Indian Journal of Science and Technology, *Vol 9(35), DOI: 10.17485/ijst/2016/v9i35/91456, September 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Exploration of Security Threat Analysis in Wireless Mobile Adhoc Network

I. Vijaya[1*], Amiya Kumar Rath[2] and Bhagabat Puthal[3]

[1]Department of Computer Science and Engineering, Siksha 'O' Anusandhan University, Bhubaneswar - 751030, Odisha, India; ivijaya@rediffmail.com
[2]Department of Computer Science and Engineering and IT, V. S. S. U. T, Burla - 768018, Odisha, India; amiyaamiya@rediffmail.com
[3]Department of Computer Science and Engineering IGIT Sarang, Dhenkanal - 759146, Odisha, India; bhagabat.puthal@gmail.com

Abstract

Objective: Mobile Adhoc Networks (MANETs) due to its principle characteristics of network infrastructure, limited resources and transmission range are more vulnerable to multitude of attacks. The objective is to classify the attacks and its counter measures to detect and eliminate malicious nodes. **Methods/Analysis:** Each attack has been analyzed briefly based on its own characteristics and behavior. Also, the defeating methodologies against network attacks have been described and evaluated as a part of the measurements. We have also proposed an Algorithm to study and analyze networks on affected conditions. We presented analytics and classification of the attacks on the different layers of the network. **Findings:** On attacked situation in network there will be no data available as the characteristics of the network are unknown. We need to simulate such types of conditions in the network. The performance of the network gets degraded at the time of attack. It was observed that the impact of attack depends on the proximity of the attacker to the source node, it is severe when close and least when far from the source. Each malicious node uses network feature (Distributed Network, Non-centralized, Hop-by-Hop communications, Open network boundary or Wireless media) to break the security. The goal is to violate security service (Availability, Data Confidentiality and Integrity). In our algorithm, we showcased the normalization of the data set such that we get the maximum and minimum values for the classification of the network. The primary groups of data types for classification are: Delay, bandwidth utilization, and drop rate and packet type). There are some secondary classification like conjunction, status of process, running services and utilization of processor. The condition of system was presented as a vector by storing the normalized values in an array. We arrived at simulating a network in attacked situations. **Applications/Improvements:** The work can be extended to find ways to calculate the threshold effectively. Group attacks can be studied and derive the relationship between the average detection delay and the mobility of the nodes.

Keywords: Attack, Affected Condition, Detect and Eliminate Malicious Nodes, MANET, Security Parameter, Threat

1. Introduction

Wireless networks are nodes with no fixed infrastructures whereas the wired network devices usually are kept within confined area. The equipments used in Mobile Ad Hoc network are usually small hand held devices carried and are backed up by the battery. They are also placed into small mobile units and are battery-powered. These devices are prone to attacks as they can be sensed and placed anywhere in the network or carried away from the network crime scene. Attackers easily get these devices to attack in wired and wireless media. In wired media, it is difficult to intercept unless there is a physical damage on the media. In the wireless medium, it is difficult to even notice as it can be as small as an Antenna[1,2].

Additionally, numerous clients of the Ad Hoc systems use gadgets in public places puts the danger of inadvertently uncovering privileged secrets. This results in threat

*Author for correspondence

of unintentionally revealing important information. The attacks encountered is usually on some conversation being held and someone overhears secret information or somebody perusing the PC screen or console from behind additionally called shoulder surfing. Some of the attacks are due to human actions like writing down passwords and user details and mail it. The recovery of this sort of data helps aggressors/attackers to figure the right passwords to system resources. This sort of attack has been given a typical name of "dumpster jumping"[3].

The threats can be classified into various diverse regions that they target. The number of different threats and attacks[4] considers the level of the attack. Attackers try to capture the human perception from them and broadcast false information. Some time attackers observe the social behavior and make decision to alter the process of attack. The decision of the appropriate process to be adopted is then adopted based on the observation.

Second classification of attacks is focusing on the data/information itself like interception and eavesdropping. Entirely basic and dynamic nature of these attacks is formation of false messages infused into networks. There are active attacks on the network services and application level which disrupt the information. Denial or degradation of network services is an example of the attack on the network services. Trojan horses or viruses infused into applications are an example of application level attacks.

The third categories of attack are physical attacks. This is not an active nature but is usually in the form of radiation interception or inductive wiretapping. It incorporates burglary of hardware, cryptographic or physical keys, and distinctive storage media. Other sorts of attacks are social engineering or as uncommon as devastation utilizing explosives or other physical power[3]. The reasons for security threats are shown in Figure 1.

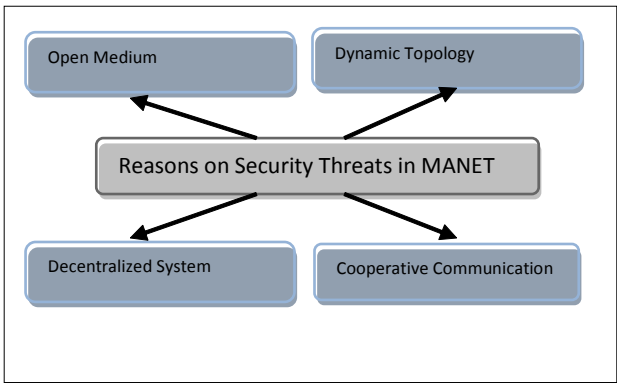

Figure 1. Reasons of security threats in MANET.

2. Related Work

The structure of an Ad Hoc network being wireless lead to malicious activities performed on the network. Devices connected in the network communicate to broadcast information and attacks on these connected devices are attacks on the routing protocol as the protocol defines how these devices broadcast the information. In this section some of these malicious activities are shown below in Table 1.

Table 1. Attacks vs malicious activity

Activity	Relative Impact	Attack
Delay	There is an increase in packet delivery time.	DOS Attack (Flooding, Jamming)
Packet Drop	Throughput is decreased due to non-arrival of packet.	Wormhole
Modify	There is a mismatch in the information of outgoing and actual packet sent	Phishing
Fabricate	Information within the sender's packet and recipient packets is not same.	Counterfeiting
Misrouting	The route of packet gets modified.	AODV

2.1 MANET Routing Protocol Attacks

2.1.1 Routing Loop

Attacker creates a routing loop by sending forged routing packets[2,5,6]. The forged routing data packets consume bandwidth and power for number of nodes. It is similar to denial-of-service attack where in the packets do not reach to the intended recipient.

2.1.2 Black Hole

Attacker sets up a route to some destination via itself and sends out forged routing packets. At the point when the actual data packets arrive they are just dropped, framing a dark gap (a black hole) where information enters yet never takes off[2,5,6].

The attacker directs the route to the destination node into an area, where its existence is not there. The forged route where the information/data is getting transmitted is never acknowledged because of this black hole.

2.1.3 Grey Hole

Attacker drops either the data packets or routing packets. Sometimes forwards routing packets but not data packets or vice-versa. This special type of black hole attack is a grey whole attack[2,5,6].

2.1.4 Partitioning

In this attacker analyses the network topology and chooses to splits up the nodes in the network and create a network partition. With partitioning the capability of communication by some nodes fail. Few nodes in the partition are disabled such that they are unable to communicate with other set of nodes. Also attacker tries to bring damage to the system by forging the data packets and sometimes attacks physically.

2.1.5 Blackmail

Ad Hoc routing protocols have the capability to address security problems by keeping list of possibly malicious nodes. Each node has a blacklist of the nodes that are bad which helps the node to ignore when setting up routing paths. In this, attacker tries to blackmail a good node and adds good nodes to their blacklists.

2.1.6 Wormhole

Attacker uses a pair of nodes that are connected through any medium either directly or indirectly. In this, the packet received by one node is forwarded to the other node. Upon receipt of the packet, the node re-broadcasts the packet into the network. It creates a clash between the data packets sent as both the packets send by the normal node and the packets tunneled back are same. It is difficult to detect because a short circuit is created for the actual routing.

Also, the ad-hoc network is controlled by selectively forwarding the packets. Attacker to gain complete control over the traffic combines this attack with partitioning attack.

2.1.7 Rushing Attack

Attacker multiplies the route request sequence numbers. The sequence numbers are maintained by reactive protocols to suppress duplicate packets at the nodes. This forged numbers at nodes suppresses the data packets assuming that these are duplicate ones. This causes disruption in the actual route discovery.

2.1.8 Resource Consumption

Attackers try to consume more bandwidth by infusing extra data packets and control packets into the Ad Hoc network. The high consumption of node resources such as bandwidth and battery affects the performance of the network. Computational cost gets increased due to ingestion of control packets. Forwarding of control information as it comes also consumes resources[7].

Stajano and Anderson named the resource consumption attack as "sleep deprivation torture"[8]. In this the battery power is drained of and the device becomes inoperable. Unnecessary control traffic is sent in the network which drains the battery. The nodes in the network go to the sleep mode thereby leads to poor throughput. The attack detection increases the overhead as the communication seems to be an ordinary one but intended to drain the battery.

2.1.9 Dropping Routing Traffic

This type of attack is prevalent in Ad Hoc network that a node acts selfishly and process only routing information that is related to it in order to conserve energy. This behavior/attack can create network instability or even segment the network.

2.1.10 Location Disclosure

Attacker gets the information of all the nodes which are available on the route towards the target node. A location disclosure attack reveals the location, topology and structure of network information of a node. This piece of information gained in turn reveals the adjacent nodes to the target or location of a participating node.

This information is gathered by time-to-live attribute of the routing packet and the addresses of the devices by sending ICMP error messages. The information about the location of the destination node is gathered from the intermediary nodes.

2.2 Attacks in Layers of Ad Hoc Networks

The attacks or the threats associated with a mobile network exist at different layers of mobile network. Some of such attacks, their associated layers and the effective solution are shown in Table 2.

Manet's vulnerabilities and lacks give rise to attacks at network layer of ISO/OSI stack. Node behaviors also contribute towards identifying attacks. There are three behavior models.

Table 2. Layers and attacks

Layer	Attacks	Solution
Application Layer	Repudiation, data corruption	Use Firewalls to detect and preventing virus, worms, malicious nodes
Transport Layer	Session hijacking	Use cryptography to ensure authentication and securing end-to-end communication
Network Layer	RP attacks, Wormhole	Protect the Adhoc routing and forwarding protocols
Data Link Layer	Traffic analysis	Provide link layer security support for MAC protocol
Physical Layer	Eavesdropping, Jamming	Use spread spectrum mechanism to prevent DOS & Jamming.

2.2.1 Behavior Node Models

- Collaborative model: In this type of model, the functions of packet forwarding and routing are executed properly.
- Selfish model: In this type of model, a node tries to disable the functions of packet forwarding and routing. To save the battery life, the node tries to misbehave.
- Malicious model: In this model due to the partition of the nodes in the network, there is a complete outage in the network while saving battery life.

We can classify attacks as: Active or Passive

2.2.1.1 Passive Attacks

In this type of passive attack, attackers don't directly communicate with the network but they monitor to find out the network information by deploying an unauthorized node. With this information attackers try to delay the communication and hijack the information causing harm. The two very common passive attacks are: Traffic Analysis and Eavesdropping.

- Eavesdropping Attacks

The attacker can analyze broadcast messages and uncover the confidential information about the network[9]. It is a kind of disclosure attack which can be carried out by either a node belonging to the network (internal node) or by a node not comprised within the network (external node).

- Traffic Analysis

Attackers utilize strategies, for example, activity rate investigation, and time-relationship monitoring. In Traffic Analysis, protocols can be used to stop communication between nodes and hence it is not a pure passive attack. In timing analysis, two packets in and out may be from the same packet flow[10]. It also helps in revealing:

- Location of nodes.
- The existence of nodes.
- The topology of the network in use.
- The role of a node.
- The source communication of a node.
- The destination communication of a node.
- And the geographic location of individuals.

2.2.1.2 Active Attacks

These attacks are launched by users to withhold the normal activities in the network. It is carried out by authorized users who have access to operate the network. The effect of these attacks causes changes in state of network such as DoS (Denial of Service) and modification of packets etc. They are broadly classified into four groups: Dropping, timing attacks, modification and fabrication. Our study also found that one attack can be classified into more than one group.

- Dropping Attacks

Dropping attacks is critical at dropping points resulting in prevention of end-to-end communications between nodes. Malicious nodes reduce the delivery rate causing the disruption the network connection where as selfish nodes preserve their resources by not forwarding the packets. All the packets that are not intended to be delivered at destination are dropped intentionally. It increases inefficiency by retransmission of data packets and reduces the network performance by discovery of new routes[11].

Attacker sometimes makes a selective dropping attack by choosing to drop only some data, route discovery and route error packets. In this case, the source node is not capable of knowing the failed links. In the event of dropping attacks the discovery of routes from source to destination gets impacted.

- Modification Attacks

Attackers take the advantage of disrupting the packets based on the information received by protocols about the nearest node and energy remaining. The packets transmitted disrupt the information of remaining energy and nearest node. A variant of this type of attack is sinkhole attack in which the compromised node is made attractive

to other nodes by attracting all nearby traffics from a particular area.

The fake routing broadcasted by the sinkhole attack becomes a basis of few other attacks like dropping attack and selective forwarding attack. A well known "Sink hole" attack is the "Black hole", described in the earlier section. There is difficulty in detection if the node happens to be either a virtual node or node doesn't belong to the network itself[12].

- Fabrication Attacks

Network packets are forged by the attackers. There is fake "active forge" and "forge reply" without any exchange or receipt of messages. To gain access to the data, extra messages are broadcasted to the packets.

Attackers exploit MANETs' features by initiating frequent packets causing Denial of Service (DoS). In this attack, the user is deprived of network resources to communicate.

There are many variants of DoS attacks, example

- Sleep deprivation torture attack.
- Routing table overflow attack.
- Ad hoc flooding attack.
- Rushing attack.

It does so by persistently interrupting the services up to the extension of suspension of services. One of the very well known DoS attack is CPU exhaustion in which the resource is overloaded with superfluous requests thereby preventing required requests to be fulfilled.

Author in [13] introduced the "Sleep deprivation" torture attack disables the node by draining the node's battery.

Flooding Attack is a DoS attack introduced in[14], against on-demand protocols. When a node needs a route it sends a Route Request messages in the network. The attacker broadcasts many Route Request messages (RREQ) to a non-available node in the network and destroys the Route Discovery property to the destination[15].

Another variant of the attack is – Routing table overflow attack. In this type of attack the attacker sends fake route promotion in the Route Discovery phase for nodes that don't exist. The property of Proactive protocols is to update routing information periodically and the Routing table attack creates overflow in the victim nodes' routing tables. This overflow in routing table information causes blockage to the table and prevents from new routes being created[16].

In the routing cache poisoning attack[8], a node updates the information of the packets into its routing that it hears. The tables are updated although the node is not on the route of the packets. The attacker sends spoofed routing information packets to neighbors that poison the routes to that neighbor node. The neighbors upon receipt of the information erroneously update their routing tables.

- Timing Attacks

DoS attacks, rushing attacks, and hello flood attacks are the types of Timing attacks. In this attackers use a technique to broadcast itself as the node that is very close to the destination node. They attract the close by node pretending to be closest node. Rushing attacks[17] occur during the Route Discovery phase. In the hello flood attack[18], the nodes broadcast Hello packets to detect neighboring nodes in which the one-hop neighbor nodes receive the messages. These received messages are never forwarded to further neighbor nodes.

- Byzantine Attack

In this attack, to locate packets into a loop[19,20], the fault routing information is injected by the malicious node to the network. Authentication can be used to protect network against this attack. There are mechanisms to defeat the attack as in[22].

- Jamming Attack

It is a kind of DOS attacks[22] in which the jammer dominates wireless interaction causing interferes through continuous wireless signal communications with in the network. The interruption obstructs the exchange of packets between the source and target and prevents real traffic source performing the function of send and receive[23].

- Snooping Attack

In snooping, the nodes try to access the packets of other nodes without their permission[24].

Transfer of packets is usually hop by hop; hence the packets are easily captured by the malicious nodes.

3. Security Parameters

3.1 Important MANET Security Parameters

"Security Parameters" are significant in all security approaches, because of networks special characteristics.

Each security approach and mechanisms proposed for security aspects must know security parameters as shown in Figure 2.

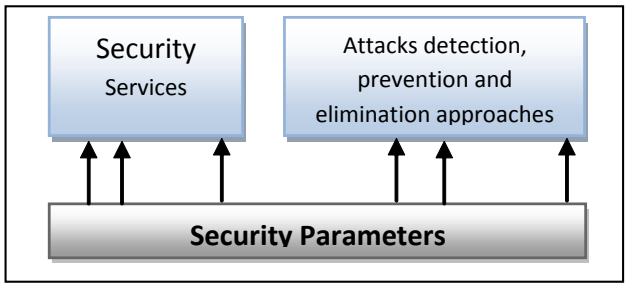

Figure 2. Relation between security parameters and security aspects.

Each of the Security parameters in MANET can be elaborated as follows:

3.1.1 Network Overhead

It is number of control packets generated. MANET uses wireless communications, increasing network overhead. Increase in overhead increases collision, congestion and packet loss. The result of this is there is increase in packet retransmission.

3.1.2 Processing Time

Processing time attributes to the delay caused by security approach. As the MANET uses dynamic topology, there are likely chances of change in neighbors over a period of time. The previous information of a node stored becomes inefficient.

3.1.3 Energy Consumption

The network nodes posses very limited energy resources. Therefore s consumption of energy in security approach should be low.

3.1.4 Accuracy

Accuracy can be achieved by defeating single or cooperative malicious nodes. Each security protocol must be aware of above stated imperative parameters. To have an increased level of satisfaction in the parameters, a trade-off is provided in some situations. Security protocols should follow these parameters for efficiency and reduce wastage in network resources.

In the following tables, we present the analysis on the attacks (Table 3.) and their defeating approaches (Table 4.) adopted. For each attack, where the attacker tries to meet the goals by violating services using MANET features.

Below are listed some of the effective approaches to detect malicious nodes.

3.2 Proposed Solution Approaches

This section presents an analytics of the proposed solution approaches and the result of each of the parameters discussed in previous sections. Table 3 shows, each of the below described proposed solution approaches.

Table 3. Analysis of proposed solutions

The Proposed Solutions	Energy Consumption	Process Overhead	Memory Overhead	Packet Overhead	Accuracy	Limitation
Routing Information	Low		Y	Y	Single Attack, Cooperative attack	Processing Time
Sniffing	High	Y	Y		Single Attack,	Cooperative Nodes
Encryption	Normal	Y	Y	Y	Single Attack, Cooperative attack	Absence of Centralized Control, Key distribution
Redundancy	High			Y	None	Packet overhead
Authentication	Low	Y		Y	Single Attack	Absence of Centralized Control, Key distribution
Dynamic Frequency	High			Y	None	Frequency knowledge

3.2.1 Routing Information

In this approach for detecting malicious nodes, controller packets are generated and used. As proposed in DRI[18], some nodes also keep additional routing table information. Limitation is control packets transmission increase processing time.

3.2.2 Sniffing

In sniffing each node captures transmission of all packets falling within its range. A lot of node energy is consumed. Malicious nodes work with each other and make themselves appear as trustable nodes, resulting in process and memory overhead.

3.2.3 Dynamic Frequency and Redundancy

These approaches can detect attack and avoid from an attack. They don't have the capability of detecting the malicious nodes but are used for detecting the path with malicious nodes. In redundancy, there is buffering of packets at the destination to keep them in sequence and then compare them with each other increasing the traffic overhead. Duplicate packets increases loss of packets, congestion and energy consumption.

3.2.4 Authentication

It is the mechanism in which there is trust between the nodes during communication between them. The recipient of the system, should be aware about the originator of the source system i.e., the destination is aware of the node information. There is no central infrastructure for key dissemination, which is a major challenge of required Authentication. The malicious node takes part in key distribution showcasing itself as a trusted node and gains the unauthorized access.

3.2.5 Encryption

In order to avoid access to data packets by malicious nodes, technique of encryption is used.

Table 4 shown below describes an analytics and classification of the attacks defined in Table 2.

The important parameters for each of the attack is analyzed and presented in Table 4. These parameters are as follows:

- Violated Service: Any kind of attack in the network breaks a security service. We introduced the most vital defeated service in this segment.
- The Proposed Solutions: The solutions presented are some of the most compelling approaches to detect and eliminate malicious nodes.
- Features leading to an attack: The feature adopted by the malicious node in MANET to break the security.
- Attack Type: This classifies whether it is an Active or Passive attack.
- Attack Goal: The most essential objective of every attack.

Table 4 : Analytics on MANET attack

Attack							Violated Service (Security service that is broken)	MANET features which lead to this attack (Feature used to break the network)	The proposed Solutions (Detect & Eliminate malicious nodes)
Name	Type		Goal (important goal of each attack)						
	Active	Passive	Resource Consumption	Accessing Packets	Modifying Packets	Dropping Packets			
Black Hole	Y					Y	Availability	Distributed Network	Routing information, Sniffing
Worm Hole	Y		Y				Availability	Distributed Network	Routing information, Sniffing, Encryption
Byzantine	Y		Y				Availability	Distributed Network	Encryption, Redundancy
Snooping			Y	Y			Data Confidentiality, Integrity	Non-centralized	Routing information

Routing	Y			Y			Availability	Hop-by-Hop communications	Routing information, Authentication
Resource Consumption	Y		Y					Non-centralized	Sniffing, Encryption
Session hijacking		Y		Y			Data Confidentiality	Non-centralized Distributed Network	Encryption, Authentication
Denial of Service	Y					Y	Availability	Non-centralized	Routing information, Sniffing
Jamming	Y					Y	Availability	Wireless media	Sniffing, Dynamic frequency
Impersonation		Y	Y	Y			Data Confidentiality, Non-repudiation	Open network boundary	Authentication
Modification		Y			Y		Integrity	Hop-by-Hop communications	Encryption
Fabrication		Y	Y		Y		Availability	Distributed Network	Sniffing, Encryption
Man-in-the-middle		Y		Y	Y	Y	Data Confidentiality, Integrity	Hop-by-Hop communications	Encryption, Authentication
Gray Hole	Y					Y	Availability	Distributed Network	Routing information, Sniffing
Traffic Analysis		Y		Y			Data Confidentiality	Hop-by-Hop communications	Encryption, Authentication

3.3 Approaches for Incorporating Security

3.3.1 Security Attributes

The field of security[26] is large and if the described attributes holds good, then we can say that the network is secure. Networks using security sensitive information exchange need to use some model controlling the attacking problems. The accompanying attributes should be considered[26] for characterizing the diverse security[4] needs of the uses of Ad Hoc network.

- Confidentiality- It is the property in which each application or node has permission to access a specified set of services of the application in use.
- Authentication- It should provide trustable communications between two different nodes.
- Availability- It is the property of the network to ensure that in-spite of all attacks the authorized node is able to provide data and services.
- Integrity- It is the ability of the authorized nodes to create, edit or delete packets.
- Non-Repudiation- This property ensures that neither source nor destination can refuse their behavior of sending or receiving data. It helps in isolation of malicious nodes.
- Certainty of discovery- This ensures that source node by the help of Route Discovery mechanism obtains the address of destination node before transmitting the packets to the destination.
- Isolation- It is preventing a given node in the network to communicate with any other node.
- Lightweight computations- Computations on route discovery.

3.3.2 Security Model

3.3.2.1 Secure Routing Protocols

To guarantee security in routing phase, a secure path is selected by some mechanism to create a path to the destination. This helps in detection of malicious nodes and eliminates it. Using IPSEC in MANET routing protocols, to create a secure path authors have presented trust based routing protocol and secure routing in[27,28]. In MANET, selecting best path is important because there may be multiple paths between two different nodes.

3.3.2.2 Security in QOS

Studies show that providing security has negative impact on QOS. Providing security in QoS helps to improve in level of security with low time or network overhead.

There are other theories and approaches to make a compromise between security and QOS[29,30].

3.3.2.3 Cluster-based Security

Authors' in[31,32], used clusters key distribution. The central key management in clustering network helps to provides more efficient situations for security protocols. Clustering ensures security, but maintaining clusters is very costly and grouping nodes in clusters is challenging.

In this paper, we presented a comprehensive analysis on security threats, attacks and solution in MANET.

Firstly, we presented the security services and attacks on MANET. Division was based on these two aspects.

Secondly, we discussed important security parameters which should be considered for avoidance of attacks and establish security in MANET.

Finally some analyses on proposed solution and classifications approaches were presented. To secure MANET, there is always a trade-off but generally the efficient way is to secure routing path and apply encryption.

3.3.3 Proposed Simulation Algorithm

On attacked situation in network there will be no data available as the characteristics of the network are unknown. We need to simulate such types of conditions in the network.

Step 1: Identify the different possible scenarios of the networks like topology, location etc.

Step 2: Simulate the network for different network scenarios.

Step 3: Collect the data using Network Simulator (NS2).

Step 4: Classify into different group based on the data type. Consider different data types as

- Delay.
- Drop Rate.
- Packet type.
- Bandwidth utilization.
- Process status.
- Services running.
- And processor utilization.

Step 5: Normalize each data set with the help of minimum and maximum values for the classification of the network.

Step 6: To represent system condition by a vector, arrange the normalized values in an array.

Step 7: After Step 5, the system states can be projected into a hyper space of n dimensions.

Step 8: Group the vectors according to the system states.

Step 9: Calculate the centre for the group and maximum radius by measuring the distance from centre point to the point of maximum distance.

Step 10: Repeat the above steps for

- m centers.
- m different states (under attack, serious attack, ok etc.) of network.
- maximum movement.

3.3.4 Simulation Profile

Table 5. Parameter settings for simulation

Parameter	Values
Space	800 x 800 flat
Percentage p of selfish nodes	p=0% to p=50%;
Model	Random waypoint model
Bit Rate	Constant
Packets size	512bit;
Packet rate	1 packet/s
Protocols	**IEEE 802.11**, **IP**, **UDP** and **CBR**

4. Conclusion and Future Work

In this paper the main attacks in MANETs are identified due to the network characteristics in terms of resources, topology architecture and security management. The limited resources are bandwidth and power; topology is dynamic and security through key management. We have studied the attacks abuse these vulnerabilities and presented a conceivable solutions against each of the attack.

We also focused on active routing attacks on protocols and networks which are classified and presented in tables. Furthermore we have proposed approach on incorporating security and simulate the network in attacked situations. Concluding, MANET security is challenging and complex. Further we need to investigate possible security risks to MANETs most thoroughly.

- The work can be extended to find ways to calculate the threshold effectively.
- More types of attacks including group attacks can be studied and their relations to the vulnerability of the protocols can be ascertained.
- Improve in sniffing approaches for as much as decreasing time and packet overhead.
- A study can be conducted on the relationship between the average detection delay and the mobility of the nodes.

5. References

1. Sahoo AJ, Akhtar MAK. Possibility and necessity measures to enhance reliability and cooperation in MANETS. Indian Journal of Science and Technology. 2014 Jan; 7(3). DOI: 10.17485/ijst/2014/v7i3/47650.
2. Murthy CSR, Manoj BS. Ad hoc wireless networks: Architectures and protocols. New Jersey, USA: Prentice Hall PTR; 2004.
3. Nichols RK, Lekkas PC. Wireless security models, threats, and solutions. USA: McGraw–Hill; 2002.
4. Amudhavel J, Brindha V. A survey on intrusion detection system: State of the art review. Indian Journal of Science and Technology. 2016 Mar; 9(11). DOI: 10.17485/ijst/2016/v9i11/89264.
5. Stamouli L, Argyroudis PG, Tewari H. Real-time intrusion detection for ad hoc networks. 6th International Symposium on World of Mobile and Multimedia Networks; 2003. p. 374–80.
6. Thangaraj SJJ, Rengarajan A. Unreliable node detection by elliptical curve diffe-hellman algorithm in MANET. Indian Journal of Science and Technology. 2016 May; 9(19). DOI: 10.17485/ijst/2016/v9i19/86081.
7. Hu Y-C, Perrig A, Johnson DB. Ariadne: A secure on demand routing protocol for ad hoc networks. In 8th ACM International Conference on Mobile Computing and Networking (Mobicom' 2002); 2002.
8. Stajano F, Anderson R. The resurrecting duckling: Security issues for ad-hoc wireless networks. 7th International Workshop Proceedings, Security Protocols; 1999. p. 1–11.
9. Hubaux J-P, Buttyan L, Capkun S. The quest for security in mobile ad hoc networks. Proc of the 2nd ACM International Symposium on Mobile Ad hoc Networking and Computing; 2001. p. 146–55.
10. Kong J, Hong X, Gerla M. A new set of passive routing attacks in mobile ad hoc networks. IEEE MILCOM Military Communications Conference, MILCOM'03; 2003. p. 796–801.
11. Yau P-W, Mitchell CJ. Security vulnerabilities in ad hoc networks. In Proc of the 7th Int Symp on Communications Theory and Applications; 2003. p. 99–104.
12. Buchegger S, Tissieres C, Le Boudec J-Y. A test-bed for misbehaviour detection in mobile ad-hoc networks- How much can watchdogs really do? 6th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '04); 2004. p. 102–11.
13. Stajano F, Anderson R. The resurrecting duckling: security issues for ad-hoc wireless networks. In Proc of International Workshop on Security Protocols, Springer; 1999.
14. Yi P, Dai Z, Zhang S, Zhong Y. A new routing attack in mobile ad hoc networks. Int Journal of Information Technology. 11(2):83–94.
15. Ning P, Sun K. How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols. Proc of the IEEE Workshop on Information Assurance; 2003. p. 60–7.
16. Wu B, Chen J, Wu J, Cardei M. A survey on attacks and countermeasures in mobile ad hoc networks. Wireless/Mobile Network Security; USA: Springer. 2006. p. 103–35.
17. Hu Y-C, Perrig A, Johnson DB. Rushing attacks and defense in wireless ad hoc network routing protocols. Proc of the ACM Workshop on Wireless Security; 2003. p. 30–40.
18. Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks. 2003; 293–15.
19. Gavini S. Detecting packet-dropping faults in mobile ad-hoc networks. USA: Washington State University; 2004.
20. Perkins C, Belding-Royer E, Das S. RFC 3561: Ad hoc On-Demand Distance Vector (AODV) routing. Network Working Group; 2003. p. 1–37.
21. Zhang Y, Lee W. Intrusion detection techniques for mobile wireless networks. Wireless Networks. 2003; 9(5):545–56.
22. Hamieh A, Ben-Othman J. Detection of jamming attacks in wireless ad hoc networks using error distribution. International Conference on Communications, ICC '09; Dresden. 2009. p. 1–6.
23. Ben-Othman J, Hamieh A. Defending method against jamming attack in wireless ad hoc networks. 34th Conference on Local Computer Networks; Zurich. 2009. p. 758–62.
24. Shaw S, Orea K, Venkateswaran P, Nandi R. Simulation and performance analysis of OLSR under identity spoofing attack for mobile ad-hoc networks. Computer Networks and Information Technologies Communications in Computer and Information Science. Berlin Heidelberg: Springer-Verlag. 2011; 142:308–10.

25. Mishra A, Jaiswal R, Sharma S. A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in ad hoc network. 3rd International Conference on Advance Computing Conference (IACC); Ghaziabad. 2013. p. 499–504.
26. Zhou L, Haas ZJ. Securing ad hoc networks. IEEE Network. 1999; 13(6):24–30.
27. Panaousis EA, Ramrekha TA, Politis C. Secure routing for supporting ad-hoc extreme emergency infrastructures. 2010 Future Network and Mobile Summit; Florence. 2010. p. 1–8.
28. Salmanian M, Li M. Enabling secure and reliable policy-based routing in MANETs. Military Communications Conference, MILCOM; Orlando, FL. 2012. p. 1–7.
29. Yu FR, Tang H, Bu S, Zheng D. Security and Quality of Service (QoS) co-design in cooperative mobile ad hoc networks. EURASIP Journal on Wireless Communications and Networking. 2013; 188.
30. Gujral R, Kapil A. Secure QoS enabled on-demand link-state multipath routing in MANETs. Information Processing and Management Communications in Computer and Information Science. 2010; 70:250–7.
31. El-Sayed A. Clustering based group key management for MANET. Advances in Security of Information and Communication. Networks Communications in Computer and Information Science, Berlin Heidelberg: Springer-Verlag. 2013; 381:11–26.
32. Zefreh MS, Fanian A, Sajadieh SM, Khadivi P, Berenjkoub M. A cluster-based key establishment protocol for wireless mobile ad hoc networks. Advances in Computer Science and Engineering, Berlin Heidelberg: Springer-Verlag; 2009; 6:585–92.