Vandana Publications
IJEMR

Volume-7, Issue-2, March-April 2017
International Journal of Engineering and Management Research
Page Number: 201-207

An Efficient Performance and Security in Mobile Ad Hoc Wireless Sensor Networks

M. Baby Anusha[1], Gayathri Parasa[2]
[1]Assistant Professor NRI Institute of Technology, INDIA
[2]Assistant Professor MVR College of Engineering, INDIA

ABSTRACT

A Mobile Ad-hoc NETwork (MANET) is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. One of the main issues in such networks is performance- in a dynamically changing topology; the nodes are expected to be power-aware due to the bandwidth constrained network. Another issue in such networks is security - since every node participates in the operation of the network equally, malicious nodes are difficult to detect. There are several applications of mobile ad hoc networks such as disaster recovery operations, battle field communications, etc. To study these issues, a scenario based simulation analysis of a secure routing protocol is done and is compared with traditional non-secure routing protocols. The scenarios used for the experiments depict critical real-world applications such as battlefield and rescue operations, which tend to have contradicting needs. An analysis of the tradeoffs between performance and security is done to gain an insight into the applicability of the routing protocols under consideration.

Keywords -- MANET, Battle field, ad hoc networks, tradeoffs.

I. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. The latest trend in wireless networks is towards *pervasive and ubiquitous computing* - catering to both nomadic and fixed users, anytime and anywhere. Several standards for wireless networks have emerged in order to address the needs of both industrial and individual users. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). In such a network, a set of mobile nodes are connected to a fixed wired backbone. WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium. For example, consider communication amongst soldiers in a battlefield, involving troops spread out over a large area. In this case, it is not only feasible to deploy a fixed wireless access point, but also risky since an enemy attack would bring down the whole network. This problem has led to a growing interest among the research community in *mobile ad hoc networks*, wireless networks comprised of mobile computing devices communicating without any fixed infrastructure. The rest of this chapter is organized as follows – initially a classification of wireless networks in use today is described followed by the background and origins of ad hoc wireless networks. The general issues in ad hoc wireless networks are then discussed, followed by a few interesting applications. The final section gives an outline of the chapters to follow.

1.1 Mobile Ad hoc and Sensor Networks

Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure.

Thus, each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes.

A sensor network is a special category of ad hoc wireless networks which consists of several sensors deployed without any fixed infrastructure. The difference between sensor networks and ordinary ad hoc wireless is that the sensor nodes may not be necessarily mobile. Further, the number of nodes is much higher than in ordinary ad hoc networks. The nodes have more stringent power requirements since they operate in harsh environmental conditions. An example of a sensor network is a set of nodes monitoring the temperature of boilers in a thermal plant. Other application domains include military, homeland security and medical care.

1.2 General Issues in Mobile Ad hoc Networks

In a mobile ad hoc network, all the nodes co-operate amongst each other to forward the packets in the network and hence, each node is effectively a router. Thus one of the most important issues is routing. This thesis focuses mainly on routing issues in ad hoc networks. In this section, some of the other issues in ad hoc networks are described.

(a) Distributed network*:* A MANET can be considered as a distributed wireless network without any fixed infrastructure. By distributed, it is meant that there is no centralized server to maintain the state of the clients, similar to peer-to-peer (P2P) networks.

(b) Dynamic topology*:* The nodes are mobile and hence the network is self-organizing. Due to this, the topology of the network keeps changing with time. Hence the routing protocols designed for such networks must also be adaptive to the changes in the topology.

(c) Power awareness*:* Since the nodes in an ad hoc network typically run on batteries and deployed in hostile terrains, they have stringent power requirements. This implies that the underlying protocols must be designed to conserve battery life, or in other words, they must be power aware.

(d) Addressing scheme*:* The network topology keeps changing dynamically and hence the addressing scheme used is quite significant. A dynamic network topology entails a ubiquitous addressing scheme, which avoids any duplicate addresses. Mobile IP is currently being used in cellular networks where a base station handles all the node addressing. However, such a scheme doesn't apply to ad hoc networks due to their decentralized nature.

(e) Network size*:* Commercial applications of ad hoc networks such as data sharing in conference halls, meetings, etc. are an attractive feature of ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network.

(f) Security*:* Security in an ad hoc network is of prime importance in scenarios of deployment such as battlefield. The three goals of security - confidentiality, integrity and authenticity are very difficult to achieve since every node in the network participates equally in the network.

II. ROUTING IN MANETS

Unlike wired networks, routing in MANETs poses unique challenges. Designers of routing protocols for MANETs need to address several issues. In this chapter these issues are identified and the routing protocols available for MANETs are classified. Then working principle of a few protocols such as DSDV, DSR, AODV, etc. are explained. Their pros and cons are also identified. This chapter concludes with a summary of routing in MANETs.

2.1 Design Issues

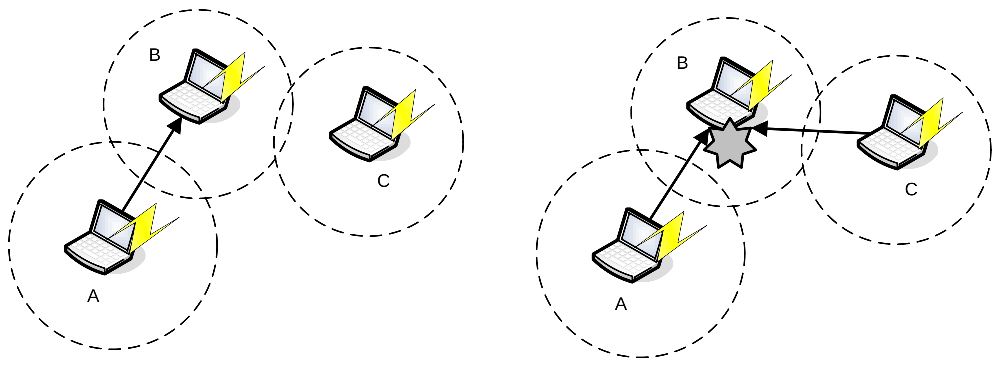
The following design issues must be considered before designing a routing protocol for MANETs [1]-

(a) Dynamic Topology: In a MANET, the network topology keeps changing with time due to the movement of the nodes, and hence the links between the nodes suffers frequent breaks. Thus the ordinary routing protocols for wired networks are not efficient since they are designed for static networks.

(b) Bandwidth constraint: The nodes in the network have a relatively low bandwidth when compared to traditional wired networks. This is an important issue to consider when designing routing protocols for MANETs since the utilization of bandwidth by the routing protocol in the network must be minimized.

(c) Error prone broadcast channel: The nodes in the MANET broadcast the information to all the neighboring nodes on the wireless channel. The channel itself is prone to several errors such as attenuation, multi-path fading, etc. Thus the routing protocol itself must be designed taking into consideration these issues.

(d) Hidden and exposed terminal Problems: The hidden terminal problem is shown in Figure 2.1.



A transmits data to B but C doesn't hear it

C transmits to B - Collision

Figure 2.1: The Hidden Terminal Problem

This problem occurs in networks using contention based protocols such as ALOHA, CSMA/CD, etc. When two nodes which are out of range of each other send data frames to a node which is within their respective radio ranges, a collision of data frames occurs. As shown in Figure.2.1, when both nodes A and C transmit data frames to node B a collision occurs. This problem can be resolved by using a mechanism called RTS/CTS handshake [2].

The exposed node problem is shown in Figure.2.2. An exposed node is one which is in the range of the transmitter, but out of the range of the receiver. In Figure.2.2, when node C is transmitting to node D, B overhears this and is blocked. Now if node B wants to transmit to node A, it cannot do so.

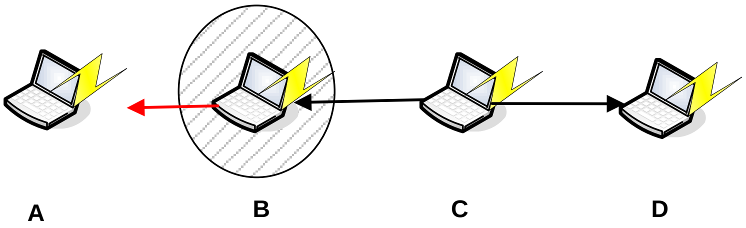


Figure 2.2: The Exposed Terminal Problem

This results in wasted bandwidth. The hidden and exposed terminal problems occur at the MAC layer and prevent successful transmission of data packets. This, in turn also affects the design of the routing protocol. In order to prevent this, the routing protocol must reduce the number of broadcast packets to minimize collisions.

(e) Resource limitations: As discussed in chapter 1, MANETs consist of nodes such as PDA, laptops, etc. which have stringent power requirements. Further, some of these devices have limited processing power. Thus the routing protocols must be efficient in terms of power conservation.

(f) QoS limitations: For applications such as multimedia, QoS guarantees must be provided by the routing protocol. However, such guarantees come at the cost of higher latency and poor performance since multimedia applications require higher bandwidth and traffic rates.

Security: Due to on open environment where MANETs are typically deployed, the routing protocols are prone to several attacks. Further, there is also the issue of secure key distribution.

III. SECURITY IN MANETS

MANETs have certain unique characteristics that make them vulnerable to several types of attacks. Since they are deployed an open environment where all nodes co-operate in forwarding the packets in the network, malicious nodes are difficult to detect. Hence, it is quite difficult to design a secure protocol when compared to wired or infrastructure-based wireless networks. This section discusses some of the issues and challenges that a designer of secure protocols faces. These issues are analyzed with respect to the primary goals of a secure protocol – confidentiality, integrity and availability, authenticity and non-repudiation. The attacks and threats allowed by existing MANET routing protocols are then discussed. The working of a few secure routing protocols which address these threats such as SEAD, ARIADNE, ARAN and SRP is then described. The next section discusses another important issue in MANETs- certificate-based authentication. It surveys some mechanisms proposed and analyzes the requirements for effective certificate-based authentication in MANETs.

3.1 Secure Routing in MANETs

This thesis primarily focuses on the security issues from a network layer perspective. As discussed in chapter 2, several routing protocols for MANETs exist though none of them address the most important issue, namely, security. In order to study the attacks and threats, and to devise a protocol which addresses them, an understanding of the operating environment is needed.

The environment can be a *managed environment*, where a common trusted authority exists such as a RADIUS server or it can be an *open environment* where there is no a priori trust relationship between the nodes. For example in a battlefield, the nodes have a common trust authority which executes the key management functions. MANETs typically fall in to the open environment type since the nodes are mobile and they establish a connection dynamically. Another possible type of environment is the *managed-open* environment, where the nodes have already established some security infrastructure. This acts as a starting point for establishing the trust relationship between nodes. Several certificate based authentication mechanisms to be discussed in section 3.4 assume such an environment. Furthermore, the environment can be *managed-hostile*, which depicts scenarios such as military networks, where security is of prime importance.

3.1.1 Attacks and Exploits on the Existing Routing Protocols

The attacks on routing protocols can generally be classified as *routing disruption* attacks (attacker tries to disrupt the routing mechanism by routing packets in wrong paths) and *resource consumption* attacks (some non-cooperative or selfish nodes may try to inject false packets in order to consume network bandwidth). Both these attacks are examples of Denial of Service (DoS) attacks. Figure 3.2 depicts a broader the classification of the possible attacks in MANETs.

3.2.2 Secure and Efficient Ad hoc Distance vector (SEAD) routing protocol

The *Secure and Efficient Ad hoc Distance vector routing protocol* (SEAD) [16] is based upon the *DSDV-SQ* routing protocol (which is a modified version of *DSDV* routing protocol). It uses efficient one-way hash functions to authenticate the lower bound of the distance metric and sequence number in the routing table. More specifically, for authenticating a particular sequence number and metric, the node generates a random initial value **x € (0,1)**$^{\rho}$ where ρ□is the length in bits of the output of the hash function, and computes the list of values h_0,h_1,h_2,h_3,…,h_n, where h_0=*x* , and h_i = H(h_{i-1}) for 0<*i* ≤ *n* , for some *n*. As an example, given an authenticated *hi* value, a node can authenticate $h_{i-3}$by computing **H (H (H (*h*$_i$-*3*)))** and verifying that the resulting value equals h_i.

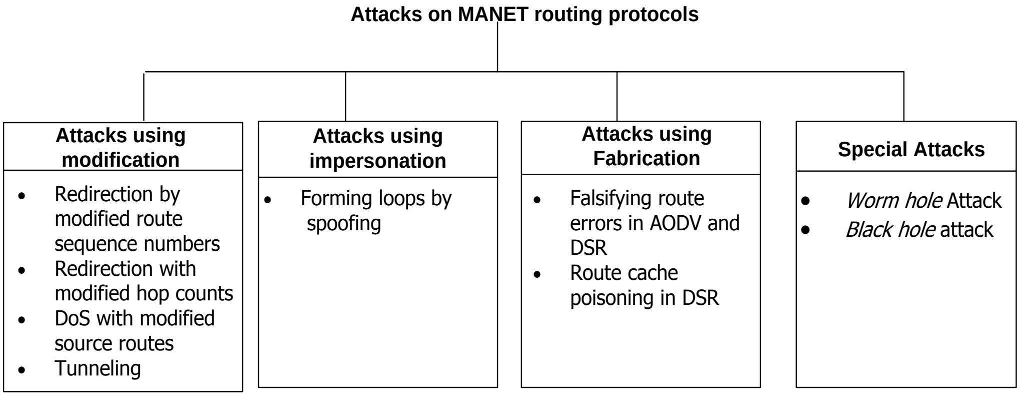

Attacks on MANET routing protocols
Attacks using modification
Redirection by modified route sequence numbers
Redirection with modified hop counts
DoS with modified source routes
Tunneling
Attacks using impersonation
Forming loops by spoofing
Attacks using Fabrication
Falsifying route errors in AODV and DSR
Route cache poisoning in DSR
Special Attacks
Worm hole Attack
Black hole attack

Figure 3.2: Classification of attacks on MANET routing protocols

IV. SIMULATION STUDY OF PERFORMANCE IN MANETS

4.1 Introduction

Over the past few years there has been a growing interest in the research community for simulation study of performance in MANETs since there is a lack of necessary infrastructure for MANETs to be deployed in a realistic scenario. A simulation study gives us an idea of how a protocol performs when it is practically employed. This approach is similar to the prototyping model in software engineering realm. However, the main challenge in the simulation study of MANETs is the dynamic nature of the network topology and the physical environment in which the nodes operate. In order to gain an insight of how a protocol performs when deployed in a realistic scenario, it is imperative that the simulation capture the exact nature of the physical environment and the movement of the nodes in the network, which might not be possible in all cases. For example consider a scenario where a set of nodes are deployed in a rescue operation. Even though the mobility of the nodes can be captured with certain realistic mobility models, the node doesn't capture the exact physical environment in which the nodes operate, such as uneven terrains, catastrophic failure of the nodes, etc.

This chapter discusses the simulation study of performance in MANETs using the network simulator ns-2 and certain realistic mobility models used to model the movement of the nodes. It is followed by a step-by-step tutorial for simulation study of MANET routing protocols using ns-2. A set of experiments conducted to study the performance of AODV in a battlefield scenario is then explained.

4.2 The ns-2 network simulator

Ns-2 is an open source discrete event simulator used by the research community for research in networking [30]. It has support for both wired and wireless networks and can simulate several network protocols such as TCP, UDP, multicast routing, etc. More recently, support has been added for simulation of large satellite and ad hoc wireless networks. The ns-2 simulation software was developed at the University of Berkeley. It is constantly under development by an active community of researchers. The latest version at the time of writing this thesis is ns-2 2.28.

The standard ns-2 distribution runs on Linux. However, a package for running ns-2 on Cygwin (Linux Emulation for Windows) is available. In this mode, ns-2 runs in the Windows environment on top of Cygwin as shown in the figure 4.1. The simulations performed (discussed in following sections) have been run in this environment.

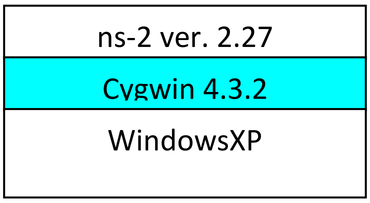


Figure.4.1: ns-2 over Cygwin

NS-2 provides a split-programming model; the simulation kernel is implemented using C++, while the Tcl scripting language is used to express the definition, configuration and the control of the simulation. This split-programming approach has proven benefits over conventional programming methods. Also, NS-2 can produce a detailed trace file and an animation file for each ad hoc network simulation that is very convenient for analyzing the routing behavior.

List of Parameters:

- Type of traffic: CBR or TCP
- Seed: starting number for random number generator
- Nr: number of node
- Nc: maximum number of connection
- Rate: number of packet per second (bit rate)

The output values can be written to a file using the > directive on the command line. This file can be used as an input to the Tcl script which is described in a later section.

(ii)setdest utility: The setdest utility developed at CMU is used to generate node movements according to the Random Waypoint Model [31]. It is available under **~ns/indep-utils/cmu-scen-gen/setdest** directory and consists of setdest{.cc,.h} and Makefile. The utility can be run with the following arguments-

**./setdest [-n num_of_nodes] [-p pausetime] [-s maxspeed] [-t simtime] **
[-x maxx] [-y maxy] > [outdir/movement-file]

The outdir/movement file specifies the output file which can be integrated with the simulation script as described in the tutorial section.

(iii) Network Animator (nam)*:* The network animator (nam) is a graphical tool used to visualize the simulation results graphically and trace the packet flow in a network as shown below –

4.4.3 Results

i. Effect of varying the number of nodes

The number of nodes was varied from 50 to 100 and the effect on PDF, NRL and AED was studied. The results can be found in table 4.3 and figures 4.3, 4.4 and 4.5.

No. Of Nodes	Packet Delivery Fraction (%)	Average End-end delay (sec)	Normalized Routing Load
50	99.91438	0.006738278	0.2570694
60	100	0.006566893	0.3088803
70	100	0.013576984	0.42168674
80	99.95756	0.032688957	0.47558385
90	99.95761	0.010179137	0.49618322
100	99.872444	0.010737591	0.553427

Table 4.3: Effect of varying the number of nodes

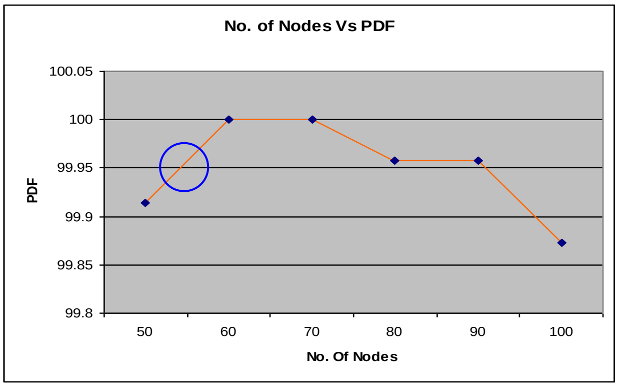


Figure 4.3: Effect of varying the number of nodes on the pause time

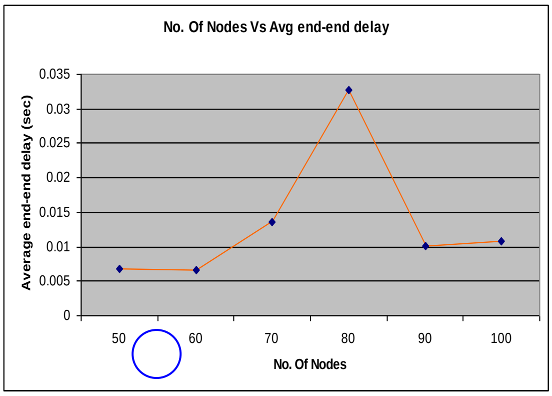


Figure 4.4: Effect of varying the number of nodes on the Average end-end delay

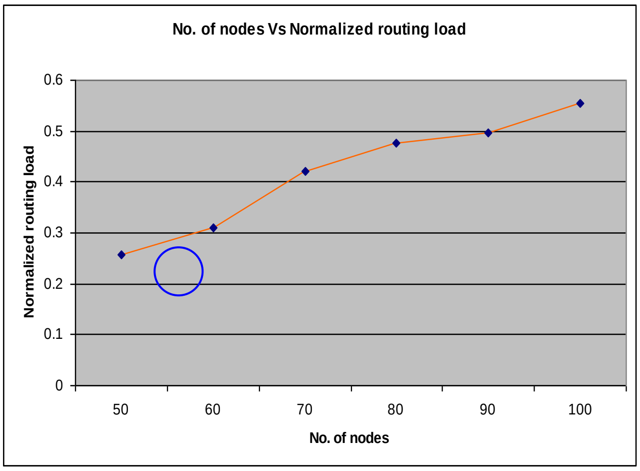


Figure 4.5: Effect of varying the number of nodes on the Normalized Routing Load

The blue circles in figures 4.3, 4.4 and 4.5 represent the "optimal points" which corresponds to the highest PDF, lowest end-to-end delay and the lowest normalized routing load. It is found that for 60 nodes we achieve this optimal point.

REFERENCES

[1] C. Siva Ram Murthy, B.S. Manoj, "*Ad Hoc Wireless Networks : Architectures and Protocols*", Prentice Hall Publishers, May 2004, ISBN 013147023X

[2] C.-K. Toh, "*Ad Hoc Mobile Wireless Networks: Protocols and Systems*", Prentice Hall publishers, December 2001, ISBN 0130078174

[3] C. Perkins and P. Bhagwat, *Highly Dynamic Destination-Sequenced Distance-Vector Routing* (*DSDV*) for Mobile Computers. In Proc. of the ACM SIGCOMM, October 1994.http://www.cs.umass.edu/~mcorner/courses/691M/papers/perkins.pdf

[4] Shree Murthy, J.J. Garcia-Luna-Aveces, "*A Routing Protocol for Packet Radio Networks*," Proc. ACM International Conference on Mobile Computing and Networking, pp. 86-95, November, 1995 http://www.pdos.lcs.mit.edu/decouto/papers/dube97.pdf

[5] C.-C. Chiang, "*Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel*," Proc. IEEE SICON '97, Apr. 1997, pp. 197–211. http://www.ics.uci.edu/~atm/adhoc/paper-collection/gerla-routing-clustered-sicon97.pdf

[6] [online] The Secan Lab, University of Luxembourg, Luxembourg. http://wiki.uni.lu/secan-lab/Distributed+Bellman-Ford.html

[7] [online] The Secan Lab, University of Luxembourg, Luxembourg. http://wiki.uni.lu/secan-lab/Count-To-Infinity+Problem.html

[8] D B. Johnson, D A. Maltz, and Y. Hu, "*The dynamicsourcerouting protocol for mobile ad hoc network*," Internet-Draft, April 2003. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[9] C.E. Perkins, E. Royer, and S.R. Das, "*Ad hoc on demand distance vector (AODV) routing*," Internet Draft, March 2000. http://www.ietf.org/internetdrafts /draft-ietf-manet-aodv-05.txt

[10] Samir R. Das, Charles E. Perkins, Elizabeth M. Royer and Mahesh K. Marina. *"Performance Comparison of Two On-demand Routing Protocols for Ad hoc Networks."* IEEE Personal Communications Magazine special issue on Ad hoc Networking, February 2001, p. 16-28. http://www.ronai.hu/./../library/Performance_comparison_of_AODV_and_DSR-Perkins.pdf

[11] David B Johnson and David A Maltz. "*Dynamicsourcerouting in adhocwirelessnetworks*". In Imielinski and Korth, editors, Mobile Computing, volume 353. Kluwer Academic Publishers, 1996.

[12] Haas Z.J, " *A new routing protocol for the reconfigurable wireless network*". In Proceedings of the 1997 IEEE 6th International Conference on Universal Personal Communications, ICUPC '97, San Diego, CA, October 1997; pp. 562 -- 566. http://www.ics.uci.edu/~atm/adhoc/paper-collection/haas-routing-protocol-icupc97.ps.gz

[13] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding royer. *"A Secure Routing Protocol for Ad Hoc Networks" (ARAN)* In International Conference on Network Protocols (ICNP), Paris, France, November 2002. www.cs.ucsb.edu/~kimaya/icnp2002.pdf

[14] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, "*Mobile Ad Hoc Networking*", ISBN: 0-471-37313-3, Wiley-IEEE Press: *Chapter 12: Ad hoc networks Security* Pietro Michiardi, Refik Molva http://www.eurecom.fr/~michiard/pub/michiardi-adhoc.pdf

[15] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "*Routing Security in Wireless Ad Hoc Network*," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[16] Yih-Chun Hu, David B. Johnson, Adrian Perrig. *"SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks"*, Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp: 3-13, Jun 2002. http://www.cs.colorado.edu/~rhan/CSCI_7143_001_Fall_2002/Papers/Perrig2002_wmcsa02.pdf

[17] Yih-Chun Hu, Adrian Perrig, David B. Johnson. *"Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks"* MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA. http://lambda.cs.yale.edu/cs425/doc/ariadne.pdf

[18] A. Perrig, R. Canetti, D. Tygar, and D. Song, "*The TESLA Broadcast Authentication Protocol*," Cryptobytes,, Volume 5, No. 2 (RSA Laboratories, Summer/Fall 2002), pp. 2-13. http://www.rsasecurity.com/rsalabs/cryptobytes/

[19] P. Papadimitratos and Z. Haas. *"Secure routing for mobile ad hoc networks" (SRP)* SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp. 27--31, January 2002. http://wnl.ece.cornell.edu/Publications/cnds02.pdf