EAI Endorsed Transactions
on Energy Web and Information Technologies
Research Article EAI.EU

A Survey on Security Issues and Challenges in Mobile Ad-hoc Network

G.Keerthana[1] and P. Anandan[2]

[1]Research Scholar, Anna University, Chennai.

[2]Professor, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai.

[1]gkeerthu21@gmail.com [2]anandanvp2000@gmail.com

Abstract

Rapid developments in the communication arena has tremendously improved the transmission procedures today. The amount of information transmission in the commercial and military applications has grown tremendously therefore the need for security concerns have also grown simultaneously since these applications involve in the transmission of confidential contents. Information transmissions in wireless networks appear to be confidential, hence it becomes mandatory to safeguard these contents from the various available offenses by means of devising suitable security mechanisms. Various types of attacks have been observed in the ad hoc networks, namely, the active and passive types, internal and external types. Integrity, identity and privacy are the three major parameters to be ensured in the design of a secure network. This survey paper discusses about the various attacks on a network together with the essential security procedures to be incorporated for securing the network.

Keywords: MANET, Mobile Ad-hoc, IEEE802.11, vulnerability, authenticity, offenses, ad hoc networks.

Received on 09 July 2018, accepted on 07 September 2018, published on 12 September 2018

3rd International Conference on Green, Intelligent Computing and Communication Systems - ICGICCS 2018, 18.5 - 19.5.2018, Hindusthan College of Engineering and Technology, India

doi: 10.4108/eai.12-9-2018.155743

1. Introduction

Computer networking today has been observed as the product of the various emerging technologies, wireless communications have occupied prime positions in today's information communication environment as a result of the massive expansions in the networking zones and this emerging technology has been named as the mobile ad hoc network (MANET). A significant unique feature of this network is that it does not rely on any fixed architectures. This network comprises of various communication nodes that are mobile in nature, nodes are not fixed at particular points they can move freely both within and outside their networking zones. Nodes in these networks communicate via the radio frequency ranges, multihop strategies would further assist in the communication procedures. Direct node to node communication is another observed possibility.

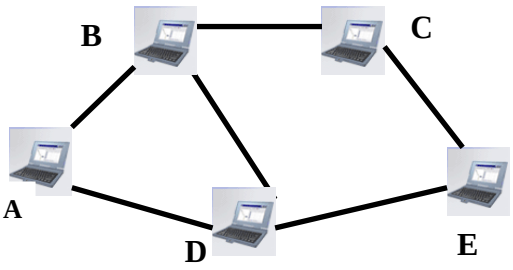

Figure 1: Representation of a Mobile ad- hoc network

Defense related security applications make use of the ad hoc networks, as these networks possess increased capabilities in safeguarding the confidential contents from the various offenses. Even though the mobile ad hoc networks inhibit certain specialized communicational qualities, they are found to be receptive to certain security threats.

As far as both the fixed and infrastructure less types of communications are concerned it is observed

that the mobile ad hoc network not only considers the various prevalent security attacks but also defines certain attacks that are unique to itself [1]. One of the significant challenges faced by the Ad Hoc Networks is security, since the transmission processes here are found to be vulnerable to the available offenses.

Various authentication procedures have been incorporated in these networks in order to enhance the strength of the adopted security features; one such is the Intrusion detection system that facilitates the identification of the unauthorized users so as to maintain the integrity of the entire transmission. Security threats encountered by the mobile ad hoc networks are found to be comparatively higher than that of the wired medium. Detection of flaws or damages in a mobile network is quite tedious because the communication nodes in such networks do not remain stable at one particular point, nodes keep moving within their frequency ranges. Another observable factor is the boundary line; as far as a mobile network is concerned it is evident that these lines are not perfectly defined. MANETs permit the nodes to leave the network at any point of time; even inclusions at any instants are common. This feature affects the integrity of the network. Sometimes it is possible for an unauthorized node to intrude into a network's transmission zone and transmit huge volumes of unethical or unintended contents so as to crash the entire network.

1.1 Attributes of the Mobile Ad-hoc Networks

Various unique attributes of the MANETs has made it popular. Few of the distinguishable features to be possessed by this network are as follows; the efficiency feature related to its node to node data transmission, protocol features enabling multihop mechanisms and finally its self governing and self configuring features. Attributes that differentiate the MANETs from the ordinary networks are as follows:

Changing network topography: The structure of a network is usually determined by its layout features, nodes inside a network would essentially provide a structure to the same, as the nodes here are not fixed defining a shape appears to be difficult. Movement of nodes ultimately deteriorates the structure of the concerned network and hence the lack of power resources.

Alternating link scope: Wireless communication systems suffer from a common problem of high bit error rate. A link or a path usually comprises of a certain number of nodes, movement of these nodes would ultimately break the concerned link and such disruptions would affect the ongoing communication process putting the entire system to a halt condition.

1. *Shared Operations:* The infrastructure of the ad hoc network is not fixed; hence the protocols and algorithms to be devised for such mobile networks must take into consideration the infrastructure less features and the changing network structures suitably.
2.
3. *Finite energy resources:* Unlike the wired devices the operations of the mobile devices are battery dependent, wired devices usually rely on a centralized system that would constantly deliver the required power. The wireless devices depend on battery power as they are not fixed, in order to make the operations of the wireless devices efficient it is mandatory to improve the power aspects of the battery systems. Few of the commonly adopted strategies involved in enhancing the power aspects of the battery system in a wireless device are as follows: (i) When certain nodes are found to be idle then these nodes can be pushed into the sleep state so as to conserve power (ii) suitable paths can be selected in a network during a transmission process in such a way that the destination node appears to be closer to the corresponding source node, in simple words selection of shorter routes in order to reduce power consumption (iii) identifying the relevant nodes required for a particular transmission process before the commencement of the process (iv) building power efficient structures (v) devising suitable strategies for minimizing the overload of the concerned network.

1.2 Objectives of the Mobile Ad-hoc Networks

Objectives to be devised before the construction of the ad hoc networks are as follows: extensibility, rapid confluences, two way transmissions, circumference freedom, etc. With rapid propagations of the ad-hoc network in various applications today, have increased the demand for certain other attributes simultaneously.

Protected routing and data transmission [4]: As the nodes in the ad hoc networks are mobile in nature the routing protocols to be adopted in these networks must possess the tendency of coping up with the changing infrastructures. Together with the infrastructure adjustments the privacy considerations must also stand uncompromised. Transmissions via wireless devices must be completely protected from the offenses so as to retain the original integrity of the confidential contents. Hence the ultimate requirement of the ad hoc network is the incorporation of a secure protocol and an efficient data transmission mechanism.

Quality of service (QoS): Ensuring the quality of the data contents in a wireless network is the most essential consideration. The QoS parameter represents the ability of a network in safeguarding the contents from attacks and in ensuring the retention of the original structure of the contents. Altogether it ensures the quality of the security mechanisms adopted. In simple words it constitutes as a set of service requirements.

Service exploration: A mobile network is

usually employed in a critical environment where human access is considered impossible in case of certain emergency situations. In such cases understanding the nodes completely and catering to its needs is considered to be a significant task. For example, let's consider the nodes employed in battlefields, identification of its requirements at appropriate time durations would enhance the efficiency of the rescue operations. Before requesting for services the nodes would involve themselves in identifying the appropriate routes in view of accessing the required services. Hence the need for service exploration in a mobile network [11].

.

2. DIFFERENT TYPES OF ATTACKS [2]

A. Ad hoc networks circumstances:

As seen previously the nodes in the mobile ad hoc networks are not stationary, they keep moving based on their requirements and hence they do not depend on any centralized controllers for their functioning. The basic principle of their functioning is that the nodes in the network coordinate in performing their transmissions efficiently as there is no mechanism to enforce the same. Absence of such enforcing mechanisms has urged the need for the trust factor among the nodes. Intrusion of an unauthorized user is a common problem here as the network fails to possess a definite structure, therefore suitable security mechanisms must be incorporated in view of ensuring secure transmissions among the authenticated users. Identification of the compromised nodes is another important task. Compromised nodes are capable of transmitting huge volumes of unintended contents into the network in view of crashing the network. Intrusion of such malicious nodes would ultimately decrease the throughput of the system. This problem can be effectively encountered if the original nodes in the concerned network are integrated together by means of suitable and authorized links. Proper organization of a network is another important factor of prime consideration as the employment of security mechanisms in an organized network appears to be simple as the nodes would readily accept and incorporate them as they are properly organized.

B. Layers involved in the Communication process:

Various layers in the mobile ad hoc networks would operate in a coordinated manner for establishing an effective transmission process. Each layer in the network possesses its own vulnerabilities. The first and foremost layer is the physical layer, it is seen that this layer also comprises of the transmission links. The nodes and links of this layer are found to be vulnerable to both the active and passive forms of attacks. Few of the predominant attacks in this layer are as follows; the Passive eavesdropping, signal jamming, denial of service (DoS) attacks, and the physical hardware tampering problems [2]. By means of suitably encoding the confidential contents on the transmission paths, offenses against them can be gradually minimized. Attacks against the hardware equipments can be considerably minimized by incorporating strong tamper-resistant hardwares.

C. Offense Levels:

Two of the common offenses in the ad hoc networks are observed to be against the fundamentally incorporated strategies and the adopted security mechanisms [4]. The fundamental strategy talks about the wireless links between the employed nodes and the security mechanisms related to the adopted routing protocols and the encapsulation procedures.

2.1 AD HOC NETWORK INTIMIDATIONS

As MANETs are infrastructure less one of the most common attacks experienced by them would be the routing attack. Most of the communications today rely on protected data transmissions as the privacy of the contents has observed to be the prime factor of consideration. This reliability on the privacy concerns has urged the need for enforcing various safety measures into the mobile ad hoc networks. Knowledge about the offenses is significant as this forms the base for devising strong security measures. Researchers are also concerned about the common offenses prevalent on these networks. Complete research about these offenses would assist in the invention of strong security mechanisms for safeguarding the data completely.

2.2 CATEGORIZATION OF THE OFFENSES

Two types of offenses are prevalent on the networks, they are:

(i) The Internal attack

(ii) The External attack.

In *Internal attacks*, the attacker would gain access to the contents of the network and would involve himself in the activities of the network, by means of impersonation or by compromising the original nodes of the network. Once the hacker gains access to the contents he would either transmit it to his authorities in order to acquire profits or would simply modify the contents to cause destructions to the network on the whole.

In *External attacks*, the motivation of the attacker is to disturb the transmission process, in this type of attack, modification of either the components or the contents within the system is impossible hence the attacker would transmit unwanted contents from outside causing traffic related problems and congestions within the network, transmitting false contents into the network and distracting the nodes from their duties are the other

measures adopted by the hacker.

Mobile ad hoc networks today are susceptible to the following types of attacks: The active and passive forms of attacks. In the active form of offense the intruder node has to bear with some of its utilized energy costs incurred during its threat behaviors. In the passive form of attack selfishness in energy conservations are observed, as there is a lack of cooperation among the attacking nodes in terms of energy conservation, this attack comes to existence [8]. In simple words active attacks are observed when the attacker attacks the nodes of a network irrespective of its energy. Its ultimate aim is to damage the network completely. Passive attacks are observed when the attacker damages the network keeping in mind its battery conservations for its own communications.

2.3 ATTACKS ON THE NETWORK LAYER

The following are few of the attacks on the network layer:

1) Black hole attack
2) Byzantine attack
3) Wormhole attack
4) spoofing attack
5) Sybil attack

1. Black hole type of attack:

This type of attack is a routing based attack, the impersonated node would receive the path requests from the source nodes, the attacker would reply by transmitting the details of fake paths to the concerned sender node stating it to be the shortest path. These attempts are made by the impersonated node with the intention of diverting the traffic to a path that is allotted for eavesdropping or to introduce the denial of service conditions.

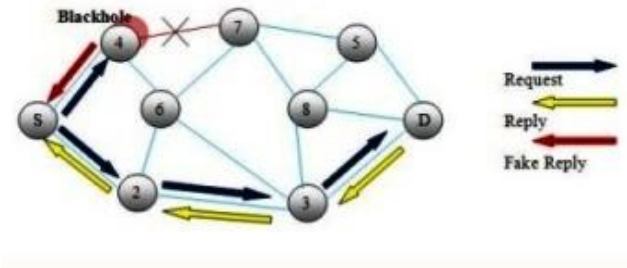

Figure 2: Black hole attack

2. Byzantine type of attack:

The attacker here would select a group of intermediate nodes in a particular networking zone and would compromise the same for performing the instructed attacks. The attacks instructed by the intruder would be to create routing loops, formation of which would completely prevent the transmission of the data materials to the intended destinations instead the packets would be revolving within the loops itself, the next type would be to simply transmit the data contents to an unintended destination. The other attacks would comprise of dropping the relevant packets outside the network which would ultimately cause a disruption in the service [10]. Observation of these offenses is not an easy task here as the functioning of the concerned network appears to be normal. As the network operation appears to be normal here, detection of these attacks is quite tedious. Following are few of the possible byzantine behaviors:

1). Nodes expressing willingness to forward packets.

2). Establishing false routes.

3). Establishing false routes in the control packet;

4). Representing itself to be a portion of the topology.

5). Extracting relevant links from the topology.

3. Wormhole type of attack:

An attacker inside a network would receive the data materials illegally and would transmit the same through another route within the same zone that is allotted for eavesdropping and illegal receptions. Tunnels have been incorporated in this type of offense for illegal transmissions, long transmission links have been designed for distances longer than that of the wired implementations. Implementation of long transmission links would compensate the functioning of the multihop protocols. Transmission of bit wise information seems to be easy here. Such transmissions would reduce the delay time incurred in obtaining the packets. Even though this attack is illegal, it offers the advantage of connecting the network efficiently. The attacker here seems to be powerful than the other available nodes in the network, this superiority enables the attacker to perform various other illegal tasks. Wormhole offense appears to be the dangerous form of offense in a mobile network. This could sometimes enable the discovery of various other routes against the routing protocols.

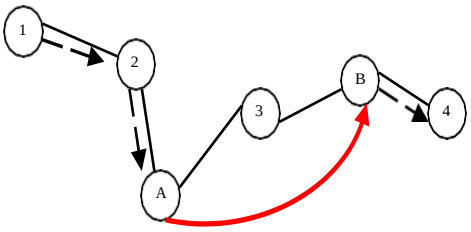

Figure 3: Representation of the wormhole attack

4. Spoofing type of attack:

Spoofing offense damages the original structure of the data materials; here a particular compromised node would imitate a genuine as there is no proper authorization

mechanism in the corresponding mobile network. Lack of proper representations of the communicating nodes in a network is the ultimate outcome of the spoofing attack; other outcomes may be seen as the formation of loops and partitions within the network. Improper authorizations may result in the transmission of illegal packets.

5. Sybil type of attack:

Any attacker node that imitates a non existing node would resemble as an integrated form of several intruding nodes that are combined together, this form of attack is so called as the Sybil type of attack. The goal of this offense is to damage the structure of the network. The nodes of a network should be properly authorized, only the authenticated nodes must be permitted for the transmissions. This attack ruins the identity of a node; destruction of original identities would pave way for the generation of false identities, using these false identities intruders can involve in the transmissions of the concerned network. Sybil attacks usually disrupt the security mechanisms incorporated in the system making it more vulnerable to attacks. Effective solutions for overcoming the defects of the Sybil offenses are yet to be identified.

Substantiate techniques can be adopted to prevent the Sybil attacks. Certain techniques for preventing these attacks have been designed on the basis of the connectivity aspects. These techniques essentially strive hard in minimizing the damages created by the Sybil attacks. The structure of a network is preserved by means of reducing the incurred damages.

2.4 DENIAL OF SERVICE ATTACK

DoS attack would prevent the genuine users from accessing the network contents. The technique adopted here is to overload the target systems so that it hangs down or appears to be inefficient in delivering the required services. Another outcome of this attack is that it denies the services requested even by the authenticated users. The DoS attacks are very common today as a result of the tremendous increase in the information contents. With massive increase in the contents the servers incorporated in various systems are getting overloaded constantly, overloaded servers are thus inefficient. Getting overloaded increases the chances of encountering the DoS attacks. Once encountered with this type of offense the network gets loaded with in contiguous messages. Two of the common DoS attacks are as follows:

1). RREQ Flood Attack: RREQ introduces unwanted messages into the network to block the normal operations of the network.

2). RREP Route loop Attack: Creation of loops inside a network would block the actual transmission path of the messages. Hence the messages would circulate inside the loop for prolonged time durations and would never reach the corresponding destinations.

2.5 DENIAL OF SERVICE ATTACK IN A DISTRIBUTED MANNER:

This type of attack takes place without the concern of a user, where the user's computer is hacked by an attacker for attacking another computer. Hacking usually encounters by taking advantage of the security susceptibilities possessed by a computer. The entire control of the system is taken over by an attacker. After the hacking process, the attacker would transmit massive volumes of unwanted data to crash the entire system; these packets may be transmitted to selected websites or emails. This attack is termed as distributed because the attacker hacks numerous systems without the knowledge of the users.

1). Resource utilization offense: This attack is also called as the sleep distress attack. Making a compromised node to utilize its battery life unnecessarily is the aim of this attack. The nodes here would be instructed to request for additional route discoveries, or would be instructed to transmit unwanted data packets.

2). Replay [6]: This offense is performed by an attacker by pushing into the networking zone the routing traffic that has been obtained earlier. The ultimate objective here is to focus on the freshness of the routes; it also involves in the identification of the poorly designed security solutions.

3). Flooding offense: The attacker's objective here is to completely drain the resources of the concerned network, the intruder here would usually concentrate on the bandwidth and battery power, draining these two resources to the maximum would damage the network. Loss in these resources would also disrupt the routing operations of the network. For instance the ad hoc on demand distance vector routing protocol can be considered, here the compromised or malicious node can transmit a huge number of repeat request messages to a destination that never exists in the concerned network. Transmission of such messages which would never receive a response would eventually flood the entire network and could lead to denial-of- service.

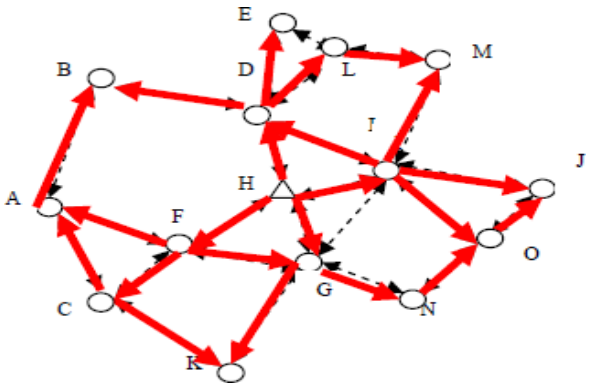

Figure 4: Representation of the Flooding offense

4). Link spoofing attack or IP spoofing attack [3] [10]: Spoofing offense commences its operation by announcing false links to the nearby nodes in a network, this process would essentially disturb the entire functioning of the network. Announcement of two false paths to the sender would essentially confuse the node and would end up in unnecessary transmissions. When a node is compromised by an attacker, then unnecessary dropping of packets and alteration of normal traffic routes would resemble as attacks. Sometimes numerous IP addresses would be generated by the fake node which does not actually exist in the concerned network. Again transmissions to such addresses would load the network.

3. INVADING THE ROUTING PROTOCOL

Various offenses disturbing the routing algorithms exist; these offenses would entirely cease the network's normal operation. Brief explanations of such offenses are given below [13] [14]:

Routing Table Overflow: Overflow of the routing table would enable the attacker to create routes that doesn't exist. The idea here is to create numerous routes to load the network excessively. There are two different types of routing algorithms in general; they are the proactive and reactive types. Proactive types would insist the user to collect the routing information prior to the process. The reactive types would specify the need for collecting the routing information only when needed. This attack would eventually cause an overflow in the routing tables. Overflows would prevent the entries of new routes.

***1). Routing Table Poisoning*:** This type of attack would make use of the compromised nodes to transmit misleading information regarding the routing table updates, or it may involve in modifying the original updates that is sent to the authenticated users. This attack would essentially result in congestions in the network or it may even turn some portions of the network inaccessible.

2). Packet Reproduction: Here the useless or unwanted packets would be taken into consideration and suitable replications on those packets would be performed. These unnecessary replications would consume additional bandwidth and battery power resources creating insufficiency of the same.

3). Route Cache Poisoning: As far as the routing protocols are considered, each node would maintain a separate routing table which would hold the necessary routing details about the entire network [14]. Messages regarding the addition of new routes or deletion of existing routes if any would be constantly updated in the routing table. Modification on such contents would essentially poison the routing table.

4). Rushing offense: The procedure of suppressing the contents regarding the routing information during the route discovery process is found to be susceptible to such attacks [12]. Together with the actual node the compromised nodes too would receive the route request messages, immediately after receiving such request messages the compromised node would transmit packets continuously to the concerned network in view of overloading the network. At times when the nodes of a particular network receives the genuine route request message, it would then be in a position to distinguish the actual messages from the messages sent by the attacker, after which it would essentially discard the packets. Identifying the secure routes in a network that is not subjected to attacks is not an easy process.

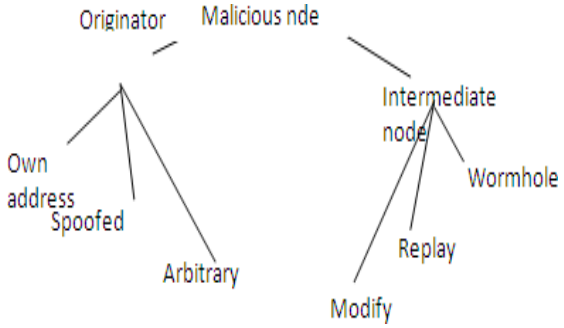

Figure 5: Representation of a malicious attack tree

4. VARIOUS OTHER ATTACKS ON A NETWORK

1). Rushing offenses: The on demand routing protocols are responsible in carrying out this attack on the ad hoc networks, a copy of every packet that is meant to be transmitted is retained at the nodes of the network. The strategy adopted here is to transmit unwanted messages in par with the genuine messages. The genuine messages are therefore misunderstood as duplicate messages and thus discarded by the nodes. Another type of attack here is called as the spoofing attack; in this type, the compromised or malicious node would impersonate itself as the original node of the network by means of modifying its IP or MAC address.

2). Gray hole offense: Gray hole attacks are more common in the ad hoc networks. This attack comprises of two different phases, in the initial phase the compromised node would send announcements stating that it has the set of valid addresses and corresponding route details relevant to the concerned destinations. In the second phase the nodes of a network would essentially involve in the task of dropping the intercepted packets with a certain probability. Gray hole attacks are quite difficult to identify when compared with that of the black hole attacks [5]. This attack expresses its fraudulent behaviors in various ways. One such expression is to continuously drop the data packets for a fixed time duration after which the compromised nodes would switch back to its usual behavior.

3). Sinkhole offenses: This type of attack would enable the malicious nodes to attract the passing data packets towards itself from all the concerned neighboring nodes of a network. This attack seems to be the most important of all the other attacks as gaining illegal access to the data packets is achieved only in this type of attack. The strategy adopted by this attack is to identify the loopholes

of the routing algorithms and thereby incorporate the same for establishing themselves as the most trusted partners of the existing original nodes of the network.

4). Location disclosure [9]: An attack that focuses on the privacy aspects of an ad hoc network is the location disclosure attack. The idea of this attack is to determine the location of a particular node; this can be achieved either by intruding into the network and thereby monitoring the structure and the incidents happening inside or by simply hacking the traffic patterns for in depth location details.

5). Jamming offense: The MAC layer is seen as the platform over which this attack takes place. This attack is a form of the denial of service attack. Any interruption in the ongoing communication procedures in a wireless network is called so as the jamming attack. This attack encounters just by preventing the progress of the real time traffic over the network. Further it would prevent the genuine nodes from transmitting data packets to the prescribed destinations.

6). Information Disclosure [12]: The aim of a secured communication is to completely protect the confidential contents from unauthorized access. Another consideration of a secured communication is to safeguard the genuine nodes from being compromised. Various other materials to be protected would include the locations of nodes, private and public keys used in the encryption and decryption process, passwords etc. Any leak in the contents of the above mentioned materials would fall into the information disclosure problem. Control data packets are sometimes more essential in the regulatory procedures, loss of those packets would again lead to the disruption of the network transmissions.

5. CONCLUSION

It is thus evident from this survey paper that the offenses against a mobile ad hoc network may take different forms depending on certain parameters as mentioned below: (1) the circumstances and surroundings in which a particular attack has been launched (2) targets devised by the hackers, especially the layers selected by an attacker to launch the attack (3) the ranges selected for implementing the attacks, this includes the incorporated security mechanisms of a system. Before designing an ad hoc network it is mandatory to focus on the security needs, so that improved safety mechanisms can be devised in order to protect the system and the transmission procedures. The devised security strategies must essentially consider the nature and the characteristic features of the various available offenses. MANETs are more susceptible to attacks as they do not exhibit a fixed infrastructure and that the communicating nodes move from one point to the other constantly. Hence MANETs require increased security levels than that of the conventional wired networks. New algorithms and security strategies can thus be devised keeping in mind the attacks on a mobile network.

REFERENCES

1] Gopalakrishnan, S. (2004) “A Survey on Wireless Network Security”, International Journal of Computer Science and Mobile Computing, 3(1): 53-68.

2] Razak, S. A., Furnell, S. M. and Brooke, P. J. (2004) 'Attacks against mobile ad hoc networks routing protocol', Proceedings of the 5th annual postgraduate symposium on the convergence of telecommunications, networking and broadcasting (PgNeT), Liverpool, 28-29.

3] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication,” International Journal of Computer Science and Security (IJCSS), 4(3): 265-274.

4] Hongmei Deng, W. Li, Agrawal, D.P.(2013), “Routing security in wireless ad hoc networks”, Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, 40(10): 70- 75.

5] Ujjal Agarwal, Yadav, P.K and Upendra Tiwari, “Security Threats in Mobile Ad-Hoc Neetwork”, International Journal of Research in Science and Technology, 3(4): 53-64.

6] Jayashree. A. Patil and Nandini Sidnal, “Survey-Secure Routing Protocols of MANET”, International Journal of Applied Information Systems, 5(4):8-15.

7] Wang YT, Chen IR, Wang DC. A survey of mobile cloud computing applications: perspectives and challenges. *Wireless Personal Communications* 2015; **80**(4): 1607–1623.

8] Hu, Y.C., A. Perrig, D.B. Johnson, (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. J. Wireless Netw., 11: 21-38.

9] K. Sanzgiri, D. Laflamme, B. Dahill, B. Levine, C. Shields and E. Royer.(2005), “An Authenticated Routing for Secure Ad Hoc Networks”. Journal on Selected Areas in Communications special issue on Wireless Ad hoc Networks.

10] Roopak, M., & Reddy, B. (2013). Blackhole Attack Implementation in AODV Routing Protocol. International Journal of Scientific & Engineering Research, 4(5): 402-406.

11] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay International Journal of Computer Science and Security (IJCSS), 4(3): 265-274.

12] L. Zhou and Z. J. Haas.(1999), “Securing Ad Hoc Networks”. IEEE Network Magazine, 13(6):24-30.

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

14] Kumar, R., Verma, P., & Singh, Y. (2013). Mobile Ad Hoc Networks and It s Routing Protocols. World Academy of Science, Engineering and Technology International Journal of Computer, Information, Systems and Control Engineering, 7(8).

15] Kumar, R., Verma, P., & Singh, Y. (2014). Review of MANET Protocols and Introduction of a New Optimized Routing Scheme using Evolutionary Algorithms and Analytical Hierarchy Process. Wireless Communication, 6(4), 161-171.

16] B. Sukla,(2008) “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks”, In proceeding of the World Congress on Engineering and Computer Science, 22-24.
17] Bing Wu, Jie Wu, Eduardo B. Fernandez, Mohammad Ilyas, Spyros Magliveras,(2007) "Secure and efficient key management in mobile ad hoc networks", Journal of Network and Computer Applications 30 (10):937-954.
18] M. Gunasekaran, P. Sampath and B. Gopalakrishnan, (2009), “AAS: An Authenticated Acknowledgement-Based Scheme for Preventing Selfish Nodes in Mobile Ad Hoc Networks”, International Journal of Recent Trends in Engineering, 1(1), : 294-298.