International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012

# A New Method for Comparing the Security of Routing Protocols in Mobile Ad Hoc Networks

Zeinab Shariat[1] , Asad Mohammadi[2], Ali Movaghar[3]
[1]Islamic Azad University of Boumehen, Tehran, Iran
shariatnaseri@ce.sharif.edu
[2]Amirkabir Universityof Technology, Tehran, Iran
ad.mohammadi@aut.ac.ir
[3]Sharif Universityof Technology, Tehran, Iran
movaghar@sharif.edu

## *ABSTRACT*

*Mobile Ad Hoc networks are networks in which users, regardless of geographical locations, can have access to its information and services. These networks are divided into 2 categories: network with structure and network without structure or Ad Hoc. Network structures are composed of fixed gates and wired networks. A mobile host can communicate with the other through a bridge called base station. A mobile host can move geographically while communicating when the host is out of the domain of a base station, it will be connected to another base station and will continue the communication,in this method the base stations are fixed. In contrast to a network structure, all nodes are portable in an Ad Hoc network and communicate dynamically and with a preferred method. All of the nodes in this network act as a router and engage in discovering and route maintenance[1].The major problem of these networks designing is that these are vulnerable to security attacks. In this paper, the threats aAd Hocnetwork and also security objectives against these threats will be reviewed and some important routing protocols for these kinds of networks, are compared and evaluated. This comparison, unlike previous comparisons, covers wide range of protocols and develops software NS2.*

## *Keywords*

*Routing protocol; wireless network;Ad Hocnetwork; Security;Security attack*

## 1. INTRODUCTION

Ad Hocmobile networks (MANET's) are a group of wireless computers, forming a communication network, that have no predetermined structure. Configuration and management of this network is not dependent on any particular user. In other word, specific networking allows formation of an autonomous complex. There are numerous scenarios that a network with a fixed structure and configuration cannot meet their needs and then networks like special networks are needed for military mission, emergency operations, commercial projects, training courses and etc. therefore, in recent years, special attention is paid to these networks. There are many problems in a specific network such as open network architecture, shared wireless media, transport and security capabilities, security is a major concern in creating a reliable wireless network connection and its importance is an equal as wired networks. But due to the mentioned problems, security solutions for wired networks do not respond directly to specific wireless network. The ultimate goal of security solution must provide full protection of all protocols.

DOI : 10.5121/ijdps.2012.3413 

One of the major security concerns in MANETs is about node to node transferring. In other words, this is about maintaining the communication between mobile nodes in wireless channels and several hops, needing a basic support of network security services.
Communicating with several hops in Ad Hocwireless network takes place in 2 stages:

1. Connecting security through a hop to a link layer (such as MAC)
2. Developing the connection to several hops through link layer routing and data promoter protocols (such as Ad Hocrouting)

In fact, in order to review the securityideas, problems and solutions of MANETs, networks layers and links must be focused on. Table 1 displays security solutions for different layers of a special wireless network.

TABLE 1.SECURITY SOLUTION FOR MANET

| Layer | Security ideas |
|---|---|
| **Application layer** | Detecting and protecting viruses, worms, program code and malicious programs |
| **Transport layer** | Detecting and clearing to end connection through hiding data |
| **Network layer** | Protecting promoter protocols and special routing |
| **Link layer** | Protecting wireless MAC protocol and producing backup of link layer |
| **Physical layer** | Preventing of attacks of services |

We need to stimulate a specific network for comparing the protocols and this network has been stimulated in NS2 [1,2,4]. The stimulated network includes models of mobility, physical layer with radio emission, radio network interface and protocol IEEE 802.11 (MAC) with distributed coordination function or DCE. The ratio network interface card (NIC) is based on WaveLan interface of lucent. The model includes collisions, propagation delay and signal attenuation data to 2 Mbps and 256 meters radio range. Protocols are for comparing DSR, AODV, DSDV, TORA, FSR, CBRP and CGSR protocols which the first four ones have been stimulated by NS2 and the rest has been added to NS2 [3].

Section 2 of the paper reviews the security of the mobile special network, section 3 methodology and model, section 4 criteria for comparing protocols and finally section 5 results of stimulation and comparison between protocols.

## 2. SECURITY OFAD HOCMOBILENETWORKS

In the Ad Hocnetworks, unlike wired networks which have some routers, each node must act as a router and promoter to the other nodes. Wireless channel is used for both authorized users and attack network. There is no monitor on traffic and there is not any control mechanism for extending it. Basically, there are 2 ways to protect the wireless Ad Hocnetwork: Pre-active method and reactive method.

Pre-active method uses various hidden techniques to prevent attacks.In contrast,reactive method detects security threats through the signs of symptom of threats and reacts against them. In the absence of a secure communication line, a complete security solution for MANETs should be established by combining the methods, and the solution consists of protection, recognition and reaction. For example, pre-active method is used to ensure the correctness of the routing and reactive method is used to protect forwarding the data. Security is like a chain that its firmness depends on its firmed joints.

Different routing protocols are suitable for different network applications. DSR protocol is efficient in networks in which nodes proxies are inactive and has low performance when proxies are active. TORA protocol, perform well in networks with active proxies.

# 3. METHODOLOGHOFWORK

The ultimate goal of this simulation is to measure routing protocol security affect by changes in network topology, while sending successfully packages to destinations. To measure this ability, a basic simulation has been considered with which results of the other simulations are compared[4,6]. Simulation was done by 50 mobile nodes in an area of 300*1500 $m^2$ and time of 900 seconds. The simulator accepts a file for each scenario in which the motion of each node and the packets generated by each node is shown and they are different in the differences in the changes that occur in these parameters. For this purpose, 210 different scenario files with changes in movement pattern and traffic load were created and then all of them were run for all seven protocols[2,7].

## 3.1. MovementModel

The NS2 simulator is used for simulation which nodes move according to random waypoint model that the movement scenarios include time stop characteristics [2]. A random destination in an area of 1500*300$m^2$ is chosen toward which a node moves with non-uniform speed between zero and its maximum velocity. When the node reaches to its destination, it stops there (in seconds) then chooses another destination and continues this manner during total simulation time. Each simulation is run in 900 seconds and stop times considered for the simulation are 0, 30, 60, 120, 130, 600 and 900 seconds. Zero stop time means a continuous movement and 900 seconds stop time shows a static network. Since protocol efficiency is very dependent on nodes movement model, so we have considered 70 different movement models for nodes. 10 different runs has been done for each time stop and 2 different values for the maximum speed of node have been considered. In next section, the simulation results with maximum speed 20m/s and average speed 10m/s and maximum speed 1m/s are shown.

## 3.2. Communication Model

For mentions simulations, we considered a constant bit rate traffic source(CBR) , transfer rate of 1, 4 and 8 packets per second, and 10, 20 and 30 sources and 64- byte and 1024-byte packets[2]. Change of total CBR source is very similar to the change of transfer rate. Thus, we considered the transfer rate as constant as 4 packages per seconds and 3 different patterns of CBR source with 10, 20 and 30 source. When we used 1024- byte packages a heavy congestion appeared because of lack of diversity of space and this problem exists for all protocols,one node or two nodes must destroy the received packages to solve the problem. If none of the nodes does not participate in load balancing then topology must be changed and size of the sent packages must be minimized to 64 bytes. All of the communication models are peer to peer and initial connections are distributed uniformly between 0 and 180 seconds [2,6]. Three communication models (10, 20 and 30 sources) are combined with 70 movement patterns and create 210 different scenarios for each nodes maximum of speed (1m/s and 20 m/s)[6].

## 3.3. Characteristics of Movement Patterns

In order to show the differences between patterns run on routing protocols, the path created by the protocol to deliver packages and numbers of topology changes in each scenario were measured [5,6]. When each packet is generated, an intermediate mechanism (a part from the protocol) estimates the nearest path between the transmitter and receiver of the package and places this value inside the package. This value will be compared by real hops that the package has passed to reach its destination. Figure(3-1) shows distribution of the shortest (nearest) paths

for all 210 scenarios for speeds of 1m/s and 20m/s. Each bar shows numbers of packets for each destination that has a certain distance at the generation time. Each data packet in the simulation must pass 2.6 hops on average to reach its destination and farthest obtainable node in the routing protocol passes 8 hops.

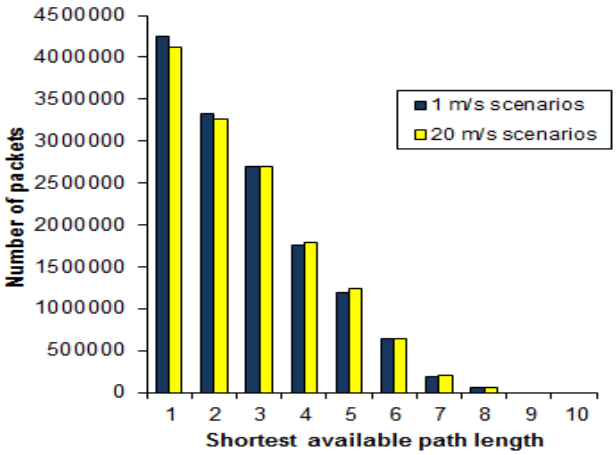



Figure (3-1) Distribution of the shortest path for each packet generated in all scenarios

Number of changes of connection of a bond were measured when a node, inside or outside of the range of direct communication goes toward another node. A specific scenario has less connection changes in time stop at 30 seconds and speed of 1m/s than time stop zero.

## 4. MEASUREMENTCRITERIA

Routing protocols are evaluated by 2 parameters and the following criteria [5]

- Packet delivery rate: the ratio between generated packets by application layer of source nodes and received packets by final destination.
- Routing overhead: total numbers of sent routing packets through simulation time.

It is necessary to mention that 40 to 120 packets per second are generated and total simulation time is 900 seconds.

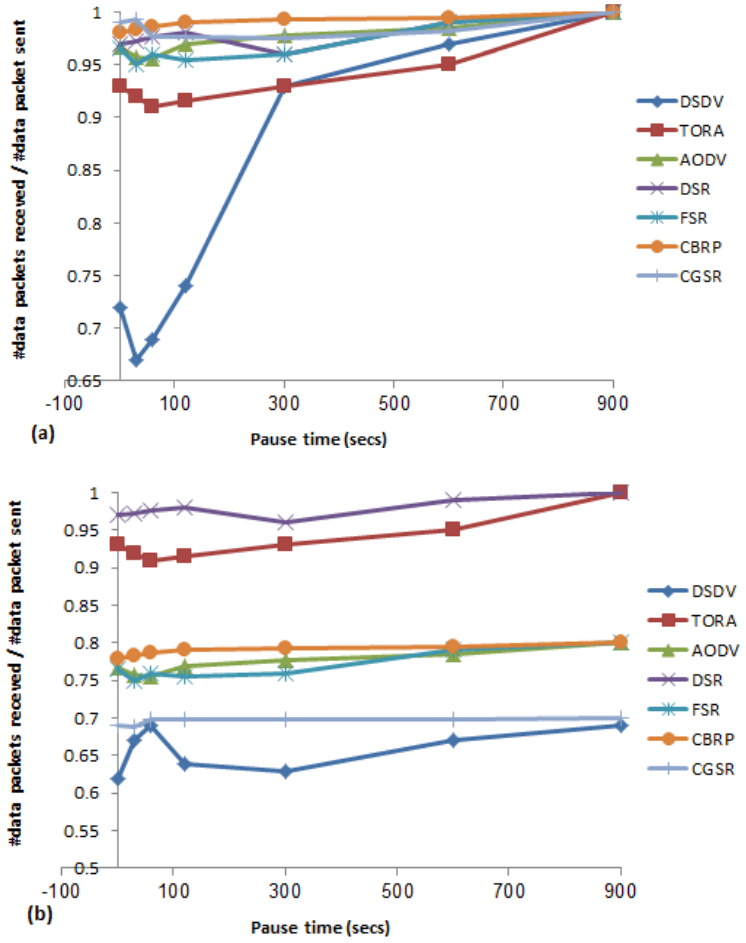
The criteria are normally measured for nodes and then the movement scenario will be run by SIP proxy activating in order to obtain its effects on the protocols.

## 5. SIMULATIONRESULTS

As previously mentioned, simulation has been done with maximum speed 20m/s (average speed 10 m/s) and 1 m/s. first, seven protocols DSR, AODV, DSDV, TORA, FSR, CBRP and CGSR were simulated based on speed 20 m/s then they are compared to the simulated data based on speed 1 m/s. There are peer to peer communication models for all simulations and each run has 10, 20 or 30 sources each generated 4 packets per second. Then security situation of nodes was changed and then SIP security proxy was activated on them and the scenarios were repeated until the reaction of each protocol was reviewed in this condition.

## 5.1. ComparisonBetweenProtocols Based on Packet Delivery Rate

Figures (5-1) and (5-2) show numbers of deliverable packets of each protocol based on rate of motion (stop time) and speed of nodes. In part (a) of any two figures, the proxy has been disabled that is the first figure shows the simulation speed 20 m/s and the second one shows the simulation speed 1m/s . Part (b) of both of the figures show the same condition with enabled SIP proxy.




Figure(5-1)(a) packet delivery rates based on stop time and speed 20m/s with enabled proxy and (b) without enabling the proxy

**Without enabling the proxy:**All of protocols deliver more than 95.5% of the packets at speed 1 m/s , In this case unlike the scenario with speed 20m/s that DSDV was not capable to converge the values,but packet delivery performance is excellent.

**With the proxy enabled:**Enabling proxy causes packet delivery rated be decreased in ratio to no proxy state of course except protocols TORA and DSR. In TORA and DSR, this ratio is not related to enabling or disabling the proxy and this concludes that these two protocols are safer than others.

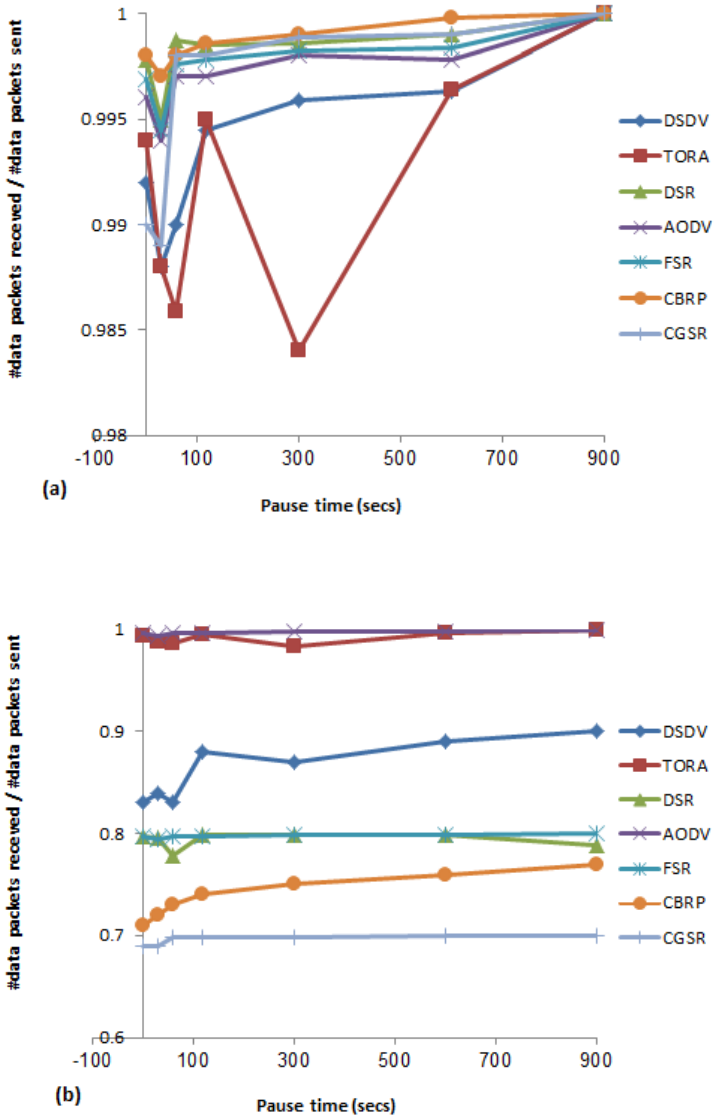



Figure (5-2) (a) packet delivery rates based on stop time and speed 1m/s with enabled proxy and (b) without enabling the proxy

## 5.2. ComparisonBetweenProtocols Based on Routing Overhead

Figures (5-3) and (5-4) show numbers of routing packets sent by each protocol in order to obtain delivery rates shown in figures 5-1 and 5-2.

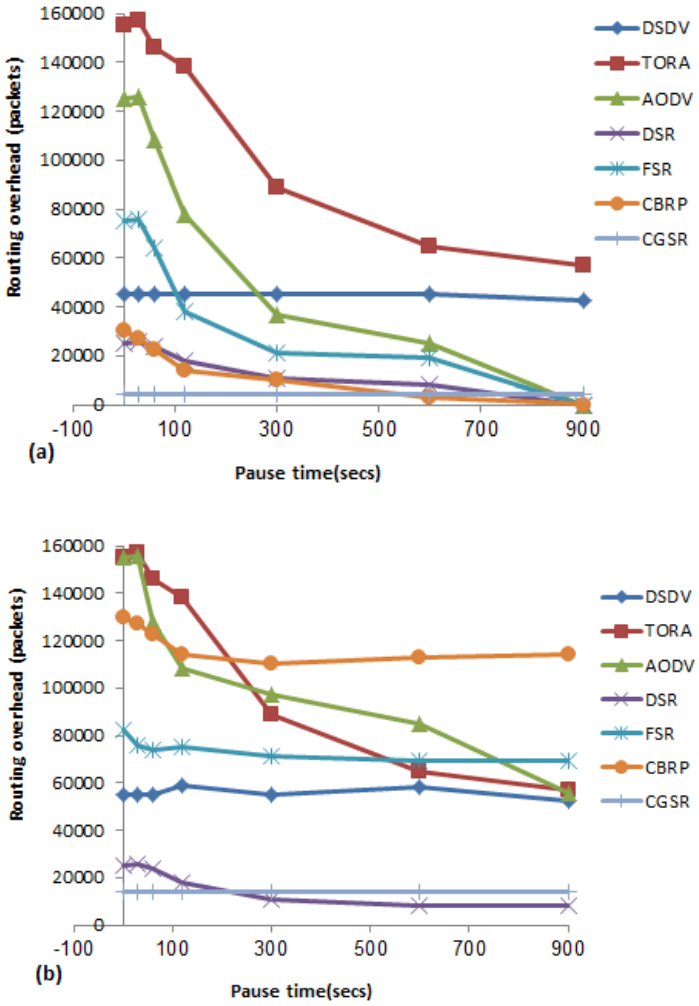



Figure 5-3 (a) routing overhead based on stop time and speed 20 m/s with enabled proxy and (b) without enabling the proxy

**Without enabling the proxy:** In low rated of movement, each routing protocol show great differences for routing overhead. DSR and AODV have not obtained serious differences between these scenarios and increasing routing overhead is only dependent to decreasing stop time.

**With the proxy enabled:** In all protocols, except TORA, enabling the proxy causes increasing the routing overhead, comparing with without enabling the proxy. But for TORA the value is not dependent on enabling or disabling the proxy and no changes in the packet delivery rate and routing overhead conclude that this protocol is more secure than others.

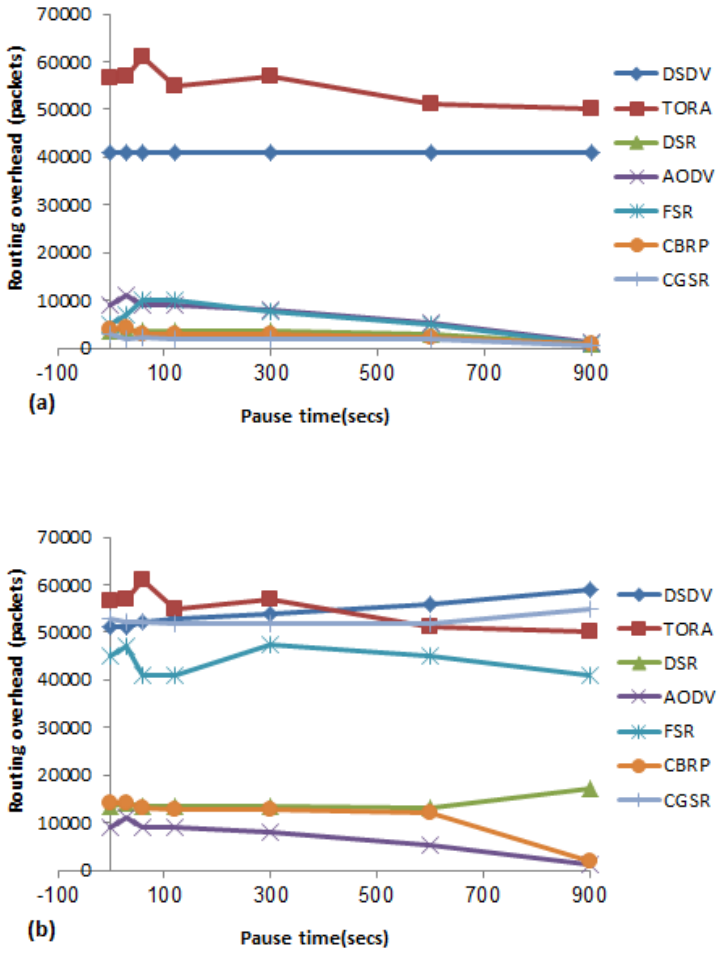



Figure (5-4) (a) routing overhead based on stop time and speed 1m/s with enabled proxy and (b) without enabling the proxy

## 6. CONCLUSION

In this paper, some Ad Hoc network routing protocols were compared based on security and with two measures, the received packet and routing overhead. About the rate of packet delay we conclude that all protocols deliver most parts of generated packets when node mobility is low and proxy is disabled (Eg, long time stop) and the value reaches to 100% when the node mobility is zero. Especially DSR, AODV, FSR, CBRP and CGSR deliver more than 95% of the packets in any rate of movement. In these scenarios, DSDV faced failure in time stop less than 300 seconds. TORA and DSR manner remain constant if the proxy is enabled and this is not dependent on enabling or disabling the proxy and this concludes that these two protocols are safer than other ones.

About routing overhead, simulations show that routing protocols have different values for routing overhead. Generally we can say that DSR has the less overhead and TORA has the most overhead. TORA, DSR, CBRP and AODV are on-demand protocols and their overheads very with rate movement and are dependent on it, but DSDV, FSR and CGSR which are table-

driven protocols are not so dependent on the rate of movement and almost show a constant manner. By maintaining the conditions and enabling the proxy, it is observed that the routing protocol for TORA remained stable and proxy did not affect it and this shows TORA high security, but overhead increased in the rest of the routing protocols. It is necessary to mention that TORA protocol acts better than other protocols in terms of security, but it is not better than other protocols in rate of packet delivery and routing overhead.

## REFERENCES

[1] E.M. Belding-Royer and C.-K. Toh.A review of current routing protocols for Ad Hoc mobile wireless networks. IEEE Personal CommunicationsMagazine, pages 46–55, April 1999.

[2] J. Kong et al. Providing robust and ubiquitous security support for mobile Ad Hoc networks. In Proc. IEEE ICNP, pages 251–260, 2001.

[3] Hu, Yih-Chun, and Adrian Perrig. "A Survey of Secure Wireless Ad Hoc Routing." In IEEE Security & Privacy, special issue on Making Wireless Work, 2(3):28-39, May/June 2004

.[4] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks." In Wireless Networks Journal, 11(1), 2005.

[5] Hu, Yih-Chun, Dave Johnson, and Adrian Perrig. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks." In *Ad Hoc Networks Journal*, 1(1):175-192, 2003.

[6] S. Corson and J. Macker Mobile Ad hoc Networking (MANET): Routing ProtocolPerformance Issues and Evaluation Considerations. RFC 2501, IETF NetworkWorking Group, January 1999.

[7] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Efficient Security Mechanisms for Routing Protocols." In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, California, February 2003.