never transported in clear and only its hash value is transmitted over the network which is the best way to protect secret over the network. An additional mechanism of security which is multi-path is proposed by the author to ensure more confidentiality.

However, the security association between each pair of nodes requires and off line dealer or a centralized authority to distribute the secret keys for each pair of nodes which is not possible in ad hoc networking.

- **The Authenticated Routing for Ad hoc Networks (ARAN):** proposed in [153], is a stand-alone solution for securing on demand routing protocols in ad hoc networking using asymmetric cryptography and digital certificates to ensure both authentication and non-repudiation. It supposes the existing of an off line certificate authority which deliver certificates to each node in the networks, the public key of the CA is publicly known in the network in order to verify the authenticity of certificates and nodes. ARAN tries to secure routing by securing the route discovery process, thus each route discovery packet includes the certificate of the initiating node, a nonce, a timestamp and the address of the destination node. Furthermore, the source node signs the route request and broadcast it over the network, each intermediate node when receiving this route request verifies the validity of the signature; sings the whole route request and rebroadcast the route request accompanied with its certificate.

Whenever, the route request arrives to destination node this last construct a route reply which contains the address of the source node, the destination's certificate, a nonce, and the associated timestamp. The destination node signs the RREP before transmitting it. The RREP is forwarded back to the initiating node by a process similar to the one described for the route discovery using unicast.

- **Secure Efficient Ad hoc Distance Vector Routing (SEAD):** SEAD is a security extension applied to Destination-Sequenced Distance-Vector (DSDV) algorithm [154]. The SEAD routing protocol employs the use of hash chains to authenticate hop counts and sequence numbers of routing information broadcasted over the network. A hash chain is defined as the application of a hash function repeatedly on the same value.

SEAD uses two mechanisms to ensure routing security the first one is TESLA and requires clock synchronization between the nodes that participate in the ad hoc network in order to ensure broadcast authenticity.

The second one requires a shared secret key between each pair of nodes and uses Message Authentication Code MAC to authenticate routing messages.

- **Secure Ad hoc On-demand Distance Vector (SAODV):** is a security extension applied to the AODV protocol [155]. The proposed extensions utilize digital signatures and hash chains in order to secure route discovery, by applying digital signature on specific fields of the header of routing packets, the goal of this proposal is to ensure the authentication of the discovered routes.

- **The Secure Link State Routing Protocol (SLSP):** has been proposed in [156] to provide secure proactive routing for mobile ad hoc networks. It secures the discovery and the distribution of link state information using public key cryptography, to avoid the burden due to the deployment of a certificate authority, nodes broadcast their certificate during flooding routing information which guaranties in someway the authentication of routing messages and the effectiveness of the security mechanism.

In general, SLSP can be divided into three components, *public key distribution*, *neighbour discovery* and *link state updates*.

The public key distribution is done by the nodes themselves by broadcasting a self signed certificate to each neighbour.

After this step, each node is able to discover and authenticate its neighbours and therefore authenticate the link state update messages.

5. Public Key Infrastructure (PKI)

A PKI is a set of components that manage digital certificate as publishing, distribution, renewal and revocation in a given community or network.

A PKI is essentially composed of Certificate Authority (CA), Registration Authority (RA) and Certificate Revocation List (CRL). Depending on the application and the environment where a PKI is deployed all or only a sub set of these components are used [157].

The most important component of a PKI is the certificate authority since it is the trusted party which signs and certifies certificates. A certificate is an electronic document which binds peaces of information (name, serial numbers, address, IP and MAC address) signed by the certificate authority. The current version of certificate is X.509 V3, however according to the requirement of each system new fields can be added to allow a perfect identification within the community, for example in a wireless ad hoc network we can add IP or MAC address [158], to be used in order to directly localize the corresponding node without the need of any other servers or infrastructure.

PKI is recognized as the most effective tool providing authentication and non repudiation in conventional networks, however providing such infrastructure for MANETs is a challenging task due to the nature of these networks such as nodes mobility and devices constraints.

For securing routing protocols in MANETs, it seems that PKI is a very powerful tool to guaranty authentication and data integrity using digital signature, however the problematic is how to distribute certificates efficiently without affecting the performance of the network and how to keep them secure [159].

Therefore, in the following sections we are going to provide an implementation of PKI for ad hoc network, the delivered certificates are used to secure routing and data over the network, by using both public key infrastructure and symmetric cryptography in order to ensure the entire security services (confidentiality, integrity, authentication…etc).

Our proposed solution makes use of the underlying routing protocol considered to be reactive as a support for certificate publishing. Certificates are self issued, which means that each node individually creates and signs its certificate without needing any trusted authority as in conventional network. This certificate is used by the rest of nodes in the network to ensure data confidentiality with this node.

Thus, each node when creates its certificate tries to publish it in order to be known by the whole network, in conventional networks this is done in a special list published by the CA. However, in ad hoc network a such mechanism can not exist due to the network characteristics, so we use the route discovery and reply mechanisms to publish certificate and makes it known by all the network, since the route discovery is flooded over the entire network and including the certificate in this request guaranty for our certificate to be known by all nodes in the network with the minimum overhead. Because the overhead due to

flooding exist with or without the certificate publishing and therefore no affect on the network performance is added to publish certificate in this case.

6. Securing reactive routing protocols using PKI

6.1 Reactive routing protocols

As defined in previous chapters, reactive protocols create route only when needed using source routing already known in conventional networks (Figure IV.4). Thus, whenever a node wants to get a route to a given node, it floods the network with a route discovery request containing its IP address and the IP address of the destination node. The route request, travels over the whole network and reaches every node in the network until it arrives to its destination. A route reply is sent by the destination node containing the necessary path to the source node.

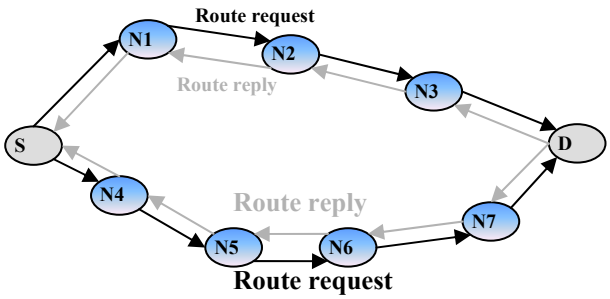


Figure IV.4 Route discovery and reply mechanism in reactive protocols

6.2 Securing reactive protocols

As devoted above, securing reactive protocols is treated in literature by proposing a set of strategies and mechanisms, however they are very complex and do not consider all the security services (integrity, confidentiality, non repudiation, authentication). Since, the majority of them give only solutions for securing the routing alone without any consideration to the confidentiality of the exchanged data after establishing a route.

Therefore, in our proposed security scheme we are going to propose a set of security mechanisms to implement a PKI for MANETs and overcome the shortcomings of the existing security frameworks. Our proposed PKI ensure both routing security and data confidentiality.

Our design manages the publishing of a self-issued certificates in a reactive fashion, without the need of any centralized or distributed authority with a great threshold of security

compared to the conventional PKI proposed in literature, the distributed certificate are used to secure end to end links between each pair of node as well as intrusion detection.

On the whole, securing reactive routing protocol in MANETs using our design is executed into two phases:

1- *The certificate publishing phase*, it uses as support the route discovery mechanism of reactive routing to publish nodes' certificate over the entire network, the use of the route discovery for certificate publishing does not overhead the network and guaranty the efficiency of certificate publishing, since the route discovery is flooded over the entire network and treated by every node in the network.

2- *The establishment of the symmetric key*, this is an optional phase used to secure end to end links over the network, in the way that each communicating nodes secure their end to end link using symmetric encryption which is periodically updated.

6.2.1 Certificate publishing

The most important problematic in PKI for ad hoc network is the confidentiality of the certificate authority and the publishing of nodes' certificate, due to device constraint since there is no device which can play the role of the CA and manage all the CA's services for the entire system lifetime. Thus, all the developed schemes of PKI make use of cooperation between nodes to guaranty a subset of PKI services.

The objective of certificate publishing is to declare that a given certificate is owned by a given person or node in a given community or a network. To do so, we propose to use the mechanism of route discovery as support for certificate publishing (Figure IV.5), in the way that when a node broadcasts a route discovery it adds its certificate in the header of the request to be transmitted for all nodes in the network, while the route request is flooded over the entire network, without needing any extra mechanisms to accomplish this task which may overhead and degrade the network performance.

To accomplish our design requirements, we suppose that each node:

1- Can independently generate a pair of public and private key and the capability to keep them secretly.

2- Can efficiently use both symmetric and asymmetric encryption, in order to accomplish traffic encryption and signature.

3- Has a self issued certificate, created and signed by the node itself without the need of any certificate authority (CA) as in conventional PKI.

4- Has a directory where it keeps the certificate of other nodes in the network to be used for verifying the integrity and the confidentiality over the network.

5- The original X.509 V3 certificate is modified by adding new field (the MAC and IP address) in order to allow a full identification of nodes over the network and allow intrusion detection based on IP and MAC addresses.

To accomplish the procedure of certificate publishing we have done some modifications on the original route discovery by adding new fields as shown in Figure 5.

1- The first field contains the certificate of the source node (S) (which launches first the route discovery); this certificate is intended to be transmitted to the entire network nodes using flooding defined by the underlying routing protocol.

2- The second field contains the certificate of intermediate nodes; this field is used by each intermediate node in which it transmits its certificate to its neighbours. Thus, each node when receiving a route discovery it drops the current certificate and replace it by its own certificate, then it re-floods it again. This mechanism allows us to publish the certificate in each node's neighbourhood.

Figure IV.5 Route discovery structure

After a moment of sending the route discovery request, we are sure that the source certificate has travelled the entire network and its is known by each node over the network, in the other hand each node in the network know its one hop certificate which ensure that each node can verifies the authenticity of its neighbourhood.

Whenever, the route request finally arrives to its destination, this last must response with a route reply with the necessary information for securing the established link between these two nodes. to do so we have also made modifications on the route reply packet by adding three fields, as shown in figure IV.6:

1- The first field contains the certificate of the destination node D to be published over the established link.

2- The second one will contain a symmetric key encrypted with the public key of the source node S retrieved from the certificate of S, which means that this key can only be read by the node S which has the corresponding private key.

3- The third one is a bit field indicates if the symmetric encryption will be used or not for securing the end to end link.

The original header of route reply	Destination node certificate	The symmetric key encrypted with the source node public key	Encryption (0/1)

Figure IV.6 Route reply structure

To explain best our design we are going to give an example to explain how our design works, we suppose that a node S wiles to find and secure a route to a destination D:

1- S constructs a route discovery request as described in Figure. 5, adds it certificate and broadcasts it.

2- Each intermediate node when receives any route discovery request:

a. It normally executes the underlying routing protocol and learns routing information from the route request.

b. It saves the certificate of the source node taken from the corresponding field "Source node certificate" in his certificate directory.

c. It also saves the certificate of one of its neighbours taken from the field of "Intermediate node certificate" if it exists.

d. It replaces the certificate in the "Intermediate node certificate" field by its certificate and rebroadcasts the route discovery.

e. If it receives multiple route discoveries with the same sequence number (the sequence number is used by reactive routing protocols to avoid routing loops) [8], it only extracts the neighbour's certificate from "Intermediate node certificate" field to be added to its certificate directory without re-broadcasting the request.

3- Whenever the request arrives to the destination D:

a. It extracts the certificates from the request as described above and adds them to its directory.

b. It checks the validity of the certificates contained in the route request, by comparing them with its certificate directory, in which it stores all the accumulated certificate during the system lifetime, otherwise if the certificate does not exist in its directory, it waits a delay *d* to receive more route requests in order to verify the validity of the certificate, if two certificates arrive from two different routes during this delay are different this means that there is a malicious node in one of the two routes, consequently, D waits for more routes and identifies the true certificate. After the achievement of the verification process, D constructs a route reply for each route discovery as described in figure IV.6 and sends them to S using unicast.

4- When receiving these replies the source node S retrieves and verifies the validity of the certificates contained in the route reply by searching them in its directory if they exist or waiting a delay *d* in order to receive more replies and compares certificates coming from

different routes, if the verification success S begins the data forwarding over the shortest path. In addition to the regular operation defined for reactive routing protocol, each packet is signed using the private key of the sender to guaranty integrity and authenticity. The signature is verified hop by hop until it arrives to its destination, in order to guaranty quick intrusion detection if any intermediate node alters any packet.

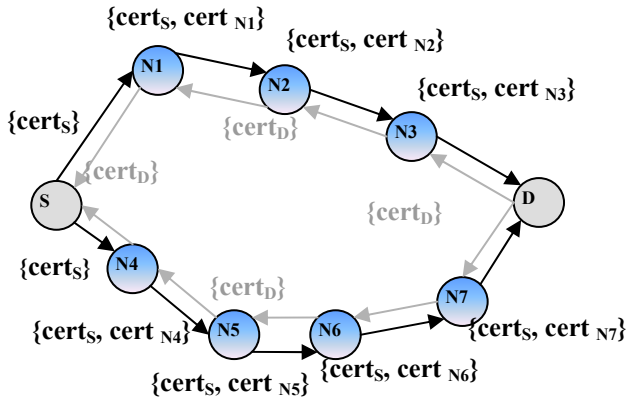


Figure IV.7 Route discovery and reply mechanism in PKI based reactive protocols

6.2.2 PKI-DSR

In order to test the performance and the feasibility of our design, we have implemented our scheme over DSR (Dynamic Source Routing). We have called the new developed protocol PKI-DSR, since it keeps the same specifications of DSR and implements our proposed scheme for PKI.

The major modifications made on DSR are done on the route discovery and reply mechanisms; hence we have extended the original structure of DSR's route discovery and reply requests, by adding new fields (described in Figure IV.5 and Figure IV.6). We have also modified the method of their treatment to accomplish the specifications of our design. Other mechanisms such as route maintenance and route cache are kept unchanged.

In the figure IV.8, we have investigated the same scenarios described in table IV.1, in order to test the capacity of PKI-DSR regarding certificate publishing, since the performance of any PKI scheme is tested according to its capacity of certificate publishing and the impact of the scheme on the network performance.

As we can observe after the achievement of the simulation each node has gathered at least 36 % of the whole certificates in the network which is very good regarding the number of connections (only 4 CBR connections) and implied nodes in these connections which is only

5 nodes. Since, the number of published certificates may increase whenever the number of connections and implied nodes increases, caused by the increasing number of route request launched for each connection.

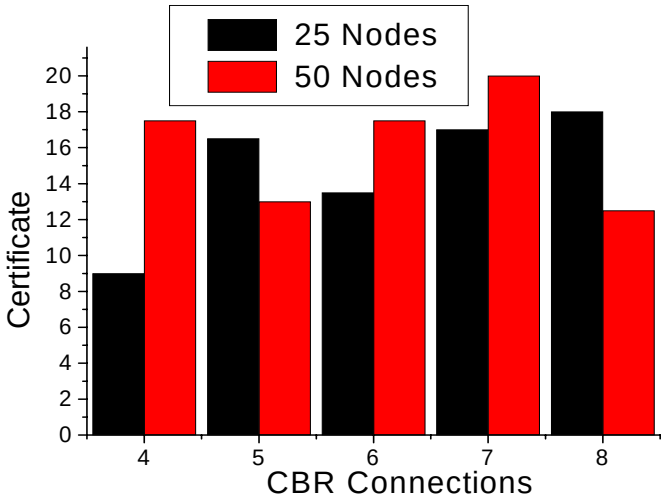


Figure IV.8 Average number of certificate

6.2.3 Intrusion detection

Intrusion detection in any security system must get more and more attention, since all the developed security schemes do not include any mechanism to detect intrusion and lets this functionality to an additional system modules or software. However, if this mechanism is included in the routing system the used security mechanism will be more powerful and efficient.

Thus, in our proposed schemes we have added some additional techniques to detect intruders. Our method for detecting intruders is essentially based on digital signature since each forwarded packet is signed by its sender to ensure both authentication and integrity; this signature is verified by each intermediate node which gives us the possibility of detecting intruders from the first attempt.

Three cases are distinguished where an attacker can be detected:

a) During the route discovery

In this case, an attacker tries to perform routing attacks as black hole attack in order to get access to the exchanged data. A way to do this is by modifying or changing the certificate contained in the header of the route discovery in order to modify the sequence of nodes contained in the path.

This attack can easily be detected by the source or the destination node, since this node checks the validity of any received certificates by looking for them in its directory or by waiting a delay to receive more route replies coming from different paths to verify the validity of certificate and detect any tentative of intrusion.

We have preferred to use multi-path for detecting black hole attacks rather than using other mechanisms such as hash chains because it is less resources consumption and it does not need any additional structures. In the other hands, after a given period each node gets sufficient certificates in its directory which allows them to verify the validity of routes.

b) During the data forwarding

To allow intrusion detection during data forwarding, we have modified the original structure of packets used by the DSR protocol in order to include a new field which contains the digital signature applied on the packet using the private key of the sender. Thus each intermediate node when receiving any packet can verify its integrity using the public key of the source node (gets it from the route discovery). If it detects that the packet is modified than an accusation request against the corresponding node is broadcasted over the entire network; whenever this accusation arrives to the source node it chooses an other route which does not contain this node or launches a new route discovery in order to establish a new route. Whenever the number of accusations against the same node reaches a given threshold from different nodes this node is completely excluded from the routing operations and any route containing this malicious node is dropped from the cache if the underlying protocol uses cache.

In order to investigate the possibility of detecting attackers using our design we have used the same scenario described in previous simulations to emulate intruder we have chosen randomly 10% of nodes to be attackers and perform data modification over the network, to emulate traffic we have used 4 CBR connections.

As we can observe in figure IV.9 all the attacks are automatically detected from the first attempt. The first attacker is detected within a delay of 10 seconds and the last one within a delay of 100 seconds. It seems that the time for detecting all attackers is approximately long; this is because some attackers have not yet participated in data forwarding until this time.

Although, attacker alters any packet it is automatically detected by its neighbours by verifying the digital signature accompanied to each packet.

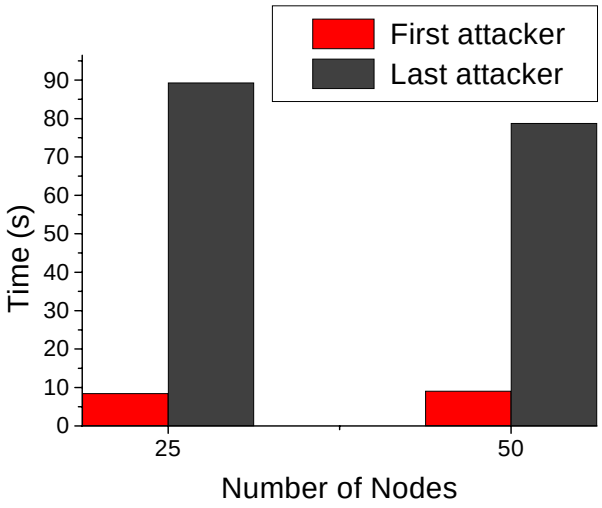


Figure IV.9 Malicious node detection delay

c) During all the system lifetime

After a portion of time and during all the system lifetime, each node will get a directory which contains a great amount of nodes' certificates collected using the mechanism of certificate publishing described above. This directory is used by each node to detect any malicious intention of its neighbours during the route discovery as well as during the data forwarding.

This mechanism will greatly avoid denial of service attacks trying to block the network services by injecting false certificates in order to perturb the regular functioning of our design.

Using certificate directory we can also prevent some attacks as black mail attack and any other impersonate attacks.

6.2.4 The performance of PKI-DSR

a) Network overhead

Any security mechanism may add a certain overhead to the network, and some of them may affect the performance of the network due to the number of unnecessary messages or request. However, our design relies on the underlying routing protocol and makes advantage of the existed mechanism to achieve the security services.

Therefore, in this section we test the performances of PKI-DSR compared to the original DSR. As we can observe in figures IV.10 and IV.11 there is no significant overhead of our design on the network performance, however in some period of the network lifetime there is insignificant overhead, this is due to the mechanism of intrusion detection (flooding of

accusations), and the waiting delay in order to receive more route requests and replies. However if there is no attackers in the network the performances of PKI-DSR are similar to DSR. This means that any overhead added by the applied security mechanism is due to the action of attackers.

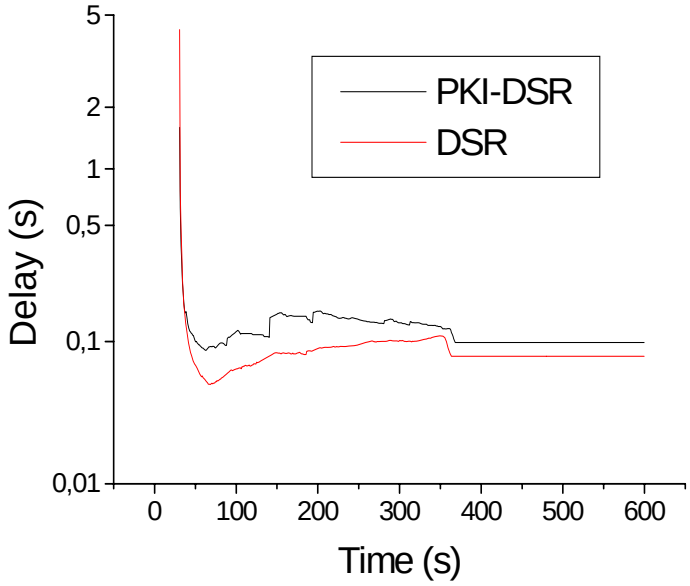


Figure IV.10 Comparison of DSR and PKI-DSR with 25 nodes.

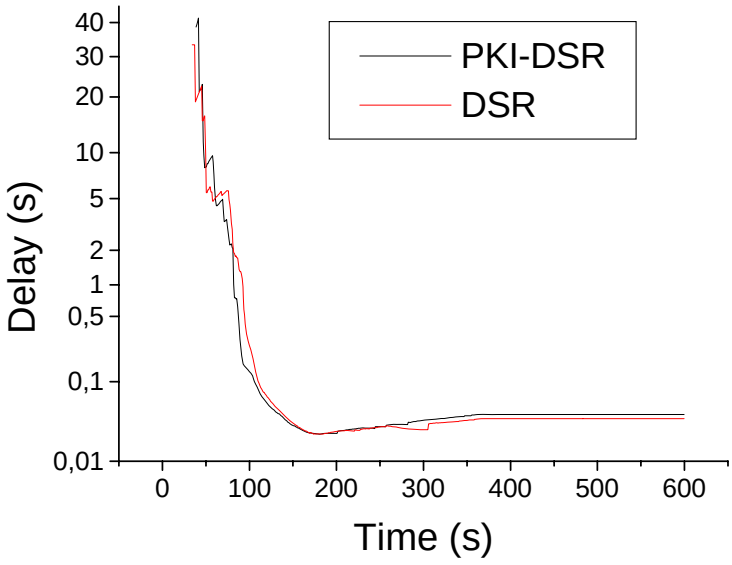


Figure IV.11 Comparison of DSR and PKI-DSR with 50 nodes

b) Scalability

This criterion deal with the network widening since in some security or routing protocols the complexity of network management increases with the network size, and some of them becomes inapplicable for certain sizes of the network. Thus, a security management protocol should have a better scaling property that can deal with a potential growth in the network size. It seems that our proposed scheme is scalable and deals efficiently with the network widening since it is based on the scalability of the underlying routing protocol which is supposed to be reactive; these kinds of protocols are scalable compared to other kind of protocols.

Our scheme is also useful for other kind of network since it is implemented on the IP layer which is common to all the existed networks as Bluetooth in opposite to link layer based security protocols which must be re-implemented for each kind of networks.

It does not need any centralized authority or off-line dealer to deliver or create certificate, since the certificates are self issued and self published.

The implementation over any reactive protocol is simple and does not need the creation of any new messages or to change the existed processes. Only some modifications on the structure of the existed request are done to include the structure of certificate. In the other hands, it does not add any overhead to the network which means that there is no effect on the network performance.

6.2.5 Symmetric key establishment

This phase is optional and it is intended to ensure the confidentiality of end to end links and prevent eavesdropping using symmetric encryption. We have used symmetric key encryption rather than asymmetric one because it is less resources and computational power consumption and can be executed quickly on big size of data.

Thus, after the establishment of the route between two nodes, they collaborate during the same phase to establish a secure channel over this route, by defining a symmetric key used for data encryption.

To accomplish the establishment of the symmetric key, we suppose that the route request has arrived to the destination node and there is no intrusion. Consequently the destination node D generates a random key and encrypts it using the public key of the source node, then it adds the encrypted key in the field reserved for this purpose Figure.6, sets to one the field reserved for the encryption Figure.6, and finally it sends the route reply. After the reception of this route reply by the source node it retrieves and decrypts the symmetric key using its private key in order to be used for data encryption.

We do not propose any cryptographic algorithm to be used, since any kind of devices and networks have its specificity. However we propose to periodically update the symmetric key to avoid any possible long term attack trying to analyse the exchanged traffic and therefore concluding the symmetric key.

The update of the symmetric key can be done by launching new route discovery mechanism as described above, since the destination node choose a random key for each new route discovery or simply launched by one of the communicating parties, which generates a new key and sends it encrypted by the public key of the other node.

The use of encryption establishes a secure tunnel between the sender and the receiver, which keeps the data out from reach of any malicious node (Figure IV.12).

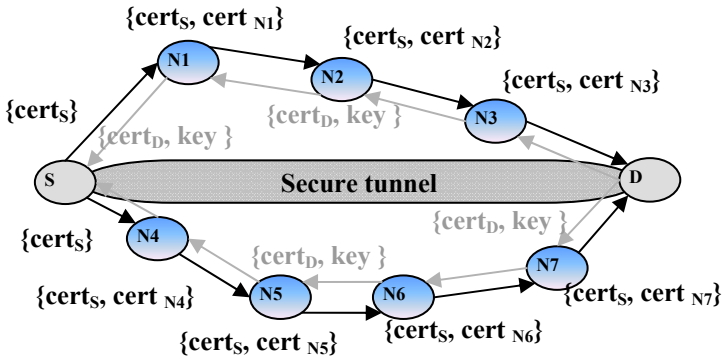


Figure IV.12 Secure tunnels in PKI-DSR

7. Security analysis

In the following paragraphs, we try to evaluate the robustness of our solution against some attacks:

- **Eavesdropping:** This passive attack can never be performed against our protocol, since the exchanged data over the network is encrypted using symmetric encryption which guaranties both efficiency and confidentiality. The encryption process is enforced by a periodic key update in order to resist against long term attacks, executed against some symmetric key encryption algorithms, by collecting a great amount of encrypted data, used after to derive the encrypting key.

- **Black hole attack:** In this attack, the malicious node tries to attract the traffic to itself; by pretending itself as the legitimate node. However, using the described mechanism of certificates publishing, each node can verify the authentication of routes and packets and detect any malicious intention of any intermediate node. Given that, both the destination and the source nodes verify the authentication of routes and certificates by comparing them with certificates contained in their certificate directory or using multi-path routing.

- **Data Modification and Insertion***:* these two attacks can not be performed against our scheme, while it uses digital signatures to provide data integrity and authentication as well as confidentiality by using symmetric encryption. Thus, only authenticated nodes which are the source and the destination node can read or modify data. We have also proved the possibility of detecting attackers using the mechanisms of digital signature by simulation.

- **Denial of service:** This attack tries to stop the service of the network by injecting false routing information. The risk of blocking the service of security in our scheme is minimized, by the use of digital signature and symmetric encryption, therefore the system automatically rejects any fabricated requests, and changes the path if any intermediate node detects that there is an attacker who tries to perform any malicious acts.

- **Avoiding other attacks,** After the bootstrapping each node may collect in its certificate directory an important amount of nodes' certificates, using the mechanism of certificate publishing described above. Accordingly, each node in the network uses this directory to verify the validity of routes and alerts and therefore avoid any other attacks as black mail attack, replay or insertion as well as impersonate attacks in which a set of attackers try to pretend themselves as legitimate nodes by colluding the legitimate ones.

8. Conclusion

In this chapter we have tried to treat the aspect of security of MANET's routing protocols, by proposing a mechanism to secure reactive routing protocols. Our proposed scheme is based on the use of the underlying requests such as route discovery and reply to publish certificate and secure end to end link without the need of any infrastructure or centralized authority.

To test the performance and the validity of our scheme we have applied its specifications on one of the most known reactive protocols which is DSR. The new protocol is called PKI-

DSR. Owing to simulation, we have proved the ability of our design to detect intruders, by the use of digital signature and hop by hop verification.

Simulations results have shown also that the execution of the operations defined in our scheme do not affect the performance of the network and it does not add a great overhead.

In the next chapter we are going to use the same idea of using PKI for security; in order to treat the aspect of security over wireless sensor networks, by proposing a lightweight implementation of PKI called μPKI.

Chapter 5

Lightweight PKI for WSN μPKI

Wireless Sensor Networks (WSN) grows in size and gain new applications in our lives ranging from military applications to civilian ones. However security in WSN was not carefully carried out, since only some symmetric encryption based protocols are proposed in literature, under the assumption that the nature of sensor nodes does not support public key encryption due to the limitation in battery and CPU power. However the new development of sensors technologies may allow more computational power and gives the possibility to use public key encryption in WSN if the used algorithm is energy efficient such as ECC. Therefore in this chapter we propose a lightweight implementation of Public Key Infrastructure (PKI). Our proposed protocol called μPKI uses public key encryption only for some specific tasks such as session key setup between the base station and sensors giving the network an acceptable threshold of confidentiality and authentication.

1. Introduction

Last dedicates have known the development of small, low cost, low power and multifunctional sensor nodes, having the possibility of sensing and collect application-specific data as temperature, pressure and movement to allow environment monitoring[160].

Such sensors networked using wireless medium are called wireless sensor network WSN, which is a collection of hundreds to thousands of sensor nodes connected to each other through short range wireless links, used as an infrastructure to forward the collected report to the centralized authority over a base station. Sensor nodes are self powered and equipped with low computational power CPU allowing the sensor to execute some specific treatment before sending a report to the centralized authority [161]. Wireless sensor networks have revolutionized the world of remote controlling due to the autonomy of sensors and their facility of deployment, ad hoc connectivity and cost-effectiveness.

The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance [162]. However, wireless sensor networks are now used in many civilian applications, including environment and habitat monitoring, healthcare applications, home automation, traffic control, environmental monitoring, or to detect and characterize Chemical, Biological, Radiological and Nuclear in some environments where the presence of human is not possible[163].

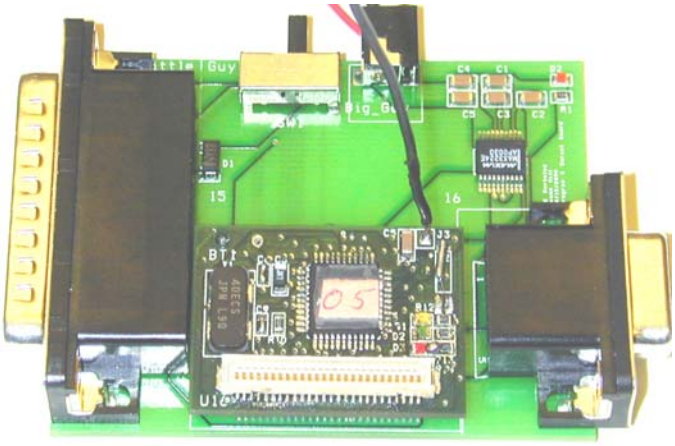


Figure V.1 The beginning of sensors

In general a sensor node includes a sensing module, a microprocessor to convert the sensor signals into a sensor reading understandable by a user and execute some treatments on the collected data before being sent or to execute network functionalities such as routing, security…etc, a wireless interface to exchange data with neighbouring sensors and the base station, a small memory to temporarily save data before being sent and a small battery to run the device [164].

Originally wireless sensors size was around 5 cm (Figure V.1), however the new developed sensors are very limited in size and typically they do not exceeds the 1 cm, which considerably limits the size of the battery or the total power available with each sensor node.

However, the recent technological development allowed to minimizing in sensor size to be smaller and computational powered with extra new capabilities of sensing. Figure V.2 shows the series of sensors developed by CITRIS (Center for Information Technology in the Interest of Society) investigators during three years 2001, 2002 and 2003 [165]. These wireless sensors can be used to sense magnetic or seismic attributes; or sense temperature or pressure in industrial sensing networks; or temperature and humidity in agricultural maintenance networks. Over a period of 2 years, the size of these sensors has decreased from a few cubic centimetres to a few cubic millimetres, and they can be powered using tiny solar cells or piezoelectric generators running on the minute vibrations of walls inside buildings or vehicles.

Figure VI.2 Progression of sensors developed by CITRIS investigators

2. Application of WSN

As presented above, sensors are various in kinds and sizes which gives them a large variety of applications, in the other hands the development in batteries technologies have given the possibility for a sensor node to ensure his needs in energy using small solar cells or piezoelectric generators giving them the possibility to be in service for long time without any intervention of humans. In the following points we try to give a limited list of applications where a sensor network can be deployed [166,167,168,169]:

- **Vehicles and cares**: used for sensing shocks in cares in order to launch air bags or other mechanism in the adequate time.

- **Nuclear reactors** : sensors are used in all the nuclear areas in order to remote monitor these areas because the intervention of human is impossible due to the radio activity of these areas which may cause lot of health problems.

- **Military:** the military field was the first interested of this technology, thus the number of application are numerous such as battlefield surveillance.

- **Seism and inundation*:*** sensor network are very helpful in catastrophes since there is no infrastructures to be used for rescue, thus the facility of deployment of WSN is the best solution to accelerate rescue interventions.

- **Intrusion detection:** Several kinds of sensor nodes are deployed in buildings at all potential entrances/exits of the building to monitor movement of personnel and any unusual or suspicious activity.

- **Traffic monitoring on Roadways:** Sensors use in this application is to supervise highways by authorities and enable fast notification of accidents or any congestion in traffic used for example by drivers in order to select an alternate route.

- **Habitat or Ecosystem Monitoring:** sensor networks are used for Studying behaviour of birds, plants and animals in their natural habitats.

3. Characteristics of WSN

As devoted above a wireless sensor network is a collection of small sensors wirelessly connected to each other generally administrated by centralized base station. Due to their architecture and their nature, wireless sensors networks could have the following characteristics [170, 171, 172, 173]:

- **Absence of infrastructure:** although in a mobile WSN there is no administrative authority attached to the network in order to maintain and organize the network, thus sensors must collaborate between themselves in order to accomplish the network configuration and organization based on multi hop links in order to connect to the base station without any infrastructure.

- **Mobile topology:** a wireless sensor can be attached to mobile objects such as in studying birds' behaviour and therefore the topology may change, consequently sensors must maintain the connectivity and the security of the network without the intervention of the administrator.

- **High number of sensors**: in general a WSN is composed of hundreds to thousands of sensors connected to each other via wireless links, thus new techniques must be elaborated in order to handle the complexity of handling the increasing number of sensors with a limited impact on the network performance.

- **Energy Constrained Devices:** Most of sensors are self powered using solar cells or piezoelectric generators. Thus, the routing and security operations that require complex mathematical calculations must be adapted to be less power consuming.

- **Limited Physical Security:** typically a WSN are installed in a hostile environment which exposes them to lot of risks of theft and compromising, and therefore the existed security mechanism must handle this criterion under the energy constraints.

- **Limited power computing:** by nature sensors are very small equipped with very small processors with limited memory and power computing.

- **Limited Bandwidth:** In WSN sensors have to rely on wireless links for communicating with each other. Usually the wireless links have less bandwidth than that of traditional wired link due to effects of fading, noise, multiple access and interference conditions.

4. Routing in WSN

As explained in previous chapters, routing in ad hoc networks is hardly carried out due to the nature of these networks such as topology changing and nodes constraints. In WSN this problematic is more challenging because sensors have only a limited amount of energy available to them, since they derive energy from a personal battery and not from a constant power supply. In the other hands they are equipped with small processors with limited power computing which makes the routing primitives more hardly carried out compared to other mobile networks. Thus, the protocols designed for these networks must strategically distribute the routing burden among sensors over the network in order to increase the average life of the overall system.

Thus, traditional routing protocols defined for conventional and wireless ad-hoc networks [174, 175] are not directly applied for wireless sensor networks due to the following reasons [176]:

- The number of sensors are very high, thus the routing protocols based on flooding are not well suitable for sensor network because this overhead the network and consume devices' energy.
- Sensor networks are data centric. Traditional networks usually request data from a specific node, but sensor networks request data based on certain attributes related to the environment.
- Adjacent nodes may have similar data. So, a mechanism must be defined to limits the number of request sent to the base station for the same reason.
- Table driven routing protocols must limit the size of their table by considering the limitation in memory of sensors.

- Sensors have very limited bandwidth and more devices' constraints compared to any other devices.
- Sensors are very often deployed in hostile environments, which mean that routing must natively implement security.
- Routing protocols must also equilibrate the use of network's nodes for routing, to replace them at the same time whenever their batteries expire.

Thus, sensor networks need protocols which are application specific, data-centric, capable of aggregating data and minimizing energy consumption. As a result, the existed routing protocols developed for both wireless and wired network are not adequate for wireless sensor networks, and new ones must be defined for WSN.

5. Sensor Network Architectures

In a wireless sensor network, sensors are very often dispersed in a large region usually without any centralized authority in order to manage the network architecture and establish connectivity from end sensors to the base station; therefore sensors must collaborate between themselves to establish this connectivity to the base station without the help of any authority.

Classically, two main architectures exists for ad hoc networks the hierarchical and the flat network architectures [177,178].

5.1 Hierarchical Network Architecture

In a hierarchical architecture, sensors are organized into clusters or regions. One node in the cluster is elected as cluster head intended to manage the cluster formation and maintenance, other sensors called cluster members are attached to one cluster.

Cluster heads manage the transmission between sensors and the base station which minimize considerably the network overhead since the aggregated data is sent to the cluster head which sent an abstract report to the base station which minimizes the traffic out clusters and therefore over the network.

Consequently, other mechanism and algorithms must be defined for clustered architecture

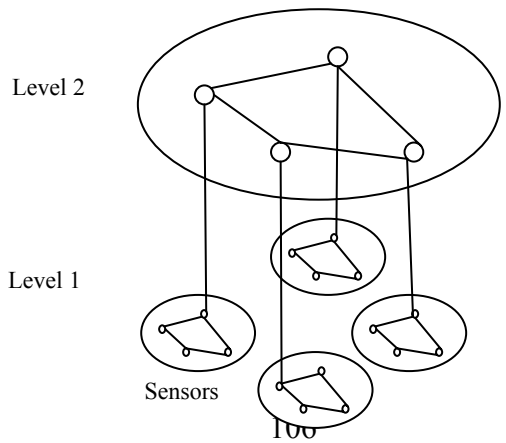


Figure V.3 Hierarchical Network

maintenance such as cluster formation and cluster heads election, in addition to new mechanisms for routing and security taking into consideration the clustered architecture for the network.

5.2 Flat Network Architecture

In flat network architecture, all nodes are equal and connections are setup between nodes and the base station, in the way that data is sent from sensors to the base station such as any other ad hoc network.

Sensors use traditional routing to establish end to end connection between the base station and end sensors.

Flat networks (figure V.4) are very suitable for stable sensor network where the collected reports are not numerous, which do not add lot of overhead to the network for their transmission to the base station.

However, routing in such architecture uses flooding which consumes lot of network resources and occasionally overhead the network.

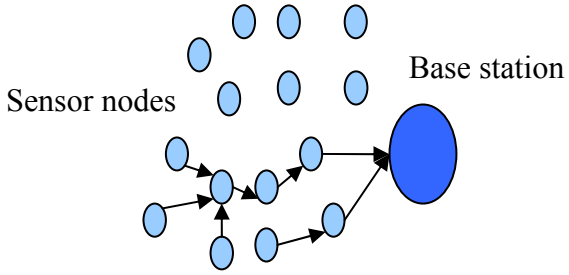


Figure V.4 Flat Network

6. Security in Wireless Sensor Networks

Security is a very important issue when designing or deploying any network or protocol. However the recently developed networks such as the wireless ones have not given the necessary attention to security when designing protocols by taking into account the specificity of these networks such as the used medium and the devices constraints. Thus, many security protocols were proposed trying to efficiently carry out the problem of security and the constraints of wireless networks. However, in sensor networks the problem of security is more challenging regarding the limitation of sensors and the area where the sensors are deployed such as battlefields [179].

The proposed schemes in literature are not secure since they use some simplified techniques to carry the limitations of sensors, given that the majority of these protocols makes use of symmetric encryption for ensuring all the security services instead of a combination of symmetric and asymmetric (public) encryption.

In order to manage security of sensor networks we are going to present in the remainder of this chapter a PKI based security scheme. By which we give a light weight implementation of PKI called micro public key infrastructure (μPKI) [180].

Our proposed infrastructure does not offer all the services of a conventional PKI; however it gives the necessary services of a conventional PKI in order to manage the distribution of session keys in a WSN, in the way that the public encryption is only used for specific services over the network to ensure authentication; however confidentiality and integrity are always achieved by symmetric encryption.

6.1 Public key cryptography for WSN

Public key cryptography was invented in seventies years, it uses two keys for both encryption and decryption. In the way that any message encrypted with one of the keys can only be decrypted with the other key. One of the keys is called private key which is kept secret by its holder, and the second one is publicly known by each entity in a given community, using these two keys, the public key cryptography can ensure both confidentiality, integrity and authentication.

However, PKI is omitted from the use in WSN, because of its great consumption of energy and bandwidth which are very crucial in sensor networks, and all the most known solutions given in literature use symmetric encryption which is more power saving.

However, last years have known the development of new cryptographic algorithms more energy efficient and giving the same threshold of security as the conventional algorithms such as RSA. Elliptic Curve Cryptography (ECC) is one of these new algorithms and it is the most promising one regarding the energy and time consumption, which makes it very attractive for data encryption in WSN. ECC offers the equivalent security with much smaller key sizes which saves memory, computational and energy power for constrained wireless devices [181].

In the other hands, the new developed sensors will be more powerful concerning the CPU and memory capacities, making public key encryption possible for small sensors in WSN.

7. State of the art of security schemes for WSN

In literature exist several key management schemes trying to solve the problem of security in WSN by taking into consideration the limitations of sensors (bandwidth and energy), the

majority of them are based on symmetric key encryption and some few ones are based on asymmetric encryption:

7.1 Symmetric encryption based schemes

- **Shared key:** this solution is the simplest way for securing WSN, it uses a single shared key to encrypt traffic over the network, and this key may be periodically updated to ensure more security against eavesdropping. In this scheme an off-line dealer load the key in sensors before deployment, then each sensor uses this key to decrypt traffic and join the network.
  As any other scheme based on single key, this scheme is vulnerable against capture attack which is more possible in sensor network, since the capture of only one sensor can compromise the shared key and then the whole network [182].

- **Secure Pebblenets**: This solution proposed by Basagni [183] is an extended version of the shared key solution. Secure Pebblenets provides group authentication, and message integrity, by using a set of symmetric keys for each security purpose. It divides the whole network into clusters and manages the security based on clustering architecture, in the way that each cluster is managed alone using this set of keys in the same way inter-cluster communication is managed using a sub-set of keys to ensure confidentiality and integrity over the whole networks.

- **Pre-distributed keys:** these solutions assume the existence of an off-line dealer which distributes a set of symmetric keys to sensors before their deployment, for example the authors in [184] proposed a random key pre-distribution scheme for WSN in which sensor obtains a subset of symmetric keys from a large key pool. After deployment, each sensor tries to find a shared key with each of its neighbors to secure the links with them. Other works have been proposed under the same idea in [185, 186, 187] trying to solve the problem of scalability and the manner of obtaining the session key between sensors and the base station.

- **Tinysec***:* is a link layer security protocol based on symmetric key encryption, TinySec [188] supports two different security options: authenticated encryption (TinySec-AE) and authentication only (TinySec-Auth). The use of MAC layer security instead of end to end security may avoid denial of service attacks, however this scheme still vulnerable to lot of attacks such as capture attacks. In other hands, this protocol can be used by any other key management scheme as an underlying tool for encryption.

- **SPINS**: Perrig and al. proposed SPINS, a suite of security protocols optimized for sensor networks [189]. SPINS has two secure blocks, namely Secure Network Encryption

Protocol (SNEP) and μTESLA, which can be run over the TinyOS operating system. SNEP is used to provide confidentiality through encryption and authentication; while μTESLA is used to provide authentication for broadcasted data.

- **Cluster based protocols:** these protocols are based on clustering, which mean that the whole network is divided into clusters [190, 191], then a set of symmetric keys are used to ensure intra and inter cluster communication as well as integrity, confidentiality and authentication over each cluster and therefore over the whole network. It seems, that the clustering architecture simplifies the management of the networks, however its management and maintenance is more challenging in WSNs regarding their constraints.

7.2 Public key based schemes

- **Simplified SSL handshake***:* In [192], the authors give the energy cost analysis of a simplified version SSL applied to WSN, which reduces the amount of exchanged data between any pair of nodes to save energy and bandwidth.
  The simplified handshake is used to setup a secure key between sensors or sensors and the base station in the network as the original SSL.
  As a brief analysis of this scheme, it seems that it is not energy saving since a handshake between each pair of sensors is too expensive concerning the amount of exchanged data, in addition a secure tunnel between each pair of nodes is not needed since only a limited links participate in communication and the rest of links are not used.
  In the other hands, this scheme can not be applied to mobile sensor networks, since the mobility of sensors needs new handshakes at each time a sensor changes its position and therefore its neighbour sensors, which consumes lot of energy.

- **TinyPK***:* The TinyPK system described in [193] is designed specifically to allow authentication and key agreement between resource constrained sensors. The protocol is designed to be used in conjunction with other symmetric encryption based protocols such as TinySec, in order to deliver secret key to that underlying protocol. To do this, they implement the Diffie-Hellman key exchange algorithm.
  As said above using a session key between each pair of sensors is not efficient and it consumes lot of energy and network bandwidth for the setup of the session key beyond of the energy consumed by the encryption algorithms. Using this scheme as an end-to-end security mechanism may be energy efficient however Diffie-Hellman key agreement is very sensitive to man in the middle attacks which can be easily performed in such situation.

- **Simplified Kerberos protocol***:* The authors in [194] proposed an adapted version of Kerberos [195] for WSN in order to setup a session key between each communicating pair of sensors by contacting a trusted third party which may be the base station or a cluster

head in a hierarchical network. They assume that a long term key is shared between each node and the trusted authority which is responsible of the generation of the secret key for each pair of sensors.

This scheme is very vulnerable against capture attacks to which sensor are very often exposed, and as the previous work the handshaking is not energy saving and it may consume lot of network resources if the trusted third party is far from the pair of nodes.

8. Encryption algorithms

8.1 Elliptic Curve Cryptography

The ECC algorithm [196] can be classified as the one of the most efficient asymmetric algorithms regarding its energy cost as well as its encryption speed, making it the base of future key management and security protocols for WSN and any other wireless ad hoc network.

In table V.1 we give the energy cost of the RSA and ECC [197] algorithms for signature and verification applied to Berkeley/Crossbow motes platform, specifically on the Mica2dots [198], as we can observe the ECC is always more efficient compared to RSA for the two used key length, given that the length of keys used by ECC are much smaller than RSA's keys which may save lot of memory space for sensors. Also, ECC's encrypted blocks are more small than the RSA's ones which saves network bandwidth during transmission.

Algorithm	Sign
RSA-1024	304
ECC-160	22,82
RSA-2048	2302,7
ECC-224	61,54

Table V.1 Energy cost of digital signature (mJ)

8.2 Symmetric cryptography

Is a cryptographic method employing a single key for both encryption and decryption [88]. The use of a single key makes the decryption process a simple reversal of the encryption process. In literature, there exist lot of symmetric algorithms such as RC4, DES and AES. In our protocol we do not propose any algorithm to be used nor the method to implement it (hard or soft), which are let for the implementation and the specificity of the environment.

8.3 Message authentication codes (MACs)

Is the common solution to ensure integrity and authentication of messages in conventional networks [88]. A MAC can be viewed as hash function applied on data packets, resulting on a digest which is encrypted by a session key shared between two entities, the encrypted digest is called MAC and it is sent with the original packet in the same message. A receiver sharing the same session key can verifies the integrity of the message by computing the MAC value and compares it with the received one if the verification fails; this means that an adversary has altered the packet during its transmission over the network. The MAC is more suitable for constrained devices rather than digital signature since it uses symmetric encryption which is more power and energy saving compared to the asymmetric encryption, in addition it does not need any additive components such as the certificate authority.

9. µPKI for WSN

In this section we are going to give an overview of µPKI (Micro Public Key Infrastructure). µPKI is a lightweight implementation of PKI for WSN since it only implements a subset of a conventional PKI services.

In µPKI, only the base station needs to be authenticated using a pair of keys. The public one is used to authenticate the base station by the sensors in the network, while the private key is used by the base station to decrypt data sent by sensors which ensure its confidentiality.

9.1 Network architecture

For the remainder of this paper and for the execution of µPKI we consider a flat sensor network composed of a set of sensor nodes wirelessly connected to each other, these sensors are used to forward the collected reports to a centralized authority or the base station. For the implementation of µPKI, we assume that:

- The base station have more computational and energy power compared to sensors.
- The base station has a pair of keys (private and public key).
- Each sensor is capable to use symmetric and asymmetric encryption, by implementing (hard or soft) each of these operations.
- Each sensor has the capacity to save at least the public key of the base station and a session key used for data encryption.
- Each sensor node gets the public key of the base station before deployment from an off-line dealer.

9.2 µPKI System bootstrapping

Before the deployment of the WSN, we suppose that an off-line dealer distributes the public key of the base station to each sensor in the network, which means that only legitimate

sensors have the possibility to authenticate the base station trough its public key, this public key is used after in the handshake between the base station and sensors, since each link between any sensor node and the base station is secured using a symmetric session key which is periodically updated.

Securing end to end links is launched by sensors in order to send collected data to the base station using an improved version of the existed handshake developed for conventional networking taking into account the specifications of sensor networks.

Two handshakes exist in µPKI, the first one between the base station and sensors intended to secure end to end transmission between them. However, the second one is intended to secure sensor to sensor communication, this handshake is established trough the cooperation of the base station which plays the role of authenticator between sensors during this phase, this handshake is optional and it is developed for some kinds of sensor networks needing intra-sensor communication.

Typically, the most important handshake is between the base station and sensors.

9.3 Base station to Sensor nodes Handshake

This handshake is very simple and efficient, aims to setup a session key between the base station and any sensor over the network used for end to end traffic encryption between these two entities. The session key is used to establish a secure tunnel between each sensor and the base station in order to protect the network traffic from exterior intruder and interior malicious sensors implemented maliciously by an exterior attacker for eavesdropping.

We suppose that a sensor node needs to setup a secured link with the base station using µPKI in order to transmit some data to the base station, thus both the base station and the sensor node collaborate to execute the following steps:

1. Generation of the session key**,** As we have said end to end links between the base station and sensors are secured using symmetric encryption, therefore any sensor willing to secure its transmission with the base station, generates a random key, encrypts it with the public key of the base station, already distributed to sensors by an off-line dealer, the use of public key encryption for this purpose protect the session key from malicious sensors and ensure the authenticity of the base station. It embeds the encrypted key in a regular message (Figure V.5) and sends it to the base station using the underlying routing protocol.

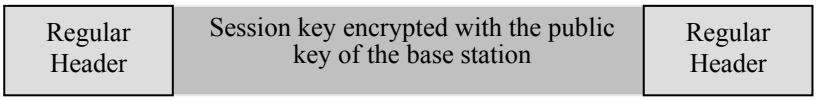


Figure V.5 structure of session key's message

- When the message containing the session key is received by the base station, it decrypts this message using its private key and saves the session key in a global table. The global table is a table where the base station saves the session keys shared with each sensor over the network. This table is maintained by the base station and contains the pairs of sensors' identifier and the corresponding session key.

- The base station encrypts an OK message using the established session key and sends it to the corresponding node; this Ok message is a challenging message ensuring the authenticity of the base station, since if this message is a successfully decrypted by the sensor using the key generated in step 1 means that the session key setup is successful (Figure V.6), otherwise an attack is assumed and therefore a new attempt is launched, by the sensor node to establish a new session key.

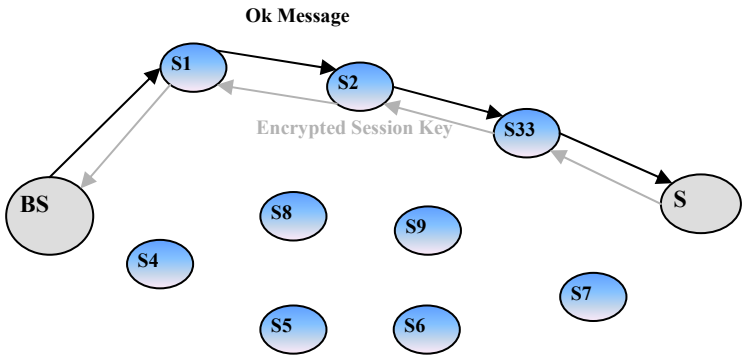


Figure V.6 Session key establishment

The purpose of any handshake is the setup of a secure tunnel between two or more entities in a given community. As we can observe µPKI handshake ensures a great level of security since the session key sent to the base station over multi hops link can not be decrypted by any malicious sensors, because it is encrypted by the public key of the base station which means that only the base station can retrieves this key using the corresponding private key, as well as the Ok message which can only be decrypted using the true session key which is only known by the base station and the corresponding sensor. All these mechanisms guaranty an acceptable level of security due to the use of both symmetric and asymmetric encryption which ensures both authentication and confidentiality.

After the establishment of this session key the sensor and the base station begin to use it for data encryption which creates a secure tunnel between each sensor and the base station and therefore all the exchanged traffic over the network is kept out of range of any third party.

9.4 Sensor to Sensor handshake

This handshake is optional and it is intended to establish a secure tunnel between sensors in the network for some special sensor networks need intra-sensor communication (Figure V.7).

Thus, after the establishment of the session key between each sensor and the base station, this handshake is simple and more secure since it is executed over the existed secure tunnels established during the fist handshake. To execute this handshake, both the base station and the corresponding sensors execute the following steps:

1- One of the two sensors sends a request to the base station in order to establish a secure tunnel with the other sensor. This request contains the identifier of the corresponding node.

2- When receiving this request the base station generates a random key for this purpose, it encrypts a copy for each sensor using the corresponding session key established during the first handshake, and sends it embedded in a message using the underlying routing protocol to each sensor.

3- When receiving the new key by sensors they begin to use it to secure data transmission between themselves.

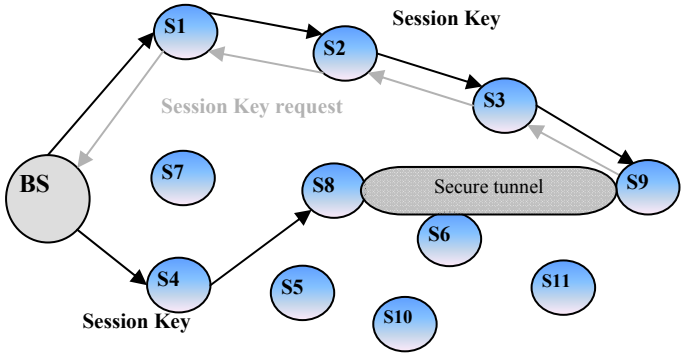


Figure V.7 Sensor to sensor handshake.

9.5 µPKI functioning

After the achievement of the handshakes, each two entities have a unique session key used to guaranty the confidentiality of the exchanged traffic using symmetric encryption.

In order to guaranty the integrity and the authenticity of the exchanged data between each communicating parties, we propose to apply on each sent packet a MAC function using the same session key. Hence, each communicating party verify the integrity and the authenticity of each packet by verifying the joined MAC, if the verification fails this means that an

attacker has altered this packet, therefore a mechanism is launched as multi-path routing to avoid this attacker. Otherwise the base station launches any mechanism to detect and exclude this sensor from the network, if it exists.

In order to use the µPKI for securing sensor networks we must modify the original packet in order to include the MAC for data integrity. As we can observe in figure V.8, the original structure of the packet is kept unchangeable; we only join to the original packet the MAC applied on the data packet, a MAC is essentially used to guaranty the integrity of control and routing messages exchanged between sensors and the base station.

Figure V.8 Data packet structure in µPKI

9.6 µPKI Key Update

A key update tries to prevent long term attack aiming to extract the encrypting keys by analyzing the encrypted traffic over the network for long time, in a WSN an automatic key update must be defined, since a network can be deployed for many days or months. Therefore, in µPKI we propose to use a periodic key update for each established session key, the period of the key update is defined by the administrator of the network according to the complexity of the encrypting algorithm and the length of the key.

µPKI's key update is very simple and does not need any additional operations, after the end of the period defined for the key update the corresponding sensor launches a new sensor to base station handshake, in order to generate new session key, since a random key is generated for each new handshake.

9.7 Joining the Network

In general a sensor network is deployed to serve for a long period however in some situations the administrator of the network needs to replace a sensor or add new sensors to the network for any reason. Therefore, if a new sensor is added to the network and wants to join the base station, the administrator of this network must only load the public key of the base station into this sensor, after getting the public key of the base station the new sensor can automatically launch a handshake and join the network if there is any report to send.

10. Security analysis

- **Scalability*:*** this propriety deals with the network widening, it is possible with µPKI, since µPKI manages the increasing number of sensor nodes by new handshakes and a new entry is created in the global table of the base station to manage this connection. In the way that each new coming sensor launches a new handshake with the base station in order to establish a secure tunnel between them and wait for an eventual data to be sent to the base station.

- **Confidentiality*:*** this aspect is ensured by the use of symmetric encryption to encrypt the exchanged traffic between the base station and sensors, since no one other then the corresponding sensor and the base station can read the exchanged data. For more confidentiality we have enforced this mechanism using periodic key update to prevent long term attacks.

- **Authentication*:*** the most important aspect in wireless sensor network is to ensure the authenticity of the base station because all the collected data is sent to it, in the other hand sensors can not implement additional mechanisms to detect malicious base stations due to their limited resources. Therefore, in µPKI we have tried to ensure authenticity of the base station using the public cryptography at the level of the base station, the authority which needs to be authenticated by sensors, using a public key pre-installed in each deployed sensor.

- **Integrity*:*** the integrity in µPKI is ensured using MAC (Message authentication codes) computed and joined to each sent packet between the base station and any sensor over the network as well as between sensors if there is any communication, in the other hand the MAC joined to each packet can also secure the underlying routing protocol.

- **Protection of the handshake:** a handshake tries to establish a session key to encrypt communication between two entities over a network. The most dangerous attack which can be performed against a handshake is man in the middle attack, in which a malicious node intercept the messages exchanged between the communicating entities during the handshake in order to get the value of the session key. Otherwise, it changes the true value with a falsified one and gets access to the exchanged data. In µPKI, man in the middle attack can not be executed since the session key is encrypted with the public key of the base station which means that only the base station can read it using the private key, and any other attempt to change the true value with a wrong one is detected using the challenge message sent by the base station to the sensor.
  For the second handshake between two sensors, it seems that it is more secure because it is controlled by the base station over secured links established during the first phase.

- **Physical attacks:** in a physical attack an attacker get access to legitimate sensors in order to recover the used encrypting keys. This kind of attacks is very frequent in sensor networks due to the environment of deployment; the solution of such attacks is to limit their effects. In µPKI, the theft does not affect the network because only one link is compromised and the other links and sensors still working normally. To overcome this kind of attack an additional mechanism in the base station can detect this attack by comparing reports coming from adjacent nodes.

11. Energy cost analysis of µPKI

The energy cost of any key management scheme is determined by the energy required for the execution of cryptographic primitives and the energy needed for transmitting the encrypted data.

According to [197], the transmission of a single byte of data requires 59,2µJ and 28,6µJ for reception; this energy is consumed by both the processor for executing network primitives and the antenna for sending or receiving any byte.

As described above, two kinds of messages exist in µPKI for both Base station to Sensor or Sensor to Sensor handshake, these messages are needed to send the session key by the sensor to the base station, the size of each message is between 64 to 256 bits (according to session key length), added to 256 bits which is the size of the underlying protocols data checksum, node's IDs and protocol headers.

Thus, the maximum size of each µPKI packet is 512 bits; the energy needed for transmitting such packet is 3,78mJ and 1,83mJ for receiving it.

As supposed above the base station is considered having unlimited resources compared to sensors, thus the energy cost of executing the handshake's primitives is not considered. Consequently, only the energy consumed by sensors is computed in the following sections.

11.1 Sensor to base station handshake

As described in section 5 for Base station to Sensor handshake a sensor needs to send one message to the base station containing the session key which consume 3,78 mJ in addition to the energy needed for encrypting this message using the public key of the base station which is 22,82 mJ according to [197]. Therefore, the energy needed for launching the handshake by each sensor is 26,6 mJ.

After receiving this message by the base station, it decrypts it, recover the symmetric key sent by the sensor and generate a challenge message encrypted with the session key and sent to the corresponding sensor. Therefore, the sensor needs to receive this message using its

antenna this message which consumes 1,83 mJ, as well as the energy needed to decrypt this message which is 0,039 mJ according to [197] if the used algorithm is AES and using 128 bits key length.

Therefore the total energy cost of sensor to base station handshake is 28,46 mJ.

11.2 Sensor to base station handshake

The Sensor to Sensor handshake is less energy consuming, since only two messages need to be exchanged with the base station

The first one for launching the handshake sent by the sensor to the base station as a request to the base station handshake which consumes 0,039 mJ.

The second message is sent by the base station to the corresponding sensors encrypted with the session key of each sensor, therefore each sensor needs to receive this message and decrypt it which consumes 3,66 mJ. Thus, the total energy cost for sensor to sensor handshake is 3,70 mJ.

Compared to the energy cost of the simplified Kerberos and SSL presented in section 3, which are respectively between 39,6 mJ and 47,6 mJ for simplified Kerberos and 93,9 mJ for simplified SSL[192] Table V.2**,** it seems that µPKI is more energy saving, which makes it applicable for WSN.

In addition to this it also guaranties a great threshold of security by using periodic key update and public key cryptography.

Operations		Energy(mJ)
Base station to Sensor handshake	Encrypt session key	22,82
	Send session key	3,78
	Receive session key	1,83
	Decrypt Ok message	0,039
Sensor to Sensor handshake		3,70
Total energy cost		32,16

Table V.2 Energy cost of µPKI Kerberos and SSL

12. Conclusion

In this chapter we have presented a light weight Public Key Infrastructure for wireless sensor network called µPKI. µPKI tries to solve the problem of security in WSN by the use of public key cryptography as a tool for ensuring the authenticity of the base station.

µPKI is composed of two phases, the first one is the µPKI sensor to base station handshake in which the base station and a given sensor node setup a session key to secure end to end link

between them, this handshake is protected and authenticated using the public key of the base station.

The second phase is the use of this session key for data encryption to ensure confidentiality and ensuring the integrity of the exchanged data using the MAC joined to each packet.

We have also proposed sensor to sensor handshakes in order to establish secure tunnels between each two sensors; this handshake is managed and supervised by the base station.

For more security a periodic key update is defined for the session key. Compared to other PKI, µPKI is energy efficient and gives a considerable threshold of security.

In the next chapter we are going to study WSN from another point of view which is energy consumption by studding the most know protocols developed for this purpose and studding the possibility and the effect of using energy control in WSNs and MANETs to save the battery power of the network nodes.

Chapter 6

Power control issues in sensor and ad hoc networks

Energy constraint in mobile ad hoc network is one of the most important issues that must be carried out by the creation of new energy aware hardware (battery and network cards), as well as the adaptation of the existed protocols (MAC, routing) to deal with the constraints of energy in mobile ad hoc networks. Thus in this chapter we are going to treat the aspect of energy saving on the MAC layer, by presenting a mechanism of power control based on the number of neighbours in a given neighbourhood, by which we give an improvement to the 802.11 MAC layer in which we include the aspect of transmission power regulation according to the status of the neighbourhood.

1. PROBLEM OF ENERGY IN AD HOC AND SENSOR NETWORKS

As presented in previous chapters, mobile ad hoc network are collection of mobile devices or sensors that communicate with each other through wireless links. A large variety of ad hoc network exist ranging from local area networks to sensor network, however, almost the network's devices are self powered on exhaustive batteries, or on special generator of power based on vibration or sun light.

In the other hands the technological development in the domain of batteries and their capacity can not go so far in the nearer future since all the existed mechanisms do not guaranty more than some few hours of the battery life time in the absence of any connection to a network such as the wireless ones. Thus, whenever a device is connected to a wireless network the energy consumption is more crucial, due to the network adapters. Typically, the majority of energy consumption in ad hoc networks is due to the network adapter (antennas), since there is a fixed threshold of energy consumed for reception and transmission of each packet. This means that the energy consumption is proportional to the number of sent packet as well as the number of received packets [199].

Therefore, new mechanisms must be defined for ad hoc networks to save devices' battery power beyond of the hardware mechanisms. These mechanisms must be additional improvements to the existed routing or MAC protocols to be energy aware, by limiting the number of operations executed by each protocol as well as the number of transmitted control messages such as the routing information diffused by each node in the network [200].

Different methods to save energy in ad hoc and sensor networks exist; some of them are defined for routing in order to limit the number of operations executed by each node, or by limiting the number of control messages diffused periodically by each node, or by including the aspect of energy in the process of route selection.

The second mechanism to save energy is the power control defined on the MAC and the physical layers, which varies the transmission power to only the needed threshold to reach the desired destination [201].

In the rest of this chapter we are going to present an improvement to the existed 802.11 MAC layer in order to include the aspect of energy in its design. Our proposed scheme of energy conservation is a power control mechanism which varies the transmission power according to the density of the neighbourhood.

2. STATE OF THE ART OF PROPOSED SOLUTION FOR ENERGY SAVING

As said above the energy conservation aspect is a very important issue in ad hoc network due to the nature of the network's devices. Therefore, this aspect is treated in literature independently at each layer:

- **Physical layer:** on the physical layer deferent technology and kinds of batteries have been developed specially to carry out the energy consumption due to the network adapter in ad hoc networks in order to extend the battery lifetime, as well as the definition of some methods to independently generate the necessary energy by each device such as in sensor networks using small solar cells or piezoelectric generators in order to generate energy and extend the network lifetime to more than two or three months.
- **Medium access control MAC:** the treatment of energy on the MAC layer is done using two methods [202]. The first one is by organizing the access to the medium by a coordinator such as in 802.15, this organization is called slotted method in which the coordinator affect to each node in a given subnet or neighbourhood a slot of time in which it can send and receive data which improves too much the energy consumption of the network's devices. The second method to save devices' battery power is using a mechanism of transmission range control in which the transmission range is changed according to the distance separating each communicating devices, by fixing the transmission range to only the necessary threshold needed to reach the destination node.
- **Routing:** saving the energy in the network layer [203] is usually done by including the aspect of energy in route selection. In the way that the metric used for route selection is improved by including the aspect of intermediate nodes status concerning the battery power. This is done in different manners the simplest one is by including in the routing metric the level of battery of each intermediate node or the sate of each pair of nodes such as in weight based routing protocol defined in chapter two. Other method are also defined to save energy for proactive routing, in which nodes minimizes the periodic defusing of network state to only a limited neighbourhood such as in FSR (Fisheye State Routing protocol).

3. DESIGN ISSUES FOR WIRELESS MAC LAYER

In this section we are going to present some of the aspect that must be taken into consideration when designing any MAC layer protocol, the current MAC standards have taken some of these aspects and the rest of these aspects is not treated efficiently by the extension given in literature such as energy and QoS [204,205]:

- **Hidden terminal problem:** the hidden terminal problem is one of the problems that occur only for the radio transmission, since the transmission range of each node does not reach the

entire neighbourhood at the same time. This phenomenon occurs whenever two nodes in the two extremities of a given neighbourhood have wait until the medium becomes free such as in figure VI.1 and begin their transmission at the same time to the same node or to other nodes which are at the same neighbourhood of the two transmitters. Thus, the radio waves arrive to their destination at the same time which causes collision; the situation may continue infinitely until one of the two nodes stop its attempts of transmission, or by using some mechanism of medium reservation.

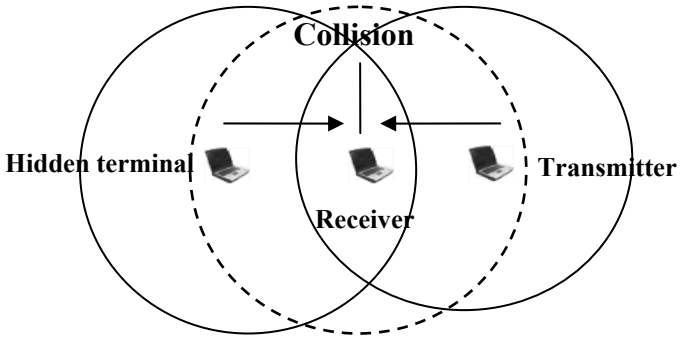


Figure VI.1 Hidden terminal problem

- **Exposed terminal problem:** this problem (Figure VI.2) occurs usually for dense network where a great number of nodes are in a limited area, regarding that the medium is shared this means that only one node can transmit at the same time and the rest of node stay waiting for medium liberation which can be too long. Thus we call the nodes in the position of listening exposed terminal, this position consume lot of battery power due to the energy consumed for the reception of great quantity of data which is not necessary.

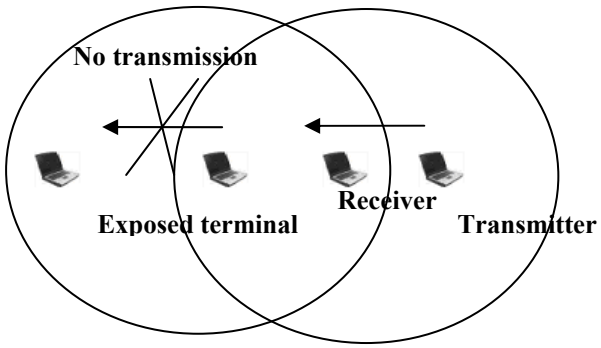


Figure VI.2. Exposed terminal problem

- **Mobility of nodes:** as devoted above devices in an ad hoc network are mobile and change their position unpredictably (Figure VI.3), which causes lot of problems at the physical and MAC layer such a slink broken, therefore any medium access protocol must take into

consideration the mobility aspect by defining some mechanism to predict the movement of the destination and modify the transmission range according to the direction of the corresponding node.

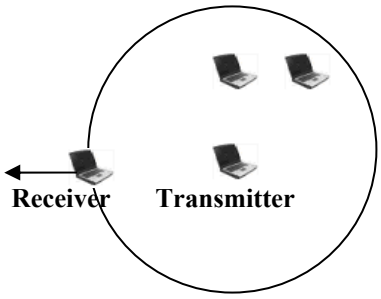


Figure VI.3 The problem of mobility

- **Not energy aware:** as said above energy is the hardest constraint for ad hoc network; however the existed routing or MAC standards have not included the aspect of energy in their design by limiting the number of operations or control messages. In addition some of the characteristics of the wireless medium such interference and fading causes lot of bit errors and consume the greatest amount of energy to their treatment, other problems such as exposed terminal wastes the energy for receiving unnecessary packets as well as hidden terminals which causes collisions and consumes devices' battery power .

4. THE IEEE 802.11 MAC LAYER

The 802.11 standard specifies a common medium access control (MAC) Layer, used by wireless devices in the majority of existed wireless networks and uses as Physical (PHY) Layer, 802.11b or 802.11a, to perform the tasks of carrier sensing, transmission, and receiving of 802.11 frames.

Typically, the MAC layer manages and organize the access to a shared medium, the 802.11 MAC layer is derived from the conventional 802.x series and uses as underlying mechanism the CSMA/CA (carrier sense multiple access with collision avoidance) which consists to avoid collision, rather than detecting it as the one defined for the previous 802.x MAC layers defined for wired network which is CSMA/CD (carrier sense multiple access with collision detection).

Each node in a 802.11 network is identified by its MAC address (exactly the same as Ethernet a 6 byte).

4.1 Medium access basis

Regarding the specificity of the wireless medium and the nature of devices the previous standards are modified to include new aspects such as power constraint and collision detection.

Thus, before any transmission a node must first gain access to the medium. The 802.11 standard defines two forms of medium access, Distributed Coordination Function (DCF) and Point Coordination Function (PCF).

DCF is mandatory and based on the CSMA/CA (carrier sense multiple access with collision avoidance) protocol. With DCF, any 802.11 stations willing to send a frame must first sense if the medium is free, if this is the case it begins the transmission of the queued frames. Otherwise if the medium is occupied by another station the corresponding station must wait a random period of time before attempting to access the medium again. This period of time is called back off window and it is doubled after each attempt until the station gains access to the medium. The random delay causes stations to wait different periods of time and avoids all of them sensing the medium at exactly the same time, finding the channel idle, transmitting, and colliding with each other, this mechanism significantly reduces the number of collisions and the corresponding retransmissions, especially when the number of active users in a limited area increases.

In the other hand the 802.11 standard defines the optional Point Coordination Function (PCF) where the access point grants access to an individual station to the medium by polling the station during the contention free period. Stations can't transmit frames unless the access point polls them first. The period of time for PCF-based data traffic (if enabled) occurs alternately between contention (DCF) periods.

4.2 Additional mechanisms

Due to the characteristics of the wireless medium and in order to improve the efficiency additional features are employed:

- **Positive Acknowledgement (ACK):** With the wireless medium a station can not sense the medium and send data at the same time because it uses the same antenna for the two purposes, as a result it can not detects collision. Thus, the 802.11 has defined an extra mechanism to detect collision which consists to send an acknowledgement ACK for each successfully received packet, if the sending station doesn't receive an ACK after a specified

period of time, the sending station will assume that there was a collision and retransmits the frame.

- **Power save Mode:** The power saving mode is defined in order to conserve the battery power when there is no need to send data. Using the power saving mode each station enter in the sleep state if there is no data to send which saves the battery power considerably since the antenna consume energy for both transmission and reception, regarding the number of exchanged data at each moment, turning off the antenna may considerably save the battery power. In order to detect any eventual attempt to receive data from a given neighbour the station must wake up periodically and sense data.
- **Fragmentation:** The fragmentation option enables 802.11 to divide each data packets into smaller frames, in order to avoid the retransmission of large frames in the presence of fading noise and interference, since large frames are more exposed to bit errors and collision or link broken due to mobility. The collision or the error on a small frame does not affect the whole packet and therefore the retransmission requires less overhead compared to big frames.
- **Use of RTS and CTS:** In order to solve the problem of hidden Nodes an extra mechanism for medium reservation is used by the 802.11 which consists on using additional packet exchanging in order to reserve the medium which may reduce considerably the number of collision and increases the medium bandwidth.

To achieve this purpose two additional control frames called RTS (request to send)/CTS (clear to send) are exchanged before any transmission. Thus, whenever a given node wiles to send data, it first sends a RTS frame to the destination node, if the receiver is able to receive data it response using CTS, the CTS frame is received by all nodes in the corresponding neighbourhood, and means that the medium is reserved for the two nodes and the rest of neighbours will not transmit until the achievement of transmission (Figure VI.4).

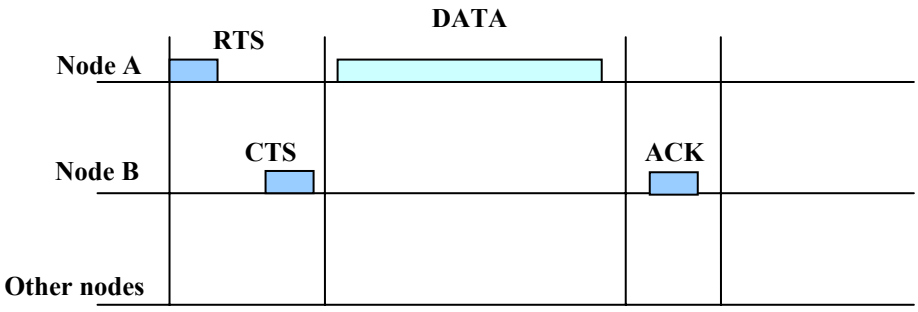


Figure VI.4 CSMA/CA with RTS/CTS

5. POWER AWARE MAC PROTOCOLS

As devoted along this chapter, solving the problematic of energy cannot be done by developing new technologies or hardware for generating more energy; however the energy conservation should be across the entire network stack by limiting in each layer the number of operations or controlling messages which consume energy.

In the chapter two we have treated the energy on the routing layer by proposing an improvement to reactive routing which consisted to improve the routing metric by including the aspect of energy in route selection by choosing the most powerful devices as intermediate nodes for routing.

Considering the problematic of energy conservation in the MAC layer should follow the three guidelines as possible:

1. Minimizing collision, since collision is the major cause of energy wasting over the network due to the packet retransmissions which consume energy for both the sender and the whole receivers and therefore affect all the system lifetime.
2. The transceivers must be switched off whenever it is possible and keep them in this state as long as possible as they consume the most energy in active mode
3. Do not use the full power for all communications over the network, and use only the necessary threshold of power to reach the desired destinations, by switching the transceivers into low power mode.

In literature there were lot of propositions to improve the efficiency of energy saving of the wireless MAC layers by developing new methods to organize the access to the medium and save the devices' energy.

In this section we are going to present a no exhaustive list of power aware MAC layers, in which each author has tried to preserve the battery power using additional features to efficiently carry out the problem of energy in ad hoc and sensor networks:

- **Sleep/wakeup mode:** as devoted above the Sleep/wakeup mode [206] tries to save devices' battery, by turning off the antenna when there is no transmission. Thus, the transceiver is permuted on or off according to a predefined protocol:

- *Periodic switching*: in this case the antenna is switched on periodically, in order to sense an eventual transmission, therefore the time in which the antenna consumes the battery power only if it is needed for reception or transmission. As a result, consuming energy for receiving unnecessary packet such as in exposed terminal problem is not possible.
- *Controlled by a coordinator:* in this case the whole network is divided into small subnet called Piconet in Bluetooth, and one of the Piconet devices is chosen to be the coordinator

which controls intra and inter Piconet transmissions, this mechanism is also called slotted mode since the coordinator divide the whole bandwidth into slots, node can send or transmit data only during predefined slots and the rest of the time nodes are in sleep mode and periodically sense for any order from the coordinator. In the same way all small Piconet are managed into great ones.

Saving energy using Sleep/wakeup mode is the most promising solution and it have proven its efficiency for Bluetooth networks, since the system lifetime is considerably increased compared to other networks such as 802.11, however the problem with this mechanism is the synchronization of the network's devices which is not possible in large ad hoc networks or high mobility networks.

Therefore, in the following sections we are going to present a set of MAC protocols, using different mechanisms to synchronize and organize devices in an ad hoc network:

- **Dynamic power saving mechanism (DPSM):** DPSM [207] is a variation of the IEEE 802.11 based on the sleep/wakeup states and makes use of a dynamically sized Ad-hoc Traffic Indication Message (ATIM) windows to achieve longer sleeping times for nodes (Figure VI.5). The IEEE 802.11 DCF time is divided into beacon intervals that are used to synchronize nodes. In the first interval every node must stay awake for the total ATIM window. This window is used to announce the status of packets ready for transmission to any receiver nodes. Such announcements are made through ATIM frames, and they are acknowledged with ATIM-ACK packets during the same beacon interval to declare that the receiver is ready for data reception. The major drawback of this mechanism is the synchronization of devices which is not evident in ad hoc network

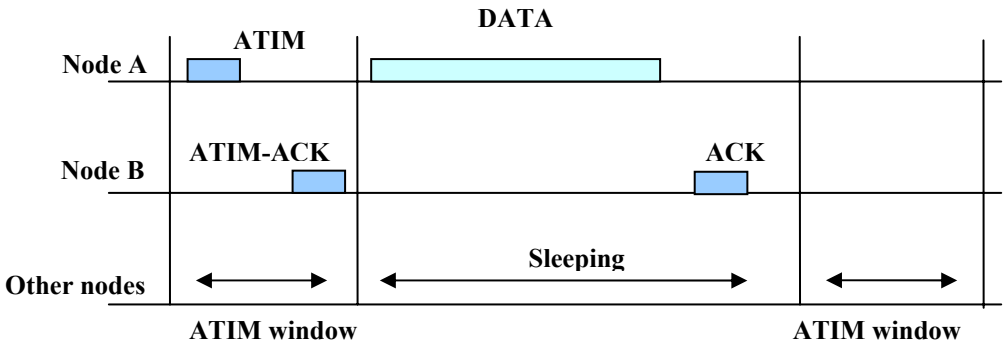


Figure VI.5 Dynamic power saving mechanism

- **Power control medium access control (PCM)** [208]**:** this approach is a power control mechanism in which each device fixes the necessary threshold of power for the transceiver to reach the desired destination. In PCM, the RTS and CTS packets defined for IEEE 802.11 are sent using the maximum available power, whereas other packet such as

data and ACK packets are sent with the minimum power required to reach sender. PCM scheme assume that the sender sends the RTS at the maximum power, this request is received by the destination node which measures the signal strength of the sender and therefore estimate the distance separating the communicating nodes. These two parameters are used to define the minimum power needed for the communication between the two nodes. As devoted by their authors this mechanism is more energy conserving compared to 802.11 and uses low operations compared to other protocols, however the mobility of nodes during data forwarding affect its performance since the fixed amount of energy must be changed at each time the nodes move.

- **Multiple channel protocols:** these methods [209] developed under this assumption tries to overcome the drawback of using single channel which causes collision with the increasing number of nodes, by more than one channel (Figure VI.6). In such approaches each channel is dedicated for a predefined purpose, some multi-channel schemes use separate channel for control packets (or signalling) and one separate channel for data transmissions, which considerably minimize collisions and bit errors and therefore improve the system efficiency and saves energy. Example of this method are Multi channel CSMA MAC protocol, Dual busy tone multiple access (DBTMA), Hop-reservation multiple access (HRMA), Multi-channel medium access control (MMAC), Dynamic channel assignment with power control (DCA-PC).

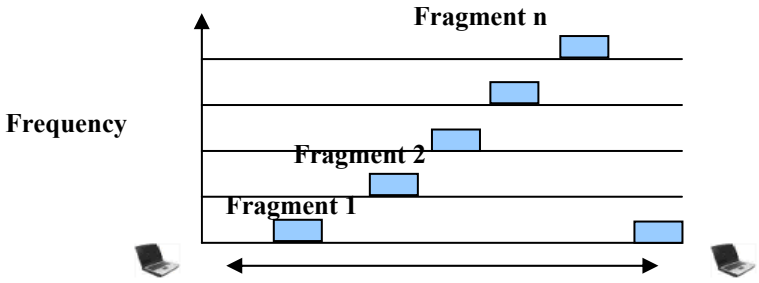


Figure VI.6 Multiple channel protocols and frequency hopping

– **Sensor Medium Access Control (S-MAC):** the S-MAC [207] protocol is essentially based on the 802.11 protocol, using RTS/CTS frames to avoid hidden terminal problems and minimize the risk of collisions. The major improvement done by S-MAC is the use of periodic sleeping/wakeup in order to minimize the energy consumption. The wakeup period of nodes is divided into two intervals; the first one is for synchronization in which one hop neighbors exchange SYNC frames, the second interval is used for data exchanging. After have send data nodes go into the sleep mode until the next wakeup period.

6. POWER CONTROL IN MANETS

Power control is the mechanism that varies the transmitting power (range) according the distance separating two communicating parties in order to save energy and improve the network capacity. The transmitting power is increased or decreased according to some criteria such as the distance between nodes or their movement.

Power control has a great importance in mobile wireless network, since it can save the battery power of network devices, and improve the network performance, by minimizing the risk of collision and interference.

6.1 Motivation of power control

Power control, can have a great affect on the network performance regarding the system lifetime as well as the network performance:

6.1.1 Energy saving

Typically MANETs are composed of wireless devices such as cellular phones, PDAs, laptops…, which are battery powered. Wireless card used by these devices to allow network connectivity consume the great part of energy of battery to transmit and receive data. The power consumed by the network card is proportional to the transmitting signal strength (power); therefore controlling the strength of the transmitted signal may save the battery power, in the way that the power of the transmitted signal is fixed to only the threshold needed to reach the desired destination rather than transmitting with the same signal strength all the time. This issue may save a great amount of energy in mobile ad hoc networks since the mobile devices are usually close to each other.

Another issue is considered in power control is the retransmission of data due to collision, according to the specifications of 802.11 MAC layer before any exchange of data, nodes first reserve the medium using CTS/RTS and then transmit data, if the data is received by the destination node, it sends an acknowledgement to achieve this operation otherwise a collision is assumed (Fig.1), and the same operations are repeated until an acknowledgement is received, the repetition of these operations consume a great amount of devices' battery power as well as overheading the network by the number of retransmission. Thus, when considering the issue of power control nodes exchange data within a limited area which decreases the number of collisions. And therefore save the device's energy.

6.1.2 Capacity improvement

The technique used by the majority of the actual MAC protocols is CSMA/CA [6]. In which any mobile device sense the medium and transmit data if the medium is free, otherwise it fell into a backoff window until the medium becomes free, it also uses RTS/CTS

mechanism to avoid the problem of hidden terminal and reserve the medium. As described above this technique consume lot of energy and reduces considerably the network throughput.

Another problem arise is the blockage of all neighbours due to the medium reservation, as shown in figure VI.7; node A transmits some data to B with a transmission range which exceeds the localisation of B, therefore nodes A, B, C cannot transmit at the same time according the CSMA/CA scheme until A finishes its transmission, therefore any queued data in C or D is blocked. This problem can be avoided if the transmitting power is fixed to the necessary amount to reach B, therefore C or D can transmit their queued data without waiting for A achievement.

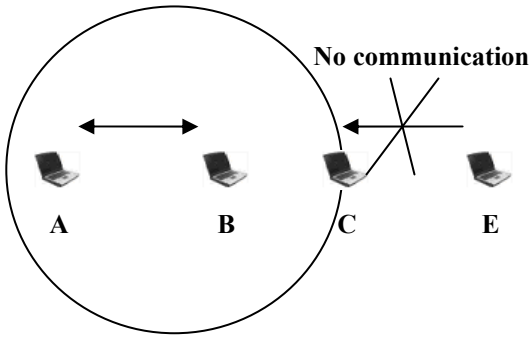


Figure VI.7 The effect of the transmission range on the network performance

6.1.3 The improvement of security

By nature a wireless network is very open and usually the transmission range of nodes exceeds the area where the network is deployed; therefore any person with the adequate network card and protocols stack can eavesdrop, attack, or use the network services. However when considering a mechanism of power control, the transmission range is fixed to only the necessary threshold to reach legitimate nodes and the probability that the signal can be captured by a malicious person is decreased (Figure VI.8), since the attacker must be so closer to legitimate nodes in order to capture the signal sent by legitimate nodes which increase the probability of its detection.

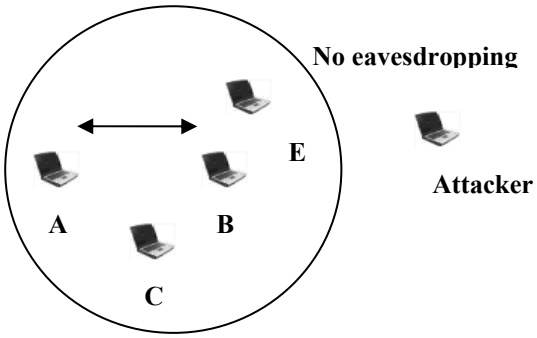


Figure VI.8 Effect of power control on the security of the network.

7. ENERGY COST ANALYSIS

Due to the nature of the used medium, when a packet is sent over a wireless link it is captured by all devices in the neighbourhood of the sender, in order to determine if this packet is intended to the corresponding node to be transmitted to the upper layers or not.

The cost of sending a packet begin on the level of the sender, since there is a fixed energy cost in transceiver circuit and a variable cost in the propagation of the signal to reach the receiver which is proportional to the transmission range. However there is another energy cost in receiving a packet by each node in the neighbourhood of the sender which is not negligible compared to the amount of energy needed for transmission. For example, in WaveLAN [210] card with omni-directional antenna, it requires 185 mA for reception and 235 mA for emission, which means that sending or receiving over a wireless medium consumes energy and therefore saving energy must pass by this two aspects.

An additional cost is added by the MAC layer to send a packet which is the power consumed to reserve the medium using signalling messages such as the RTS/CTS requests and the acknowledgement, therefore the total cost of sending a packet is given as:

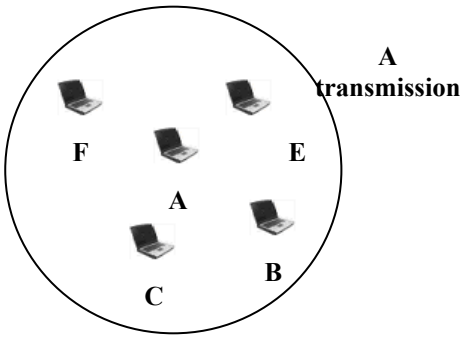
$$W = ETx + ERx + Em$$

Where ETx and ERx are the energy consumption for transmission and reception, Em is the energy consumed by the MAC layer.

To show best the energy cost in a wireless network let consider the example of figure VI.9 when node A wants to transmit a packet to node B:

1- ***A*** collaborates with ***B*** to reserve the medium using RTS/CTS
2- If the reservation success then ***A*** sends the packet to ***B***.

3- In the same time the messages sent by ***A*** and ***B*** are received by ***C, D*** and ***F.***



FigureVI.9 Energy cost analysis.

Therefore, for a successful transmission from A to B the energy consumed by each node in this neighbourhood is:

Node A: $W_A = \mathbf{ER_{RTS/CTS} + ET_{RTS/CTS} + ET_{Data} + ER_{Ack}}$

Node B: $W_B = \mathbf{ER_{RTS/CTS} + ET_{RTS/CTS} + ER_{Data} + ET_{Ack}}$

Node C: $W_C = \mathbf{2ER_{RTS/CTS} + ER_{Data} + ER_{Ack}}$

Node D: $W_D = \mathbf{2ER_{RTS/CTS} + ER_{Data} + ER_{Ack}}$

Node E: $W_E = \mathbf{2ER_{RTS/CTS} + ER_{Data} + ER_{Ack}}$

Node F: $W_F = \mathbf{2ER_{RTS/CTS} + ER_{Data} + ER_{Ack}}$

Where:

$\mathbf{ER_{RTS/CTS}}$ **:** the energy consumed for receiving CTS or RTS.

$\mathbf{ET_{RTS/CTS}}$: the energy consumed for sending CTS or RTS.

$\mathbf{ER_{Data}}$ **:** the energy consumed for receiving data.

$\mathbf{ET_{Data}}$**:** the energy consumed for sending data.

$\mathbf{ER_{Ack}}$**:** the energy consumed for receiving acknowledgement.

$\mathbf{ET_{Ack}}$**:** the energy consumed for sending acknowledgement.

Therefore the total energy consumed by a given neighbourhood for a successful transmission of a single data packet is given as:

$\mathbf{W=10ER_{RTS/CTS}+2ET_{RTS/CTS}+ 5ER_{Data}+ ET_{Data} + 5ER_{Ack} + ET_{Ack}}$.

As shown in this equation, the energy consumed by the system is very important when the number of receivers nodes is high, and this issue is very worst if the area where the network is deployed is very small or whenever there is collisions or retransmissions. Therefore, there is a great amount of consumed power due to the reception of undesirable data by each node in a given neighbourhood which can be avoided by minimizing the range of transmission to reach only the desired ones, by considering a mechanism of power control.

8. OUR PROPOSED SCHEME FOR POWER CONTROL

8.1 Description of our strategy

As described above power control in ad hoc network is mandatory in order to save the battery power and extend the system lifetime, thus in our proposed scheme we try to regulate the transmission power according to the distance separating each sender and its neighbourhood, by computing an averaged value of the necessary power to reach the maximum of nodes in a given neighbourhood [211].

Equation (VI.1) gives the reception power P_r for a signal transmitted with power P_t at a distance d, assuming no fading:

$$P_r = P_t \times G_r \times G_t \times \frac{\lambda^2}{(4 \times \pi \times d)^2} \quad \text{....(VI.1)}$$

Where

P_r = received power,

P_t = transmitted power,

G_t =antenna gain of the transmitter,

G_r = antenna gain of the receiver,

λ = wavelength,

d = distance.

Therefore when having all information (transmission and reception power sender's and receiver's gain), the distance separating a sender and a receiver can be given as:

$$d = \sqrt{P_t \times G_r \times G_t \times \frac{\lambda^2}{P_r (4 \times \pi)^2}} \quad \text{....(VI.2)}$$

As said above, our proposed scheme gives an averaged transmitting power in order to reach the maximum of neighbours, therefore when receiving any packet the corresponding node construct a table where it saves the necessary threshold of power to reach each destination in the corresponding neighbourhood. To do so we must execute the following steps:

1- *Packet capture:* each node captures all the transmitted packets in its neighbourhood and gets from that packet the following information :
   a. The MAC address of the sender.
   b. The gain of the antenna of the sender.
   c. The transmitting power of the sender.

   All this information is saved in a global table, which is used in the next step.

2- This information is used to compute the distance (equation (VI.2)) separating the corresponding node from each node of its neighbourhood and therefore the necessary power to reach that node, using the following equation:

$$P_t = TR_r \times \frac{(4 \times \pi \times d)^2}{G_r \times G_t \times \lambda^2}$$

Where TR_r is the necessary threshold allowing the receiver to correctly receive a packet.

3- The computed P_t is saved in the same table, in order to compute an averaged transmitting power to reach the maximum of neighbours.

$$P_{ar} = \frac{1}{N} \sum P_t$$

As we can observe in figure VI.10, our proposed mechanism decrease the transmission range to reach only a limited number of neighbours compared to the full power one, which saves the battery power of both the sending node and its neighbours.

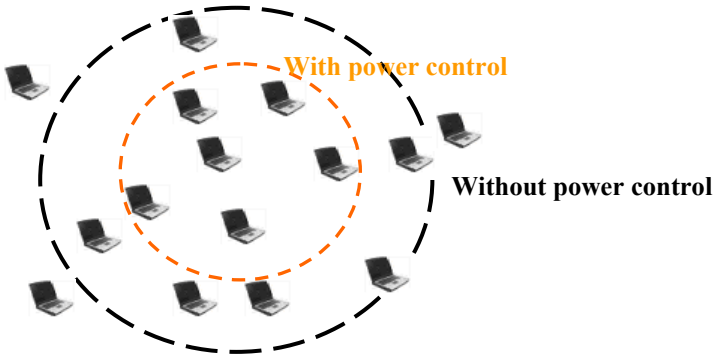


Figure VI.10 Energy cost analysis.

To make in practice the specifications of our protocol we have made some modifications on the original MAC layer frame in order to include in its header the two necessary parameters to compute distance by the receiver which are:

1- The gain of the antenna of the sender.
2- The transmitting power of sender.

9. SIMULATION RESULTS

In order to test the performance of our proposed scheme and test its feasibility we have implemented our scheme in the network simulator NS2 [116], we have made the necessary modifications described above on the 802.11 MAC and the physical layer in order to implement the specifications of our proposed scheme.

Simulations are done on a set of nodes ranging from 10 to 100 nodes in the area of 670*670 m^2 in order to test the reaction of our scheme in different cases. Then, we have fixed the number of nodes to 50 and we have varied the pause time, we have also used some CBR

(Constant Bit Rate) connections with packet length of 512 Kbytes to emulate traffic over the network, other simulation parameters are listed in table VI.1.

Parameters	Values
Network size	670*670 m^2
Number of Nodes	10,20,40,60,80,100
Max speed	20 m/s
pause Time	0,50,60,100,150,200s
CBR connections	4
Routing protocol	DSR
Simulation time	200s

Table VI.1 simulation parameters

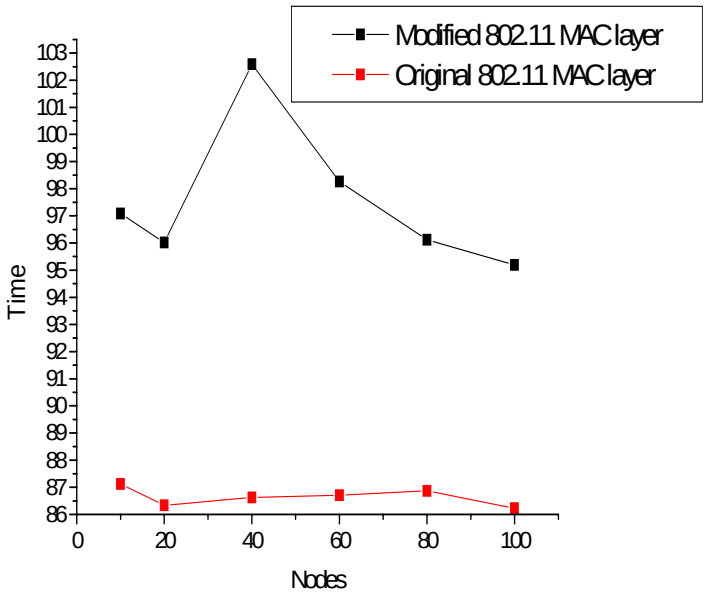


Figure VI.11 The time of the first died node

In figure VI.11 we have varied the number of nodes from 10 to 100 then we have measured the time at which the first node fails down making the beginning of the system failure. As we can observe our proposed scheme always gives best results and the battery lifetime is extended to more than 10 %.

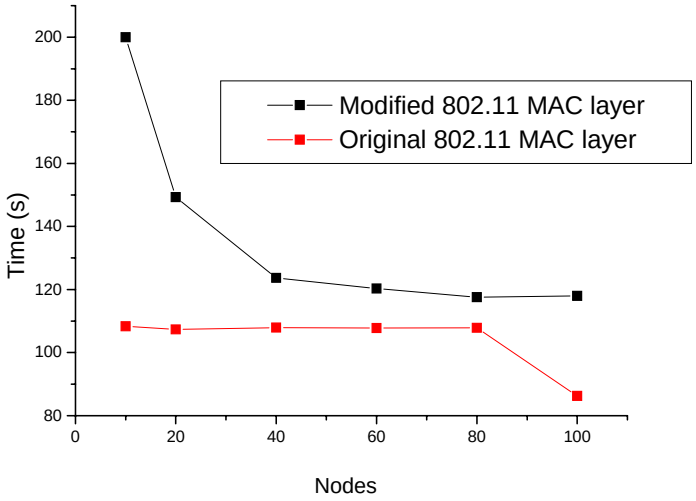


Figure VI.12 System life time

In figure VI.12 we have measured the system lifetime according to the number of nodes, as shown our improvement to the 802.11 MAC layer always gives best results compared to the original 802.11 MAC layer, and the system lifetime is extended to more 40 % in some situation, and more than 10 % in the majority of cases.

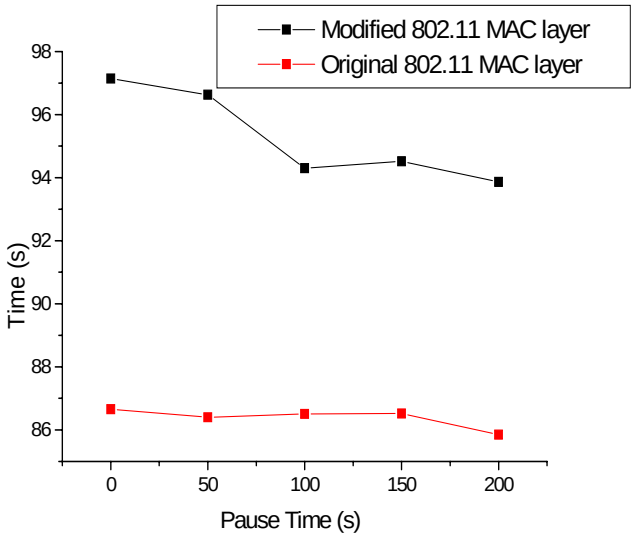


Figure VI.13 The time of the first died node

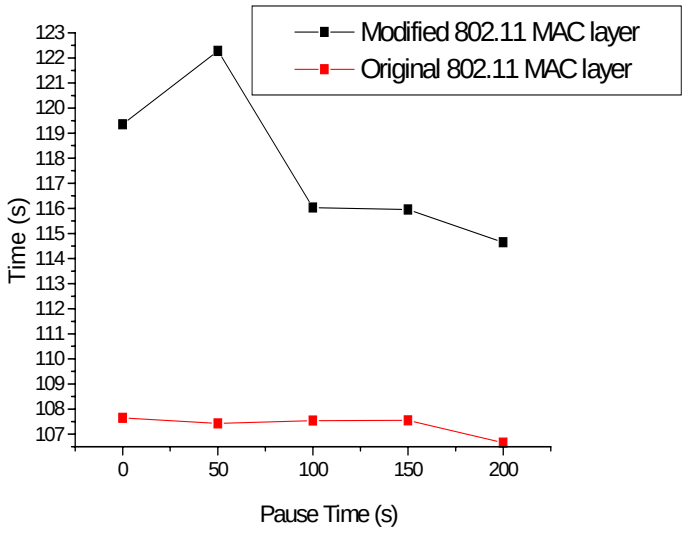


Figure VI.14 System life time

In figures VI.13 and VI.14 we have fixed the number of nodes to 50 nodes and we have varied the pause time from 0 s to 200 s (static network); and we have measured the time of the first died node and the system lifetime. As we can observe our proposed scheme always gives best results and the battery and the system lifetime is extended to more than 20%.

10. CONCLUSION

As presented above, power control in wireless networks is an important issue since it can solve lot of problems in addition to the conservation of the mobile nodes battery, such as the security of the network and the improvement of the quality of service.

Our modifications on the network stack are done on the 802.11 MAC layer, since this layer is a direct contact with the physical layer responsible for data transmission on the medium.

In our scheme the transmission power for each node is computed in the MAC layer, and transmitted to the physical layer to regulate the transmission power.

As shown in the last section, simulation results show that our proposed scheme is energy efficient since it conserves the battery power of node and extends the system lifetime to more than 10 % which is very good compared to the original MAC layer and other MAC layers.

General conclusion

Along this thesis, we have tried to treat the most crucial problematic and challenging tasks of mobile ad hoc networks (MANETS) which are security, routing and energy. The advantages of this network such as the wireless medium, the flexibility and mobility of the network devices are also the most challenging parameters for routing and security.

Our study during the three years of this thesis have given us the possibility to deeply understand the characteristics of wireless ad hoc networks and their effects on security energy and routing. This has given us the possibility to develop more than one scheme to ensure security and routing in ad hoc and sensor networks.

To ensure security over ad hoc networks we have proposed a simplified implementation of PKI over reactive protocols taking advantages of the existed routing procedures to ensure PKI services such as certificate publishing, renewal and revocation which has considerably saved the network performance. Using the same strategy we have proposed a lightweight PKI for sensor networks, which constitute an effective security mechanism compared to existed schemes regarding power consumption.

In the domain of routing we have proposed two strategies for routing based on cross-layering and swarm intelligence, these two techniques will be more promising for ensure effective routing in ad hoc networks since they are developed specially for these networks and taking all their characteristics into consideration.

Finally, we have treated the aspects of energy saving by proposing a mechanism of power control implemented on the MAC layer which have considerably saved the battery power of the network devices and extended the system lifetime.

However, the new development in wireless technologies and their applications in the human life such as vehicular and personal have given birth to new problematic and therefore more effort must be done to make in practice the existed strategies of routing and security for the new fields of applications.

Thus, in our future work we are going to make in practice artificial intelligence based techniques to solve the rising number of wireless networks problematic and applications specificities by developing new methods and algorithms ensuring both routing and security over this kind of networks.

Routing protocols in MANETs

Proactive (table-driven) protocols

- CGSR (Clusterhead Gateway Switch Routing protocol) - Clusterhead Gateway Switch Routing protocol (CGSR) [Murthy96] S. Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97.
- DBF (Distributed Bellman-Ford routing protocol) - SHREE MURTHY, J.J. GARCIA-LUNA-AVECES Distributed Bellman-Ford routing protocol (DBF), A Routing Protocol for Packet Radio Networks, Proc. ACM International Conference on Mobile Computing and Networking, pp. 86-95, November, 1995.
- DSDV (Higly Dynamic Destination-Sequenced Distance Vector routing protocol) - C. E. PERKINS, P. BHAGWAT Higly Dynamic Destination-Sequenced Distance Vector (DTDV) for Mobile Computers Proc. of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp 234-244.
- HSLS (Hazy Sighted Link State routing protocol) - CESAR SANTIVANEZ AND RAM RAMANATHAN Hazy Sighted Link State routing protocol (HSLS),BBN Technical Memorandum No. 1301, August 31, 2001.
- HSR (Hierarchical State Routing protocol) - ALAN O'NEILL HONGYI LI HIERARCHICAL STATE ROUTING PROTOCOL Internet Draft, draft-oneill-li-hsr-00.txt Distance Source Distance Vector routing protocol (DSDV)
- LCA (Linked Cluster Architecture) - M. GERLA, J. T. TSAI Multicluster, Mobile, Multimedia Radio Network ACM Wireless Networks, VOl 1, No.3, 1995, pp. 255-265
- MMRP (Mobile Mesh Routing Protocol) - K. GRACE Mobile Mesh Routing Protocol (MMRP).
- OLSR (Optimized Link State Routing Protocol) - PHILIPPE JACQUET, PAUL MUHLETHALER, AMIR QAYYUM, ANIS LAOUITI, LAURENT VIENNOT, THOMAS CLAUSEN Optimized Link State Routing Protocol Internet Draft, draft-ietf-manet-olsr-04.txt, work in progress, June 2001.
- STAR (Source Tree Adaptive routing protocol) - J.J. GARCIA-LUNA, M. SPOHN Source Tree Adaptive Routing Internet Draft, draft-ietf-manet-star-00.txt, work in progress, October 1999.

- TBRPF (Topology Broadcast based on Reverse-Path Forwarding routing protocol) - BHARGAV BELLUR, RICHARD G. OGIER, FRED L. TEMPLIN Topology Broadcast Based on Reverse-Path Forwarding (TBRPF) Internet Draft, draft-ietf-manet-tbrpf-01.txt, work in progress, June 2001.
- WRP (Wireless Routing Protocol) - Wireless Routing Protocol (WRP) [Chen98] Tsu-Wei Chen and Mario Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks" Proc. IEEE ICC'98, 5 pages.

Reactive (on-demand) protocols

- ARA (Ant-based Routing Algorithm for Mobile Ad-Hoc Networks) - Mesut Günes et. al., ARA - the ant-colony based routing algorithm for manets, In Stephan Olariu, editor, Proceedings of the 2002 ICPP Workshop on Ad Hoc Networks (IWAHN 2002), pages 79-85, IEEE Computer Society Press, August 2002.
- ABR (Associativity Based Routing protocol) - C.-K. TOH ASSOCIATIVITY-BASED LONG-LIVED ROUTING (ABR) PROTOCOL , Internet Draft.
- AODV (Ad hoc On Demand Distance Vector routing protocol) - C. PERKINS, E.ROYER AND S. DAS Ad hoc On-demand Distance Vector (AODV) Routing, Internet Draft, draft-ietf-manet-aodv-11.txt, work in progress, Aug 2002.
- BSR (Backup Source Routing protocol) - SONG GUO, OLIVER W. YANG Performance of Backup Source Routing (BSR) in mobile ad hoc networks p 440-444, Proc. 2002 IEEE Wireless Networking Conference
- CHAMP (CacHing And MultiPath routing protocol) - ALVIN C. VALERA, WINSTON K.G. SEAH AND S.V. RAO, CHAMP: A Highly-Resilient and Energy-Efficient Routing Protocol for Mobile Ad hoc Networks. In Proceedings of the 5th IEEE Conference on Mobile and Wireless Communications Networks (MWCN 2002), Stockholm, Sept 9 - 11, 2002.
- DSR (Dynamic Source Routing protocol) - D. JOHNSON, D. MALTZ, Y-C. HU AND J. JETCHEVA: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks, Internet Draft, draft-ietf-manet-dsr-09.txt, work in progress, April 2003.
- DSRFLOW (Flow State in the Dynamic Source Routing protocol) - YIH-CHUN HU, DAVID B. JOHNSON, DAVID A. MALTZ Flow State in the Dynamic Source Routing Protocol Internet Draft, draft-ietf- manet-dsrflow-00.txt, work in progress, June 2001.
- FORP (Flow Oriented Routing Protocol)

- LBR (Link life Based routing), B. S. Manoj, R. Ananthapadmanabha, and C. Siva Ram Murthy, "Link life Based Routing Protocol for Ad hoc Wireless Networks", Proc. of The 10th IEEE International Conference on Computer Communications 2001 (IC3N 2001), October 2001.
- LMR (Lightweight Mobile Routing protocol) - M.S. CORSON AND A. EPHREMIDES Lightweight Mobile Routing protocol (LMR) ,A distributed routing algorithm for mobile wireless networks, Wireless Networks 1 (1995).
- LUNAR (Lightweight Underlay Network Ad hoc Routing) - CHRISTIAN TSCHUDIN AND RICHARD GOLD Lightweight Underlay Network Ad hoc Routing (LUNAR).
- RDMAR (Relative-Distance Micro-discovery Ad hoc Routing protocol) - G. AGGELOU, R. TAFAZOLLI Relative Distance Micro-discovery Ad Hoc Routing (RDMAR) protocol Internet Draft, draft-ietf-manet- rdmar-00.txt, work in progress, September 1999.
- SSR (Signal Stability Routing protocol) - R. DUBE, C. D. RAIS, K. WANG, AND S. K. TRIPATHI Signal Stability based adaptive routing (SSR alt SSA) for ad hoc mobile networks, IEEE Personal Communication, Feb. 1997.
- TORA (Temporally-Ordered Routing Algorithm routing protocol) - V. PARK, S. CORSON TEMPORALLY-ORDERED ROUTING ALGORITHM (TORA) VERSION 1 Internet Draft, draft-ietf-manet-tora-spec- 03.txt, work in progress, June 2001.
- PLBR (Preferred link based routing)-- R. S. Sisodia, B. S. Manoj, and C. Siva Ram Murthy, "A Preferred Link Based Routing Protocol for Ad Hoc Wireless Networks", Journal of Communications and Networks, Vol. 4, No. 1, pp. 14-21, March 2002.

Hierarchical protocols:

- CBRP (Cluster Based Routing Protocol) - M. JIANG, J. LI, Y. C. TAY Cluster Based Routing Protocol (CBRP) Functional Specification Internet Draft, draft-ietf-manet-cbrp.txt, work in progress, June 1999.
- CEDAR (Core Extraction Distributed Ad hoc Routing) - RAGHUPATHY SIVAKUMAR, PRASUN SINHA, VADUVUR BHARGHAVAN Core Extraction Distributed Ad hoc Routing (CEDAR) Specification, Internet Draft, draft-ietf-manet-cedar-spec-00.txt
- DDR (Distributed Dynamic Routing Algorithm) - NAVID NIKAEIN, HOUDA LABIOD, CHRISTIAN BONNET Distributed Dynamic Routing Algorithm (DDR)

for Mobile Ad Hoc Networks, in proceedings of the MobiHOC 2000 : First Annual Workshop on Mobile Ad Hoc Networking & Computing

- GSR (Global State Routing protocol) - Global State Routing protocol (GSR) [Iwata99] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks" IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79.
- FSR (Fisheye State Routing protocol) - MARIO GERLA, GUANGYU PEI, XIAOYAN HONG, TSU-WEI CHEN Fisheye State Routing Protocol (FSR) for Ad Hoc Networks Internet Draft, draft-ietf-manet-fsr-00.txt, work in progress, June 2001.
- HARP (Hybrid Ad Hoc Routing Protocol) - NAVID NIKAEIN, CHRISTIAN BONNET, NEDA NIKAEIN Hybrid Ad Hoc Routing Protocol - HARP, in proceeding of IST 2001: International Symposium on Telecommunications
- LANMAR (Landmark Routing Protocol for Large Scale Networks) - MARIO GERLA, XIAOYAN HONG, LI MA, GUANGYU PEI Landmark Routing Protocol (LANMAR) Internet Draft, draft-ietf-manet- lanmar-01.txt, work in progress, June 2001.
- ZRP (Zone Routing Protocol protocol) - ZYGMUNT J. HAAS, MARC R. PEARLMAN, PRINCE SAMAR THE BORDERCAST RESOLUTION PROTOCOL (BRP) Internet Draft, draft- ietf-manet-zone-zrp-04.txt, work in progress, July 2002.
- BRP (Bordercast Resolution Protocol) - ZYGMUNT J. HAAS, MARC R. PEARLMAN, PRINCE SAMAR THE BORDERCAST RESOLUTION PROTOCOL (BRP) Internet Draft, draft- ietf-manet-zone-brp-02.txt, work in progress, July 2002.
- IARP (Intrazone Routing Protocol) - ZYGMUNT J. HAAS, MARC R. PEARLMAN, PRINCE SAMAR THE INTRAZONE ROUTING PROTOCOL (IARP) Internet Draft, draft-ietf- manet-zone-iarp-02.txt, work in progress, July 2002.
- IERP (Interzone Routing Protocol) - ZYGMUNT J. HAAS, MARC R. PEARLMAN, PRINCE SAMAR THE INTERZONE ROUTING PROTOCOL (IERP) Internet Draft, draft-ietf- manet-zone-ierp-02.txt, work in progress, July 2002.

Geographical protocols:

- DREAM (Distance Routing Effect Algorithm for Mobility) - S. BASAGNI, I. CHLAMTAC, V. R. SYROTIUK, B. A. WOODWARD A Distance Routing Effect Algorithm for Mobility (DREAM) In Proc. ACM/IEEE Mobicom, pages 76-84, October 1998.

- GLS(Grid) (Geographic Location Service) - JINYANG LI, JOHN JANOTTI, DOUGLAS S. J. DE COUTU, DAVID R. KARGER, ROBERT MORRIS A Scalable Location Service for Geographic Ad Hoc Routing M.I.T. Laboratory for Computer Science
- LAR (Location-Aided Routing protocol) - Y.-B. KO, V. N. H. Location-Aided Routing in mobile Ad hoc networks In Proc. ACM/IEEE Mobicom, pages 66-75, October 1998.
- GPSAL (GPS Ant-Like Routing Algorithm) - Daniel Câmara, Antonio Alfredo F. Loureiro, A Novel Routing Algorithm for Hoc Networks, Baltzer Journal of Telecommunications Systems, 18:1-3, 85-100, Kluwer Academic Publishers, 2001."
- ZHLS (Zone-Based Hierarchical Link State Routing) - JOA NG, I-TAI LU Zone-Based Hierchical Link State Routing (ZHLS). An abstract routing protocol and medium access protocol for mobile ad hoc networks Submitted for partial fulfillment of the requirements for the degree of doctor of philosophy (Electrical engineering) in January 1999.

Power aware protocols:

- ISAIAH (Infra-Structure Aodv for Infrastructured Ad Hoc networks) - ANDERS LINDGREN AND OLOV SCHELÉN Infrastructured ad hoc networks In Proceedings of the 2002 International Conference on Parallel Processing Workshops (International Workshop on Ad Hoc Networking (IWAHN 2002)). pages 64-70. August 2002.
- PARO (Power-Aware Routing Optimization Protocol) - J. GOMEZ, A. T. CAMPBELL, M. NAGHSHINEH, C. BISDIKIAN, T.J. WATSON POWER-AWARE ROUTING OPTIMIZATION PROTOCOL (PARO) Internet Draft, draft-gomez-paro-manet-00.txt, work in progress, June 2001.
- PAMAS (PAMAS-Power Aware Multi Access Protocol with Signaling Ad Hoc Networks) - S. SINGH, C.S. RAGHAVENDRA PAMAS & PAMAS-Power Aware Multi Access Protocol with Signaling Ad Hoc Networks

References

[1]Charles E.Perkins. ”Ad hoc Networking”, Addison Wesley, 2001

[2]Ramanathan, R.; Redi, J. “A brief overview of ad hoc networks: challenges and directions”. IEEE Communications Magazine, Volume: 40 Issue: 5, 2002 pp: 20 -22.

[3]Aurelien Geron, “WIFI et securité, QoS et WPA“, Lavoisier, 2002.

[4]Frodigh, M., Johansson, P. and Larsson, P. “Wireless Ad-hoc Networking -- The Art of Networking Without a Network”. Ericsson Review, 4, 2000.

[5]K. AL AGHA, G. PUJOLLE, G. VIVIER. “Réseaux de mobiles et réseaux sans fil“, 2nd edition, Eyrolles, 2005

[6]Jagannathan Sarangapani. “Wireless Ad Hoc and Sensor Networks Protocols, Performance, and Control”, Taylor &&Francis Group, LLC, 2007.

[7]IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification – Amendment 1: High-speed Physical Layer in the 5 GHz Band”. IEEE Std. 802.11a, 1999.

[8]IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements “Part 11: Supplement to 802.11-1997, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band”. IEEE Std. 802.11-1999.

[10]IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements “Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications”. IEEE Std. 802.3, 2002.

[11]IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements “IEEE 802.a, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications: High-speed Physical Layer in the 5 Ghz Band, Supplement to IEEE 802.11 Standard” Sep., 1999.

[12]IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements “IEEE 802. b, Part 11 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications”, IEEE Std 802. b, 1999

[13]IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification – Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band”. IEEE Std. 802.11g, 2003.

[14]IEEE WG, Draft Supplement to Standard for Telecommunications and Information Exchange between Systems-LAN/MAN Specific Requirements- “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS)”, 802.11e Draft 3.1, May, 2002.

[15]IEEE Standards for Information Technology. “IEEE Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operations”. IEEE Std. 802.11f-2003.

[16]S. Lindsey, K. Sivalingam and C.S. Raghavendra, " Power Aware Routing and MAC protocols for Wireless and Mobile Networks", in Wiley Handbook on Wireless Networks and Mobile Computing; Ivan Stojmenivic, Ed., John Wiley & Sons, 2001
[17]A.Mishra and W.A.Arbaugh. "An Initial Security Analysis of the IEEE 802.1X Standard". Technical Report CS-TR-4328,UMIACS-TR-2002-10,Univ.Maryland,Feb.2002.
[18]IEEE Standards for Information Technology. Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification – Amendment 6: Medium Access Control (MAC) Security Enhancements". IEEE Std. 802.11i-2004.
[19]Houda Labiod, Hossam Afifi. "De Bluetooth a WIFI securité, qualité de service et aspects pratique", hermes-science,2004.
[20]Tom Karygiannis, Les Owens. « Wireless Network Security 802.11, Bluetooth and Handheld Devices 802.11, Bluetooth and Handheld Devices 802.11, Bluetooth and Handheld Devices 802.11, Bluetooth and Handheld Devices, Recommendations of the National Institute of Standards and Technology ». Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, November 2002.
[21]Arunabha Ghosh, et. al., "Broadband Wireless Access with WiMAX/802.16: Current Performance Benchmarks and Future Potential". IEEE Communications, Vol. 43, No. 2.
[22]C. Eklund, R. B. Marks, K.L. Stanwood, S. Wang. " A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access". IEEE Communications Magazine, June 2002.
[23]J.P. Castro, "The UMTS Network and Radio Access Technology: Air Interface Techniques for FutureMobile Systems", April 2001.
[24]W. WEBB. "Introduction to Wireless Local Loop". Artech House, 2000
[25]P. HELTZEL. "Complete Wireless Home Networking". Prentice Hall, 2003
[26]P. ROSHAN, J. Leary. "Wireless Local-Area Network Fundamentals". Cisco Press, 2003.
[27]C. K. TOH. "Ad-hoc Mobile Wireless Networks: Protocols and Systems". Prentice Hall, 2001.
[28]F. ZHAO, L. GUIBAS. "Wireless Sensor Networks", Morgan Kaufmann Publishers, 2004.
[29]Carlos F.Garcia-hermandez and al, "Wireless sensor networks and applications", International Journal of Computer Science and Network Security, Vol.7, No.3, pp. 264-273, March 2007.
[30]R.Prasad, "Basic Concept of Personal Area Networks", WWRF, Kick off Meeting, Munich, Germany, 2001.
[31]A.Cerpa,J.Elson,M.Hamilton,and J.Zhao. "Habitat monitoring:Application driver for wireless communications technology". Proc.ACM SigComm Conf.,Costa Rica,April 2001.
[32]Rajeev Shorey, A.Ananda Mun Choon Chan Wei Tsang. "mobile,wireless,and sensor networks technology,applications,and future directions". 2006 by John Wiley &Sons,
[33]IEEE Computer Society. "IEEE Standard for Local and metropolitan area networks: Port-Based Network access control". October 2001.
[34]S.Capkun, L.Buttyan, and J.-P. Hubaux, "Self-organized Public-key Management for Mobile Ad hoc Networks", IEEE Transactions on Mobile Computing, vol. 1, no. 2, January-March 2003.
[35]L.Chen and W. B. Heinzelmann. "QoS-Aware Routing Based on Data rate Estimation for Mobile Ad Hoc Networks". Selected Areas in Communications, IEEE Journal on Volume 23, Issue 3, March 2005 pp. 561 - 572.

[36]C. Toh, H. Cobb, and D. Scott. “Performance evaluation of battery-life-aware routing schemes for wireless ad hoc networks”. IEEE International Conference on Volume 9, 11-14 June 2001 pp. 2824 - 2829.
[37]S. Yi, P. Naldurg, and R. Kravets, “Security-Aware Ad hoc Routing for Wireless Networks” Proc. 2nd ACM Symp. Mobile Ad hoc Networking and Computing (Mobihoc’01), Long Beach, CA, October 2001, pp. 299-302.
[38]S. Toner, and D. O'Mahony, “Self-Organising Node Address Management in Ad hoc Networks”. Personal Wireless Communications, IFIP-TC6 8th Int’l. Conf. (PWC 2003), 2003, pp. 476-483.
[39]Guy Pujolle, “les réseaux”, edition 2003, Eyrolles.
[40]Douglas Conner, “TCP/IP architecture, protocoles et applications “, DUNOD, 2001.
[41]R. Perlman “Interconnections: Bridges, Routers, Switches, and Internetworking Protocols”. Addison-Wesley, Reading, MA, 2000.
[42]C.Siva Ram Nurthy and B.S. Manoj. “Ad hoc wireless networks Architectures and Protocols”. le Prentice Hall, 2004.
[43]T. Clausen, P. Jacquet, and L. Viennot, “Comparative Study of Routing Protocols for Mobile Ad hoc Networks”. Med-Hoc-Net’02, Sardegna, Italy, September 2002.
[44]Xiaoyan Hong; Kaixin Xu; Gerla, M. “Scalable routing protocols for mobile ad hoc networks”. IEEE Network , Volume: 16 Issue: 4 , July-Aug. 2002, pp: 11 -21
[45]D. JOHNSON, D. MALTZ, Y-C. HU AND J. JETCHEVA. “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks”. Internet Draft, draft-ietf-manet-dsr-09.txt, work in progress, April 2003.
[46]C. PERKINS, E.ROYER AND S. DAS. “Ad hoc On-demand Distance Vector (AODV) Routing”. Internet Draft, draft-ietf-manet-aodv-11.txt, work in progress, Aug 2002.
[47]V. PARK, S. CORSON. ”TORA (Temporally-Ordered Routing Algorithm routing protocol)”. Internet Draft, draft-ietf-manet-tora-spec- 03.txt, work in progress, June 2001.
[48]Mesut Günes et. al. “ARA - the ant-colony based routing algorithm for manets”. In Stephan Olariu, editor, Proceedings of the 2002 ICPP Workshop on Ad Hoc Networks (IWAHN 2002), pages 79-85, IEEE Computer Society Press, August 2002.
[49]A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks". IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79.
[50]S. Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97.
[51]MARIO GERLA, GUANGYU PEI, XIAOYAN HONG, TSU-WEI CHEN. “Fisheye State Routing Protocol (FSR) for Ad Hoc Networks”. Internet Draft, draft-ietf-manet-fsr-00.txt, work in progress, June 2001.
[52]JACQUET, PAUL MUHLETHALER, AMIR QAYYUM, ANIS LAOUITI, LAURENT VIENNOT, THOMAS CLAUSEN. “Optimized Link State Routing Protocol”. Internet Draft, draft-ietf-manet-olsr-04.txt, work in progress, June 2001.
[53]Tsu-Wei Chen and Mario Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks" Proc. IEEE ICC'98.
[54]C. E. PERKINS, P. BHAGWAT. “Higly Dynamic Destination-Sequenced Distance Vector (DTDV) for Mobile Computers” Proc. of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp 234-244.
[55]Arpacioglu, Small, and Haas, “Notes on scalability of wireless ad hoc networks,” Internet draft, work in progress, December, 2003.

[56]ZYGMUNT J. HAAS, MARC R. PEARLMAN, PRINCE SAMAR. “The Bordercast Resolution Protocol (BRP)”. Internet Draft, draft- ietf-manet-zone-zrp-04.txt, work in progress, July 2002.
[57]M. JIANG, J. LI, Y. C. TAY. “Cluster Based Routing Protocol (CBRP)”. Functional Specification Internet Draft, draft-ietf-manet-cbrp.txt, work in progress, June 1999.
[58]A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks". IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79.
[59]NAVID NIKAEIN, CHRISTIAN BONNET, NEDA NIKAEIN. “Hybrid Ad Hoc Routing Protocol – HARP”. proceeding of IST 2001: International Symposium on Telecommunications.
[60]Camp, T.; Boleng, J.; Williams, B.; Wilcox, L.; Navidi, W. “Performance comparison of two location based routing protocols for ad hoc networks” INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE , Volume: 3 , 2002 Page(s): 1678 –1687
[61]Stojmenovic, I. “Position-based routing in ad hoc networks”. IEEE Communications Magazine, Volume: 40 Issue: 7, July 2002 Page(s): 128 –134
[62]S. BASAGNI, I. CHLAMTAC, V. R. SYROTIUK, B. A. WOODWARD. “A Distance Routing Effect Algorithm for Mobility (DREAM)”. In Proc. ACM/IEEE Mobicom, pages 76-84, October 1998.
[63]JINYANG LI, JOHN JANOTTI, DOUGLAS S. J. DE COUTU, DAVID R. KARGER, ROBERT MORRIS. “A Scalable Location Service for Geographic Ad Hoc Routing”. M.I.T. Laboratory for Computer Science
[64]Y.-B. KO, V. N. H. “Location-Aided Routing in mobile Ad hoc networks”. In Proc. ACM/IEEE Mobicom, pages 66-75, October 1998.
[65]Daniel Câmara, Antonio Alfredo F. Loureiro. “A Novel Routing Algorithm for Hoc Networks”. Baltzer Journal of Telecommunications Systems, 18:1-3, 85-100, Kluwer Academic Publishers, 2001.
[66]J. GOMEZ, A. T. CAMPBELL, M. NAGHSHINEH, C. BISDIKIAN, T.J. WATSON “Power-Aware Routing Optimization Protocol (Paro)”. Internet Draft, draft-gomez-paro-manet-00.txt, work in progress, June 2001.
[67]S. SINGH, C.S. RAGHAVENDRA PAMAS & PAMAS-Power Aware Multi Access Protocol with Signaling Ad Hoc Networks
[68]B.KADRI, M. Feham and M.ABDELLAH, “Weight based DSR for Mobile ad hoc networks", IEEE international conference on information and communication technologies from theory to application, IEEE ICTTA 2008.
[69]D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris. “A High-Throughput Path Metric for Multi-Hop Wireless Routing”. Proceedings of the 9th ACM International Conference on Mobile Computing and Networking (MobiCom '03), San Diego, California, September 2003
[70]D. S. J. De Couto, D. Aguayo, B. A. Chambers, and R. Morris, “Performance of Multihop Wireless Networks: Shortest Path is Not Enough”. Proceedings of the First Workshop on Hot Topics in Networking (HotNets-I), Princeton, New Jersey, October 2002
[71]R. Draves, J. Padhye, and B. Zill, “Comparison of Routing Metrics for Static Multi-Hop Wireless Networks”, ACM Special Interest Group on Data Communications (SIGCOMM), Portland, OR, August 2004.
[72]Dominique Dhoutaut, “ Etude du standard IEEE 802.11 dans le cadre des réseaux ad hoc : de la simulation à l’expérimentation “, doctorate thesis, Decembre 2003.

[73]H. Badis, A. Munaretto, K. Al Agha, and G. Pujolle. "QoS for Ad hoc Networking Based on Multiple Metrics: Data rate and Delay," In the proceedings of IEEE MWCN2003, Singapore, October 2003.
[74]Ronan de Renesse, Mona Ghassemian, Vasilis Friderikos, A. Hamid Aghvami, "QoS Enabled Routing in Mobile Ad Hoc Networks," 3G Mobile Communication Technologies, 2004. 3G 2004. Fifth IEE International Conference on 2004 pp. 678-682.
[75]Tor Inge Skaar, Tor-Erik Thorjussen, "Security Specification, Access Control and Dynamic Routing for Ad-Hoc Wireless Networks applied to Medical Emergencies". Project report Norwegian University of Science and Technology Faculty of Information Technology, Mathematics and Electrical Engineering, 2003.
[76]S. Lindsey, K. Sivalingam and C.S. Raghavendra, " Power Aware Routing and MAC protocols for Wireless and Mobile Networks", in Wiley Handbook on Wireless Networks and Mobile Computing; Ivan Stojmenivic, Ed., John Wiley & Sons, 2001
[77]A. Bruce McDonald, and Taieb F. Znati. "A Mobility-Based Framework for Adaptive Clustering in Wireless Ad Hoc Networks". IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 17, NO. 8, AUGUST 1999
[78]S. Shakkottai, T. S. Rappaport and P. C. Karlsson, "Cross-layer Design for Wireless Networks," IEEE Communications Magazine, vol. 41 , No. 10, October 2003, pages 74-80.
[79]V. T. Raisinghani, A. K. Singh, S. Iyer, "Improving TCP performance over Mobile Wireless Environments using Cross-Layer Feedback", Personal Wireless Communications IEEE International Conference 15-17 Dec. 2002 Pages:81 – 85.
[80] W. Li, Z. Bao – yu, "Study on Cross – Layer Design and Power Conservation in Ad hoc Network", IEEE PDCAT'2003, 27-29 Aug. 2003 Pages:324 – 328.
[81]Hai Jiang, Weihua Zhuang, and Xuemin (Sherman) Shen. "Cross-Layer Design for Resource Allocation in 3G Wireless Networks and Beyond". IEEE Communications Magazine, December 2005.
[82]Chiara Buratti, Andrea Giorgetti, Roberto Verdone. "Cross-Layer Design of an Energy-Efficient Cluster Formation Algorithm with Carrier-sensing Multiple Access for Wireless Sensor Networks". Journal on Wireless Communications and Networking 2005:5, pages 672–685.
[83]John Rittinghouse, James Ransome. "Wireless operational security". Digital Press, 2004.
[84]Guy Pujolle. "Securité Wifi". Eyrolles, 2004.
[85]Tara M., Charles R.Elden. "Wireless security and privacy Best Practices and Design Techniques". Addison Wesley, 2002.
[86]Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao. "On Countermeasures to Traffic Analysis Attacks". In: Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY.2003.
[87]A. Nash, W. Duane, C. Joseph and D. Brink, "PKI: Implementing and Managing Security", McGraw-Hill 2001, ISBN 0072131233
[88]Bruce Schneier. « Cryptographie appliqué algorithms, protocols et code sources en C ». 2 nd edition John Wiley & Sons, New York. 2002.
[89]Mohsen Guizani. "Security and Trust in Mobile Ad Hoc Networks". Proceedings of the 4th Annual Communication Networks and Services Research Conference (CNSR'06). 2006.
[90]L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks". IEEE Networks, Volume 13, Issue 6 1999.
[91]H. Luo and S. Lu. "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks". Technical Report 200030, UCLA Computer Science Department, 2000.
[92]J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang."Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks". IEEE ICNP, 2001.

[93]H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang.“Self-securing Ad Hoc Wireless Networks”. IEEE ISCC, 2002.
[94]J-P. Hubaux, L. Buttyán and S. Capkun. “The Quest for Security in Mobile Ad Hoc Networks”. ACM, 2001.
[95]M. Bechler., H.-J. Hof, D. Kraft, F. Pahlke, L. Wolf,2004. ”A Cluster-Based Security Architecture for Ad Hoc Networks”. IEEE INFOCOM
[96]B.KADRI, A.M’HAMED, M. FEHAM. “A new management scheme of cluster based PKI for ad hoc networks using multi-signature”. IEEE Global Information Infrastructure Symposium, 2007.
[97]J. Broch, D. Maltz, D. Johnson, Y.-C. Hu, and J. Jetcheva ieA Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocolsle, Proceedings of the IEEE/ACM International Conference on Mobile Computing and Networking (MOBICOM), October 1998, pages 85-97.
[98]E. M. Royer and C.-K. Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networksle”, IEEE Personal Communications Magazine, April 1999, pages 46-55
[99] C. E. Perkins, E. M. Royer, S. R. Das,” Quality of Service for Ad hoc On-Demand Distance Vector Routing”, draft-perkins-manet-aodvqos-02.txt, IETF Internet Draft, work in progress, October 2003.
[100]K. N. Sridhar, J. Lillykutty, and S. Rajeev, “Performance Evaluation and Enhancement of Link Stability Based Routing for MANETs”, INTERNATIONAL WORKSHOP ON MOBILE AND WIRELESS NETWORKING (MWN 2004), Montreal, Quebec, Canada, August 15, 2004.
[101]P. Papadimitratos, and Z.J. Haas, “Secure Routing for Mobile Ad hoc Networks,” Proc. Communication Networks and Distributed Systems, Modeling and Simulation
Conf. (CNDS’02), San Antonio, Texas, January 2002, pp. 27-31.
[102]R. Guerin, A. Orda, D. Williams. “QoS Routing Mechanisms and OSPF Extensions”, August, 1999, Network Working Group, Rrequest for Comments: 2676.
[103]Chang JH, Tassiulas L. “Energy conserving routing in wireless ad-hoc networks”, ln INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, Volume 1, 26-30 March 2000 pp. 22 - 31.
[104]J. Li, C. Blake, D. S. J. D. Couto, H. I. Lee, and R. Morris, “Capacity of Ad Hoc Wireless Networks,” in MOBICOM 2001, July 2001.
[105] Anmol Sheth and Richard Han. A mobility-aware adaptive power control algorithm for wireless lans, a short paper. IEEE CAS Low Power Workshop, August 2002.
[106]B.KADRI, D. Moussaoui and M.Feham, “A cross layer design for QoS implementation for ad hoc networks applied to DSR", IEEE international conference on information and communication technologies from theory to application, IEEE ICTTA 2008.
[107]B.KADRI, M. Feham and M.ABDELLAH, “Weight based DSR for Mobile ad hoc networks", IEEE international conference on information and communication technologies from theory to application, IEEE ICTTA 2008.
[108]C. Zhu and M. Corson. QoS routing for mobile ad hoc networks. In IEEE INFOCOM, 2001.
[109]S. Henerer , « Diffserv et son application à la qualité de service »,Avril 2003.
[110]Shigang Chen, Klara Nahrstedt, “Distributed Quality-of-Service Routing in Ad Hoc Networks”, IEEE journal on selected areas in communications, vol. 17, no. 8, August 1999
[111]H. Xiao, K.G. Seah, A. Lo, K.C. Chua, "A flexible quality of service model for mobile ad-hoc networks", in: Proceedings of IEEE Vehicular Technology Conference, vol. 1, pp. 445–449,May 2000.

[112]M. Jain and C. Dovrolis, “End-to-end available bandwidth: Measurement methodology, dynamics, and relation with TCP throughput,” in Proceedings of ACM SIGCOMM, Pittsburg, PA, USA, Aug. 2002.
[113]R. Prasad, M. Murray, C. Dovrolis, and K. Claffy, “Bandwidth estimation: metrics, measurement techniques, and tools,” IEEE Network Magazine, 2003.
[114]Strauss, Katabi, and Kaashoek, “A measurement study of available bandwidth estimation tools,” in ACM SIGCOMM Internet Measurement Workshop, 2003.
[115]Y. Choi, H.-N. Lee, and A. Garg, “Measurement and analysis of wide area network (wan) traffic,” in SCS Symposium on Performance Evaluation of Computer and Telecommunication Systems, July 2000.
[116]The Network simulator The Network Simulator ns-2. Project web page available at http://www.isi.edu/nsnam/ns/.
[117]R. Wattenhofer, L. Li, P. Bahl, and Y.-M. Wang, “Distributed Topology Control for Power Efficient Operation in Multihop Wireless Ad Hoc Networks,” in INFOCOM 2001, vol. 3, pp. 1388–1397, April 2001.
[118]Qun Li, Javed A. Aslam, and Daniela Rus. Online power-aware routing in wireless ad hoc networks. In Mobile Computing and Networking, pages 97{107, 2001.
[119]V. Roduplu and T. Meng. Minimum energy mobile wireless networks. In IEEE JSAC, pages 1333{1344, 1999.
[120]E. Bonabeau, M. Dorigo, and G. Théraulaz, “Swarm intelligence: from natural to artificial systems”, Oxford University Press, 1999.
[121] J. Baras and H. Mehta, “A Probabilistic Emergent Routing Algorithm for Mobile Ad hoc Networks.” In Proc. Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, pages 3-5, 2003.
[122]N. Minar, K. H. Kramer, and P. Maes, "Cooperating Mobile Agents for Dynamic Network Routing," Software Agents for Future Communications Systems, chapter 12, Springer Verlag, 1999.
[123]G. DiCaro and M. Dorigo, “Ant Colonies for Adaptive Routing in Packet-Switched Communications Net-works”, Proc. PPSN V - Fifth Internatinal Conference on Parallel Problem Solving from Nature, pp. 673-682, Amsterdam, Holland, September 27-30, 1998.
[124]S. Lipperts and B. Kreller, "Mobile agents in telecommunications networks - a simulative approach to load balancing", Proc. 5th Intl.
[125]M. Dorigo and G. Di Caro, “Ant colony optimization: a new meta-heuristic”, Proc. 1999 Congresson Evolutionary Computation, July 6-9, 1999, pp. 1470-1477
[126]M. Dorigo, V. Maniezzo, and A. Colorni, "The ant system: optimization by a colony of cooperating agents", IEEE Transactions on Systems,Man, and Cybernetics, Part B, vol. 26, no. 1, pp. 29-41, 1996.
[127]M. Heusse, D. Snyers, S. Guérin, and P. Kuntz, "Adaptive agent-driven routing and load balancing in communication network", Proc. ANTS'98,First International Workshop on Ant Colony Optimization, Brussels, Belgium, October 15-16, 1998.
[128]T. White, "Swarm intelligence and problem solving in telecommunications", Canadian Artificial Intelligence Magazine, Spring, 1997.
[129]T. White, "Routing with swarm intelligence", Technical Report SCE-97-15, Systems and Computer Engineering Department, Carleton University, September, 1997.
[130]T. White and B. Pagurek, "Towards multi-swarm problem solving in networks", Proc. Third International Conference on Multi-Agent Systems (ICMAS '98), July, 1998, pp 333-340.
[131]F. Ducatelle, G. Di Caro, and L. M. Gambardella, "Ant Agents for Hybrid Multipath Routing in Mobile Ad Hoc Networks," Proc. Second Annual Conference on Wireless On-demand Network Systems and Services WONS 2005, pp. 44-53, 2005.

[132]Siva Kumar.D and Bhuvaneswaran.R.S, “Proposal on Multi agent Ants based Routing Algorithm for Mobile Ad-Hoc Networks”, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.6, June 2007.
[133]M. Heissenbuettel and T. Braun, “Ants-based routing in large scale mobile ad hoc networks”. Kommunikation in verteilten Systemen KiVS’03, Leipzig, Germany, 2003.
[134]K. Oida and M. Sekido, "An agent-based routing system for QoS guarantees", Proc. IEEE International Conference on Systems, Man, and Cybernetics, Oct. 12-15, pp. 833-838, 1999.
[135]M. Gunes,, U. Sorges, and I. Bouazisi, “ARA - the Ant-Colony Based routing Algorithm for MANETs”, Proc. ICPP Workshop on Ad Hoc Networks, Vancouver, Canada, 2002, 79-85.
[136]R. Schoonderwoerd, O. E. Holland, J. L. Bruten, and L. J. M. Rothkrantz, "Ant-Based Load Balancing in Telecommunications Networks", Adaptive Behavior, 2, pp. 169- 207, 1996.
[137]S. Lipperts and B. Kreller, "Mobile agents in telecommunications networks - a simulative approach to load balancing", Proc. 5th Intl. Conf. Information Systems, Analysis and Synthesis, ISAS'99, 1999.
[138] Wedde, H.F., and al.” BeeAdHoc: An Energy Efficient Routing Algorithm for Mobile Ad Hoc Networks Inspired by Bee Behavior”. GECCO’05, Washington, DC, USA. , June 25–29, 2005.
[139]A. Bieszczad, B. Pagurek, and T. White, “Mobile agents for network management”, IEEE Communication Surveys, Fourth Quarter 1998, vol. 1, no. 1, 1998.
[140]Zhou Lianying and Liu Fengyu, “A Swarm-Intelligence-Based Intrusion Detection Technique”, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.7B, July 2006
[141]K. N. Sridhar, J. Lillykutty, and S. Rajeev, Performance Evaluation and Enhancement of Link Stability Based Routing for MANETslt, INTERNATIONAL WORKSHOP ON MOBILE AND WIRELESS NETWORKING (MWN 2004), Montreal, Quebec, Canada, August 15, 2004
[142] M.l Gerharz, C. de Waal, M. Frank, and P. Martini, “Link Stability in Mobile Wireless Ad Hoc Networkslt, Proceedings of the 27th Annual IEEE Conference on Local Computer Networks (LCN), Tampa, Florida, November 2002.
[143]Houda labiod, “Réseaux mobile ad hoc et réseaux sans fils“, lavoisier, 2006.
[144]Touradj Ebrahimi and al, “Cryptographie et securité des systèmes et réseaux“, lavoisier , 2006.
[145]B.KADRI, M. Feham and M.ABDELLAH, “A new management scheme of cluster based PKI ", poster in 3rd international conference on e-business and telecommunication networks Portugal, 2006.
[146]J.-F. Raymond, “Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems,” Proc. Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, July 2000, pp. 7-26.
[147]S. Murphy, “Routing Protocol Threat Analysis,” Internet Draft, October 2002.
[148]S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon K. Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”, In Proceedings of the International Conference on Wireless Networks, Las Vegas, June, 2003.
[149]A.D. Wood, and J.A. Stankovic, “Denial of Service in Sensor Networks”, IEEE Computer, vol. 35, no. 10, October 2002, pp. 54-62.
[150] Patroklos Argyroudis and Donal O'Mahony, “Secure Routing for Mobile Ad hoc Networks”, IEEE Communications Surveys and Tutorials, vol. 7, no. 3, pp 2-21, 2005.
[151]Thomas Engel, Daniel Fischer, Thomas Scherer, and Dagmara Spiewak, “A Survey on Security Challenges in Next generation Mobile Networks”, The Third International

Conference on Mobile Computing and Ubiquitous Networking (ICMU 2006), London, UK, October 11-13 2006.
[152]Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks", IEEE Communication Societies (INFOCOM 2003), IEEE Press, pp. 1976-1986, 2003.
[153]B. Dahill, B. N. Levine, E. Royer, C. Shields, ARAN: A secure Routing Protocol for Ad Hoc Networks, UMass Tech Report 02-32, 2002.
[154]Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.
[155]Manel Guerrero Zapata, "Secure ad hoc on-demand distance vector routing", Mobile Computing and Communications Review Vol.6, No.3, pp 106-107, 2002.
[156]Panagiotis Papadimitratos, Zygmunt J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks", in the Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), pp 379, 2003.
[157]Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks", Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), 2002.
[158]Peter Gutmann, "Simplifying Public Key Management", IEEE computer society, 2004.
[159]S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad hoc Routing for Wireless Networks", Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, Long Beach, CA, USA, pp. 299-302, 2001
[160]David Culler, Deborah Estrin, and Mani Srivastava, "Overview of Sensor Networks", IEEE Computer society, Vol. 37, No. 8, pp. 41-49, 2004
[161]S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "The design of an acquisitional query processor for sensor networks," in In Proc. of (SIGMOD'03), San Diego, CA, June 2003.
[162]I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, Vol. 38, No. 4, pp 393–422.
[163]I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communication Magazine, vol. 40, no. 8, pp. 102–116, Aug. 2002.
[164]A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, vol. 47, no. 6, pp. 53--57, 2004.
[165]CITRIS, Center for Information Technology Research in the Interest of Society. Web Page. http://www.citris-uc.org
[166]Kazem Sohraby, Daniel Minoli, Taieb Znati, "WIRELESS SENSOR NETWORKS, Technology,Protocols,and Applications", by John Wiley &Sons,Inc, 2007.
[167]Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002) 'A Survey on Sensor Networks', IEEE Communications Magazine, vol 40 issue 8, pp 102-114, 2002.

[168]Carlos F.Garcia-hermandez and al, "Wireless sensor networks and applications", International Journal of Computer Science and Network Security, Vol.7, No.3, pp. 264-273, March 2007.
[169]Aditya K. Gupta, Sandhya Sekhar, and Dharma P. Agrawal, "Efficient Event Detection by Collaborative Sensors and Mobile Robots", In Ohio Graduate Symposium on Computer and Information Science and Engineering, Dayton, Ohio, June 2004.
[170]L. Schwiebert, S.D.S. Gupta, and J. Weinmann, "Research challenges in wireless networks of biomedical sensors", MobiCom 2001

[171]X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan. Sensor network configuration under physical attacks. Technical Report Technical Report (OSU-CISRC-7/ 04-TR45), Dept. of Computer Science and Engineering, The Ohio-State University, July 2004.
[172]Kahn,J.M.,Katz,R.H.,and Pister,K.S.J.,Next century challenges:mobile networking for smart dust,Proceedings of the ACM MOBICOM Washington,D.C.,1999, pp.271-278.
[173] J. Chang and L. Tassiulas, "Energy Conserving Routing in Wireless Ad-hoc Networks," Proceedings of IEEE Infocom, pp. 22-31, 2000.
[174]J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva, "A Performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols". In Proc. Of 4th Annual ACM/IEEE International Conference on Mobile Computing(MOBICOM), ACM, October 1998.
[175]A. Manjeshwar and D. P. Agrawal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," In Proc. Of 15th International Parallel and Distributed Processing Symposium (IPDPS '01) Workshops, 2001.
[176]A. Manjeshwar and D. P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," In Proc. Of International Parallel and Distributed Processing Symposium (IPDPS '02) Workshops, 2002
[177] J. Hill, R. Szewczyk, A.Woo, S. Hollar, D. Culler, and K. Pister, "System Architecture Directions for Network Sensors," In Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems, pp. 93–104, November 2000.
[178]O.Moussaoui and al, "Efficient saving in wireless sensor networks through hierarchical-based clustering", In proceeding of the international IEEE Global Information Infrastructure Symposium, Marrakeche, Morocco, pp. 226-229, July, 2007.
[179]H. Chan and A. Perrig. Security and privacy in sensor networks. IEEE Computer Magazine, pages 103-105, 2003.
[180]D. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," in Proc. of 1stIEEEInternational Conference on Sensor and Ad Hoc Communications and Networks, Oct 2004.
[181]Wander, A.S., Gura, N., Eberle, H., Gupta, V., and Shantz, S.C., "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", In proceedings of PerCom pp. 324-328, 2005.
[182]J. Deng, R. Han, and S. Mishra. Countermeasuers against traffic analysis in wireless sensor networks. Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.
[183]S. Basagni, K. Herrin, E. Rosti and Danilo Bruschi. "Secure Pebblenets", Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, pp. 156 – 163, 2001.
[184]L. Eschenauer, V.D. Gligor, "A key-management scheme for distributed sensor networks", in Proceedings of the 9th ACM conference on Computer and Communication Security, pp. 41-47, November 2002.
[185]H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," In IEEE Symposium on Security and Privacy, Berkeley, California, pp. 197–213, May 2003.
[186]Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," In ACM CCS 2003, pp. 62–72, October 2003
[187]D. Liu and P. Ning, "Location-Based Pairwise Key Establishments for Relatively Static Sensor Networks," in 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03), October 31, 2003 George W. Johnson Center at George Mason University, Fairfax, VA, USA.

[188]C. Karlof, N. Sastry, and D. Wagner. Tinysec “A link layer security architecture for wireless sensor networks”, In Second ACM Conference on Embedded Networked Sensor Systems (SensSys 2004), pp. 162–175, November 2004.
[189]Perrig and al. “SPINS: Security Protocols for Sensor Networks”, Mobile Computing and Networking, pp.189-199, 2001 Rome, Italy.
[190]Benamar KADRI, Mohammed FEHAM, Abdallah M’HAMED. “A new management scheme of cluster based PKI for ad hoc networks using multi-signature”, In proceeding of the international IEEE Global Information Infrastructure Symposium, Marrakeche, Morocco, pp 167-172, 2007.
[191]S.Banerjee and S.Khuller. A clustering scheme for hierarchical control in multi-hop wireless networks. Proc. IEEE INFOCOM’2001, 2001.
[192]R. C. Merkle. Protocols for public key cryptosystems. In Proceedings of the IEEE Symposium on Research in Security and Privacy, April 1980.
[193]R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus. Tinypk, “securing sensor networks with public key technology”. In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN ’04), pp 59–64, 2004.
[194]Johann.G, Alexander.S, Stefan.T. “The Energy Cost of Cryptographic Key Establishment”, in Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, pp. 380–382, (ASIACCS 2007).
[195]J. T. Kohl and B. C. Neuman. The Kerberos Network Authentication Service (Version 5). Internet Engineering Task Force (IETF), Internet Draft RFC 1510, Sept. 1993.
[196]D. Hankerson, A. Menezes, S. Vanstone, “Guide to Elliptic Curve Cryptography”, Springer-Verlag New York, ISBN 0-387-95273-X, Inc. 2004.
[197]N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz, “Comparing elliptic curve cryptography and RSA on 8-bit CPUs”, in Proceedings of the Sixth Workshop on Cryptographic Hardware and Embedded Systems (CHES'04), Cambridge, MA, USA, pp. 119-132, 2004.
[198]Crossbow Technology Inc., Processor/Radio Modules, http://www.xbow.com/
[199]R. Min, M. Bhardwaj, N. Ickes, A. Wang, and A. Chandrakasan, “The hardware and the network: Total-system strategies for power aware wireless microsensors,” in Proc. of the IEEE CAS Workshop on Wireless Communications and Networking, Pasadena, CA, USA, Sep. 2002.
[200]W.R.Heinzelman, A.Chandrakasan, and H.Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In HICSS, 2000.
[201]S. Narayanaswamy, V. Kawadia, R. S. Sreenivas, and P. R. Kumar, “Power control in ad-hoc networks: Theory, architecture, algorithm and implementation of the COMPOW protocol,” in Proc. of European Wireless 2002. Next Generation Wireless Networks: Technologies, Protocols, Services and Applications, Florence, Italy, Feb. 25-28 2002, pp. 156–162.
[202]S. Singh and C. Raghavendra, “Power efficient MAC protocol for multihop radio networks,” in The Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 1998, pp. 153–157.
[203]S. Singh, M. Woo, and C. S. Raghavendra, “Power-aware routing in mobile ad hoc networks,” in Mobile Computing and Networking, 1998, pp. 181–190.
[204]H. Ju, I. Rubin, and Y. Kuan, "An Adaptive RTS/CTS Control Mechanism for IEEE 802.11 MAC Protocol", in Proceedings of IEEE Vehicle Technology Conference (VTC), vol.2, April 2003, pages:1469 – 1473
[205]S. Xu and T. Saadawi, “Revealing the problems with IEEE 802.11 medium access control protocol in multi-hop wireless ad hoc networksln, Computer Networks: The International

Journal of Computer and Telecommunications Networking, Vol. 38, No. 4, March 2002, pages 531 Œ 548
[206]Hossam Hassanein, Tiantong You, Hussein T.Mouftah, Infrastructure-based MAC in wireless mobile ad-hoc networks", Ad Hoc Networks vol 3, pp 717 –743, 2005.
[207]Sunil Kumar,Vineet S.Raghavan,Jing Deng, "Medium Access Control protocols for ad hoc wireless networks:A survey", Ad Hoc Networks, vol 4, 2006, pp 326-258.
[208]E.S.Jung,N.H.Vaidya, "A Power Control MAC protocol for ad hoc networks", in ACM International Conference Mobile Computing and Networking (MOBICOM),September 2002.
[209]C.-H.Yeh,H.Zhou,"A new class of collision-free MAC protocols for ad hoc wireless networks", in the Proceedings of the Intertnational Conference on Advances in Infrastructure for e-Business,e-Education,e-science,and e-Medicine on the Internet,January 2002.
[210]ORiNOCO. Orinoco wavelan radio. http://www.orinoco.com , 2000.
[211]B.KADRI and M.Feham, "Power control issues in 802.11 MAC layer for mobile ad hoc networks ", International Conference of Web and Information Technologies, ICWIT'08, 2008.

- **International Publications:**

  - B.KADRI, M.Feham, and M.ABDELLAH, “Lightweight PKI for WSN (µPKI)", International Journal of Network Security, Vol.10, No.3, PP.194–200, May 2010.
  - B.KADRI, M.Feham, and M.ABDELLAH, “Securing reactive routing protocols in MANETs using PKI (PKI-DSR)", accepted in the journal of security and communication networks, Wiley 2008.
  - B.KADRI, M. Feham and M.ABDELLAH,” Secured Clustering Algorithm for Mobile Ad hoc Networks”, international Journal of Computer Science and Network Security, 2007.
  - Benamar KADRI, Mohammed FEHAM, Abdallah M’HAMED, “A PKI over ant-colony based routing algorithms for MANETs AntPKI”, sent to the International Journal of Network Security.

- **International communications:**

  - B.KADRI and M.Feham, “Power control issues in 802.11 MAC layer for mobile ad hoc networks ", International Conference of Web and Information Technologies, ICWIT'08, 2008.
  - B.KADRI, D. Moussaoui and M.Feham, “A cross layer design for QoS implementation for ad hoc networks applied to DSR", IEEE international conference on information and communication technologies from theory to application, IEEE ICTTA 2008.
  - B.KADRI, M. Feham and M.ABDELLAH, “Weight based DSR for Mobile ad hoc networks", IEEE international conference on information and communication technologies from theory to application, IEEE ICTTA 2008.
  - B.KADRI, M. Feham and M.ABDELLAH, “A new management scheme of cluster based PKI using multi-signature", IEEE International Global Information Infrastructure Symposium, 2007.
  - B.KADRI, M. Feham and M.ABDELLAH, “A new management scheme of cluster based PKI ", accepted as poster in 3rd international conference on e-business and telecommunication networks Portugal, 2006.

- **Papers waiting for response:**

  - Benamar KADRI, Mohammed FEHAM, Amine ADJEZIRI, Nabil LASSAR, “Cluster based µPKI pour les réseaux de capteurs sans fil”, sent to a national conference 2009.
  - Benamar KADRI, Abdallah M’HAMED, Mohammed FEHAM, “Link Quality Based Ant Routing Algorithm for MANETs (LQARA)”.

- **Other Activities:**

  - Member of STIC Labs. University of Tlemcen, Algeria.
  - Member of IEEE Communications and Information Security Technical Committee, a committee responsible of organizing IEEE sponsored and co-sponsored conferences having a security track over the world, http://www.comsoc.org/cistc/
  - Contribute in many international conferences as member of their Technical Program Committee:
    - The Communication and Information Security Symposium (CISS), IEEE ICC'09-CISS, June 14-18, 2009. Dresden, Germany.
    - The second International Conference on New Technologies, Mobility and Security, NTMS'2008. 5-7 November, 2008 in TANGIER, MOROCCO**.** http://www.ntms-conference.org/ntms-ommittees.html.
    - IEEE Global Communications Conference, IEEE GLOBECOM 2008. 30 November to 4 December 2008, New Orleans, USA. http://www.comsoc.org/confs/globecom/2008/ techprog.html**.**
    - International Workshop on Multimedia Security in Communication, IEEE MUSIC'08. 25-27 August 2008, Hangzhou, China. http://www.music-com.org.
    - Fifth Annual IEEE Consumer Communications & Networking Conference, IEEE CCNC 2008. 10-12 January 2008 in Las Vegas, Nevada, USA. http://cms.comsoc.org/CCNC_2008/Content/Home/Committee.html
    - The 2nd IEEE International Conference on Wireless Broadband and Ultra Wideband Communications, IEEE-AusWireless 2007. 27–30 august 2007 in Sydney, Australia. http://auswireless.eng.uts.edu.au/index.htm , (www.ieee.org).
  - Help in reviewing in the international journal of network security.
  - Supervisor of many engineer licence and DEUA projects at the university of Tlemcen in different departments:
    - GUEUZZEN Youcef, YOUBI Abdelmounaim, "proposition d'un protocol d'économie d'énergie TMM-DSR pour les réseaux de capteurs",2008/2009.
    - DEJEZIRI Med amine, LASSAR Nabil, " securité dans les réseaux de capteurs cluster based µPKI", 2008/2009.
    - SAKHI Hakim, SEBAGH Abderahmane, " Gestion de paie " ,2008/2009.
    - MEHAMMEDI Fatima Zohra, " gestion de personnel ", 2008/2009.
    - MEHAMMEDI MOHAMMED, "développement d'une application mobile pour l'exploitation du coran MobileCoran " ,2007/2008.
    - CHELDA WAFAA, BENSOUNA KHADIJA,"la sécurisation des échanges SMS sur les réseaux GSM, SMS encryption System (SMS-ES)", 2006/2007.
    - AMAMOU NAWEL, " gestion d'un établissement" ,2009/2007.
    - SLATNA FATIHA, MAROUF FATIMA,"gestion du personnel au niveau de la CANAS", 2005/2006.
    - BENDAHOU ABDERRAHIM, BENAHCEN ISMAIL, "gestion de scolarité ",2005/2006.