IJASRM
International Journal of Advanced Scientific Research and Management, Volume 3 Issue 2, Feb 2018.
www.ijasrm.com
ISSN 2455-6378

A Review on Security Issues, Challenges and their Solutions in MANETs

Kshitiz Agarwal, Mukul Rustagi and Surjeet

ECE, Bharati Vidyapeeth's College Of Engineering, GGSIPU
Paschim Vihar, Delhi, India

Abstract

Mobile Ad hoc Networks are basically an infrastructure less network of transportable devices having wireless communication capabilities. In such networks, nodes can join at any time and at any place dynamically. Mobile nodes can simultaneously act as an intermediate router as well as source or destination. Nodes can move in random motion, hence network topology changes dynamically. This makes such networks an autonomous system of mobile nodes having centralized administration. In MANETs each node has limited transmission range so packets are forwarded from source node to destination node in a network with the help of multi routing. With the transmission of packets over wireless networks there are many issues and challenges that are encountered. The issue of security of data has been considered as the main parameter in this paper.

Keywords: *MANETs, routing, security issues.*

1. Introduction

The [1] revolution of wireless networks are bringing fundamental changes to data networking, telecommunication and are making integrated networks a reality. By making the user free from the cord, personal communications networks such as wireless LAN's, mobile radio networks and cellular systems harbor the promise of fully distributed mobile computing and communications anytime, anywhere. Focusing on the networking and user aspects of the field, wireless networks are becoming fastest growing areas of interest. Ad hoc networks are self-organizing, rapidly deployable and self-configurable. A MANET is formed by a group of mobile wireless nodes communicating with each other via wireless links in a distributed topology without any centralized controlled system as shown in Figure 1.

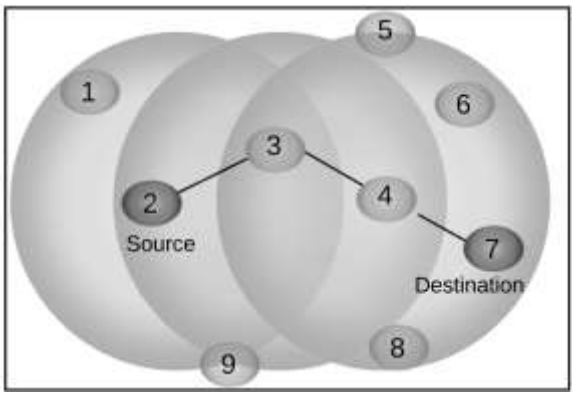

Figure 1 Basic MANET

The nodes are mobile and can form the network whenever required. The mobility of nodes made it hard to find out a network topology used by nodes at any time for routing. Moreover, the node mobility provides dynamic changing topology and failure of route frequently which results in packet loss and makes the transmission less efficient. MANETs [2] were initially proposed for military applications and currently their use has been enlarged. Examples of applications include emergency disaster relief, military battle field communication, sensing or controlling a region, sharing information during a lecture or conference and etc. In the above example, nodes exhibit high mobility and they require easy installation that is why manets finds applications in these sectors. There are some issues in MANETs like multicasting, multiple routes, distributed operation and security issues. This paper mainly focuses on network layer and its issues mainly on security of data during transmission. The issues like wormhole attack, blackhole and grayhole attack, sinkhole attack, flooding, spoofing, rushing and sybil attack have been discussed. Moreover, if any heavily loaded node is congested, it can cause packet loss and buffer overflow which results in longer end-to-end delay, degradation in throughput and loss of transport connections. Rest of the paper is organized

as follows. Section 2 gives description of various network parameters. Section 3 tells about the security mechanism followed by the network layer. Section 4 defines the various security issues and their effects on the network. Section 5 analyzes all issues and gives the related work in every issue. Finally, Section 6 concludes the paper and gives future directions.

2. Network Layer Metrics

Some parameters are defined to evaluate network performance which has been defined below:

End to End Delay: Time [3] taken for a packet to be transmitted across a network from source to destination. It is used in IP network monitoring and differs from round-trip time (RTT) in that only one way path is measured i.e. from source to destination.

Jitter: It [4] is variation in the delay of the receiving packet. The effects of jitter can be seen in real time applications like video streaming. It is caused due to the congestion in the network.

Throughput: It [5] is the maximum data rate. Commonly it is measured in bits per second (bps), as in megabits per 2 second (Mbps) or gigabits per second (Gbps).

Packet Loss Ratio: Percentage [6] of total packets sent, which are not received at the packets final destination node.

Route Lifetime: Mathematically [7] calculated expected lifetime of a route, which depends on node mobility.

3. General Security Mechanism

General Security Mechanism [8] is divided into two types mainly as preventive and reactive mechanism. The former avoids any type of attack as firewalls and cryptographic systems while the latter believes in taking action on demand to mitigate intrusions, as Intrusion Detection Systems (IDS). Moreover, preventive and reactive solutions are not efficient to put all attacks and intrusions off. So there is third defense line added as Intrusion Tolerance as shown in Figure 2. Main [9] motive of such mechanism is to attain survivability and it can only be done by the use of preventive, reactive and tolerant approaches operating together. The preventive measures will be the first obstacle for attacks, blocking certain ones and incapable of preventing others. Some attacks can succeed in intruding into system (or network) and reactive defenses will come into action, trying to detect and stop them. However, reactive defenses have also limitations and intruders can reach down to infect the network. In order to guarantee the system operation even in the presence of intrusions, intrusion tolerance techniques need to be applied, until preventive or reactive defenses can adapt themselves and take actions against the attack or intrusion. The idea of working all three mechanisms together keeping in mind the survivability properties i.e. resistance, recognition and recovery.

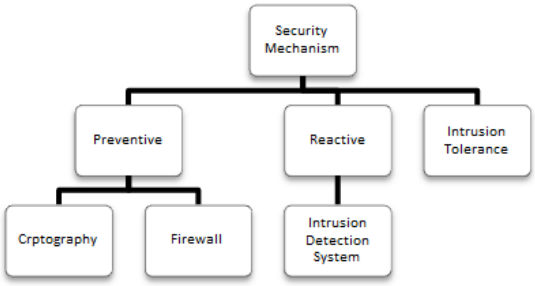

Figure 2 General Security Mechanisms

Resistance is the property of a system to repel or obstruct attacks. User authentication, passwords, firewalls and cryptography are examples of mechanisms used to reach it. Recognition is the system capacity to detect attacks and damage done to system. Examples of recognition mechanisms are intrusion detection by patterns and passwords. Recovery is the capability of restoring disrupted information or functionality within time constraints, limiting the damage and maintaining essential services.

4. Issues of Data Security in MANETs

MANETs are prone to many security issues. Characteristics as dynamic topology, limited resources, limited physical security and no centralized infrastructure make those networks vulnerable to passive and active attacks. In passive attacks, packets containing secret information may be dropped making a concern for a network. Active attacks include sending packets or data forms to undefined destinations, missing packets, influencing other nodes and modifying the content of packets.

4.1 Wormhole Attack

In [10] worm hole attack a tunnel is made between two malicious node that tunnel is known as worm hole. It itself advertise as shortest path between source and destination and when wormhole attacks happens it prevents transmission from the other paths as it advertise itself as shortest path. Hence, all the

IJASRM International Journal of Advanced Scientific Research and Management, Volume 3 Issue 2, Feb 2018.
www.ijasrm.com
ISSN 2455-6378

data transmits through this tunnel only so it can drop/alter the transferred data packets as shown in Figure 3 and Figure 4. In Figure 3, tunnel is AXB and in Figure 4, tunnel is AXX'B where A is source and B is destination.

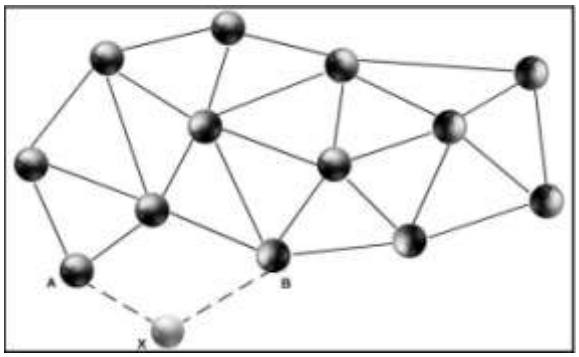

Figure 3 Wormhole created by node X'

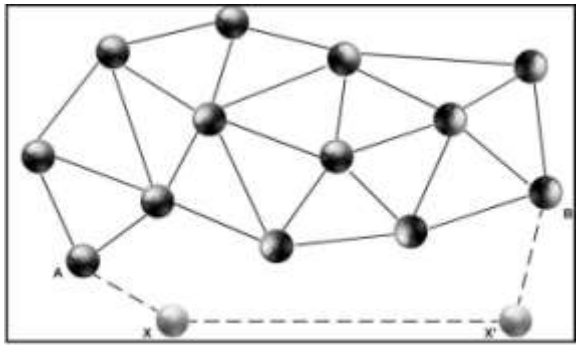

Figure 4 Longer wormhole created by two collision nodes X and X'

4.2 Grayhole Attack

Grayhole [11] attack is the special version of black hole attack. In black hole attack malicious node place somewhere in between source and destination and advertise the path between the source and attacker (malicious node) as the shortest path then capture the packet and drop it whereas in case of gray hole, dropping of data is done in 3 selective and statistical manner.
Here in Figure 5, the attacker node is E which drops the packet to node D only and forward to others nodes forming a gray hole.

4.3 Blackhole Attack

In [12] black hole attack, attacker takes the advantage of vulnerabilities in AODV, DSR during route discovery process. In reactive protocol, sender broadcasts RREQ packet in order to send data to destination node.

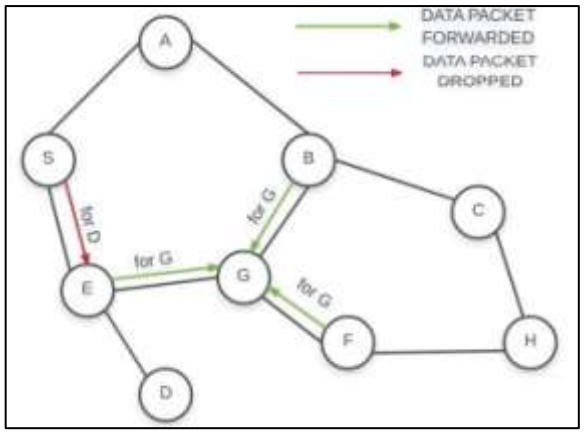

Figure 5 Grayhole Attack

Node with highest destination sequence number is considered as having the shortest path towards destination hence, malicious node took advantage of having highest destination sequence number and send this false RREP packet and then source select path through this malicious node and reject reply packets from other nodes, this is called black hole attack as shown in Figure 6.

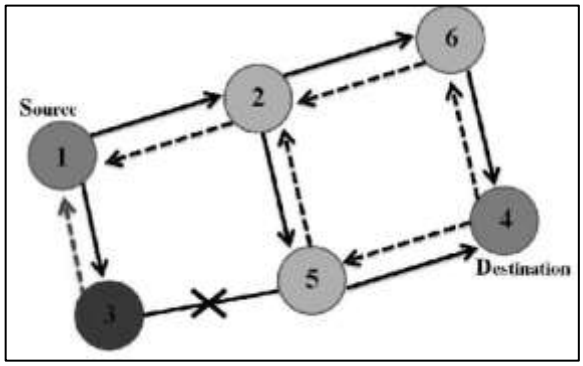

Figure 6 Blackhole Attack

4.4 Rushing

An [13] action that is taken against on-demand routing protocols is termed as rushing attack. Basically, in the case of these protocols it is stated that nodes must forward the first received Route Request from each route immediately and all other received Route Requests are ignored. This is done in order to avoid cluttering. The attack consists, for the adversary, in quickly forwarding its Route Request messages when a route discovery is initiated. But if the Route Requests that first reach neighbor's node turned out to be of attacker, then any other route will also include the attacker as shown in Figure 7.

IJASRM
International Journal of Advanced Scientific Research and Management, Volume 3 Issue 2, Feb 2018.
www.ijasrm.com
ISSN 2455-6378

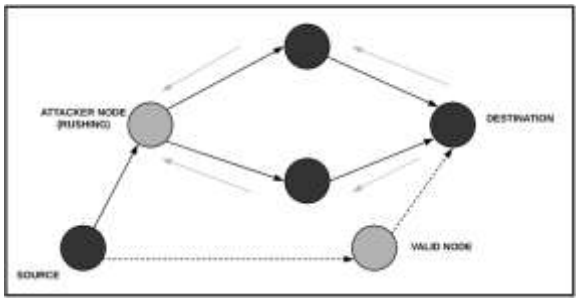

Figure 7 Rushing Attack

4.5 Sinkhole Attack

In [13] the case of sinkhole attack, the intruder compromises one node of the network and introduces its own node in the network which is used to launch attack. This node is situated close to base station because in case of wireless sensor networks, many nodes send data to base station only and thus it does not need to target all the nodes in the network but only those close to the base station. This node initially operates on the routing mechanism of the network and after attracting all the traffic to itself it sends fake routing information to the neighboring nodes and launch attack as shown in Figure 8.

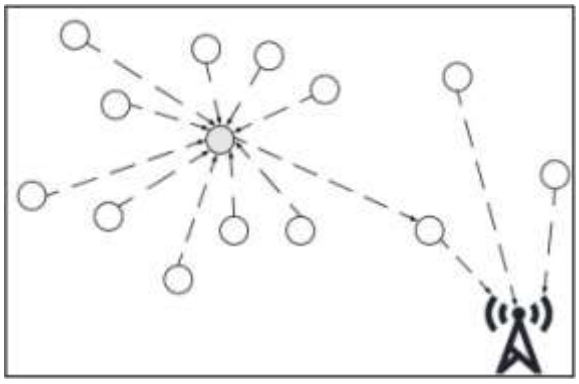
Figure 8 Sinkhole Attack

4.6 Hello Flood Attack

Some [14] routing protocols in Wireless Sensor Networks require nodes to broadcast hello messages to tell about their existence to the neighboring nodes. A node which receives such a message may assume that it is within a radio range of the sender. However in some cases this assumption may be false, sometimes a laptop-class attacker broadcasts routing or other information with such large enough transmission power that could convince every other node in the network that the attacker is its neighbor. Hence the network is left in a state of confusion. Protocols which are dependent on localized information exchange between neighboring nodes for network topology maintenance/reconstruction or flow/error control are mainly affected by this type of attack. An attacker does not necessarily need to construct legitimate traffic in order to use the hello flood attack. It can simply re-broadcast overhead packets with enough power to be received by every other 4 node in the network.

4.7 Spoofing

A spoofing attack [15] is when a malicious party imitates another device or node present in the network in order to launch attack against network hosts, manipulate data, spread malware or give alternate access controls. Some of the most common methods are IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks.
In an IP address spoofing attack, an intruder sends IP packets from a false (spoofed) source address in order to create confusion among the nodes as shown in Figure 9.

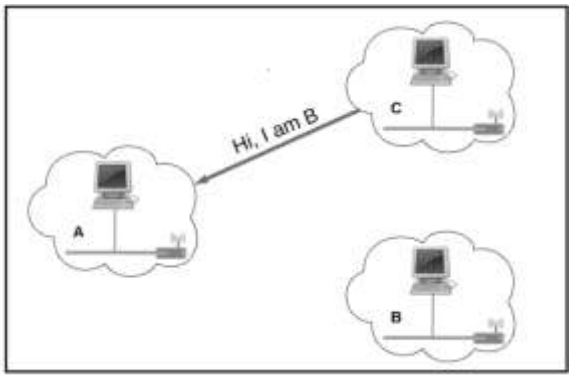

Figure 9 IP Spoofing

ARP is used to transmit data from IP address to MAC address. In an ARP spoofing attack, the malicious party sends spoofed messages across the LAN in order to establish a connection of its MAC address with the legitimate member of the network. This type of attack results in sending the data to the attacker instead which was meant for Host IP address. Malicious parties commonly use ARP spoofing to steal information, stop traffic on a LAN. ARP spoofing only works on local area networks that use the Address Resolution Protocol.

The Domain Name System (DNS) is a system that provides domain names with IP addresses. Devices which are on Internet all have some DNS associated with them to respond to URLs or email addresses. In a DNS server spoofing attack, a malicious party modifies the DNS server in order to reroute a specific domain name to a different IP address. In many cases, the new IP address will be for a server that is actually controlled by the attacker and

IJASRM
International Journal of Advanced Scientific Research and Management, Volume 3 Issue 2, Feb 2018.
www.ijasrm.com
ISSN 2455-6378

contains files infected with malware. These are mainly used to spread worms and viruses.

4.8 Sybil Attack

In MANET [16] the medium of transmission of data packets is air and they do not have a central node to administer the network. So the routing is mainly based on a unique node address. This property of MANET can be exploited by the attacker by using fake identities. That is the attacker can either use random fake identity or the identity of authorized node. This type of attack is called Sybil attack. These attacks causes lot of packets to be routed towards the fake identity nodes which makes severe attacks. The presence of this type of attack in the network makes it difficult to find the intruded node, and also this prevents a fair resource allocation among the nodes. In Figure 10, two types of nodes are shown, one is trusted group of nodes and other is Sybil attacker nodes .The Sybil attackers are basically nodes with random identity or identity of authorized node. The link from the trusted node region to Sybil attacker region helps the Sybil attacker to capture information which is send through it.

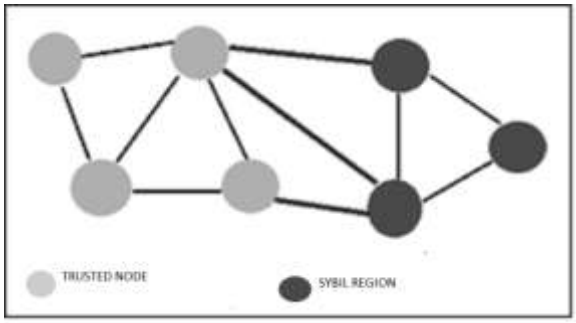

Figure 10 Sybil Attack

5. Proposed Solutions for Attacks

There have been many approaches towards finding the solutions of security attacks, hereby mentioned are earlier proposed solution for each issue respectively.

5.1 Wormhole Attack

Network [17] can be protected from the worm hole attack in two ways, they are packet leashes and sector.

a) Packet lashes: It is the mechanism of detection of wormhole attack. Here leashes means packet that restrict the maximum allowable transmission distance of packet. There are two types of lashes:

i. Geographical lashes

ii. Temporal leashes

b) Security tracking of node: This method uses series of first one bit exchange to bind the maximum distance between two adjacent or neighbor node to prevent it from worm hole attack. This uses the hardware to provide fast processing between sender and receiver and to make sure the accuracy of time.

5.2 Blackhole Attack

There are three mechanisms which provide protection from black hole attack. They are TOGBAD, SAR and DPRAODV protocol [17].

TOGBAD: It [17] is detection mechanism of black hole attack which is based on topology graph. It compare actual number of neighbors with number of neighbor a node should have therefore it only works for proactive protocol because it is not feasible to obtain complete topology information in case of reactive protocol.

SAR (Secure Aware Routing protocol): It [17] is based on on-demand routing protocol and the main focus in original protocol is to find the shortest path from source to destination for transmitting the data means that they only consider the length of the route. But in SAR it incorporates security metric into RREQ packet so that they can track the changes in forwarding which depends on RREQ. Whenever a node receive the RREQ packet, SAR ensures that node process or forward only those packet who have authorization from the immediate node, it allows node to drop the packet if it is not fulfilling the security requirement. Drawback of SAR is that it is not able to find the shortest path as its major focus on the secure path rather than the shortest path. If nodes in the shortest path satisfy all the security constraints then SAR can find the shortest path.

DPRAODV (Detection, Prevention and Reactive AODV): DPRAODV [17] is the better version of AODV it uses dynamic threshold value to classify the node as malicious node. In AODV, RREP packet sent by any intermediate node is accepted only if its destination sequence number is higher than one in routing table. But DPRAODV make use of threshold value, if Distance sequence number of any node is higher than the threshold value then it would be treated as malicious node and that node is added to blacklist. The control packet named ALARM keeps the record of blacklist node which is send by the node to all neighbors to alert them. If node receives packets from the blacklisted node, it simply discards them.

5.3 Grayhole Attack

In [17] Gray hole, each node generates evidence while forwarding the packet using a aggregated signature algorithm. This algorithm helps to find the malicious node by detecting whether the node is dropping the packet or not. Another mechanism which is used to detect gray hole attack is that all the nodes maintain their neighbors forwarding information after specific interval of time and check communication status with the neighbor whether it is being communicated or not, then starts the detection procedure and this procedure is done by comparing the number of CTS and RTS messages, if the node is found to be suspicious then it confirms with its neighbors after it takes the decision about the malicious node.

5.4 Rushing

To [18] prevent the rushing attack we can use three mechanisms together, they are secure neighbor detection, secure route delegation and randomized route request forwarding. In secure neighbor detection, each neighbor is allowed to verify that the other node is within a given maximum transmission range. Here we use a three round mutual authentication protocol that uses precise delay timing that make sure that the other node is within the transmission range. In the first round the starting node sends a neighbor solicitation packet by unicast method or broadcast method. In next round by receiving the neighbor solicitation packet, the received node sends back a neighbor reply packet. At final round the starting node sends neighbor verification packet containing broadcast authentication of a timestamp and source to destination link. Secure route delegation mechanism is used to verify that all the secure neighbor detection procedure are performed between two neighboring nodes. In randomized message forwarding, random selection technique can be used to prevent the rushing attackers in dominating all other routes to destination. Two parameters are used for selection of randomized forwarding, the number of request packets to be collected and algorithm which can choose timeouts. If the number of requests chosen is very large, the randomized forwarding will reply more on the time out, which increase the latency and reduce the security.

5.5 Sinkhole Attack

The [19] technique used is Non-Cryptographic Method, it is designed to make every node aware of the entire network so that any rightful node will not listen to the cheating information or fake routing information from malicious or compromised node which leads to sinkhole attack. Two algorithms are involved in this system. Firstly Agent Navigation algorithm tells how a mobile agent gives whole network routing information to nodes and checks every node. Secondly Data Routing algorithm tells how a node uses the global network information to route data packets. This method has very high overhead if number of nodes are more in WSN. But in this, every node has to store a lot of data in itself hence its efficiency decreases, but by using certain reduction filter techniques this can be decreased and then it becomes an efficient method.

5.6 Hello Flood Attack

Algorithm [20] for hello flood prevention Begin
1: If a node receives hello message from a node S then
2: If Signal strength of received hello message = fixed signal strength in radio range
3: Then node s is classified as a friend
4: Node accepts hello message and perform necessary function
5: Else
6: If Signal strength of received hello message fixed signal strength in radio range
7: Then nodes sends puzzle to node S
8: If reply message of correct answers comes in fixed time threshold
9: Then Node is classified as friend and accepts the request and performs function
10: Else Signal strength of received message ¿ fixed signal strength in radio range
11: Then Node S is classified as stranger and rejects the further requests from S.
12: End

5.7 Spoofing

Common [21] measures that are used for prevention of spoofing attack include:
i) Packet filtering: Packet filters inspect packets which are transmitted across a network. These filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information.
ii) Avoid trust relationships: Organizations should develop protocols that rely on trust relationships as little as possible. It is significantly easier for attackers to run spoofing attacks when trust relationships are in place because trust relationships only use IP addresses for authentication.

iii) Use spoofing detection software: There are many programs available that help organizations detect spoofing attacks, particularly ARP Spoofing. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed. iv) Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols strengthens spoofing attack prevention efforts by encrypting data before it is sent and authenticating data as it is received.

5.7 Sybil Attack

There [22] are mainly two methods to detect the Sybil attack they are PASID (Passive ad-hoc Sybil identity detection) and PASSIVE-GD.
In Passive Ad-hoc Sybil Identity Detection, a single node can detect Sybil attacker by recording the identities like MAC or IP addresses of other nodes that hears transmission. By this addresses the node builds a profile of which nodes are heard together. Thus this method helps in revealing the Sybil attackers. When the network contains more nodes in less space the rate of false positives will increase. Thus the node will have only fewer chances to hear its neighbors. To prevent this we have a method where multiple trusted nodes can share their observation with other nodes to increase the accuracy of detection. Next method used for detection of Sybil attack is PASIDGD that is mainly an extension of PASID. This method is used to reduce false positives that may occur when a group of nodes moving together is identified as a single Sybil attacker. Here they exploit the property of channel, that is a single channel transmits only serially and independent nodes transmit in parallel that makes considerably higher collision. So by detecting collision at MAC level we can identify the Sybil attacker of this type.

6. Conclusion

The dynamic nature of MANETs makes it more vulnerable to attacks at different layers. In this paper we have done a survey on security issues in MANETs and their possible detection mechanism. The comparison between different detection methods is also done here. In future there may be ways to defeat these protection mechanisms. So this is a further potential area of research in which more powerful detection mechanisms can be invented.

References

[1] Murthy CSR and Manoj RS, Ad Hoc Wireless Networks: Architectures and Protocols , Prentice Hall: 202-280,(2004).
[2] Raza N, Aftab MU, Akbar MQ, Ashraf O and Irfan M, Mobile Ad-Hoc Networks Applications and Its Challenges. Communication and Networks, 8: 131-136, (2016).
[3] Wang J, Dong W, Cao Z and Liu Y, On the Delay Performance Analysis in a Large-Scale Wireless Sensor Network. Real-Time Systems Symposium (RTSS) 2012 IEEE 33rd: 305-314, (2012).
[4] Awad SS, Analysis of accumulated timing-jitter in the time domain. Instrumentation and Measurement IEEE Transactions, Vol 47: 69-73, (1998).
[5] Corson S.and Macker J, Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. ACM SIGMOBILE Mobile Computing and Communication Review, Vol 3: 11- 13, (1999).
[6] Mancikam P, GuruBaskar T, Girjia M and Manimegalai D, Performance Comparisons of Routing Protocols in Mobile Ad Hoc Networks. International Journal of Wireless and Mobile Networks, Vol 3 (Issue 1): 98-106, (2011).
[7] Parvez N,Mahanti A and Williamson C, An Analytic Throughput Model for TCP NewReno. IEEE/ACM Transactions Network, vol. 18 (Issue 2): 448-461, (2010).
[8] IEEE Communications Surveys Tutorials, Vol. 11 (Issue 1), (2009).
[9] Lima MN, dos Santos AL and Pujolle G, A survey of survivability in mobile ad hoc networks. IEEE Communications Surveys and Tutorials, Vol 11 (Issue 1): 66-77, (2009).
[10] Anuj J and Sminesh CN, An Improved Clustering-based Approach for Wormhole Attack Detection in MANET. IEEE, Vol. 4 (Issue 3): 149-154, (2014).
[11] Goyal P, Parmar V and Rishi R, Manet: Vulnerabilities, Challenges, Attacks, Application. International Journal of Computational Engineering Management, Vol. 11: 32-37, (2011).
[12] Panicker VA, International Journal of Computer Science and Information Technologies, Vol. 5 (Issue 3): 3437-3443, (2014).
[13] Yang H, Luo H, and Ye F, Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications, Vol 11 (Issue 1): 38-47, (2004).

[14] Yu T and Zhu YG, Research on Cloud Computing and Security. Distributed Computing and Applications to Business Engineering Science (DCABES) 2012 11th International Symposium: 314-316,(2012).
[15] M AN and Khokhar SMRH, A Review of Current Routing Attacks in Mobile Ad hoc Networks. International Journal of Computer Science and Security, Vol 2 (Issue 3): 18 - 29, (2008).
[16] Levine BN, Shields C and Margolin NB, A Survey of Solutions to the Sybil Attack. Tech Report, University of Massachusetts Amherst, Amherst, MA, 2006-2052, (2006).
[17] Schweitzer N and Stulman A, Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks. IEEE Transactions on Mobile Computing, Vol 16 (Issue 8): 2178-2183, (2017).
[18] Hu YC, Perrig A and Johnson DB, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. Proc.2nd ACM workshop on Wireless security: 30-40, (2003).
[19] Baskar R, Raja PCK, Joseph C and Reji M, Sinkhole Attack in Wireless Sensor Networks-Performance Analysis and Detection Methods. Indian Journal of Science and Technology, Vol 10 (Issue 12), (2017).
[20] Singh VP, Jain S and Singhai J, Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. IJCSI International Journal of Computer Science Issues, Vol 7 (Issue 3): 23-27, (2010).
[21] Kannhavong B, Nakayama H, Nemoto Y, Kato N and Jamalipour A, A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, Vol 14 (Issue 5): 85-91, (2007).
[22] Mamatha GS and Sharma SC, Network Layer Attacks and Defense Mechanisms in MANETS-A Survey. International Journal of Computer Applications, Vol 9 (Issue 9): 12-17, (2010)