IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

An Analysis of ASRP Secure Routing Protocol for MANET

Tarun Dalal[1], Gopal Singh[2]

[1]M.tech Student, Department of Computer Science and Applications,
M. D. University, Rohtak-124001, Haryana, India
tarundalal88@gmail.com

[2]Assistant Professor, Department of Computer Science and Applications,
M. D. University, Rohtak-124001, Haryana, India
gsbhoria@gmail.com

Abstract

Mobile ad hoc networks (MANET) can be defined as a collection of large number of mobile nodes that form temporary network without aid of any existing network infrastructure or central access point. Each node participating in the network, acts both as host and a router and must therefore is willing to forward packets for other nodes. The characteristics of MANET provides large amount of degree of freedom and self-organizing capability that make it completely different from other network. Due to this nature of MANET, design and development of secure routing is challenging task for researcher in an open and distributed communication environments.

The main work of this paper is to address the security issue, because MANET is generally more vulnerable to various attacks, so we proposed a secure routing protocol for MANET, named ASRP (Authenticate Secure Routing Protocol) based on DSDV (Destination- sequence distance vector). This protocol is designed to protect the network from malicious and selfish nodes. We are implementing Extended Public key Cryptography mechanism in ASRP in order to achieve security goals.

Keywords: *MANET, Security, Cryptography. DSDV, OLSR, SEAD, SAR, SOADV, Ariadne, Aran, EPKCH.*

1. INTRODUCTION

MOBILE AD-HOC NETWORKS - Ad hoc networks offer methods for self-organizing networks. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multi-hop paths through the network to any other node.

Thus, this is the idea of Mobile ad hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network. The area of mobile ad hoc networking deals with devices equipped to perform wireless communication and networking. Wireless devices form a network as they become aware of each other's presence. They communicate directly with devices inside their radio range in a peer-to-peer nature.

ROUTING IN MANETS - Routing in mobile ad hoc networks faces additional problems and challenges when compared to routing in traditional wired networks with fixed infrastructure. There are several well known protocols in the literature that have been specifically developed to cape with the limitations imposed by ad hoc networking environments. Most of the existing routing protocols follow two different design approaches to confront the inherent characteristics of ad hoc networks, named the table-driven and the source-initiated on-demand approaches. Routing Protocols characteristics and types are shown in table.

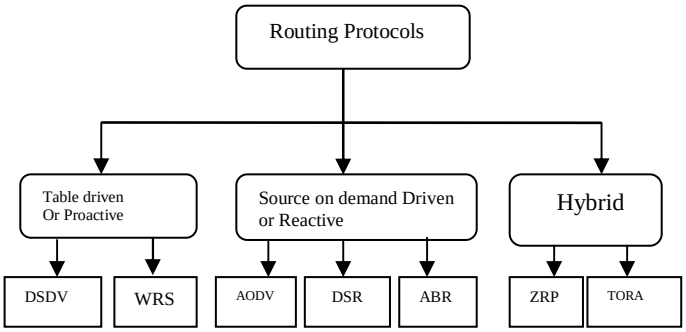

Table-Driven Ad-Hoc Routing Protocols:- Table-driven ad hoc routing protocols maintain at all times routing information regarding the connectivity of every node to all other nodes that participate in the network. Also known as proactive, these protocols allow every node to have a clear and consistent view of the network topology by propagating periodic updates. Therefore, all nodes are able to make immediate decisions regarding the forwarding of a specific packet. As an example of two protocols that follow the table driven design approach we will briefly present the Destination-Sequenced Distance-Vector (DSDV) protocol and the Optimized Link State Routing (OLSR) protocol.

-Destination Sequenced Distance-Vector Routing (DSDV):- DSDV is a table-driven routing protocol based on the Bellman-Ford algorithm. The DSDV protocol can be used in ad hoc networking environments by assuming that each participating node acts as a router. Each node must maintain a table that consists of all the possible destinations. DSDV protocol adds a sequence number to each table entry assigned by the destination node, preventing the formation of routing loops caused by stale routes. The routing tables are maintained by periodically transmitted updates by each router to all the neighboring routers.

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

-Optimized Link State Routing (OLSR):- The Optimized Link, State Routing (OLSR) protocol is a proactive link state routing protocol based on the Open Shortest Path First (OSPF) protocol. OLSR has been specifically developed, to support mobile ad hoc networks. The OLSR protocol can be conceptually divided into three different operations, namely neighbor sensing, distribution of signaling traffic and distribution of topological information. The distribution of topological information function is realized with the use of periodic topology control messages that result in each node knowing a partial topology graph of the network which is then used for the computation of optimal routes. Types of Attacks in MANETs: Flooding Attack, Black hole Attack, Link Spoofing Attack, Wormhole Attack, Colluding Miss-relay Attack.

SOURCE-INITIATED ON AD HOC ROUTING PROTOCOLS - According to this approach a route is created only when the source node requires one to a specific destination. A route is acquired by the initiation of a route discovery function by the s node. The data packets transmitted while a route discovery is in process are buffered and are sent when the path is established. An established route is maintained as long as it is required through a route maintenance procedure. The Ad hoc On-demand Distance Vector (AODV) routing protocol and the Dynamic Source Routing protocol are examples of this category of protocols, also known reactive protocols.

-Ad hoc On-demand Distance Vector Routing (AODV):- The AODV protocol Uses route request (RREQ) messages flooded through the network in order to discover the paths by a source node. An intermediate node that receives a RREQ replies to it using a route reply message only if it has a route to the destination whose corresponding destination sequence number is greater or equal to the one contained in the RREQ. This effectively means that an intermediate node replies to a RREQ only if it has a fresh route to the destination. Otherwise, an intermediate node broadcasts the RREQ packet to its neighbors until it reaches the destination.

-Dynamic Source Routing (DSR):- The Dynamic Sour Routing protocol is based on a method known as source routing. The route discovery process in DSR is similar to the one used by AODV, except that each intermediate node that broadcasts a route request packet adds its own address identifier to, a list carried in the packet. The destination node generates a route reply message that includes the list of addresses received in the route request and 'transmits it back along this path to the source. Route maintenance in DSR is accomplished through the confirmations that nodes generate when they can verify that the next node successfully received a packet.

SECURITY GOALS:-

-***AUTHENTICATION***: This service verifies the identity of node or a user to be able to prevent impersonation. Authentic can be provided using encryption along with cryptographic hash function, digital signature and certificates.

-***CONFIDENTIALITY***: Keep the information sent unreadable to unauthorized users or nodes. One way to keep information confidential is to encrypt the data, and another technique is to use directional antennas, it also ensures that the transmitted data can only be accessed by the intended receivers.

-***INTEGRITY***: Ensure that the data been not altered during transmission. The integrity service can be provided using cryptography hash function along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.

-***AVAILABILITY***: Ensure that the intended network security services listed above are available to the intended parties when required. The availability is typically endure by redundancy physical protection and other non-cryptographic means, e.g. use of robust protocol.

-***ACCESS CONTROL:*** To prevent unauthorized use of network services and system resources: Obviously, access control is tied to authentication attributes. In general, access control is the most commonly type of service in both network communications and individual computer systems.

-***VULNERABILITY IN MANET:*** Malicious and selfish nodes are the ones that fabricate attacks against physical, link, network, and application-layer functionality. Current routing protocols are exposed to two types of attacks.

- Active attacks
- Passive attacks

Table: Classification of Security Attacks

Active attacks	Spoofing, Fabrication, Wormhole Attack, Modification, Denial of Service
Passive Attacks	Eavesdropping, traffic analysis, monitoring

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.

• **Spoofing:** Occurs when a malicious node misrepresents its identity order to alter the vision of the network topology that a benign node can gather.

• **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 neighbor can no longer be contacted.

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

• **Wormhole Attack:** An attacker record packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols.

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

• **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. The nature of ad-hoc networks, where several routes exist between nodes and routes are very dynamic gives ad hoc a built-in re to Denial of Service attacks, compared to fixed networks.

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. The goal of opponent is to Obtained information that is being transmitted. Passive attacks are very difficult to detect because they do not involve any alteration of data.

• **Black-hole attack**: In a black hole attack a malicious node advertising itself as having a valid route to the destination. With this intension the attackers consume or intercept the packet without any forwarding. An attacker can completely modify the packet and generate fake information, this cause, the network traffic diverted or dropped.

• **Rushing attack:** If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a norm multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne.

• **Replay attack**: An attacker that performs a replay attack retransmitted valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solution.

• **Location disclosure attack**: An attacker discover the Location of anode or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques; or with simpler probing and monitoring approaches Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in .the traffic pattern. The leakage of such information is devastating in security.

SECURE AD HOC ROUTING: There exist several proposals that attempt to architect a secure routing protocol for mobile ad hoc network, In order to often protection against in the previous section. There are several solution proposed by researcher, they are either completely new stand-alone protocol or in some cases incorporation of security mechanism into existing one like DSDV and AODV Since routing is an essential function for ad hoe networks, the integrated security procedures should not hinder its operation. In order to analyze exiting solution in structured way we have classified them into three categories; Solution based on Symmetric cryptography, solution based on Asymmetric cryptography and Hybrid solution.

SYMMETRIC CRYPTOGRAPHY SOLUTIONS:-

-SEAD- The Secure Efficient Ad hoc Distance Vector (SEAD) is a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector (DSDV) algorithms. For developing SEAD, the table driven approach is followed. It is also known as proactive routing protocol. In order to find shortest path, between two nodes, the distance vector routing protocol utilizes a distributed version of Bellman Ford Algorithm. The SEAD routing protocol proposed two different methods in order to authenticate the source of each routing updates. The first method require clock synchronization between nodes that participate in the network and the second method require the existence of shared secrete between each pair of nodes.

-SRP: Secure Routing Protocol (SRP) was developed based on estimation Source Routing protocol (DSR). The operations of SRP require the existence of a Security association (SA) between source node initiating a route query and the destination node. The security association can be utilized in order to establish shared secret key between the two nodes, which is used by SRP. The SRP protocol appends a header (SRP header) to the packet basic protocol. The source node sends a route request with a query sequence number (QSEQ) that is used by the destination in order to identify outdated requests a random query identifier (QID) that is us identify the specific request. The intermediate nodes broadcast the query to their neighbors, after updating their routing tables.

-Ariadne: Ariadne is a secure routing protocol developed by Yih-Chun F David B. Johhson and Adrian Perrig based on the Dynamic Source Routing protocol (DSR). Ariadne is an on-demand routing protocol, which find routes as when it required, dynamically. Ariadne uses MAC and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime. It contains two phases in its routing mechanism; Route discovery and Route maintenance.

ASYMMETRIC CRYPTOGRAPHY SOLUTIONS

-ARAN: The Authenticate routing for ad hoc network (ARAN) is a secure routing protocol for MANET, developed by Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz and Elizabeth M. Belding-Royer based on AODV. ARAN utilizes cryptography mechanism in order to achieve security goals such as; authentication, message integrity, and non-repudiation in ad-hoc network. It uses asymmetric cryptography to secure routing in an ad hoc network and require universal

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

trusted third party. It consists of three distinct opera stages: the first stage is the preliminary certification process that requires existence of a trusted certificate authority (CA). The second operational stage of the protocol is the route discovery process that provide end-to-end authentication. The third operation stage of ARAN protocol is optional and ensures that the shortest path is discovered. ARAN uses public key cryptography and a central certification authority server, for node authentication and neighbor node authentication in route discovery. It prevents spoofing attacks using a timestamp.

-SAR: SAR was developed using a trust-based framework. Each node in the network is assigned with a trust level. So the attacks on this framework can be analyzed based on trust level and message integrity. Security of SAR can be evaluated in terms of trust level and message integrity.

Trust Level*:* SAR routing mechanism is based on the behavior associated with the trust level of a user. It is a binding between the identities of the user are the associated trust level. To follow the trust hierarchy, cryptographic technique like: encryption, public key certificates shared secrets, etc. are employed.

Message integrity: The compromised nodes can utilize the information flow between nodes and reading of packets to: launch attacks. It results in corruption of info confidentiality of the info and in de of network services. The Security analysis on the attack patterns is based on the trust based framework. So the analysis depends on the key management used and the cryptographic systems applied.

HYBRID SOLUTIONS:- In this category we have included the secure routing protocols that employ both symmetric and asymmetric cryptographic operations. The most common approach is to digitally sign the immutable fields of routing messages in order to provide integrity and authentication, and to use hash chains to protect the hop count metric.

-SAODV: Secure Ad hoc On-demand Distance Vector (SAODV) is a proposal for security extensions to the AODV protocol. The proposed extensions utilize digital signatures and hash chains in order to secure AODV packets. In order to facilitate the transmission of the information required for the security mechanisms, SAODV defines extensions to the standard AODV message format. These SAODV defines extensions consist of the following fields. The hash function field identifies the one way hash function that is used. SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and has chain is used to prevent the altering of node counts.

Table: Shows mapping between the attack patterns and protocols

Protocols	***SEAD***	***Ariadne***	***SRP***	***ARAN***	***SAR***	***SOADV***
DoS	Yes	Yes	Yes	Yes	Yes	Yes
Tunnelling	Yes	Yes	Yes	Yes	Yes	Yes
Spoofing	Yes	No	No	No	No	No
Blackhole	Yes	No	No	No	No	No
Wormhole	Yes	Yes	Yes	Yes	Yes	Yes
Routing table overflows	Yes	No	No	No	No	No

Yes = Attack Possible, No = Attack not Possible

II. EXISTING WORK

INTRODUCTION TO EXTENDED PUBLIC KEY CRYPTOGRAPHY: The word "Cryptography" is derived from Greek word means "secrete writing." It provides set of mathematical tools for securing information. Cryptography can be used to protect sensitive and valuable information from malicious hackers. The fundamental goals of cryptography are: confidentiality, data integrity, authentication and non-repudiation. There are mainly two categories of cryptography mechanism that are used for designing security based system. One is Symmetric key Cryptography and other is Public key Cryptography.

SYMMETRIC KEY CRYPTOGRAPHY: This crypto-system used same key for both encryption and decryption. It is also known as Secrete key Cryptography. Both sender and receiver have the same key, when they communicate to each other.

The Advantages of Symmetric key Cryptography are:

- Widely used and very, popular,
- Very fast relative to other crypto-system, and
- Cipher text is compact.

The Disadvantages of Symmetric key Cryptography are:

- Non-repudiation is not possible,
- Require large number of keys to communicate.
- Key length is small compared to public key cryptography.

PUBLR KEY: CRYPTOGRAPHY:- This crypto-system uses two keys, one key for called public key and other key for decryption called private key or secrete key (Also known as Asymmetric key cryptography). Each user has two key one public key and other private key. The public key of each user is available to all other user in public key database. The public key and private key are mathematically linked. Encryption is performed using public key and decryption is performed using private key.

The Advantages of Public key Cryptography are:

- Support Non-repudiation
- Consider to be very secure, and
- The number of keys managed by each user is much less than symmetric key cryptography

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

The disadvantages of public key cryptography are:
• Much slower than Secrete Key cryptography
• Key length is large
• Cipher text is much larger than plain text.

III. PROPOSED WORK

EXTENDED PUBLIC KEY CRYPTOGRAPHY (EPKCH):- The extended Public key Cryptography is a modified form of public key cryptography. To generate public key and private key, each node utilized RSA algorithm. This cryptosystem is mainly designed for securing data during packet forwarding operation and also to detect malicious and selfish node during network initialing and packet forward operation. As we discussed above the symmetric key cryptography and public key cryptography are limited in their operation, they do not possess the requisite feature to secure the MANET operation. So, existing public key cryptography mechanism has been extended to secure the MANET operation. The extended public key cryptography mechanism is basically suited for MANET environment but apart from MANET, it is suited well for other environment also. Confidentiality is the basic feature provided by the public key cryptography but extended public key cryptography also provides authentication, non-repudiation and integrity.

COMPARISON: The following is the comparison table of the EPKCH with other.

Support for	Symmetric key Cryptography	Public Key Cryptography	Extended Public Key Cryptography
Non-repudiation Features	No	No	Yes
Message Authentication features	No	Yes	Yes
Packet modification Features	No	No	Yes
Number of key required for the n node	N*(n-1)/2	2*n i.e. n private key and n public key	2*n i.e. n private key and n public key

INTRODUCTION TO DESIGN, DEVELOPMENT AND SIMULATION OF ASRP: The ASRP is a proactive secure routing protocol. The design of ASRP follows the table driven approach, in which each node maintains, a node into table regarding network structure, route information from a particular source to its all possible destinations and information about other nodes. When a new node enters into network all the nodes updated its own info table. This means that every node have complete knowledge about the network structure. The ASRP is a proactive secure routing protocol. The design of ASRP follows the table- driven app in which each node maintains, a node info table regarding network structure, route information from a particular source to its all possible destinations and information about other nodes. When a new node enters into network all the nodes updates its own info table. This means that every node have complete knowledge about the network structure. When nodes finish initialization they switch themselves to Lazy mode (LM), where they are waiting for forward the packet. Lazy mode is the default mode of each node when they do not do an If any node wants to forward the Pack Forward packet they switch from lazy mode to monitor mode (MM), and then to packet forwarding mode (PFM). As soon as they finished the packet forwarding they switch back to lazy mode. In lazy mode the lazy node forwards the Pack Lazy packet to its neighbor node.

So, there are four modes corresponding to different activity of node. The IM is responsible for the establishment of MANET LM is the default Ode of the node where they do not do anything MM mode is responsible for monitoring the network and node, while nodes leaving and joining the network, The IM also detects the malicious and selfish node Within the network The PFM also detects the malicious and selfish node during packet forwarding operation.

ASSUMPTIONS: Proposed secure protocol aims to protect the network from attackers. Proposed schemes work under several assumptions as follows.
- The network link should be bidirectional that is, if node A is able to transmit to node B, then B must also l able to transmit to A
- The wireless interface should support promiscuous mode operations that is, each node can receive a copy of the messages being transmitted by other nodes within its receiving range
- A public key infrastructure must exist in the MANET under consideration. Each mobile node stores the public key of all other nodes.
- The trust relation could be instantiated. For example: by knowing public key of other nodes.
- There must be a security association between source node and destination node.
- There must be a security association between source node and destination node.
- The existence of security association should be justified because, host choose to employ a secure communication schemes and consequently, should be able to authenticate each other.

IV. CONCLUSION

Wireless mobile ad hoc networks present difficult challenges to routing protocol designers. Mobility, constrained bandwidth, and limited power cause frequent topology changes. The very basic nature of the mode of

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

communication is the main concern because anything that moves over the open air medium is susceptible to be picked up by unauthorized access. In ASPR protocol we discuss activity of nodes which they are shown during the MANET operation and these activities are grouped into modes along their working.

V. FUTURE SCOPE

The proposed secure routing protocol, ASRP, is a proactive routing protocol based on table driven approach. For the future work, we can use hybrid approach or reactive approach in ASRP to implement a new secure routing protocol. We can also add another mode or existing one can be extended to handle some exceptional condition. The public key cryptography algorithm can also be extended to future enhance the security in MANET.

VI. REFRENCES

[1] Raj Tirthraj,Verma A K, " Survey and Analysis of secure routing protocols for MANETs," in the proceeding of National Conference on cutting Edge Computer and Electronics Technology (CECT 2009), Pantnager, February14-16,pages501-06

[2] E.M Royer, C.K Toh,"A Review of Current Routing Protocol for Ad Hoc Mobile Wireless Network," IEEE Personal communication,vol-2,no.6,6 April 2007, pp46-55

[3] Zapata, M.G.," Secure ad-hoc on demand distance vector (SAODV) routing, IETF MANET, internet draft (Work in progress),draft-guerreromanet-saodv-00.txt,2001. Accessed 10/10/2006.

[4] C.E Perkins, E.M. Royer, and S. Das, "Ad hoc On-demand Distance Vector(AODV),"RFC3561, july 2005.

[5] C.Murthy and B.Manoj, "Ad hoc Wireless Network: Architectures and Protocols" Prentice Hall PTR,2005.

[6] A.Verma, "Mobile Ad hoc Network (MANETs): An Introduction", in TIC Newscaster(a quarterly newsletter of Thapar technology Campus), pp.13-14, April 2004.

[7] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L: Security in mobile ad hoc networks Challenge and solution. IEEE wireless communication, 11,1,(2004), 38-47.

[8] A K Verma, mayank Dave and R C Joshi, "Classification of Routing Protocols in MANET", at National Symposium on Emerging Trends in Networking & Mobile Communication (NSNM-2003),pp. 132-139, Sept 5-6, 2003.

[9] Y.C. Hu, A. Perrig, and D.B. Johnson," Ariadne: A Secure On Demand Routing Protocol for Ad hoc Network," in Proceeding of 8 ACM Int'l, Conf. on Mobile comp, Georgia, September2003.

[10] M. llyas, "The Handbook of Ad hoc Wireless Network," CRC Press, 2003.

[11] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", http://www.cl.cam.ac.uk/~fms27/duckling/duckling.html, April 1, 2000.

[12] B. R. Smith and J.J. Garcia-Luna-Aceves, "Securing the Border Gateway Routing Protocol," Proceedings of Global Internet '96, November 1996.

[13] D. B. J., Yih-Chun Hu, Adrian Perrig, "Ariadne: A secure on-demand routing protocol for ad-hoc networks", Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), Sept. 2002.

[14] Kai Inkinen, "New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes", Helsinki University of Technology T-110.551, Seminar on Internetworking, Sjökulla, 2004-04-26/27.

[15] Wenjia Li, Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks- A Survey", Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, http://www.cs.umbc.edu/~wenjia1/ 699_report.pdf, 2008

[16] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, September 2002, pages 12-23.

[17] K. Sanzgiri, B. Dahill, B. Levine, E. Royer and C. Shields. A Secure Routing Protocol for Ad hoc Networks. Proceedings of the tenth IEEE International Conference on Network Protocols, November 2002, pages 78-87.

[18] Y. Hu, D. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. In Fourth IEEE Workshop on Mobile Computing Systems and Applications, June 2002, pages 3-13.

[19] Sonja Buchegger and Jean-Yves Le Buddec, "Increasing Routing Security in Mobile ad hoc Network," IBM Research Report: RR 3354,2001

[20] C.E Perkin and E.M Royer, "The Ad hoc On-demand Distance Vector Routing Protocol," in C.E Perklin(ed.), Ad hoc Networking; pp173-219;Addison-2000.

[21] B.Dahill, B.N. Levine,E. Royer, and C. Shields, "ARAN: A Secure Routing Protocol for Ad hoc Network," UMass tech Report 02-32, 2002.

[22] A. Salomaa, "Public Key Cryptography," Springer-Verlag,1996.

[23] B.Schneier, Applied Cryptography,Wiley,1996

[24] P.Papadimitratos and Z.Haas, "Secure Routing for Mobile Ad hoc Network," in proc.ofCNDS 2002.

[25] M.G Zapata and N. Asokan, "Secure Ad hoc Routing Protocols," in Proceeding of the ACM Workshop on Wireless Security, Atlanta, GA September, 2002.