Vol.2 Issue.4, Pg.: 215-223
April 2014

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

RESEARCH ARTICLE

THE SIMULATION STUDY OF PROTOCOL PERFORMANCE AND SECURITY IN MOBILE AD HOC NETWORKS

T. MURUGESH[1], M.ELAMPARITHI[2], MCA, M.Phil

[1]**Research Scholar, Sree Saraswathi Thyagaraja College,Pollachi – 642 107,**

[2]**Assistant Professor, Department of MCA, Sree Saraswathi Thyagaraja College,Pollachi – 642 107**

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, Performance, Security, Simulation.

1. INTRODUCTION

A wireless network in general consists of a set of mobile hosts which communicate to other mobile hosts either directly or via an access point (base station). The following is a broad classification of wireless networks-

1.1 Wireless LANs and PANs

A Wireless Local Area Network (WLAN) consists of a set of mobile users communicating via a fixed base station or an access point. The mobile node can be any device such as a palmtop, PDA, laptop etc. as shown in Figure 1.1.

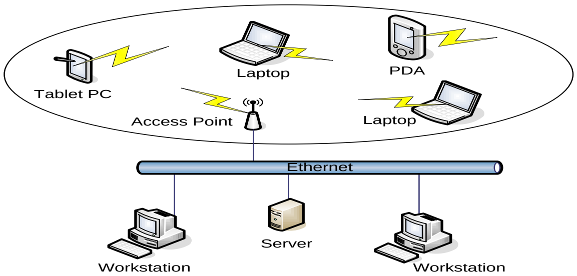

Figure 1.1: Wireless LAN

Such networks are usually deployed in offices, cafeterias, universities, etc. and are most prevalently used nowadays. There are three types of WLANs – Independent Basic Service Set (**IBSS**), Basic Service Set (**BSS**) and Extended Service Set (**ESS**). A detailed classification is beyond the scope of this thesis. IEEE 802.11 is an adopted international standard for wireless LANs which provides transmission speeds ranging from 1 Mbps to 54 Mbps in either the 2.4 GHz or 5 GHz frequency bands. The latest version of this standard in use today is IEEE 802.11g which provides a bandwidth of up to 54 Mbps.

A Wireless Personal Area Network (WPAN) consists of personal devices which communicate without any established infrastructure. The IEEE 802.15.1 standard for Wireless Personal Area Networks, also called popularly as the Bluetooth is currently being used for short range communication such as in digital cameras, PDAs, laptops, etc.

1.2 Wireless WANs and MANs

Nowadays, the trend is towards a *wireless internet* consisting of mobile nodes accessing the internet without the help of any backbone network. This type of network is based on the *cellular* architecture in which a large area to be covered is divided in to several cells, each having a fixed base station. Each cell consists of several mobile terminals (MT) which communicate to other mobile terminals in a same cell through the base station as shown in Figure1.2.

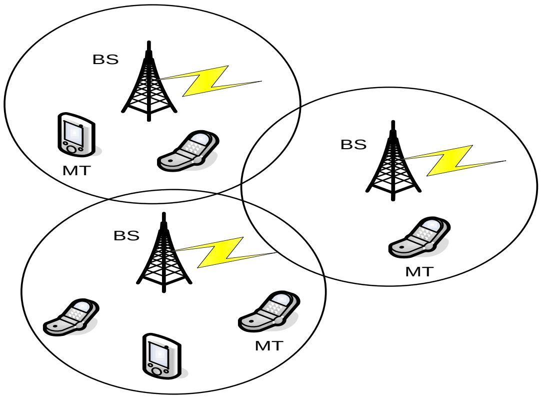

Figure 1.2: A Cellular network

The communication between nodes in different cells is carried on by a procedure called *handoff* which involves communication between the base stations in the two cells. Cellular networks have constantly evolved from the First Generation Cellular Systems (1G) to the Third Generation Systems (3G). Today, most wireless data communication takes place across 2G cellular systems such as TDMA, CDMA, PDC, and GSM, or through packet-data technology over old analog systems such as CDPD overlay on AMPS. Although traditional analog networks, having been designed for voice rather than data transfer, have some inherent problems, some 2G (second generation) and new 3G (third generation) digital cellular networks are fully integrated for data/voice transmission. With the advent of 3G networks, transfer speeds should also increase greatly.

Wireless Metropolitan Area Networks (WMANs) are networks that typically span several kilometers and cover large parts of cities. The IEEE 802.16 which is based on the OSI model is a standard used for such types of networks. It is mostly used for real time data and multimedia applications such as digital video and telephony.

Wireless WANs, which can bridge branch offices of a company, cover a much more extensive area than wireless LANs. In wireless WANs, communication occurs predominantly through the use of radio signals over analog, digital cellular, or PCS networks, although signal transmission through microwaves and other electromagnetic waves is also possible.

1.3 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. As shown in Figure.1.3, there are no base stations and every node must co-operate in forwarding packets in the network.

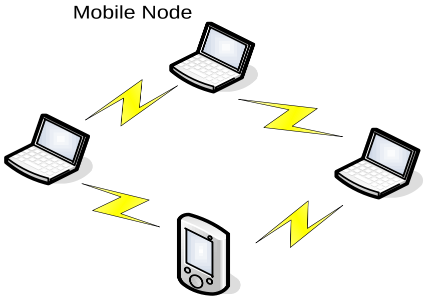

Figure 1.3: A Mobile Ad Hoc network

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.

2. ROUTING IN MANET

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 Classification of the Routing Protocols

Several routing protocols have been proposed for ad hoc networks. In this section a broad classification of these routing protocols is given. Only the unicast routing protocols are considered and an in-depth classification of all available protocols is beyond the scope of this thesis. Figure 2.3 shows the classification of the routing protocols for MANETs. At one end are the table-driven or proactive routing protocols such as the Destination Sequenced Distance Vector (DSDV) routing protocol, Wireless Routing Protocol (WRP), etc. At the other end, are the on-demand or reactive protocols such as Dynamic Source Routing (DSR) protocol and the Ad hoc On-demand Distance Vector (AODV) routing protocols.

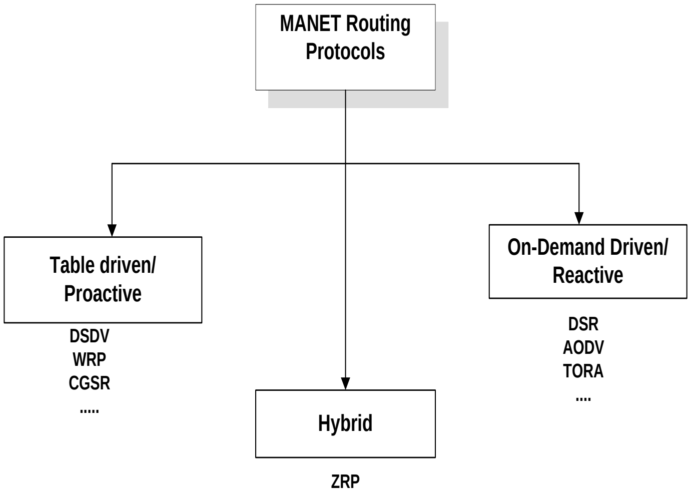

Figure 2.1: Classification of MANET routing protocols

2.1.1 Table-driven/Proactive Routing Protocols

In table-driven or proactive protocols, the nodes maintain an active list of routes to every other node in the network in a routing table. The tables are periodically updated by broadcasting information to other nodes in the network. Thus, they are an extension to the wired network routing protocols such as the Routing Internet Protocol (RIP). Any node wishing to communicate with another node has to obtain the next hop neighbor on the route to the destination from its routing table. Some examples of table-driven routing protocols are Destination Sequenced Distance-Vector routing protocol (DSDV), Wireless Routing Protocol (WRP), Cluster Switch Gateway Routing protocol (CGSR), etc. In the following sections, working of DSDV and WRP are explained, and the general pros and cons of table-driven routing protocols are enumerated.

2.1.2 Destination Sequenced Distance Vector (DSDV) Routing Protocol

The Destination Sequenced Distance Vector (DSDV) protocol is a proactive routing protocol based upon the distributed Bellman Ford algorithm. In this routing protocol, each mobile host maintains a table consisting of the next-hop neighbor and the distance to the destination in terms of number of hops. It uses *sequence numbers* for the destination nodes to determine "freshness" of a particular route, in order to avoid any short or long-lived routing loops. If two routes have the same sequence number, the one with smaller distance metric is advertised. The sequence number is incremented upon every update sent by the host. All the hosts periodically broadcast their tables to their neighboring nodes in order to maintain an updated view of the network. The tables can be updated in two ways – either *incrementally* or through a *full dump*. An incremental update is done when the node doesn't observe any major changes in the network topology. A full dump is done when network topology changes significantly or when an incremental update requires more than one NPDU (Network Packet Data Unit).

2.1.3 Wireless Routing Protocol (WRP)

The Wireless Routing protocol (WRP) is a table-driven protocol based upon the distributed Bellman Ford algorithm and is similar to DSDV. The difference between DSDV and WRP is the number of tables maintained at each node.

2.2 On-Demand/Reactive Routing Protocols

In contrast to table driven routing protocols, on-demand routing protocols find route to a destination only when it is required. The on-demand protocols have two phases in common – route discovery and route maintenance. In the route discovery procedure, a node wishing to communicate with another node initiates a discovery mechanism if it doesn't have the route already in its cache. The destination node replies with a valid route. The route maintenance phase involves checking for broken links in the network and updating the routing tables.

2.2.1 Dynamic Source Routing (DSR) Protocol

The Dynamic Source Routing Protocol is an on-demand routing protocol which is based on the concept of *source routing*. In source routing, a sender node specifies in the packet header, the complete list of nodes that the packet must traverse to reach the destination node. This essentially means that every node just needs to forward the packet to its next hop specified in the header and need not check its routing table as in table-driven routing protocols. Furthermore, the nodes don't have to periodically broadcast their routing tables to neighboring nodes.

2.2.2 Ad hoc On-demand Distance Vector (AODV) Routing Protocol

The Ad hoc On-demand Distance Vector routing protocol [9] inherits the good features of both DSDV and DSR. The AODV routing protocol uses a reactive approach to finding routes and a proactive approach for identifying the most recent path. More specifically, it finds routes using the route discovery process similar to DSR and uses destination sequence numbers to compute fresh routes.

2.2.3 Comparison of DSR and AODV

Table 2.3 provides a comparison of the features of DSR and AODV:

Protocol / Feature	DSR	AODV
Destination sequence numbers	Not used	Used
Link Layer acknowledgements	Not Required	Required (using HELLO beacons) for link breakage detection
Routing mechanism	Source routing – Multiple route caches for each destination	Table driven – one entry per destination. Sequence numbers used for
Route storage mechanism	Using route caches	Using routing tables
Timers	Not Used	Used
Multiple Route caches	Yes	No
Optimizations	Salvaging, Gratuitous route replies (RREP) and Route Error (RERR), non-propagating route requests	Expanding ring search

Table 2.1: Comparison of the features of DSR and AODV

The main difference is the source routing employed by DSR in contrast to table-driven routing used by AODV. Due to this, DSR has a higher routing load when the size of the network increases since each packet header has typically more information when compared to AODV. Another important difference is that AODV requires link layer acknowledgements or HELLO beacons at periodic intervals in order to detect link breaks. However, DSR avoids this feature and hence more efficient. Further, DSR stores multiple route caches for a destination whereas AODV does not. It has been found that this has an impact on the end-to-end delay and the delivery fraction as the size of the network increases. DSR has been found to perform well in lightly loaded networks, whereas AODV performs well in more stressful networks (with higher density of nodes). AODV also benefits from its timer mechanisms by maintaining fresher route entries as compared to DSR, which doesn't implement any timers. Besides, in DSR all requests reaching a destination node are replied to, whereas in AODV the destination replies only once to the request arriving first and ignores others.

3. SECURITY IN MANET

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.

Depending on these environments, several attacks and threats allowed by the existing routing protocols have been discovered. The existing routing protocols have been enhanced to address these attacks.

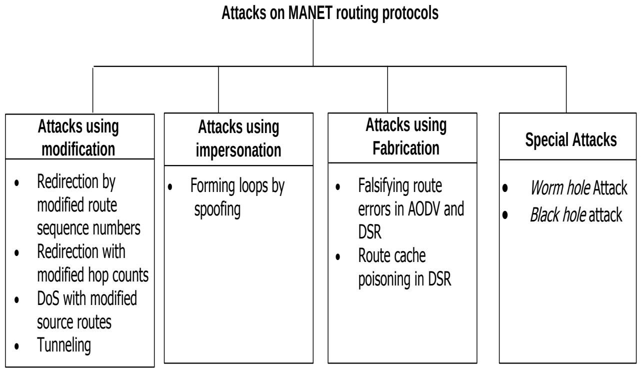
Attacks on MANET routing protocols
Attacks using modification
Redirection by modified route sequence numbers
Redirection with modified hop counts
DoS with modified source routes
Tunneling
Attacks using impersonation
Forming loops by spoofing
Attacks using Fabrication
Falsifying route errors in AODV and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

Figure 3.1: Classification of attacks on MANET routing protocols

4. SIMULATION STUDY

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. 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.

4.1 Experimental Setup and Metrics

The ns-2 simulator was used for the experiments. We now describe the traffic pattern, the scenario description and the metrics that were used for the experiments.

4.1.1 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 4.1 and figures 4.2, 4.3 and 4.4.

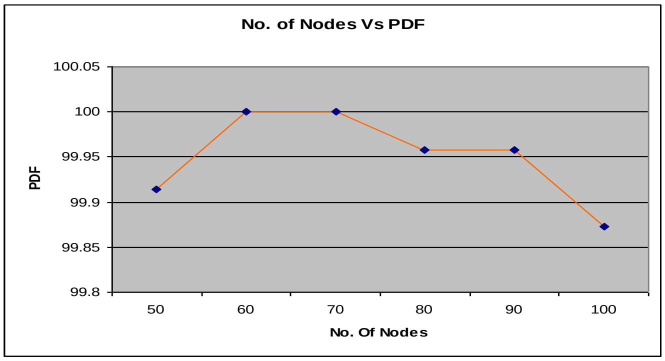

Figure 4.1: Effect of varying the number of nodes on the pause time

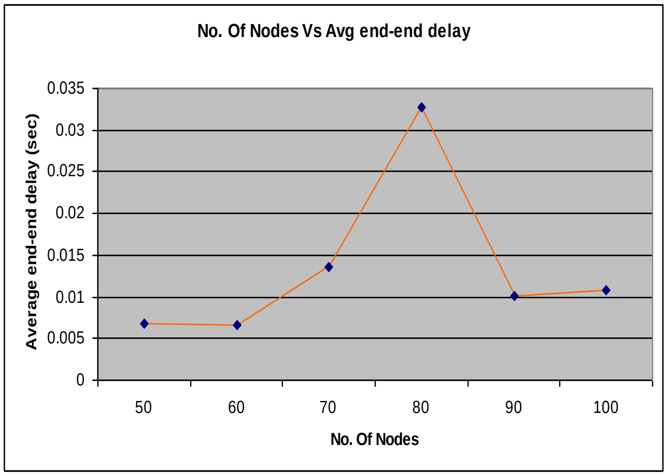

Figure 4.2: Effect of varying the number of nodes on the Average end-end delay

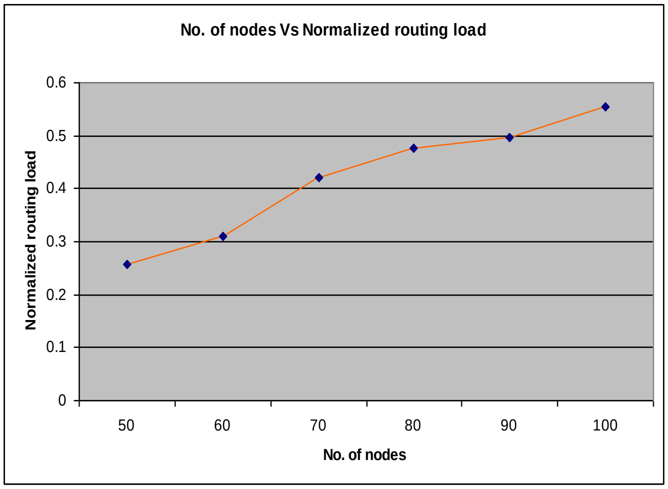

Figure 4.3: Effect of varying the number of nodes on the Normalized Routing Load

The blue circles in figures 4.1, 4.2 and 4.3 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.

4.1.2 Effect of varying the pause time

The effect of varying the pause time on the three metrics are shown in table 4.4 and the corresponding graphs are shown in figures 4.5, 4.6 and 4.8. It can be inferred that as pause time varies, the packet delivery fraction also increases. This is due to the fact that as pause time increases, the relative mobility of the nodes decreases, and hence the congestion also decreases in the network.

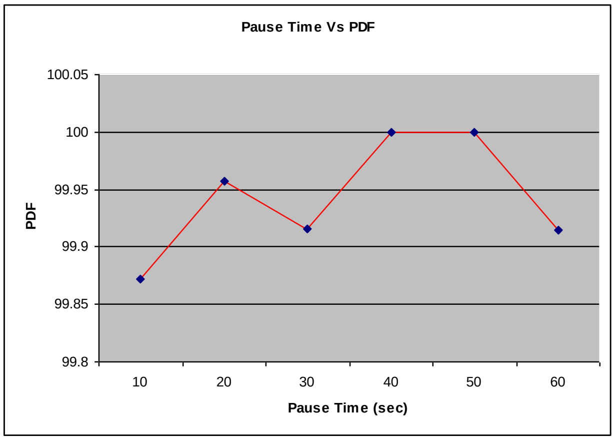

Figure 4.4: Effect of varying the pause time on PDF

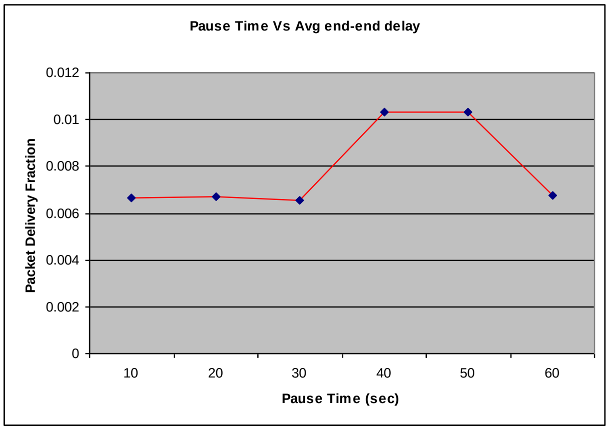

Figure 4.5: Effect of varying the pause time on average end to end delay

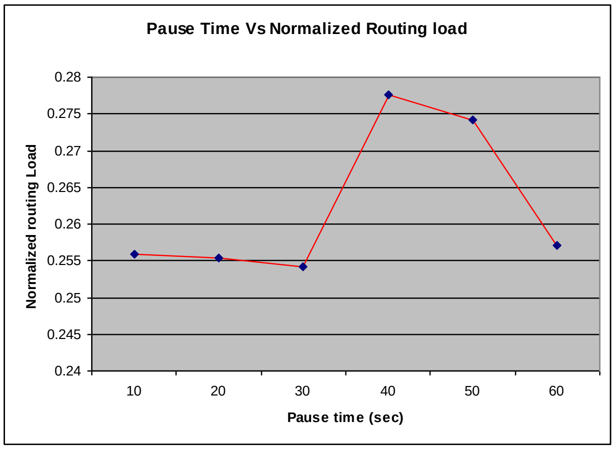

Figure 4.6: Effect of varying the pause time on NRL

From figures 4.4, 4.5 and 4.6 it can be inferred that for a pause time of 20 sec (represented by a blue circle), we obtain optimal values for the three metrics.

5. CONCLUSIONS

For the battlefield scenario, AODV has found to perform well for lower pause times (20 sec), higher density of nodes (9 per group) and smaller networks. As the network size increases, the performance drops due to a table-driven approach. However, since it does not use source routing, it has a much lower end to end delay for In order to analyze the performance of routing protocols in practice, such a scenario-based approach is vital. It also helps identify the suitable routing protocol for an optimal network size, the mobility of the nodes, the network density and a given traffic pattern.

A more comprehensive study of other routing protocols such as DSR, TORA, DSDV, etc. is needed to choose the right protocol for a given scenario.

6. REFERENCES

[1] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. *"Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks"***.** MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA.http://www.ece.cmu.edu/~adrian/projects/secure-routing/ariadne.pdf

[2] Manel Guerrero Zapata**.** *"Secure Ad hoc On-Demand Distance Vector Routing"***.** ACM Mobile Computing and Communications Review (MC2R), 6(3):106--107, July 2002. http://lambda.cs.yale.edu/cs425/doc/zapata.pdf

[3] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad. *"Chapter 30: Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network"*. , CRC PRESS Publisher, 2003.

[4] Sadasivam Karthik, Vishal Changrani, T. Andrew Yang. *"Scenario Based Performance Evaluation of Secure Routing in MANETs"*.http://sce.uhcl.edu/sadasivamk/MANETII05-draft.pdf

[5] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu and Jorjeta Jetcheva. *"A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols"*. IEEE Journal on Selected Areas in Communication, 1999.
http://monarch.cs.rice.edu/monarch-papers/mobicom98.pdf

[6] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, and Joo-Han Song. *"Experimental Comparisons between SAODV and AODV Routing Protocols"*. In proceedings of the 1st ACM workshop on Wireless multimedia, 2005.
http://www.ece.ubc.ca/~vincentw/C/LRWSc05.pdf

[7] Samir R. Das, Charles E. Perkins, Elizabeth M. Royer. *"Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks"*. Proceedings IEEE Infocom page 3-12, March 2000.
http://www.cs.ucsb.edu/~ebelding/txt/Perkins_PerfComp.pdf

[8] D B. Johnson, D A. Maltz, and Y. Hu. *"The dynamic source routing 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] C.Siva Ram Murthy and B. S. Manoj. "*Ad hoc wireless networks: Architecture and Protocols".* Prentice Hall Publishers, May 2004, ISBN 013147023X.

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

[12] David B. Johnson David A. Maltz Josh Broch. **"***DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks'.*In Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.
http://www.cs.ust.hk/~qianzh/COMP680H/reading-list/johnson01.pdf

[13] M. Marina and S. Das. "*Performance or Route caching strategies in Dynamic Source Routing*". Proceedings of the Int'l Workshop on Wireless Networks and Mobile Computing (WNMC) in conjunction with Int'l Conf. on Distributed Computing Systems (ICDCS), Washington, DC, USA, 2001.
http://www.cs.utsa.edu/faculty/boppana/papers/phd-tdyer-dec02.pdf