IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 5, Ver. III (Sep. - Oct. 2016), PP 29-36
www.iosrjournals.org

A Survey of Network Security in Mobile Ad-Hoc Network

Ashwini Pillai[1], Anurag Kumar[1], Mrs.Ajina[2]
[1]*UG Student, Department of Computer Science & Engg, Sir MVIT, Bangalore*
[2]*Assistent Professor Department of Computer Science & Engg, Sir MVIT, Bangalore*

Abstract: *This paper describes the concept of ad hoc networking and the security issues faced by giving its background and presenting some of the security challenges that are faced by the mobile ad hoc network. Ad hoc wireless communication between devices is defined as a scheme, often referred to as ad hoc networking, which allows devices to establish communication,anytime and anywhere without the aid of a central infrastructure.Before the incorporation of technologies of bluetooth and wifi ,ad hoc networks was often associated with communication on combat fields due to which security in the system has become a major issue. Due to its vulnerable nature, the security threats that disrupts its development .To solve these issues the vulnerabilities in networks are analysed first .Then we discuss the security criteria and main attack types existing in ad hoc network .Finally we bring in the current security solutions for the mobile ad hoc network.*

Keywords: *Mobile Ad Hoc Network, Security, vulnerabilities.*

I. Introduction

In recent years, due to the growth of technologies such as mobile computing devices, including laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world.Computing will now rely on the capability provided by the personal computers,and the concept of univcrsal computing emerges and becomes one of the research hotspots in the computer science society.The users use the device and use the information anywhere they want to which has made it necessary to adopt wireless network as the interconnection method.It is not possible for the universal devices to get wired network link whenever and wherever they need to connect with other universal devices because of which researchers have opted for Mobile Ad Hoc Network .

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies using which people and vehicles can be internetworked in areas where requires wireless connections. In MANET, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other.

Ad hoc devices incorporate communication based on Wi-Fi which allow them to interact with each other using wireless (one hop) and mobile(multihop) networks . Therefore, any physical scenario providing these communication services to people on the move becomes a potential collaboration arena. Features of mobile ad hoc network: Unreliability of wireless links between nodes. There is limited energy supply for the wireless nodes and the mobility of the nodes, hence the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly.The nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network and this causes changing routing information. Lack of incorporation of security: Due to the changing of topology of the ad hoc networks often ,it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.Because of these features , the mobile ad hoc networks are more prone to suffer from the malicious behaviours than the traditional wired network because of which security issues need to be taken care of.

In Section 2, the vulnerabilities that make the mobile ad hoc networks insecure are discussed. In Section 3, we survey the current security solutions for the mobile ad hoc networks. In Section 4, the conclusion is drawn for the paper.

II. Vulnerabilities of the Mobile Ad Hoc Networks

Security is much more difficult to maintain in the mobile ad hoc network than in the wired network due to following reasons:-

2.1. Lack of Secure Boundaries:

The meaning of this vulnerability is that there is not such a clear secure boundary in the mobile ad hoc network which can be compared with the clear line of defence in the traditional wired network. This has originated due to the nature of the MANET that includes freedom to join, leave and move inside the network.In case of wired network, adversaries must get physical access to the network medium, or even pass through several lines of defence such as firewall and gateway before they can perform malicious behaviour to the targets. However, in the MANET, the adversary is in the radio range of any other nodes it can communicate with those nodes in its radio range and thus join the network automatically and does not require adversary to gain the physical access to visit the network not providing boundaries for access leading to potentially dangerous network accesses making the mobile ad hoc network prone to attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node, at any time, and target to any other node's in the network. To make matters worse, there are various link attacks that can jeopardize(put into) the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks.

The attacks include:-A. Passive Attacks :

In passive attacks, attackers don't disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. The attacker only looks and watches the transmission and does not try to modify or change the data packets.

Two types of passive attacks are:

1. Traffic analysis: In this attack, attacker monitors packet transmission to infer important information such as a source,destination and source-destination pair.
2. Eavesdropping: In Eavesdropping, attackers obtain some confidential information e.g. private key, public key, location or even password of the node that should be kept secret during transmission.

B. Active Attacks:

In the active attacks, some false information is introduced by nodes to confuse the network topology. They can either attract traffic to them and then drop or compromise the packets. The sent false information can lead packets to the wrong node and cause congestion in one area. The attacks can either target at the routing procedure or try to flood the networks.

Various types of active attacks are:

1. Sinkhole Attack: A sinkhole node tries to attract the data toward itself from all neighbouring nodes by generating fake routing information and shows itself as legal nodes for the route.The node attempts to draw all network traffic, modifies the data packets, decrease the network life-time, complicates network and finally destroy it.
2. Flooding Attack:In this attack, a malicious node injects false packets to consume the available resources onto the network, not allowing valid users use resources for valid communication.
3. Replay: This attack usually targets the freshness of routes. An attacker firstly records the message and then resend the old message to the other nodes to make updates to their routing table to stale routes.
4. Rushing Attack: In Rushing attack, attacker forward routing packets as quick as possible to gain access to multicast forwarding group before the legal node slowing down the performance of network .

C. Common attacks in MANETs:

1. Denial-of-service with modified source route: In the denial-of-service, a malicious node in between can successfully send an erroneous route message to the source route to disrupt the service.

2. Tunneling Attack: In tunneling attack two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. 3. Wormhole Attack:

In Wormhole an attacker records packet at one location in the network, tunnels them to another location, and retransmits them back into the network. This attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.

4. Black hole Attack: In Black hole attack a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept and in this way it can compromise the service.

5. Spoofing Attack: In Spoofing a single malicious node in the ad hoc network can spoof the nodes identity in order to forward packets through it.

2.2. Lack of Centralized Management Facility:

Ad hoc networks do not have a centralized piece of management machinery such as a named server, which lead to some vulnerable problems.Firstly, the absence of centralized management machinery makes the detection of attacks a very difficult problem as monitoring the traffic in dynamic and large scale isn't easy.It is also prone to failures such as path breakages, transmission impairments and packet dropping.Second, lack of centralized management machinery will impede the trust management for the nodes as it requires all the nodes to cooperate in the network operation, while no security association can be assumed for all the network nodes.Third, some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure. Because there is no centralized authority, and decision making in MANET is sometimes decentralized, the adversary can make use of this vulnerability and perform some attacks that can break the cooperative algorithm .

2.3. Restricted Power Supply:

Due to the mobility of nodes in the ad hoc network, it is common that the nodes in the ad hoc network will rely on battery as their power supply method unlike the nodes in the wired network which can get electric power supply from the outlets,which means that their power supply should be approximately infinite. The nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems.The first problem that may be caused by the restricted power supply is denial-of-service attacks. Since target node is battery-restricted, either node can continuously send additional packets to the target and ask it routing those additional packets,or it can induce the target to be trapped in some kind of time-consuming computations which causes target node to exhaust.A cluster of neighbouring MANET nodes can randomly and fairly elect a monitoring node that will observe the abnormal behaviours in the network traffic for the entire cluster.Some selfish nodes not wanting to cooperate in the monitoring node election process, fails the election when there are too many selfish nodes.

2.4. Scalability:

Unlike the traditional wired network in which its scale is generally predefined when it is designed does not change much during the use, the scale of the ad hoc network keeps changing all the time because of the mobility of the nodes in the mobile ad hoc network.Hence,the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously.

III. Security Solutions to the Mobile Ad Hoc Networks

As we discussed several vulnerabilities that potentially make the mobile ad hoc networks insecure in the previous section for which, solutions need to be found. In this section, we survey some security schemes that help in solving issues.

3.1. Criteria:

Before the solutions are surveyed, it necessary to judge how a MANET is secure or not.

3.1.1. Availability: The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This is challenged mostly during the denial-of-service attacks.

3.1.2. Integrity: On physical and media access control layer, jamming techniques are used to interfere with communication on physical channel. It disrupts the routing protocol on network layer but brings down high level services on higher levels.e.g: key management service.

It guarantees the identity of the messages when they are transmitted and can be ensured mainly in two ways malicious altering and accidental altering.

3.1.3. Confidentiality: Confidentiality means that certain information is only accessible to those who have been authorized to access it.

3.1.4. Authenticity: This assures that the communication is genunie answer is necessary for the participants to prove their identities to ensure the authenticity. If there is no authentication mechanism, the adversary could impersonate a benign node that accesses confidential resources, or even propagate some fake messages to disturb the normal network operations.

3.1.5. Non-repudiation: Non-repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. become unavailable. It is not practical to perform the traditional DoS attacks in the MANET because of the distributed nature of the services and being more vulnerable than the wired networks because of the interference-prone radio channel and the Authorization:Entity is issued alimited battery power.In the practice, the credential, specifiying the privileges and permissions it has and cannot be falsified, by the certificate authority and allows different level of users.

3.1.6. Anonymity: Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software and cannot be disclosed.

3.2. Attack Types in Mobile Ad Hoc Networks:

Attacks are classified as:

(i). External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

(ii). Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by accesing a new node by impersonation or directly compromising the current node.

External attacks are similar to the normal attacks in the traditional wired networks in that the adversary is in the proximity but not a trusted node in the network, therefore, this type of attack can be prevented and detected by the security methods such as membership authentication or firewal.Internal attacks are far more dangerous than the external attacks because the compromised nodes are originally the benign users of the ad hoc network they can easily pass the authentication and get protection from the security mechanisms. As a result, the adversaries can make use of them to gain normal access to the services that should only be available to the authorized users in the network, and they can use the legal identity provided by the compromised nodes to conceal their malicious behaviours.

3.2.1. Denial of Service (DoS):

This aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target that exhaust the processing power of the target and make the services provided by the target attackers exactly exactly use the radio jamming and battery exhaustion method

3.2.2. **Impersonation**:

Its a severe threat to the security as there is no proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes and these compromised nodes joins network as normal node and conducts malicious behaviours such as propagate fake routing information and gain inappropriate priority to access some confidential information.

3.2.3. **Eavesdropping**:

The goal is to obtain some confidential information that should be kept secret during the communication. The confidential information may be location, public key, private key or even passwords of the nodes as these are very important to the security state of the nodes,must be kept away from the unauthorized access.

3.2.4. Attacks against Routing:

Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path.The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack .

Impersonating another node to spoof route message.Advertising a false route metric to misrepresent the topology.Sending a route message with wrong sequence number to suppress other legitimate route messages.Flooding Route Discover excessively as a DoS attack.Modifying a Route Reply message to inject a false route.Generating bogus Route Error to disrupt a working route.Suppressing Route Error to mislead others.

Validating the messages is difficult due to mobility and constantly changing topology of the mobile ad hoc There are some more sophisticated routing attacks, which include Wormhole attacks , Rushing attacks and Sybil attacks.The second category of attacks are difficult to prevent .Strategies in this type one is selfishness, in which the malicious node selectively drops route messages that are assumed to forward in order to save its own battery power; the other is denial-of-service, in which the adversary sends out overwhelming network traffic to the victim to exhaust its battery power.

3.2.5.Location Disclosure: It targets the privacy requirements of an ad hoc network.By using traffic analysis techniques or just by discovering the location of a node, or structure of the entire network.

3.2.6.Black Hole: False route is injected by the node that replies to the route requests it receives, advertising itself as having the shortest path to a destination. These fake replies divert traffic through the malicious node for eavesdropping, or attract all traffic to it in order to perform a doS dropping packets 3.2.7.Replay: The routing traffic captured earlier is injected into the network traffic ,it targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

3.2.8. Wormhole: The wormhole attack involves the cooperation between two malicious nodes that participate in the network. Two nodes of which node A being the malicious node communicates with node B sharing a private link with node A.Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is packet leashes.

3.2.9.Blackmail: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. The security property of proves to be useful in such cases since it binds a node to the messages it generated.

3.2.10.Rushing Attack: This results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. For example, DSR, AODV,and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. develop Rushing Attack Prevention (RAP), a generic defence against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

3.2.11.Breaking the neighbour relationship: An intelligent filter used to modify or change information in the routing updates or even intercept traffic belonging to any data session. 3.2.12.Masquerading: An outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol do main by compromising authentication system. 3.2.13.Passive Listening and traffic analysis:Exposed routing information is gathered by intuder does not effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected.

3.3 Schemes to deal with the attacks: In the last subsection, we have introduced several attack types in the mobile ad hoc network. Therefore, some security are to be found to deal with them

3.3.1 Intrusion Detection Techniques According to the definition in the Wikipedia:

An Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems .In this architecture, every node participates in the intrusion detection and response activities by detecting signs of intrusion behaviour locally and independently, which are performed by the built-in IDS agent. However, the neighbouring nodes can share their investigation results with each other and cooperate in a broader range.The cooperation takes place when certain nodes does not have evidence to figure out the intrusion type in that case the node that has detected the anomaly requires other nodes in the communication range to perform searches to their security logs in order to track the possible traces of the intruder.

Architecture is in such a way that all of the IDS agents can work independently and locally and cooperate with each other to detect some intrusion behaviours in a larger range as well, to detect attack early and efficiently IDS is placed in each alyer of eac node.The problems that are not considered :one is the limited battery power problem causing some nodes to behave in a selfish manner during the cooperative intrusion detection process, the other is the possible overhead that is brought by the multi-layer integrated intrusion detection and response mechanism compared with the original single-layer intrusion detection mechanism.

3.3.1.1. Cluster-based Intrusion Detection Technique for Ad Hoc Networks:

Due to the limited power supply in the ad hoc network, this framework may cause some nodes behave in a selfish way and doesnt cooperate with other nodes to save their battery power violating the original intention of this cooperative intrusion detection architecture. To solve this problem,this technique is used .A MANET can be organized into a number of clusters in such a way that every node is a member of at least one cluster, and there will be only one node percluster that will take care of the monitoring issue in a certain period of time, which is generally called cluster-head. A cluster is a group of nodes that as the clusterhead, all of the other nodes in this cluster should be within 1-hop vicinity reside within the same radio range with each other, which means that when a node is selected.Fairness contains two levels of meanings: the probability of every node in the cluster to be selected as the clusterhead should be equal, and each node should act as the cluster node for the same amount of time. Efficiency of the process means that there should be some methods that can select a node from the cluster periodically with high efficiency.Basically there are four states in the cluster formation protocol: initial, clique, done and lost.All the nodes in the network will be in the initial state at first, which means that they willmonitor their own traffic and detect intrusion behaviours independently,clique computation and clusterhead computation must be finished before proceding. A clique is defined as a group of nodes where every pair of members can communicate via a direct wireless link. Once the protocol is finished, every node is aware of its fellow clique members. Then a node is randomly selected from the clique to act as the clusterhead.Cluster Valid Assertion Protocol and Cluster Recovery Protocol are used for validation and recovery issues .

3.3.1.2. Misbehavior Detection through Cross-layer Analysis:

Attackers may simultaneously exploit several vulnerabilities at multiple layers but keep the attack to each of the vulnerabilities stay below the detection threshold so as to escape from capture by the single-layer misbehavior detector this is known as cross layer misbehavior .The scenario is detected by cross-layer misbehavior detector, in which the inputs from all layers of the network stack are combined and analyzed by the cross-layer detector in a comprehensive way.It is important to find out how to make the cross-layer detection more efficient.Different viewpoints may be available for the same attack .Therefore it is necessary to figure out the possible solution if there are different detection results generated by different layers.How much the system resource and network overhead will be increased due to the use of cross-layer detector compared with the original single-layer detector is also found. Due to the limited battery power of the nodes, the system and network overhead brought by the cross-layer detection should be considered and compared with the performance gain caused by this method.

3.3.2 Secure Routing Techniques:

There are 5 types of solutions provided in this category:

- Authenticating in all phases : avoids external attack ,spoofing and modifies sequence no. but this requires certificate authority or keysharing mechanism.
- Trust level : prevents attacks by authentication on higher level nodes it faces the same problem as pevious one and is difficult to define trust levels.
- Secure neighbour verification: attacks are prevented by authentication and rushing ,it requires certificate authentication and key sharing mechanisms and important overhead when mobility increases.
- Randomizing message forwarding: prevents attacks by rushing but has latency problems.
- Onion encryption: it reduces all kinds of external attacks ,spoofing but has high computational cost.

3.3.2.1. Defence Method Against Wormhole Attacks in Mobile Ad Hoc Networks:

Wormhole attack is a threatening attack.In this attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and replays them there into the network. This confuses the routing issue in mobile ad hoc network because the nodes that get these replayed packets cannot distinguish it from the genuine routing packets. Moreover, for tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route, which makes the victim node be more likely to accept the tunneled packets instead of the genuine routing packets. As a result, the routing will be severely interfered by the wormhole attack.

A leash is any information that is added to a packet designed to restrict the packet’s maximum allowed transmission distance. There are two main leashes, geographical leashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed-of-light.Either type prevents the wormhole attack, because it allows the receiver of a packet to detect if the packet travelled further than the leash allows. The TIK protocol implements temporal leashes and provides efficient instant authentication for broadcast communication in wireless networks. When used in conjunction with precise timestamps and tight clock synchronization, TIK can prevent wormhole attacks that cause the signal to travel a distance longer than the nominal range of the radio, or any other range that might be specified.

3.3.2.2. Defense Mechanism against Rushing Attacks in Mobile Ad Hoc Networks:

Rushing attack is a new attack that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. This attack is damaging because it can be performed by a relatively weak attacker. The initiator node initiates a Route Discovery for the target node. If the ROUTE REQUESTs for this Discovery forwarded by the attacker are the first to reach each neighbour of the target, then any route discovered by this Route Discovery will include a hop through the attacker. That is, when a neighbour of the target receives the rushed REQUEST from the attacker, it forwards that REQUEST, and will not forward any further REQUESTs from this Route Discovery. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes containing at least two hops. Secure Neighbour Detection allows each neighbour to verify that the other is within a given maximum transmission range.

3.3.2.3. Watchdog and Path rater:

Watchdog and Pathrater are two main components of a system that tries to improve performance of ad hoc networks in the presence of disruptive nodes, the specific working Watchdog determines misbehaviour by copying packets to be forwarded into a buffer and monitoring the behaviour of the adjacent node to these packets. It snoops to decide if the adjacent node forwards the packets without modifications or not and the matched snooped packets with the observing nodes buffer are discarded; whereas packets that stay in the buffer beyond a timeout period without any successful match are flagged as having been dropped or modified. If the violations becomes greater than a certain predetermined threshold, the violating node is marked as being malicious and this information is passed to the Parthrater component for inclusion in path rating evaluation. Pathrater on an individual node works to rate all of the known nodes in a particular network with respect to their reliabilities. Ratings are made, and updated, from a particular node's perspective. Misbehaviour is detected as packet mishandling/modification, whereas unreliable behaviour is detected as link breaks.

3.3.3 Routing security in ad hoc:

Routing protocols for Ad hoc networks cope well with dynamically changing topology but are not designed to accommodate defence against malicious attackers. Routers exchange network topology informally in order to establish routes between nodes. Detection of compromised nodes through routing information is also difficult due to dynamic topology of Ad hoc networks. Routing protocols for Ad hoc networks must handle outdated routing information to accommodate dynamic changing topology. False routing information generated by compromised nodes can also be regarded as outdated routing information. As long as there are sufficient numbers of valid nodes, the routing protocol should be able to bypass the compromised nodes, this however needs the existence of multiple, possibly disjoint routes between nodes and make use of an alternate route if the existing one appears to have faulted.

3.4. Security Solutions in the Mobile Ad Hoc Networks:

In this section, we survey the security solutions in the mobile ad hoc networks. First we analyze the main security criteria for the mobile ad hoc networks, which should be regarded as a guideline for us to find the solutions to the security issues in the mobile ad hoc networks. We then point out various attack types that mainly threaten the mobile ad hoc networks. According to these attack types, we survey several security schemes that can partly solve the security problems in the mobile ad hoc networks.

IV. Conclusion

In this survey paper, we try to inspect the security issues in the mobile ad hoc networks caused due to the mobility and open media nature. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. First we briefly introduce the basic characteristics of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention. We then discuss some typical and dangerous vulnerabilities in the mobile ad hoc networks,most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and limited battery power; whose existence has made it necessary to find some effective security solutions which protects the mobile ad hoc network from all kinds of security risks.Finally we introduce the current security solutions for the mobile ad hoc networks werein we start with the discussion on the security criteria in mobile ad hoc network, which acts as a guidance to the security-related research works in this area followed by the main attack types that threaten the current mobile ad hoc networks. In the end, we discuss several security techniques that can help protect the mobile ad hoc networks from external and internal security threats.During the survey, we also find some points that can be further explored in the future, such as some aspects of the intrusion detection techniques can get further improved.

References

[1] Rajneesh Narula, Rajneesh Narula, Kaushal, Anish Arora *Security Issues of Routing Protocols in MANETs 2012*

[2] Wenjia Li and Anupam Joshi *Security Issues in Mobile Ad Hoc Networks – A Survey*

[3] Karan Singh, R. S. Yadav, Ranvijay International Journal of Computer Science and Security, Volume (1): Issue (1) 52 *A review paper on network security*

[4] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.*

[5] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book. *The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.*

[6] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in *Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC.*

[7] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003*.

[8] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, San Antonio, TX, January 2002.

[9] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in *Proceedings of ACM MOBICOM'02,* 2002.

[10] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in *Proceedings of ICNP'02,* 2002.

[11] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, in *Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000),* pages 275–283, Boston, Massachusetts, August 2000.

[12] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, *IEEE Internet Computing,* pages 63–70, July-August 1999.