Improved Security for Attacks in MANET using AODV

Dadaso Mane
PG Student, Department of Computer Engineering
D. Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India

Deepali Gothwal
Assistant Professor, Department of Computer Engineering
D. Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India

Abstract- Mobile ad hoc network (MANET) is a dynamic infrastructure-less network with a lack of centralized management. MANET is a collection of mobile nodes which is formed mechanically where nodes exchange packets to allow communication among nodes hop by hop which are outside the wireless transmission range. Due to this ad hoc networks are vulnerable to attacks those influence network performance and reliability. Entire network may collapse without security feature in routing protocols. Currently, numerous routing protocols have been proposed for MANET. In this paper we have modified AODV routing protocol to fulfill the high level security goal like data integrity. The comparative analysis of values obtained for number of packets received, Average end-to-end delay, Bandwidth utilization and Energy consumption has been done from implementation of proposed system using simulating environment NS2.35.

Keywords – Network Security, Ad-hoc networks, AODV, Secure Routing Protocols, Security service.

I. INTRODUCTION

MANET has dynamic topology which forms network with a group of autonomous mobile nodes or devices connected through wireless links without centralized management. In MANET, each mobile node consists of wireless transmitter and receiver allowing communication with other nodes in its radio transmission range. In order to forward a packet from source node to destination node that is out of its radio range, the intermediate nodes in the network should be cooperative which is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time as shown in fig. 1 [1].

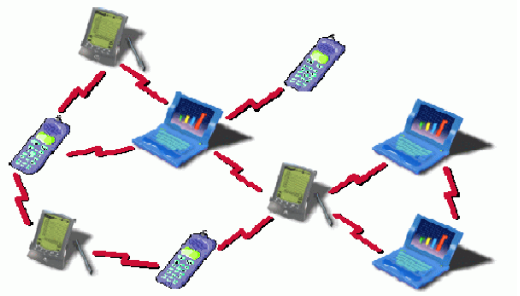

Fig.1. Mobile Ad hoc Networks

There are several characteristics of MANETs which present challenges such as shared wireless medium, open peer-to-peer network architecture, and highly dynamic network topology. Due to the lack of a centralized administration, routing protocols in MANET dependent on cooperation between nodes and assumed that all nodes act in a well behaved way and provides reliability during communication. However, in a hostile environment scenario, each malicious node will initiate routing attacks to stop routing operations or denial-of-service (DoS) attacks [4] for denying services to trustable nodes.

The rest of the paper is organized as follows. Related work II. Proposed system algorithm and mathematical model are explained in section III. Experimental results are presented in section IV. Concluding remarks are given in section V.

II. RELATED WORK

In MANET, there are two approaches for protection: proactive (e.g., OLSR) and reactive (e.g., AODV). In reactive routing protocols, nodes find routes only when they must send data to the destination node whose route is unknown. Whereas, in proactive protocols, nodes periodically exchange topology information, and hence nodes can obtain route information any time they must send data [3]. Attacks in ad hoc networks can be classified as: active or passive attacks [1]. In the case of passive attack, the attacker node listens to the channel without sending any message during communication. It attempts to discover valuable information rather than disrupting the operation of a protocol. In the case of active attack, the attacker node will be directed to stop the normal operation of each individual node or degrade the performance of the ad hoc network as a whole.
Mobile nodes doing communication in MANET face many attacks which include denial of service, packet delay, packet modification, packet dropping, and spoofing, etc. In order to combat such attacks, MANET protocols must meet necessary security goals. The goal of the security solutions for MANET is to provide security requirements such as Data confidentiality, data integrity, authentication, availability, non-repudiation and access control [2]. Above security requirements can be implemented in routing protocols based on the requirements.

These security goals are briefly defined as follows:

- *Authentication* ensures that communication from one node to another is genuine. In other words, it ensures that a malicious node cannot masquerade as a trusted network node.
- *Data confidentiality* ensures that a certain network content is never disclosed to unauthorized entities other than its (their) desired recipient(s). Data confidentiality is generally achieved by using cryptographic mechanisms such as symmetric or asymmetric data encryption.
- *Integrity* denotes the authenticity of data sent from one node to another. That is, it ensures that a message sent from node A to node B was not modified by any malicious node C during its transmission.
- *Non-repudiation* is the ability to ensure that a node cannot deny the sending of a message that it originated.
- *Availability* ensures services are usable when needed, thus routes returned by ad hoc routing protocols must be valid and must remain functional.

The attacks against MANETs and implementing security mechanisms to obtain security goals may be at any level of the protocol stack. For instance, confidentiality can be part of the application-transport layer to provide end-to-end data privacy or can provide link-to-link security at the link layer. Present protocol security enhancements generally focus on each individual goal, directing towards the route discovery phase as well as data communication phase [7]. Moreover to route discovery and data communication, the MANET routing protocol developer must also consider the underlying cryptographic mechanisms to provide secure solutions.

Secure Routing

In MANET there are various possible attacks, to protect against these attacks a routing protocol must fulfill a set of requirements [9] to ensure that the specified path from source to destination works correctly in the presence of malicious nodes. Currently, numerous secure routing protocols that enacts with malicious nodes that can stop the present working scenario of a routing protocol by changing routing information, by artifacting false routing information and by acting like other nodes.

1. SAODV (Secure Ad-hoc On-Demand Distance Vector) SAODV [13, 15] is a proposed set of extensions of AODV routing protocol. There are two techniques: one way hash chains used to secure the hop count information and digital signatures used to authenticate the non-mutable fields of the message. These two techniques are used to provide authentication, message integrity and non-repudiation in ad hoc networks. It needs the use of Key Management Scheme. The primary drawback of this protocol is it requires large amount of processing power and degrades the speed of the process to some extent due to the use of Public Key Cryptography.

2. ARAN (Authenticated Routing for Ad-hoc Networks) ARAN [12] is a standalone protocol based on AODV which provides authentication, message integrity and non-repudiation in ad-hoc networks by using cryptographic public key certificates issued by an authorized entity. It is followed by a route process to ensure end-to-end security services. But it requires the use of trusted certification server. The primary drawback of this protocol is each node that exchanges a route discovery or a route reply message must be signed. This process is very much power consuming and results into increase in the size of the routing messages at each hop during communication.

3. SRP [11].The Secure Routing Protocol (SRP) provides end-to-end authentication which can be implemented in existing ad-hoc routing protocols with many security enhancements. The ultimate goal of the proposed scheme is to incorporate a security association between the sender node initiating the query and the intended destination. A shared secret has been established between sender node and destination node using this security association. By the use of a shared secret, the non-mutable fields of the forwarded routing messages are protected. This scheme is reliable where a number of non-colluding nodes are present, and provides correct routing information time-to-time. In SRP, the intermediate nodes those exhibit arbitrary and malicious behaviors are not accounted during communication.

4. ARIADNE [16], an on-demand secure ad hoc routing protocol, depends on highly efficient symmetric cryptography to provide security against malicious nodes. It prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes. ARIADNE uses a shared key between the two parties and the MAC that ensures end-to-end authentication of a routing message. Efficient combination of one way hash function and shared keys makes ARIADNE more secure. ARIADNE provides a protection against attacks that modify and fabricate routing information. When it is used with an advanced version of TESLA [17], it is immune to wormhole attacks. However, it is still vulnerable to selfish node attack. General security mechanisms are very reliable but key exchanges are complicated, making ARIADNE infeasible in the current ad hoc environments.

III. Proposed system Algorithm and mathematical model

A. Steps to create message digest at sender and receiver end

There is a Message Digest with hash value of IV as a key to provide data integrity. This mechanism produces a message digest using initial vector (IV) which is available with sender and receiver of an AODV message. And then message digest will be transmitted to receiver which receives it by decrypting it. The Message Digest with a hash value of IV as a key will be obtained as follows:

a. Every time a node originates a RREQ, a RREP or a RERR message, it performs the following operations:

- It uses initial vector value of hash function h that is to be used to make message digest.
- Sets Hash-Function field by initial vector.
  Hash-Function = h Where, h is the value of hash function.
- Get the value of initial vector, and this initial vector is available as a key with all nodes.
- Generates Message-Digest by using initial vector value for the first time.
  For next transmissions to generate message digest hash value of initial vector will be used.
  Message-Digest = h (initial vector) Where, h is a hash function. h(x) is the result of applying the function h to x.

b. In addition, every time a node receives a RREQ, a RREP or a RERR message, it performs the following operations in order to verify the valid message:

- Use the initial vector value to decrypt the message digest available with target node for the first time.
- Uses the hash value of initial vector for subsequent message digests for the decryption and verifies that the received message is equal to the value contained in the Message-Digest field of received AODV message.

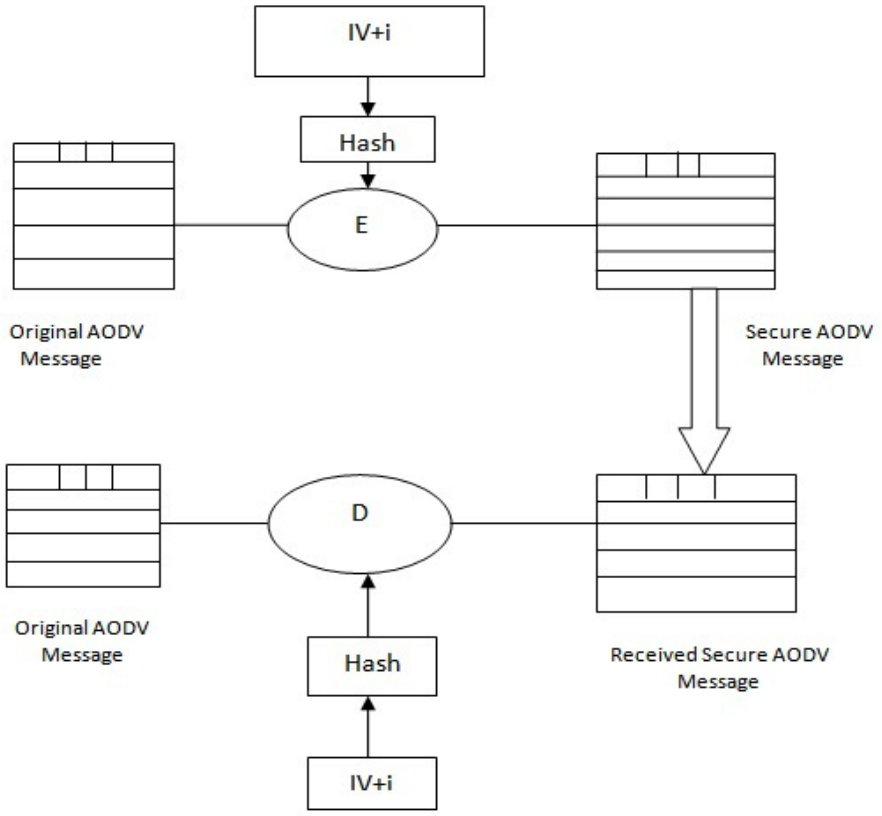

Figure 2: Message encryption and decryption using hash value of IV as a key

B. Mathematical Model of the proposed system

The objective is encrypting the data and decrypting at destination end using hash value of IV as a key. To overcome such a situation, sender and receiver nodes will have a unique value i.e. Initial Vector (IV). This IV will be used to encrypt and decrypt the message for the first time. When second message will be sent during that time using SHA1 hash value of IV will be generated and used to encrypt and decrypt the message and so on. When there will be number of messages exchanged among all the nodes, it will be difficult to find the exact message for the attacker node after some time. This is the advantage of this technique.

Assumption: Initial Vector (IV) value is available with sender and receiver.

Sender side:

Initialize Counter to IV (for first time only);
While (there is a packet to be sent) do;
If (first packet);
i=0;
Encrypt packet using IV as a key;
C= E (M, IV);
Send packet(C);
Continue;
Else (second packet onwards)
i++;
IV'= IV+i;
H= SHA1 (IV');
Encrypt packet using H as a key;
C= E (M, H);
Send packet(C);

Continue;

Receiver side:

Verify destination of Packet and accept it only if intended destination;
Initialize Counter to IV (for first time only);
While (there is a packet to be sent) do;
If (first packet);
i=0;
Decrypt packet using IV as a key;
M= D (C, IV);
Send packet (M);
Continue;
Else (second packet onwards)
i++;
IV'= IV+i;
H= SHA1 (IV');
Decrypt packet using H as a key;
M= D(C, H);
Send packet (M);
Continue;

IV. EXPERIMENT AND RESULT

In a given constrained environment, proposed system providing more secured communication which fulfills security requirement such as message authentication, data confidentiality and data integrity security requirements but consuming much power of nodes. The proposed system's focus is more concentrated to provide better secure routing using modified AODV by the use of Initial Vector (IV) concept and security algorithm SHA

Parameter	**Value**
MANET area	600 _ 600 sq. m.
Total no. of nodes	25
Movement Pattern	Random Way-point
Node Speed	0 up to 20ms
No. of packets generated	1000 packets per CBR
Application	CBR
Size of packet	512 bytes
Simulation time	200 seconds

Table1: Simulation Pattern

NS-2 is a discrete event, object oriented, simulator developed by the VINT project research group at the University of California at Berkeley. The Monarch research group at Carnegie Mellon University [8] has developed a simulator which includes: nodes mobility, a realistic physical layer that includes a radio propagation model, radio network interfaces and the IEEE 802.11 Medium Access Control (MAC) protocol using the Distributed Coordination Function (DCF).

MD5 is faster but not secure than SHA1. It produces a message digest of 128 bits. MD5 provides essentially no security against collisions: it is easy to find collisions in MD5. In contrast, SHA1 appears to be much more secure than MD5 but slower. It produces a message digest of 160 bits. SHA-1 is not only used for security but also for ensuring that the data has not changed. While there are some known attacks on SHA1, they are much less serious than the attacks on MD5. For this reason, SHA1 is a much better choice than MD5. The simulation experiments are developed and simulated on an Intel Corei5 2.40 GHz machine using Ubuntu 10.11 with 4 GB RAM and the network simulator NS2 version NS-2.35.

1. *Average end-to-end delay*: the average delay between the sending of packets by the source and its receipt by the receiver. End-to-end delay indicates how long it took for a packet to travel from the CBR source to the application layer of the destination. It represents the average data delay an application or a user experiences when transmitting data. It is given by equation

$$Da=Tr-Ts$$

Where, Da- average end-to-end delay, Tr- Received packet time, Ts- Sent packet time.

Nodes	End-to-end Delay(MD5)	End-to-end Delay (SHA1_IV)
0	0.02568	0.3688
5	0.02640	0.3789
11	0.02688	0.4522
12	0.02752	0.4074
14	0.02832	0.4212

Table 2: Experiment values of End-to-end Delay for MD5 and SHA_ IV

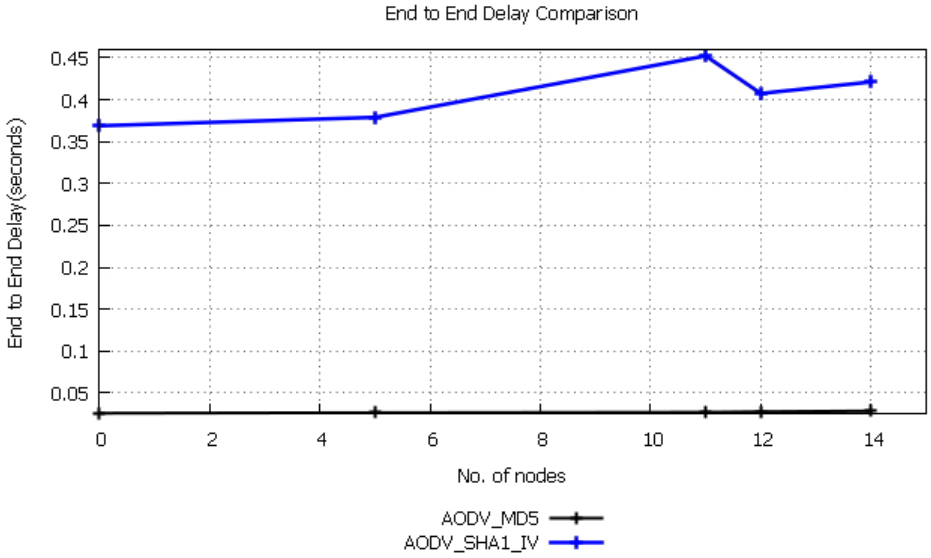

Figure 3: Graph of No. of nodes vs Delay

2. *Bandwidth Utilization*: the average rate of successful data transfer through a communication path.

Nodes	Bandwidth Utilization(MD5)	Bandwidth Utilization(SHA1_IV)
0	5.9135	63.6652
5	5.9807	63.6652
11	5.9807	63.6652
12	6.1151	63.6652
14	6.2495	63.6652

Table 3: Experiment values of Bandwidth Utilization for MD5 and SHA1_IV

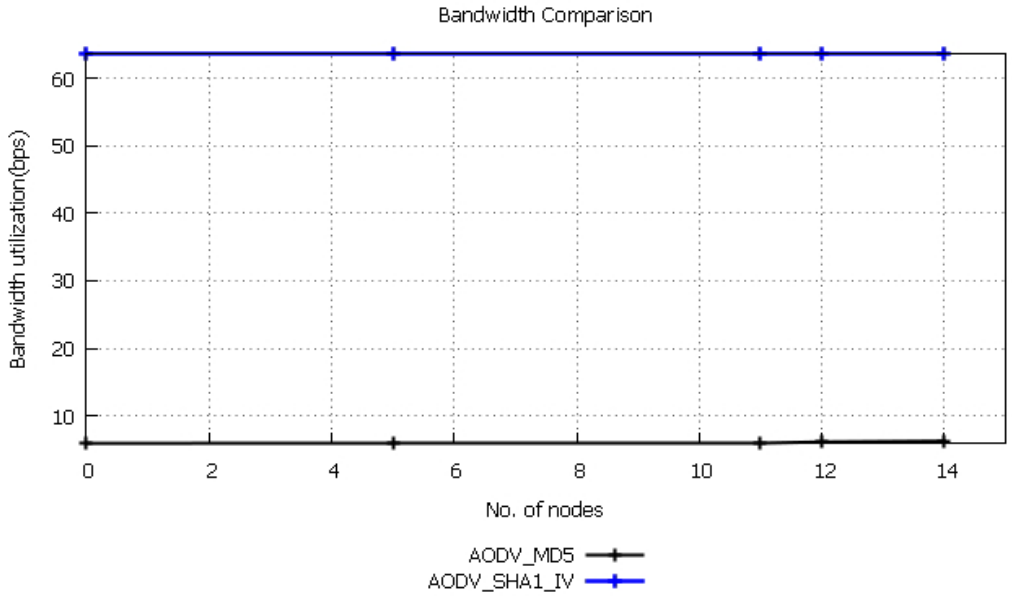

Figure 4: Graph of No. of nodes vs Bandwidth Utilization

3. *Packet Delivery ratio*: the ratio of number of data packets delivered to the destinations to the number of data packets generated by the sources. Packet delivery ratio is calculated by dividing the number of packets layer of the source (i.e. CBR source). It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ratio, the more complete and correct is the routing protocol.

Nodes	No. of packets received(MD5)	No. of packets received(SHA1_IV)
0	321	4611
5	330	4737
11	336	5653
12	344	5093
14	354	5265

Table 4: Experiment values of Packets received for MD5 and SHA1 IV

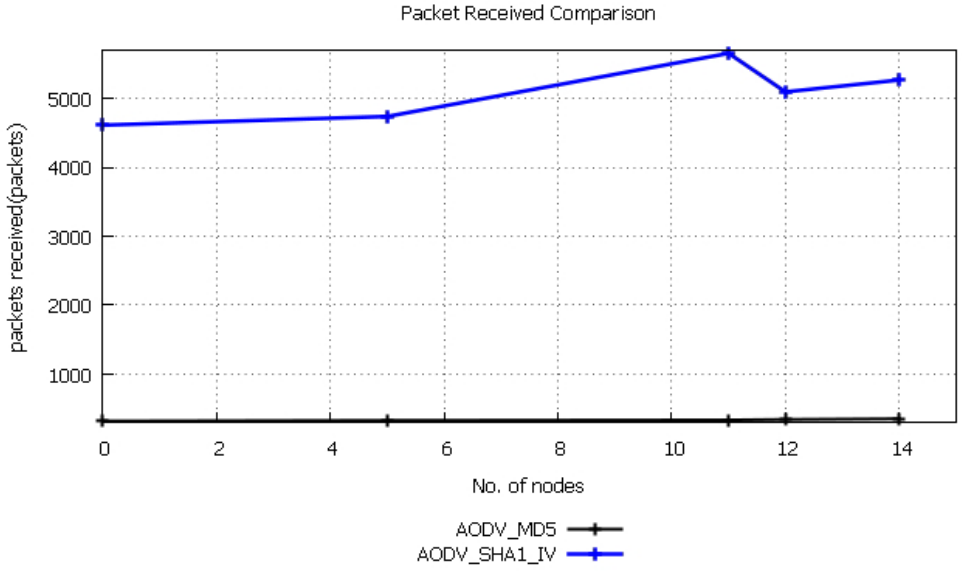

Figure 5: Graph of No. of nodes vs. packets received

V.CONCLUSION

Mobile ad hoc networks (MANETs) are a hostile environment where secure routing protocols should be applied. A secure routing protocol is expected to be able to offer the five basic security services, i.e., date confidentiality, data integrity, authentication, non-repudiation and access control. There are different MANET security issues, and the special features of this new environment make it more vulnerable to threats, and that solutions developed for standard networks are often either unsuitable or not directly applicable in this environment. In the proposed mechanism, we are implementing security using a new concept Initial Vector (IV) along with standard security algorithm SHA1 which is better than MD5 by modifying AODV. The proposed mechanism mainly focuses on the message authentication, data confidentiality and data integrity security requirements. As far as performance parameters are concerned, number of packets received at sink and bandwidth utilization values are better than previous one.

Future work should be focused not only on increasing the effectiveness of the security methods but also economical to make them suitable for a MANET environment. Furthermore, any proposed solution can work only with a single attack and is still vulnerable to unexpected attacks. Therefore, MANET researchers should also concentrate on exploring, as well as providing solutions to all possible attacks to make a MANET a secure and reliable network. And finally, the best routing protocol could be chosen, but still totally depends on the requirements of that routing environment or systems; either to have best performance or best security.

REFERENCES

[1] Christian Lochert, Bjorn Scheuermann, and Martin Mauve, A survey on congestion control for mobile ad hoc networks, Wireless Communications and Mobile Computing, Vol. 7, pp. 655-676, June.2007.

[2] "Secure Mobile Ad hoc Routing ", by Xu Li, Amiya Nayak, Isabelle Ryl, David Simplot and Ivan Stojmenovic .(IEEE 2007).

[3] "A survey of Routing attacks in mobile ad hoc networks ", by Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and nei kato, Tohoku University Abbas Jamalipour,University of Sydney. (IEEE 2007).

[4] A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers, IEEE Commun. Lett., vol. 9, no. 4, Apr. 2005, pp. 363-65.

[5] C. E. Perkins, E. M. Belding-Royer, and S. Das. RFC3561: Ad hoc On-Demand Distance Vector (AODV) Routing. IETF, The Internet Society, July 2003.

[6] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90-100, 1999.

[7] D. Djenouri, L. Khelladi, and A. N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks ", IEEE Commun. Surveys & Tutorials, vol. 7, no. 4, 2005, pp. 2-28.

[8] The CMU Monarch Project. The CMU Monarch Project's Wireless and Mobility Enhancements to ns. http://www.monarch.cs.cmu.edu. Work in progress.

[9] B. Dahill, B.N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks ", Proceedings of the international conference on Network Protocols (ICNP), p.p. 78-87, 2002.

[10] Manel Zapata, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, INTERNET DRAFT (September 2006) draft-guerrero-manetsaodv-06.txt

[11] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation (CNDS), January 2002.

[12] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks ", Proceedings of IEEE journal on selected areas in communications, Volume 23, No. 3, March 2005.

[13] M.G. Zapata, N. Asokan, Securing ad hoc routing protocols, in: Proceedings of ACM Workshop on Wireless Security (WiSe), Atlanta,September 2002.

[14] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks, "Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[15] M. G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols,"Proc. 3rd ACM Wksp. Wireless Security, 2002, pp.1-10.

[16] 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.

[17] A. Perrig, R. Canetti, D. Song and J.D. Tygar, "Efficient and secure source authentication for multicast," in: Proceedings of the Network and Distributed System Security Symposium, NDSS'01 (February 2001) pp. 35-46.