KNOWLEDGECUDDLE PUBLICATION

International Journal of Computer Engineering and Science, August- 2014

An Overview of security issues in Mobile Ad hoc Networks

Vikaram Agrawal[1], Hiral Chauhan [2]

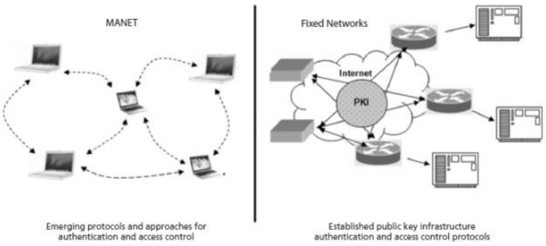
Department of Information Technology, BVM Engineering College. V V Nagar[1]
ME Student, Department of Computer Engineering, BVM Engineering College, V V Nagar[2]
agrawal.vm@gmail.com[1]
hiral_chauhan4u@yahoo.co.in[2]

ABSTRACT: **Mobile ad hoc networks (MANETs) are collections of self-organizing mobile nodes with dynamic topologies and no centralized authority. Each node participating in the network acts both as host and a router. So each node can participate to transfer data packet to destination node but suppose one node in network is removed at time it is very difficult to maintain the information about all node. The main advantage and disadvantage of MANETs provides large number of degree of freedom and self-organizing capability of that make it completely different from other network. Due to the nature of MANETs, to design and development of secure routing is challenging task for researcher in an open and distributed communication environments. In MANET, the more security is required in comparison to wired network. If source node chooses this fake route, malicious nodes have the option of delivering the packets or dropping them.**

Keywords: MANETs, Security, Cryptography.

I. INTRODUCTION

WIRELESS cellular system has been in use since 1980s.Wireless system operates with the aid of a centralized supporting structure such as an access point. Recent advancement of wireless technologies like Bluetooth [3], IEEE 802.11 [4] introduced a new type of wireless system known as Mobile ad-hoc network (MANETs) [1, 2, 5, 6], which operate in the absence of central access point. It provides high mobility and device portability's that enable to node connect network and communicate to each other. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network. User has great flexibility to design such a network at cheapest cost and minimum time.


MANET
Fixed Networks
Internet
PKI
Emerging protocols and approaches for authentication and access control
Established public key infrastructure authentication and access control protocols

MANETs are largely used in military, rescue operations and even in mobile phones using Bluetooth. As the popularity of MANETs is increasing with the increase in scientific techniques, one of the biggest threats that still reside over MANETs is security [10]. Due to its topology less nature security has become one of its main issues. Different challenges faced by MANETs are [10]:

A. Confidentiality
B. Integrity
C. Authentication
D. Non-Repudiation

In recent years many routing protocols have been introduced for MANETs. These protocols are divided into 3 categories-

A. Reactive

B. Proactive
C. Hybrid

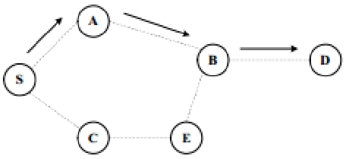
II. FEATURES OF MANETs

A mobile ad hoc network has following features [1, 7]:

A. *Autonomous Terminal:* In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router.

B. *Distributed Operation:* The nodes in MANET collaborate amongst themselves, where each of them acts as a relay to implement functions.

C. *Multi-hop Routing:* When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate node [8]



D. *Dynamic Network Topology:* The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly.

E. Light-weight Terminal: The MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage.

III. WEAKNESSES OF MANETs

Since nodes in mobile network can move freely, the network tends to change its topology very frequently. This mobile nature of the nodes may create many security and other issues in MANETs [7]:

A. *Lack of Centralized Management:* It is impossible to detect attacks.
B. *Infrastructure less*: Detecting faults in network is not easy.
C. *Dynamic Topology*: Results in weaker relationship among nodes.
D. *Packet Loss*: Mobility of nodes, bit rate error and interference causes packet loss.
E. *Mobile Nodes:* It is easy for malicious nodes to enter any network and hinder communication.
F. *Security:* Mobile nodes itself perform the major networking tasks, so it is easy for any attacker to acquire data.
G. *Resource Availability*: Providing security in mobile network requires various resources and architectures.

IV. APPLICATIONS

Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network [7].

The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. It includes:

- Military Battlefield
- Sensor Networks
- Commercial Sector
- Medical Service
- Personal Area Network

V. VULNERABILITY IN MANETS

Malicious and selfish nodes are the ones that fabricate attacks [9] against physical, link, network, and application layer functionality. Current routing protocols are exposed to two types of attacks:

- Active attacks
- Passive attacks

5.1 Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. These attacks can be classified into further following types:

1. *Spoofing:* Spoofing occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather [2].

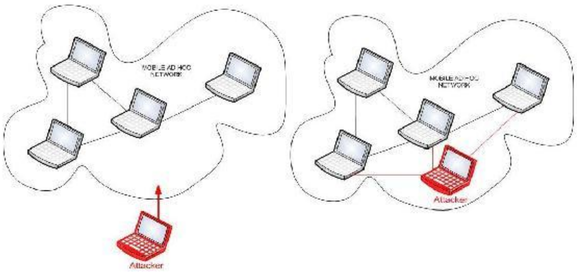


Fig. 1 Spoofing (Man in the middle)

2. *Fabrication:* The notation “fabrication” is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbour can no longer be contacted [5].

3. *Wormhole Attack:* An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunnelled. This tunnel between two colluding attackers is referred as a wormhole.

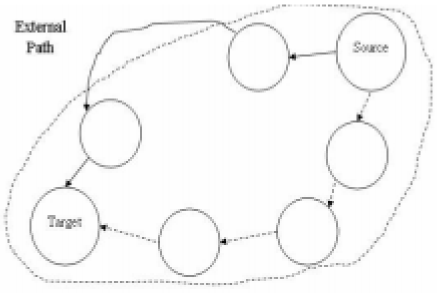


Fig. 2 Wormholes

4. *Modification:* The attacker performs such attacks is targeted to integrity of data, by altering packet or modifying packets.

5. *Denial of Service:* This active attack aims at obstructing or limiting access to a certain resource. The resource can be a specific node or service or the whole network.

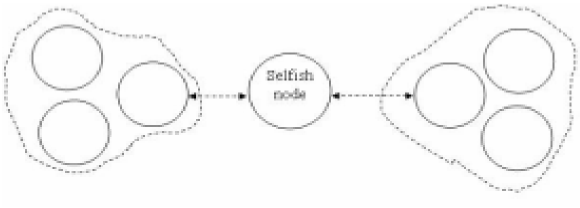


Fig. 3 Denial of Service Attack

6. *Sinkholes:* In a sinkhole attack, a compromised node tries to attract the data to it from all neighbouring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighbouring nodes. Sinkhole attacks can also be implemented on Ad hoc networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate.

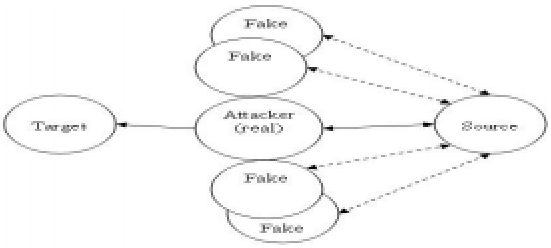


Fig. 4 Sink Hole

7. *Sybil Attacks:* Malicious nodes in a network may not only impersonate one node, they could take up the identity of a group of nodes, and this attack is called the Sybil attack. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from point A to point B. A consequence of this is that attackers have harder time to destroy the integrity of information. However, if a single malicious node is able to represent several other nodes, the effectiveness of these measures is significantly degraded.

The attacker may get access to all the data or may alter all packets in the same transmission so that the destination node/s cannot detect the change in packets anymore. In trust-based routing environments, representing multiple identities can be used to deliver fake recommendations about the trustworthiness of a certain party, hereby attracting more traffic to it; in ideal starting point for further attacks. However, in the case of Multipath protocols which send data redundantly, not relying on one path only, the problem of sinkholes can be reduced. Probabilistic protocols which measure the trustworthiness of a network can help detecting sinkholes within the network.

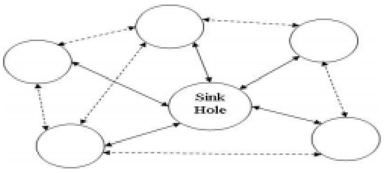


Fig. 5 the Sybil Attack

5.2 Passive Attacks

In passive attacks the attacker does not perturb the routing protocol, instead try to extract the valuable information like node hierarchy and network topology from it. Passive attack is in nature of eavesdropping on, or monitoring of, transmission. The goal of opponent is to obtained information that is being transmitted [5]. Passive attacks are very difficult to detect because they do not involve any alteration of data.

5.3 Other Advanced Attacks

There are different types of attacks which are vulnerable to MANETs and which are active at different layers of network. Few of them are discussed below [10]:

1. *Black hole Attack:* The black hole attack is active at the network layer. It has two properties [11] First is that the attacker sends fake routing information, claiming that it has the valid route to the destination. Second, the malicious node targets the routing packets, drops them instead of normally forwarding them.

2. *Byzantine Attack:* In this attack an intermediate node or a set of intermediate nodes work in collusion and carry out attacks such as creating routing loops, forwarding packets on non – optimal path which results in disruption and degradation of the routing system.[11]

3. *Routing Attacks:* These types of attacks include attacks related to the routing table which are routing table overflow, routing table poisoning, packet replication, rushing attack etc.

4. *Resource consumption Attack:* This type of attack involves the illegal resource consumption of the network which includes battery life or by unnecessary forwarding packets to the malicious nodes.

5. *Session hijacking Attack:* Session hijacking attack is the attack which is active in the transport layer. The first step of the attacker is to spoof the IP address of the source node and determine its sequence number and hence perform denial of service attack on the source. [11]

6. *Cryptographic Attacks:* Cryptography is considered as a powerful tool to maintain confidentiality and authentication of the information which is to be sent. It also hinders the illegal access of data by attackers by its key management system .These types of attacks include digital signature attack, pseudorandom number and hash collision attacks.

VI. ROUTING IN MANETs

The choice of the route being selected is done by the routing algorithm [1]. As in Fig 2 it is clearly shows the classification of the routing protocols.

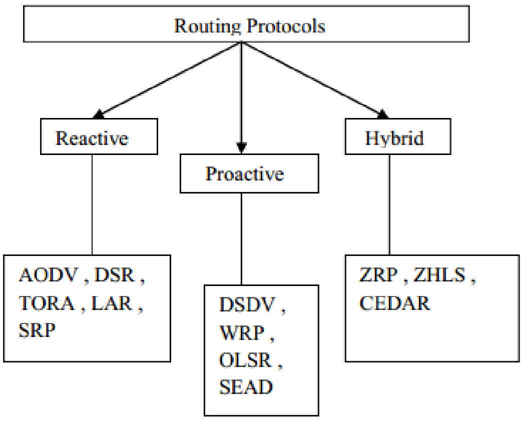


Fig 6: Different routing protocols in MANETs

6.1 Reactive protocol:

Reactive protocols are also called on-demand protocols because they maintain or discover route only on demand [12]. A control message is flooded to the routes to discover the appropriate route. It only establishes the route when any node in the network wants to send a message or a packet to another node in the network. The advantage of these protocols are that it reduces the routing table overflow and its major disadvantage is that due to its on demand nature while route discovery a longer delay is been found. The example of this type of protocol are DSR (dynamic source routing), AODV (ad hoc on demand distance vector routing), LAR (location aided routing), TORA (temporally ordered routing algorithm).

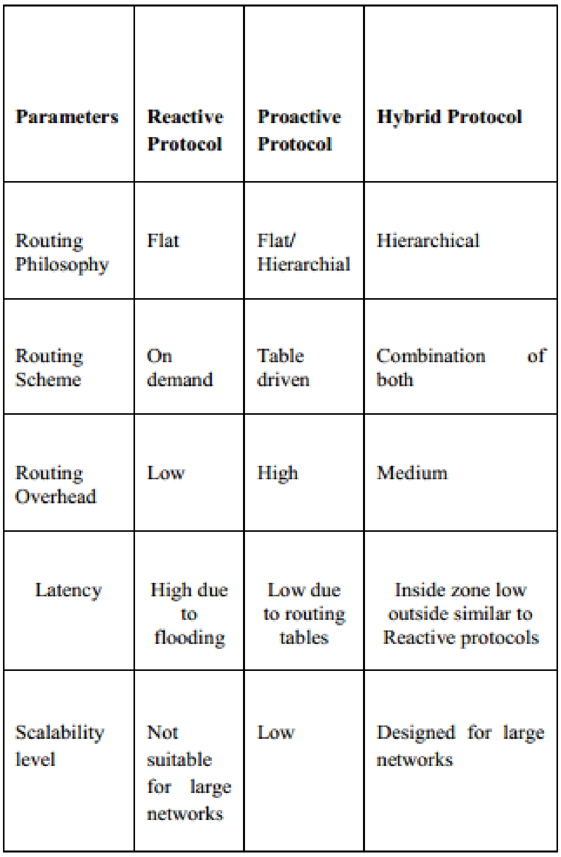
6.2 Proactive protocol:

Proactive protocols are also named as table driven routing protocol. They maintain the routing table of the entire network constantly. Each node has to maintain one or more tables to store routing information and response to changes in network topology by broadcasting and propagating. [13] The routing tables are constantly updated whenever the network topology changes. Each node in the network sends a broadcast message to the entire network if there is any change in the network topology. This feature of maintaining routing entries of the entire network may affect the routing table but it provides the actual information of the entire network. For very large network the proactive routing protocols may not be recommended because they maintain entries of each node in the network which causes more bandwidth consumption and overload to routing table. The examples of proactive routing protocol are DV (distance vector), DSDV (destination sequence distance vector), OLSR (optimised link state routing), and WRP (wireless routing protocol) which is an enhanced version of DSDV.

Hybrid protocols:

As according to the name hybrid routing protocols are a combination of both reactive and proactive routing protocols. Basically to overcome the shortcomings of reactive and proactive routing protocol the hybrid is used. It uses the route discovery and on demand mechanism of reactive routing protocol and the routing table management mechanism of proactive routing protocol. In hybrid routing protocol a large network is divided into zones. The routing inside the zones is done by using reactive approach and the routing outside the zone is done using reactive approach. [14] It is the most effective and appropriate routing protocol amongst all. The examples of hybrid protocols are ZRP (zone routing protocol), ZHLS (zone based hierarchical state).

Table 1. Comparison of routing protocols



Parameters	Reactive Protocol	Proactive Protocol	Hybrid Protocol
Routing Philosophy	Flat	Flat/ Hierarchial	Hierarchical
Routing Scheme	On demand	Table driven	Combination of both
Routing Overhead	Low	High	Medium
Latency	High due to flooding	Low due to routing tables	Inside zone low outside similar to Reactive protocols
Scalability level	Not suitable for large networks	Low	Designed for large networks

VII. METHODS TO SECURE ROUTING PROTOCOLS

AODV does not take security into account: AODV messages are neither encrypted nor authenticated nor integrity protected, and basically always assumed as trusted. Based on the possibility to forge packets and on the distributed and uncontrolled nature of the network many attacks are possible.

Due to these attacks many security techniques have been implemented on AODV. Those techniques are discussed below –

SAODV – Secure AODV is an extension to AODV routing protocol. It is proposed by M. Zapata and N. Asokan. It is based on public key cryptography and hash algorithm. SAODV routing messages (RREQs, RREPs, and RERRs) are digitally signed, in order to guarantee their integrity and authenticity. [15] There is a key management system which makes it possible for each node to obtain public keys from the other nodes of the network. How this is achieved depends on the key management scheme. Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). For the non-mutable information, authentication is performing in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information. To preserve the collaboration mechanism of AODV, SAODV includes a kind of delegation feature that allows intermediate nodes to reply to RREQ messages. This is called the double signature: when a node A generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on a fictitious RREP message towards intermediate node itself.

A-SAODV – Adaptive secure AODV is another approach to secure AODV routing protocol from attacks and from malicious users. It is based on the AODV-UU implementation by Uppsala University. Unlike AODV-UU, A-SAODV is a multithreaded application. [16] In A-SAODV, there are two execution threads: one carries the cryptographic operations and the other to all other functions (routing message processing, SAODV routing table management, timeout management, SAODV message generation, and data packet forwarding). The two threads communicate via a first input first output (FIFO) queue containing all the messages that must be signed or verified. [16]

SEAD – Secure efficient Ad hoc distance vector is a proactive routing protocol. It is another routing protocol which is secure as it is based on one – way hash functions to provide authentication. Each node contains its individual hash chains which are separated into segments to prevent an attacker to forge sequence numbers. [17]

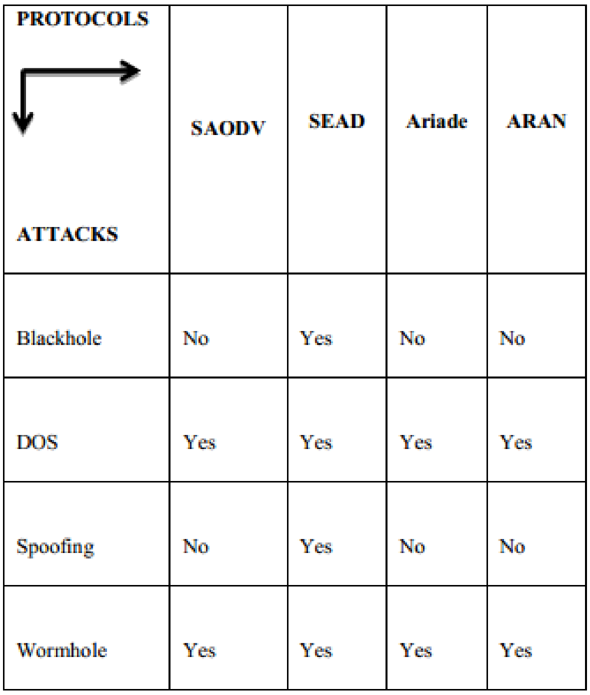
ARIADNE - It is another On-Demand Routing Protocol presented by Hun, Johnson & Perrig based on DSR. It is a secure on-demand routing protocol that can authenticate messages using one of the three ways: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signature[17]. The protocol is based on two steps- to verify that the route is authentic and to check that no node is missing from the route. However Ariadne is vulnerable to wormhole attack.

ARAN - It is proposed by Dahill. Authenticated Routing for ad hoc networks detects the attacks from malicious nodes and also protects the network from forged actions. It uses cryptographic certificates for authentication purpose. The certificate includes the IP of the node, the public key of the source node, a timestamp of the time at which the certificate was created and another timestamp of the time at which the certificate expires. This is the first step which is covered. After the successful completion of the first step second step is preceded. It discovers the shortest path to the destination. It is an on- demand routing protocol. It is successful in protecting the network against impersonation attack but is vulnerable to wormhole attack. [17]

VIII. RELATION BETWEEN ATTACKS AND PROTOCOLS

Relation between attacks and different security protocols is shown in table 2[1].

Table 2. Relation between attacks and protocols



PROTOCOLS → ↓ ATTACKS	SAODV	SEAD	Ariade	ARAN
Blackhole	No	Yes	No	No
DOS	Yes	Yes	Yes	Yes
Spoofing	No	Yes	No	No
Wormhole	Yes	Yes	Yes	Yes

III. CONCLUSION

From the article of MANET routing protocol it would be specified that if there are some changes or modification are done then all protocol can better result to provide excellent QoS. We can also reduce the packet drop ration, energy and time required to transfer packet from one node to other nodes. With some changes in protocol they can give good result in security as well.

REFERENCES

[1]. Vikram M. Agrawal, Samip A. Patel, "A STUDY ON SECURITY LEVEL OF AD HOC ROUTING PROTOCOL TO FIND OTHER APPROACH WITH DSDV", in IJCET (IAEME) Volume 4, Issue 6, November - December (2013), pp. 240-246. ISSN 0976 – 6367(Print), ISSN 0976 – 6375(Online)

[2]. B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[3]. Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2010.

[4]. Janne Lundberg, Routing Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security,

[5]. http://citeseer.nj.nec.com/400961.html.2000.H. Dang,W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, 0163-6804, pp. 70-75, October 2009.

[6]. Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capkun. The Quest for security in Mobile Ad Hoc Networks. Proceedings of the 2010 ACM International Symposium on Mobile ad Hoc networking & computing, Long Beach, CA. 2001.

[7]. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," Security Protocols, 7th International Workshop, LNCS, Springer-Verlag, 2009.

[8]. Kuldeep Sharma, Neha Khandelwal and Prabhakar.M, "An Overview Of security Problems in MANET," http://psrcentre.org/images/extraimages/155.pdf

[9]. Sevil Şen, John A. Clark, Juan E. Tapiador , "Security Threats in Mobile Ad Hoc Networks", Department of Computer Science, University of York, YO10 5DD, UK

[10]. Saloni Sharma and Anuj Kumar Gupta, "A Comprehensive Review of Security Issues in Manets," http://anujkgupta.webs.com/pxc3888277.pdf

[11]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Carde "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" in proceedings of WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.) 2006 Springer

[12]. R.Devi, B.Sumathi, T.Gandhimathi, G.Alaiyarasi, "Performance Metrics of MANET in Multi-Hop Wireless Ad Hoc Network Routing Protocols" in proceedings of International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005 National Conference on Architecture, Software system and Green computing.

[13]. Priyanka Goyal, Vinti Parmar, Rahul Rishi " MANET: Vulnerabilities, Challenges, Attacks, Application" in proceedings of IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[14]. Robinpreet Kaur & Mritunjay Kumar Rai "A Novel Review on Routing Protocols in MANETs" in

[15]. proceedings of Undergraduate Academic Research

[16]. Anil Suryavanshi and Dr. Poonam Sinha "Efficient techniques for saodv in mobile adhoc network" in proceedings of Journal of Global Research in Computer Science, Volume 2, No. 8, August 2011.

[17]. Mohd Anuar Jaafar and Zuriati AhmadZukarnain "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment" in proceedings of European Journal of Scientific Research ISSN 1450-216X Vol.32 No.3 (2009), pp.430-443

[18]. Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani "A Survey of Secure Mobile Ad Hoc Routing Protocols" in proceedings of IEEE communications surveys & tutorials, vol. 10, no. 4, fourth quarter 2008.