Different Types of Attacks on Integrated MANET-Internet Communication

Abhay Kumar Rai abhay.jk87@gmail.com
Department of Electronics & Communication
University of Allahabad
Allahabad, 211002, India

Rajiv Ranjan Tewari rrt_au@rediffmail.com
Department of Electronics & Communication
University of Allahabad
Allahabad, 211002, India

Saurabh Kant Upadhyay saurabhup01@gmail.com
Department of Electronics & Communication
University of Allahabad
Allahabad, 211002, India

Abstract

Security is an important issue in the integrated MANET-Internet environment because in this environment we have to consider the attacks on Internet connectivity and also on the ad hoc routing protocols. The focus of this work is on different types of attacks on integrated MANET-Internet communication. We consider most common types of attacks on mobile ad hoc networks and on access point through which MANET is connected to the Internet. Specifically, we study how different attacks affect the performance of the network and find out the security issues which have not solved until now. The results enable us to minimize the attacks on integrated MANET-Internet communication efficiently.

Keywords: Ad hoc networks, Home agent, Foreign agent, Security threats.

1. INTRODUCTION

Mobile ad hoc network has been a challenging research area for the last few years because of its dynamic topology, power constraints, limited range of each mobile host's wireless transmissions and security issues etc. If we consider only a stand-alone MANET then it has limited applications, because the connectivity is limited to itself. MANET user can have better utilization of network resources only when it is connected to the Internet. But, global connectivity adds new security threats to the existing active and passive attacks on MANET. Because we have to consider the attacks on access point also through which MANET is connected to Internet.

In the integrated MANET-Internet communication, a connection could be disrupted either by attacks on the Internet connectivity or by attacks on the ad hoc routing protocols. Due to this reason, almost all possible attacks on the traditional ad hoc networks also exist in the integrated wired and mobile ad hoc networks. Whatever the attacks are, the attackers will exhibit their actions in the form of refusal to participate fully and correctly in routing protocol according to the principles of integrity, authentication, confidentiality and cooperation. Hence to design a robust framework for integrated MANET-Internet communication we have to minimize attacks on the internet connectivity and also on the ad hoc routing protocols.

The rest of the paper is organized as follows. Section 2 explores the related work in the area of attacks on MANET- Internet communication and stand alone MANET. Section 3 represents a detailed description of different types of attacks on integrated MANET- Internet communication. In this section we consider most common types of attacks on mobile ad hoc networks and on access point through which MANET is connected to the Internet. Specifically, we study how different attacks affect the performance of the network. We also discuss some secure routing protocols for integrated MANET- Internet communication and find out the security issues which have not solved until now. Finally section 4 is about conclusions and future work.

2. RELATED WORK

In this section we explore related work on security challenges in integrated MANET-Internet and stand alone MANET.

The attacks on stand alone MANET and MANET-Internet communication have been normally studied separately in the past literature. [1, 2] have considered only the attacks on stand alone MANET. [3, 4] have proposed the frameworks to provide security from different types of attacks on MANET but they have considered only the attacks on the stand alone MANET. Xie and Kumar [5] and Kandikattu and Jacob [6] have considered both types of attacks (on MANET- Internet and on stand alone MANET communication) but their proposed routing protocols have considered them separately.

3. ATTACKS ON MANET-INTERNET COMMUNICATION

An integrated Internet and mobile ad hoc network can be subject to many types of attacks. These attacks can be classified into two categories, attacks on Internet connectivity and attacks on mobile ad hoc networks.

3.1 Attacks on Internet Connectivity

Attacks on Internet connectivity can be classified into following categories:

3.1.1 Bogus Registration

A bogus registration is an active attack in which an attacker does a registration with a bogus care-of-address by masquerading itself as some one else. By advertising fraudulent beacons, an attacker might be able to attract a MN (mobile node) to register with the attacker as if MN has reached HA (home agent) or FA (foreign agent). Now, the attacker can capture sensitive personal or network data for the purpose of accessing network and may disrupt the proper functioning of network. It is difficult for an attacker to implement such type of attack because the attacker must have detailed information about the agent.

3.1.2 Replay Attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it.

Suppose any mobile node A wants to prove its identity to B. B requests his password as proof of identity, which A dutifully provides (possibly after some transformation like a hash function); at the same time, C is eavesdropping the conversation and keeps the password. After the interchange is over, C connects to B presenting itself as A; when asked for a proof of identity, C sends A's password read from the last session, which B accepts. Now, it may ruin the proper operation of the network.

3.1.3 Forged FA

It is a form of network attack in which a node advertises itself as a fraudulent FA then MN’s under the coverage of the forged FA may register with it. Now, forged FA can capture the sensitive network data and may disrupt the proper functioning of the network.

In general, attacks on Internet connectivity are caused by malicious nodes that may modify, drop or generate messages related to mobile IP such as advertisement, registration request or reply to disrupt the global Internet connectivity.

Bin Xie and Anup Kumar [5] have proposed a secure routing protocol for integrated MANET-Internet communication. It achieves the goals of preventing the attacks from malicious nodes. If a node counterfeits a registration by inventing a non-existent address, its registration will fail at HA while HA validates the secret key of the malicious node. It prevents attacks due to bogus registration requests, replay attacks caused by malicious nodes, preventing the attacks of advertising fraudulent beacons by a counterfeit agent and preventing the attacks using old registration messages by a malicious node. But the proposed protocol uses digital signature based hop by hop authentication in route discovery which floods the route request in entire network. Hence every node in the network gets involved in the signature generation and verification process which consumes a lot of node's resources.

Ramanarayana & Jacob [6] have proposed a protocol named as secure global dynamic source routing protocol (SGDSR) in which the mutual authentication of MN, FA and HA is carried out with the help of public key and shared key cryptography techniques. It uses light weight hash codes for sign generation and verification, which greatly reduces the computational load as well as processing delay at each node without compromising security. But it also uses public key cryptography partly in the mutual authentication of MN, FA and HA which increases computational overhead.

K. Ramanarayana and Lillykutty Jacob [7] have proposed a light weight solution for secure routing in integrated MANET-Internet communication named as IGAODV (IBC-based secure global AODV). The secure registration process adopted in this protocol supports mutual authentication of MN, FA and HA with help of identity based cryptography techniques. All the registration messages contain time stamp to avoid replay attacks and signature to protect the message from modification attacks and to ensure that the message is originated by an authorized party. Registration process builds trust among MN, HA and FA and ensures that they are communicating with authorized nodes and not with any fraudulent node. But it does not prevent from many internal attacks.

Vaidya, Pyun and Nak-Yong Ko [8] have proposed a secure framework for integrated multipath MANET with Internet. In this scheme a secret key between mobile node and home agent is shared between them for authentication purpose. Therefore, it is not possible for an attacker to obtain the secret key S_{MN-HA}, so it has no knowledge of session key. Since session key is frequently changed so this will prevent guessing attack. The temporary session key that is distributed by the HA can be used to encrypt the communications data. This provides the data confidentiality between the FA and MN over the air. To achieve a high level of security, it is designed that a node only accepts messages from verified one hop neighbors. The proposed protocol provides a secure framework for global connectivity with multipath MANET but it does not prevent many internal attacks.

3.2 Attacks on Mobile Ad hoc Networks

Attacks on mobile ad hoc networks can be classified into following two categories:

3.2.1 Passive Attacks

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard. There is an attack which is specific to the passive attack a brief description about it is given below:

3.2.1.1 Snooping

Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data

transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage. Governments may snoop on individuals to collect information and prevent crime and terrorism.

Although snooping has a negative aspect in general but in computer technology snooping can refer to any program or utility that performs a monitoring function. For example, a snoop server is used to capture network traffic for analysis, and the snooping protocol monitors information on a computer bus to ensure efficient processing.

3.2.2 Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks. Brief descriptions of active attacks are given below.

3.2.2.1 Network Layer Attacks

The list of different types of attacks on network layer and their brief descriptions are given below:

3.2.2.1.1 Wormhole Attack

In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

For example in Fig. 1, **X** and **Y** are two malicious nodes that encapsulate data packets and falsified the route lengths.

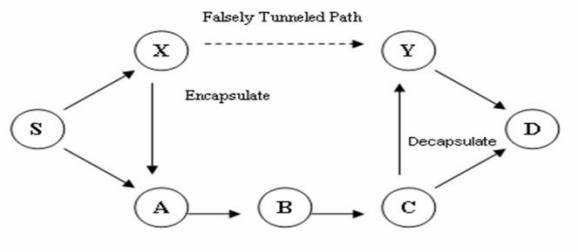

FIGURE 1: Wormhole attack

Suppose node **S** wishes to form a route to **D** and initiates route discovery. When **X** receives a route request from **S, X** encapsulates the route request and tunnels it to **Y** through an existing data route, in this case {**X --> A --> B --> C** --> **Y**}. When **Y** receives the encapsulated route request for **D** then it will show that it had only traveled {**S --> X --> Y --> D**}. Neither **X** nor **Y** update the packet header. After route discovery, the destination finds two routes from **S** of unequal length: one is of 4 and another is of 3. If **Y** tunnels the route reply back to **X**, **S** would falsely consider the path to **D** via **X** is better than the path to **D** via **A**. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network.

The wormhole attack is particularly dangerous for many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. For example, when used against an on-demand routing protocols such as DSR [9], a powerful application of the wormhole attack can be mounted by tunneling each route request packet directly to the destination target node of the request. When the destination node's neighbors hear this request packet, they will follow normal routing protocol processing to rebroadcast that copy of the request and then discard without processing all other received route request packets originating from this same route discovery. This attack thus prevents any routes other than through the wormhole from being discovered, and if the attacker is near the initiator of the route discovery. This attack can even prevent routes more than two hops long from being discovered. Possible ways for the attacker to then exploit the wormhole include discarding rather than forwarding all data packets, thereby creating a permanent Denial-of-Service attack or selectively discarding or modifying certain data packets. So, if proper mechanisms are not employed to protect the network from wormhole attacks, most of the existing routing protocols for ad hoc wireless networks may fail to find valid routes.

3.2.2.1.2 Black hole Attack

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

For example, in Fig. 2, source node S wants to send data packets to destination node D and initiates the route discovery process. We assume that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and immediately sends the response to node S. If the response from the node 2 reaches first to node S then node S thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 2. As a result, all packets through the malicious node is consumed or lost.

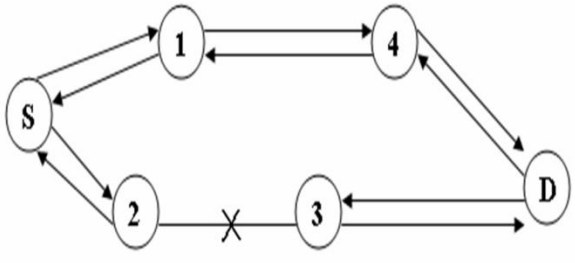

FIGURE 2: Black hole attack

3.2.2.1.3 Byzantine Attack

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets [10] which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior.

3.2.2.1.4 Information Disclosure

Any confidential information exchange must be protected during the communication process. Also, the critical data stored on nodes must be protected from unauthorized access. In ad hoc networks, such information may contain anything, e.g., the specific status details of a node, the location of nodes, private

keys or secret keys, passwords, and so on. Sometimes the control data are more critical for security than the traffic data. For instance, the routing directives in packet headers such as the identity or location of the nodes can be more valuable than the application-level messages. A compromised node may leak confidential or important information to unauthorized nodes present in the network. Such information may contain information regarding the network topology, geographic location of nodes or optimal routes to authorized nodes in the network.

3.2.2.1.5 Resource Consumption Attack

In this attack, an attacker tries to consume or waste away resources of other nodes present in the network. The resources that are targeted are battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. The attacks could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to nodes. Using up the battery power of another node by keeping that node always busy by continuously pumping packets to that node is known as a sleep deprivation attack.

3.2.2.1.6 Routing Attacks

There are several attacks which can be mounted on the routing protocols and may disrupt the proper operation of the network. Brief descriptions of such attacks are given below:

Routing Table Overflow: In the case of routing table overflow, the attacker creates routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. In the case of proactive routing algorithms we need to discover routing information even before it is needed, while in the case of reactive algorithms we need to find a route only when it is needed. Thus main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes.

Routing Table Poisoning: In routing table poisoning, the compromised nodes present in the networks send fictitious routing updates or modify genuine route update packets sent to other authorized nodes. Routing table poisoning may result in sub-optimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

Packet Replication: In the case of packet replication, an attacker replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

Route Cache Poisoning: In the case of on-demand routing protocols (such as the AODV protocol [11]), each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past. Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar objectives.

Rushing Attack: On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [12]. An attacker which receives a route request packet from the initiating node floods the packet quickly throughout the network before other nodes which also receive the same route request packet can react. Nodes that receive the legitimate route request packets assume those packets to be duplicates of the packet already received through the attacker and hence discard those packets. Any route discovered by the source node would contain the attacker as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the attacker. It is extremely difficult to detect such attacks in ad hoc wireless networks.

3.2.2.2 Transport Layer Attacks

There is an attack which is specific to the transport layer a brief description about it is given below:

3.2.2.2.1 Session Hijacking

Session hijacking is a critical error and gives an opportunity to the malicious node to behave as a legitimate system. All the communications are authenticated only at the beginning of session setup. The attacker may take the advantage of this and commit session hijacking attack. At first, he or she spoofs the IP address of target machine and determines the correct sequence number. After that he performs a DoS

attack on the victim. As a result, the target system becomes unavailable for some time. The attacker now continues the session with the other system as a legitimate system.

3.2.2.3 Application Layer Attacks

There is an attack that is specific to application layer and a brief description about it is given below:

3.2.2.3.1 Repudiation

In simple terms, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication. Example of repudiation attack is a commercial system in which a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction Non-repudiation is one of the important requirements for a security protocol in any communication network.

3.2.2.4 Multi-layer Attacks

Here we will discuss security attacks that cannot strictly be associated with any specific layer in the network protocol stack. Multi-layer attacks are those that could occur in any layer of the network protocol stack. Denial of service and impersonation are some of the common multi-layer attacks. Here we will discuss some of the multi-layer attacks in ad hoc wireless networks.

3.2.2.4.1 Denial of Service

In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. A denial of service (DoS) attack can be carried out in many ways. The classic way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of ad hoc wireless networks, there exist many more ways to launch a DoS attack in such a network, which would not be possible in wired networks. DoS attacks can be launched against any layer in the network protocol stack [13]. On the physical and MAC layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the QoS being offered by the network. On the higher layers, an adversary could bring down critical services such as the key management service.
For example, consider the following Fig. 3. Assume a shortest path exists from **S** to **X** and **C** and **X** cannot hear each other, that nodes **B** and **C** cannot hear each other, and that **M** is a malicious node attempting a denial of service attack. Suppose **S** wishes to communicate with **X** and that **S** has an unexpired route to **X** in its route cache. **S** transmits a data packet toward **X** with the source route **S --> A -> B --> M --> C --> D --> X** contained in the packet's header. When **M** receives the packet, it can alter the source route in the packet's header, such as deleting **D** from the source route. Consequently, when **C** receives the altered packet, it attempts to forward the packet to **X**. Since **X** cannot hear **C**, the transmission is unsuccessful.

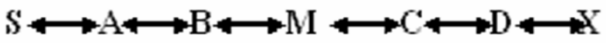

FIGURE 3: Denial of service attack

Some of the DoS attacks are described below:

Jamming: In this form of attack, the attacker initially keeps monitoring the wireless medium in order to determine the frequency at which the destination node is receiving signals from the sender. It then transmits signals on that frequency so that error-free reception at the receiver is hindered. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are two commonly used techniques that overcome jamming attacks.

SYN Flooding: In this form of attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYN-ACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the response of ACK packet. Without any response of ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed-size table while it awaits the acknowledgement of the three-way handshake, all of these pending connections could overflow the buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection. Normally there is a time-out associated with a pending connection, so the half-open connections will eventually expire and the victim node will recover. However, malicious nodes can simply continue sending packets that request new connections faster than the expiration of pending connections.

Distributed DoS Attack: Distributed denial of service attack is more severe form of denial of service attack because in this attack several adversaries that are distributed throughout the network collude and prevent legitimate users from accessing the services offered by the network.

3.2.2.4.2 Impersonation

In this attack, a compromised node may get access to the network management system of the network and may start changing the configuration of the system as a super-user who has special privileges. An attacker could masquerade as an authorized node using several methods. It may be possible that by chance it can guess the identity and authentication details of the authorized node or target node, or it may snoop information regarding the identity and authentication of the target node from a previous communication, or it could disable the authentication mechanism at the target node. A man-in-the-middle attack is an example of impersonation attack. Here, the attacker reads and possibly modifies messages between two end nodes without letting either of them know that they have been attacked. Suppose two nodes A and B are communicating with each other; the attacker impersonates node B with respect to node A and impersonates node A with respect to node B, exploiting the lack of third-party authentication of the communication between nodes A and B.

In the protocol given by Bin Xie and Anup Kumar [5], there is a defense mechanism due to which a node cannot generate a valid route discovery message by spoofing or inventing an IP address. In the route discovery process, control messages created by a node must be signed and validated by a receiving node. Therefore the route discovery prevents anti-authenticating attacks such as creating routing loop, fabrication because no node can create and sign a packet in the name of a spoofed or invented node. Since there is no centralized administration hence MN's can change their identities easily. But in the proposed approach, the ad hoc host's home address is bound with their identities in ad hoc network. Therefore, it becomes difficult for any ad hoc host to masquerade itself by creating a valid address. Nonce and timestamp make a route request or route reply containing unique data to prevent duplication from a malicious node. But, it is not secured from some internal attacks like resource consumption attack, black hole attack.

In the protocol given by Ramanarayana & Jacob [6], the secure registration adopted prevents impersonation, modification and fabrication attacks by any fraudulent node but gives no security from internal attacks such as black hole attack, wormhole attack and resource consumption attack.

The protocol given by K. Ramanarayana and Lillykutty Jacob [7] is resistant against modification and fabrication attacks on the source route because intermediate nodes authenticate the route based on the token, which is not revealed until the exchange of route request and route reply has finished. In the route request phase end-to-end authentication avoids impersonation of source and destination nodes. End-to-end integrity in the route request phase avoids modification attacks caused by intermediate nodes. Hop-by-hop authentication in the route reply phase avoids external malicious nodes to participate in the routing protocol and avoids the attacks caused by them. But the proposed protocol is not resistant to collaborative, black hole and gray hole attacks.

In the protocol proposed by Vaidya, Pyun and Nak-Yong Ko [8], modification attacks have been removed. Route request and route reply packets are signed by the source node and validated by intermediate nodes along the path. If there are altered packets, they would be subsequently discarded. Hence route request and route reply packets remain unaltered and modification attacks are prevented. Every routing

message is signed by the sender and its certificate and signature are verified by the receiver. This prevents spoofing and unauthorized participation in routing, ensuring nonrepudiation. The proposed approach binds the MN's IP address and MAC address with public key. Neighbor discovery process in this scheme assures the communication between authenticated one-hop neighbors. Since only sender can sign with its own private key hence nodes cannot spoof other nodes in route instantiation. Destination node's certificate and signature are included in the route reply, ensuring that only the destination can respond to route discovery. Hence, it is not possible for any MN to masquerade itself by spoofing or inventing an address in route discovery. The proposed protocol provides a secure framework for global connectivity with multipath MANET and provides the security mechanism for the above discussed attacks but it does not prevent many internal attacks.

4. CONCLUSION AND FUTURE WORK

We have discussed security issues related to integrated mobile ad hoc network (MANET)-Internet and stand alone MANET. The proposed mechanisms until now have solved many security issues related to integrated MANET-Internet communication but they have not solved them completely. So, we can design a security mechanism by which we can minimize or completely remove many of those attacks.

In future, we will propose to design a robust framework that uses minimal public key cryptography to avoid overload on the network and uses shared key cryptography extensively to provide security. The performance analysis of the protocol shall be done using NS-2 simulation software. It is expected that it shall minimize the security attacks due to both integrated MANET-Internet and stand alone MANET.

REFERENCES

1. Nishu Garg, R.P.Mahapatra. "MANET Security Issues". IJCSNS International Journal of Computer Science and Network Security, Volume.9, No.8, 2009.

2. Hoang Lan Nguyen, Uyen Trang Nguyen. "A study of different types of attacks on multicast in mobile ad hoc networks". Ad Hoc Networks, Volume 6, Issue 1, Pages 32-46, January 2008.

3. F. Kargl, A. Geiß, S. Schlott, M. Weber. "Secure Dynamic Source Routing". Hawaiian International Conference on System Sciences 38 Hawaii, USA, January 2005.

4. Jihye Kim, Gene Tsudik. "SRDP: Secure route discovery for dynamic source routing in MANET's". Ad Hoc Networks, Volume 7, Issue 6, Pages 1097-1109, August 2009.

5. Bin Xie and Anup Kumar. "A Framework for Internet and Ad hoc Network Security". IEEE Symposium on Computers and Communications (ISCC-2004), June 2004.

6. Ramanarayana Kandikattu and Lillykutty Jacob. "Secure Internet Connectivity for Dynamic Source Routing (DSR) based Mobile Ad hoc Networks". International Journal of Electronics, Circuits and Systems Volume 2, October 2007.

7. K. Ramanarayana, Lillykutty Jacob. "Secure Routing in Integrated Mobile Ad hoc Network (MANET)-Internet". Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Pages 19-24, 2007.

8. Vaidya, B., Jae-Young Pyun, Sungbum Pan, Nak-Yong Ko. "Secure Framework for Integrated Multipath MANET with Internet**"**. International Symposium on Applications and the Internet, Pages 83 – 88, Aug. 2008.

9. David B. Johnson and David A. Maltz. "Dynamic Source Routing in Ad Hoc Wireless Networks". In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153–181. Kluwer Academic Publishers, 1996.

10. B. Awerbuch, D. Holmer, C. Nita Rotaru and Herbert Rubens. “An On-Demand Secure Routing Protocol Resilient to Byzantine Failures”. Proceedings of the ACM Workshop on Wireless Security 2002, Pages 21-30, September 2002.

11. C. E. Perkins and E. M. Royer. "Ad Hoc On-Demand Distance Vector Routing". Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, Pages 90-100, February 1999.

12. Y. Hu, A. Perrig, and D. B. Johnson. “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols”. Proceedings of the ACM Workshop on Wireless Security 2003, Pages 30-40, September 2003.

13. L. Zhou and Z. J. Haas. “Securing Ad Hoc Networks”. IEEE Network Magazine, Volume. 13, no. 6, Pages 24-30, December 1999.