ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

Volume - 5, Issue - 2, March – April - 2019, Page No. 210 - 225

Attacks and Security Issues of Mobile Ad Hoc Networks

Ravindra Maan, Archana Morya, Gopesh Sharma

Assistant Professor, Department of Electrical Engineering, Arya College of Engineering & Research Centre, Jaipur

Assistant Professor, Department of ECE, Arya College of Engineering & Research Centre, Jaipur

Abstract

Mobile Ad Hoc Network has acknowledged a large amount of interest among users by forming a temporary network. MANET does not have any fixed infrastructure. Due to the dynamic changing topology+, such type of network suffers various challenging issues like limited wireless range of nodes, dynamic topology, bandwidth consumption, transmission errors etc.

MANET has no clear line of defense; Security is a priority for safe communication in any environment. The mischievous nodes can attack from both the sides of the network. In the existence of false nodes, the major concern of such networks is to layout the effective security solution, which protects MANET from distinct routing attacks. All the nodes in the network forward the data towards the destination; therefore, MANET is more prone to attacks by malicious nodes, such as black hole, wormhole, Denial of Service (DoS), eavesdropping, spoofing, etc.

This paper, firstly deals with the challenges faced by the MANET. Secondly, it focuses on significant security attacks and safety issues of mobile ad hoc networks. And finally, it mentions the recent research work done on security solutions for wireless network.

Keywords: Security Goals, Attacks, Security issues, Detection Schemes, Black hole.

Introduction

The advancement of mobile computing devices, including laptops, mobile phones, PDAs, mobile digital devices, etc., has led to a gradual change in the computing world [6]. Several electronic platforms can be used by the individual user in the sync, through which they can access all required information when and where necessary. And to support this ubiquitous computing methods: Mobile Ad Hoc Networks has attracted the concentration of many researchers [5].

These networks works on wireless mobile nodes, that dynamically organizes in inconsistent and limited network topologies. Nodes can precisely connect with each other in the setup environment, within radio ranges [1] [11] [17] While nodes which are not in straight range, can also be used to connect altogether. It reduces fixed infrastructure like centralized administration, access points or base stations are connected by wireless links. The nodes in reach with environment can approach the common radio link for easy sharing and configuration in a dedicated infrastructure, but security between the nodes requires the formation of a secure connection. Therefore, it is necessary to provide an appropriate configuration for a secure dedicated network.

The main advantage of this network is its low cost and easy maintenance. There are many custom routing algorithms that allow creating networks in different circumstances. MANET is classified into two parts, proactive and reactive routing algorithms [13] [14].

Proactive routing algorithm continuously maintains updated network and the current routes, but sometimes it may generate an irrelevant overhead to keep the routing tables, whereas reactive routing algorithm creates way only on demand basis. The interactive routing protocol needs moderate road creations that can delay the actual transmission of data. When sources have no other option to direct their packet to the end node, in this case, the proactive routing algorithm excels in favor of creating faster paths [2] [4] [9] [15].

MANET's wireless link is capable of connecting attacks ranging from illegal eavesdropping to effective intervention. Attacks on a custom mobile network can enter from any address and go to any node, thus violating the basic security requirements. So, it makes difficulty to catch accurate node in the network [15] [20].

With an increase in practical devices, as well as in mobile communications, custom networks are gaining importance with applications on a large scale. It allows devices to make connections in the system by counting and discarding nodes within the network. MANET applications range from broadband networks to mobile nodes and highly dynamic networks to small fixed networks that are strained by battery resources [6]. Besides this, the application which includes MANET for its services are:

- Military battlefield.
- Commercial sector.
- Local level.
- Personal Area Network (PAN).
- Sensor networks.

Properties of Mobile Ad hoc Networks

Some special features of MANET which should be considered here are as follows [1] [13]:

Dynamic Topology: The topology of mobile ad hoc networks changes very fast and unreliable due to continuously changing node mobility. The link connections among the terminals of the network are based on the adjacency of one node to another. Mobile ad hoc network should be kept on updating with traffic conditions as well as with the mobility patterns of the nodes for proper information. As they make their connections with the neighboring node on the fly. Moreover, a MANET user needs both ad hoc as well as public access node for proper networks.

Bandwidth: MANETs have significantly lower bandwidth capacity in comparison with fixed networks. The used air interface has higher bit error estimate, which provokes the conventional link standards. The wired network uses higher bandwidth values because the channel over which the wireless terminals communicate is subjected to noise, fading and interference, and has less bandwidth range.

Energy: Mobile devices are dependent on batteries for their supply of energy, is a very limited kind of resource. Energy preservation acts a very vital role in any wireless or sensor network devices. It has to be used in a proper and effective way. Optimization may be the way possible for energy conservation in mobile devices.

Security: The nodes carrying the information have to face the same and issues in MANET like other network does. MANET has special kind to threat in it likewise, black hole attack, wormhole attack, denial of service etc. Mobile devices

have higher security risks other than static operation. This is due to dynamic nature and in increasing traffic nodes may use crosswire links with each other and harm the network.

Autonomous: In MANET, there is no requirement of centralized administration for mobile node management. Each node behaves like autonomous node which serves both host as well as the router. Mainly duplicate endpoints and switches there in MANET.

Distributed Operation: The operations of the network are managed among the nodes of the network, as there is no central control authority or any background support system to relay. The nodes itself involved in functions to perform the appropriate functions like routing, security, updating routing tables etc.

Multi-Hop Routing: Based on routing protocol and link layer perimeters, routing algorithms can be defined as single hop and multi hop routing. In terms of structures and implementation multi hop routing is difficult from single hop routing. In this, the data packet will use more than one intermediate node to travel down from source to destination [1].

Light- Weight Terminals: In many cases, the mobile nodes are not having proper memory size, CPU processing techniques, storage with battery life time.

Infrastructure-Less and Self Operated: There are several advantages of mobile ad hoc networks likewise easy network formation , speed and no use of fixed infrastructure is there. These kinds of features make the MANET network most attractive to work with.

Challenges in MANET

No Secure Boundaries: In comparison with wired network, there is any security access in mobile ad hoc networks. In MANET, one can easily gain the control over the network, if the nodes are in proper frequency range. Despite of MANET, wired network have physical access to the network medium via firewall or gateways [13].

Power and Computational Limitations: Limited power supply is there in mobile ad hoc devices, due to wireless network setup in comparison with wired networks. Its power backup mainly depends on the battery support system which gives limited access only.

Lack of Centralized Management Facility: Due to no central authority, mobile ad hoc network has to face many problems and issues in managing the network of nodes setup. Especially in large scale ad hoc area and heavy traffic area MANET is least able to find or detect the malicious nodes or harmful attacks within the network [1].

Cooperativeness: No cooperation can be seen between the nodes of the mobile ad hoc networks. And due to this non cooperative behavior, the malicious node can easily able to enter in the network as a routing agent and harms the network thoroughly.

Security Goals of MANET: The Goals of security mechanism of MANETs are briefly summarized as follow

Availability: Ensure availability of network services in the context of various attacks in the environment. Availability is mainly concerned with the resources, which can heal the network services immediately [1] [13]. Some attacks have programmed counteragent such as encryption and authentication, whereas some attack requires different sort of actions to limit or get back from loss in the availability services [10]

Confidentiality: Confidentiality ensures that data is only available by the relying party. Protect data from attacks [4].

Integrity: Integrity ensures that it is granted only to parties authorized to change information or messages. It also protects the message, because the transmission does not get any damage. Integrity services apply to any type of message, whether message flow, message, or fields specified in the message [1] [13].

Authentication: Authentication verifies with soothe that a link is accurate [2]. Without authentication, malicious node will try to gain illegal access to reserves and sensitive information, and also tries to agitate the operations of the other nodes [4] [10].

Non-Repudiation: Non-rejection places an end to the sender or recipient to oppose a sent message [3]. Therefore, when a message is delivered, the destination node can prove that the data was sent by the intended sender and vice versa.

Scalability: Scalability is very important aspect on safety account. An MANET is abiding of large no. of nodes. Potential security must be manageable in managing large networks [2]. Otherwise, the attacker maliciously uses the fresh added node in the network and will use it to approach the entire system.

Anonymity: In this, all the data that is used to identify the authorized user of node, they must be stored confidential and must not be assigned to the same node or structure [10].

Attacks: We have considered many of the requirements that must be obtained to ensure the security of a dedicated mobile network. In extension, there are other more specialized and functional security functions, including automatic installation, privacy, and location [7]. Dealing with important security facts usually referred to as the main threats that violate security prospects in the name of attacks. Attacks on MANIT are as follows

Black-Hole Attack: Black hole attack drops all the data packets crossing it. Here, false node behaves like a black hole [1] [16]. If the attacking node is a pairing node between the components of the network, it will surely detach the network in two separate components [11] [12] [17].

Cooperative Black-Hole: Likewise Black-Hole attack, in this attack too, malicious nodes make damages to the network [2]. It has the ability to fully destroy the functions of the network. Detection method is like Black-Hole attack, the only solution to prevent this attack is to find alternate way to the end station, if it exists and secure routing with suitable routing protocol.

Gray-Hole Attack: It also ignores packets, but its procedure is defined for specific conditions or time constraints [12] [14]. The data drops to a particular node, while the alternative contract acts normally. It also ignores data in a certain time period, while acting normally in other situations. But with this concept [4], it is troublesome to encounter an attack that leads to a node or depends on it [19].

Jellyfish Attack: The jellyfish attack differs from black hole attack and the grayhole attack. Instead of filtering data, it delays packets before delivery of these packets [2]. It even transmits a string of data that is sent to it and receives it in an arbitrary order. It stops the natural flow of the control system used by the contract in order to send a decent. This will increase the delay factor from end to end and will result in QoS degradation.

Worm Hole Attack: The hole in the MANET connects two isolated points using the shortest roads and aligns the router by shortening the circuit to the grid and removing the flow of the beam [4].If this route acts as the cheapest route to the destination, these pseudo-nodes will be chosen consistently to transfer data to the terminal [11].

HELLO Flood Attack: This will cause the network to be flooded with a high-quality track with a powerful transmitter. Now, each node will redirect its packets to this node in belief that it will be the finest path to the destination. If a node does not deliver its own packet to this attacking node, then the only high power transmitter will convince all nodes to be its neighbors.

Bogus Registration Attack: In this, the malicious node itself is defined as a different node, either through the transmission of a stolen beacon or by recording false beacons in the active node. After registration, packets sent can be damaged and can shake the network completely [10]. The malware node first wish's to recognize the integrity of the adjacent nodes and network topology. Encoding packets prior sending and discovering protected paths will limit the attack to some extent, because the malicious node does not have prior knowledge of the encryption scheme.

Man in Middle Attack: The attack node in this attack overlaps with a valid path and tries to output the packets flowing through it. To perform this attack, the erroneous node must first be a component of this path. This can be executed either by temporarily entering the node, sending a once-captured malicious beacon or entering the next routing timeout event. To protect packets, this attack, which flows through MANET, encodes individual data.

Rushing Attack: In reactive routing protocol, individual node before sending its data transmits a RREQ (route request) message to neighboring nodes and reliable routes replies with RREP came to sender node with suitable route information. Some techniques use an equivalent cancellation mechanism to limit path request and network response messages [2]. It exploits the corresponding suppression mechanism. It redirects a fast false RREP to fit other nodes. Because of the corresponding deletion, the original RREP message will be deleted from the real node and the malicious node will share the path [10].In the attack, the attacker sends data to the upcoming node at a later time, filtering is performed. The delay in delivery of data to the end node will increase.

Cache Poisoning: In routing protocols, individual node carries some fresh transmission routes until timeout occurs for individual entry. If some malicious node achieves a routing attack it will then remain in the node's routing table until the timeout expires. The attacking node will display a zero scale in all of its final stations. Before becoming a member of the path, a malicious contract can trigger its counterfeit activity. The consequences of caching poisoning can be defined either over the use of restrictive belts or through symbolic authentication [10].

Blackmailing: In this case, the attacking contract will be accused of an honest point as a dangerous obstacle. A list of acceptable and unacceptable contracts mentioned in the contract review will be submitted to MANET. A few protocols try to improve them more reliably using the majority voting principle, but if they are sufficient, no. Of the attacking nodes becomes a MANET part, it will ignore this security also. Another effect of this attack is to display invalid RREP messages against an unacceptably high cost for many nodes.

Sybil Attack: Sybil's attack maintains multiple false identities, mimicking the presence of several points in the network [2]. Therefore, one node can assume the role of many nodes and can control many nodes at the same time. It depends on generating identities in the system.

Denial of Service (DoS): This attack is intended to determine the possibility of a particular node or even services for all dedicated networks [1]. DoS attacks are performed on a traditional wired network using a flood mode to exhaust network

traffic, so that supply provided by the destination becomes unattainable [11].Although, it is not practical to perform because of distributed attributes of the network. Moreover, the mobile ad hoc networks are more challenging than fixed networks due to limited battery supply. In practice, counterfeit contracts use wireless interference and battery consumption to perform denial of service attacks [17].

Impersonation: There is a risk to the security of the dedicated mobile network, if there is no correct authentication method between nodes [4].You can easily capture some points in the grid and merge them as primary points. In this way, harmful nodes can enter the network and begin their false activity.

Eavesdropping: The goal of this attack is to have some secret information and keep it confidential during the transmission [1]. Confidential information includes the site, public key, private key or even contract passwords. This data is very important for security reasons.

Attacks against Routing: The motto of malicious node is to destroy the routing process. They are divided into two groups: attacks on routing protocols and attacks on packet transmission / delivery [6] [15]. Attacks on routing protocols prohibit the process of routing information from sender to receiver. Packet forwarding attacks block packet delivery on a fixed path [9] [14].

Related works in security system for MANET

Noguchi, Hayakawa, 2018worked on multiple route reply forwarding and filtering technique. This method is used to solve the security issues created by black hole attack in the network. AODV routing protocol is used on this method, to find the packet delivery ratio (PDR), throughput and overhead consequences of the network. The technique will check the threshold value of the attacking node and accordingly request the highest sequence number of the RREP packet to the source node for the particular RREQ packet. It will also check the average quality of path between source and destination node. Such techniques can able to resolve the PDR, throughput and overhead issues of the network with much higher rates.

Swain, Pattanayak and Pati, 2017 used three routing protocols i.e. TBS, SDR, MAODV routing protocols. These routing protocols are used to solve the problems caused by the malicious nodes in the network for improving PDR with less delay and power consumption factors simultaneously. Author concluded that TBS routing protocol comes out to be the best one as compared to SDR and MAODV. TBS protocol consumes less power with lesser delay rates and gives higher PDR factor.

Reda, Azer, 2017 worked on two routing protocols i.e. AODV and DSR routing protocols. These protocols were used to find the packet drop rate and the percentage of nodes which are able to fight back to the attacker nodes of the network for their survival. For this, researcher has generated two scenarios, first is normal mode and second mode is with malicious attacker nodes. AODV shows better performance in normal mode due to its cache maintenance. In second mode, AODV and DSR both drops packet as malicious node harms the network, but still AODV has better outcomes due to its reactive nature.

Shabut, Dahal, Kaiser, Hossain, 2017 did a research work on Tactical MANET i.e. T-MANET. It is used in vehicles, automobiles, stations for detection purposes. In this, DSR routing protocol is used to solve the basic and important issues

of T-MANET like damages done by black hole, gray hole and selfish node in the network. DSR protocol is used, as it may help the network to improve its PDR and throughput factors. Author used three different techniques like cryptography detection technique, trustworthy detection technique and detection method technique. After using such techniques black hole and gray hole shows the similar results but selfish node gives improved results i.e. higher PDR and throughput on all the techniques and vice versa.

Rishiwal, Agarwal, Yadav, 2016 worked on H-MANET i.e. heterogeneous and homogenous MANET. To find scalability, lesser energy scenario and heterogeneity, author used AODV routing protocol for research. After simulation only delay is been maintained by homogenous MANET, whereas heterogeneous comes out with better PDR, throughput, higher no. of alive nodes and lesser energy consumption factor.

Matre and Karandikar, 2016 did a research work on AODV and MAOMDV i.e. modified ad hoc on demand multicast distance vector routing protocol. This is done for security enhancement in MANET. Cryptographic patterns were used with MAOMDV routing protocol to ensure the security of data. Three different parameters were used likewise positive events, negative events and opinion. In positive events, routes ensure the connectivity between neighboring nodes. In negative events, route dislocates and no neighboring node information is there. Whereas, in opinion ensures that data is sent or delivered through network safely. With increasing number of nodes and area, MAOMDV shows higher PDR and throughput with less delay factor I comparison to AODV.

Paramasivan, Prakash, and Kaliappan., 2015 used a method named game theory with dynamic bayesian signaling game (DBSG) and perfect bayesian equilibrium theory (PBE) with AODV, CBRP and SRP-GM routing protocol. This method is used to find the malicious nodes, utility, strategy of nodes, throughput, and overhead latency issues in the network created by nodes. This process simulates that DBSG is more effective in finding malicious nodes and can perform accurate sending and receiving of data in particular time span whereas, PBE does the same process but with greater delay.

Sari, 2014 worked on USM and RAS i.e. utility sensor mechanism and rate adaptation scheme with AODV routing protocol. These methods are used to improve the throughput and delay functions of IEEE 802.11 section and DCF section in data link layer. This will improve the harms caused by DDOS and jamming attacks in the network. Author concluded that, these two techniques are highly recommendable for changes and detection mechanism to great extent, which can control the PDR, throughput and delay factor altogether.

Khalil, Bataineh, Qubajah and Khreishah., 2013 introduced new routing protocol .i.e. ARAN-Z, authenticated routing ad hoc network with zone routing protocol and compared to simple ARAN and ZRP routing protocol. This is done to find the better PDR, routing load in bytes and packets, average path length and latency of the network. As attacker node will harm more in higher node mobility area and denser network. However, ARAN-Z comes out with better results because it shows higher PDR and lesser latency with increasing routing load factor in comparison to ARAN and ZRP.

Ganesh andAmutha, 2013 worked on new routing protocol i.e. efficient and secure routing protocol based von SNR and dynamic clustering (ESRPSDC). This is done to secure the energy consumption of wireless sensor network. There is no security and surety of nodes in the wireless sensor network. Malicious node can attack any time and harm the network. Here, this new routing protocol is compared with LEACH and PEGASIS routing protocol to find PDR, delay with load in

the network and no. of malicious nodes in the network. As ESRPSDC routing protocol helps to increase the PDR and reduces delay with less SNR ratio.

Table I: Literature Survey of Various Detection and Prevention Methods.

Author Name	Paper Title	Method Name	Routing Protocol	Tool Used	Remarks
Noguchi, Hayakawa., 2018	Black Hole Attack Prevention Method Using Multiple RREP's in Mobile Ad Hoc Net	Multiple Route Reply And Filtering Technique	AODV	NS-2	To check the threshold value of the black hole node and highest average sequence number of RREP packet to the source node for particular RREQ packet in the network.
Swain, Pattanayak and Pati., 2017	Study and Analysis of Routing Issues in MANET	Three Different routing protocols are used to solve the security issues	MAODV,SDR,TBS	NS-2	To produce better PDR with less delay and power consumption rate caused by malicious node.
Reda, Azer., 2017	Correlation between Protocol Selection And Packet Drop Attack Severity In Ad Hoc Network	Two scenarios were created namely, normal mode and malicious mode for survival of the nodes present in the network in presence of attacking node	AODV,DSR	OPNET	To find the packet drop rate and the percentage of the node, it will fight back against malicious node for their survival.
Shabut, Dahal,	Malicious Insider	Cryptography detection	DSR	NS-2	To solve the issues of T-MANET, likewise

Kaiser, Hossain., 2017	Threats in the Tactical Manet	technique, trustworthy detection technique and detection method technique			black hole, gray hole and selfish node attack for improved PDR and throughput factor.
Rishiwal, Agarwal, Yadav., 2016	Performance of the AODV Protocol for H-MANETs	Comparison between AODV and H-MANET	AODV, H-AODV	NS-2	To balance the scalability, heterogeneity and energy consumption factor present in the network.
Matre and Karandikar., 2016	Multipath Routing Protocol for Mobile Ad Hoc Networks	Cryptographic patterns are used with MAOMDV routing protocol	AODV,MAOMDV	NS-2	Three parameters were used like positive events, negative events and opinion for PDR, throughput and lesser delay factor in the network.
Paramasivan, Prakash, and Kaliappan., 2015	Development of a Secure Routing Protocol using Game Theory Model in Mobile Ad hoc Network	Game Theory with Dynamic Bayesian Signaling and Perfect Bayesian Equilibrium Theory	AODV,CBRP,SRP-GM	NS-2	To find the malicious node, utility, strategy of nodes, throughput, overhead and latency issues created by the mobile nodes of the network.
Arif Sari.,2014	Security approaches in ieee802.11 MANET	Utility Source Mechanism (USM) and Rate Adaptation	AODV	OPNET	For improved throughput and lesser delay function in ieee 802.11 section and the DCF section in

		Scheme (RAS)			the data link layer harmed by DDOS and jamming attack in the network.
Khalil, Bataineh, Qubajah and Khreishah., 2013	Distributed Secure Routing Protocol for Mobile Ad Hoc Networks	Introduced new routing protocol i.e. ARAN-Z	AODV,ARAN, ARAN-Z	GLOMOSIM	This is done for the improved PDR, routing load in bytes and packets, average path length and latency of the network, as attacker node harms the higher node mobility area and larger area network.
Ganesh and Amutha., 2013	Efficient and Secure Routing Protocol for Wireless Sensor Network Through SNR Based Dynamic Clustering Mechanisms	New routing protocol is introduced i.e. Efficient and secure routing protocol based on SNR and dynamic clustering method (ESRPSDC)	ESRPSDC,LEACH, PEGASIS	GLOMOSIM	To secure the energy consumption of wireless sensor network, as there is no security and surety of the nodes in the wireless sensor network.

Security Schemes in MANET

Intrusion Detection Techniques: Intrusion Detection Technique detects unwanted changes in the systems. Each node in your mobile networks is associated with detection to detect harmful activity across the network, performed by the IDS agent. Although, adjoining nodes can contribute their results altogether and participate with each other, to track the intruder [22]. The sync between nodes takes place only when a node encounter unwanted happening in the network.

Cluster-based Intrusion Detection Technique for Ad Hoc Networks: It helps ad hoc networks to detect intrusions in a better way. In this technique, MANET is grouped into number of clusters showing that individual node is a part of at least one cluster called cluster head, which will take care of the network for particular time period. Cluster selection

process should be effective and efficient. Efficiency here means that the selection of node for cluster head, from the cluster should be of high efficiency.

Misbehavior Detection through Cross-layer Analysis: The detector can also capture the weak cross-section behavior attack, where the inputs of all the network stack layers are mixed and scrutinized by a cross-layer detector [24]. Overload factor due to limited battery supply is the fundamental problem caused by the detection method across the layer.

Watchdog and Pathrater: Watchdog and Pathrater schemes, tries to enhance the performance of an ad hoc network against malicious node [23]. Watchdog observes the misbehavior of copied packets circulated to surf and cross verifying the behavior of the node adjacent to these packets. Sloops down to find the adjacent node, which sends the packets unchanged or not. Discarded packets are ignored if compared to the observed node buffer; while packets that survive in the buffer outside a specified waiting period without any successful match are deleted or modified. In this case that particular node is liable for sending the packet as suspicious node. Information about false nodes is forwarded to the Pathrater scheme. It works on individual node to estimate all of the accepted nodes of the network according to their authenticity. Evaluations of ratings are done on a particular node's performance. Misbehaving with other nodes will be rated to -100.

A Secure Ad Hoc Routing Approach using Localized Self healing Communities: A self-healing society was established in the concept that mobile data transmission relies on direct neighbors to deliver packets in the network. Since a self-healing society works to function as a "good" cooperative node in society. Only particular configuration and reconfiguration protocol are used for the initial configuration of a self-healing community that corrects society if there is any change in mobility or change of topology.

Security Solutions in Mobile Ad hoc Networks: To implement solutions on the security concerns in MANET, we must elaborate the two most commonly used approaches, which are:

Prevention: It is designed to eradicate the malicious activity of the attacks. They desire encoding techniques to maintain authentication, confidentiality, integrity, and non-rejection of routing information. Different proposals use different types of strategies such as symmetric algorithms, asymmetric algorithms, one-way fragmentation methods, each with different commitments and objectives. Categories of the above categories are:

Prevention by Asymmetric Cryptograph: This method specifies the basic schemes for protocols. A secure network or network is required that is similar to distributing public keys or digital certificates in an ad-hoc network [2]. Numerically, a network containing xx nodes requires public keys stored in the grid. SAODV and ARAN are the two routing methods specified here.

Prevention using symmetric cryptography: This method is used to avoid attacks between routing patterns. Symmetric keys are used as wired network. SAR and SRP are the two techniques given by this scheme [25].

Prevention by one way chain: This method also prevents routing protocol from attacks. Protects modification of routing information such as metrics, sequence number, and source path. SEAD is located in this category [2].

Detection and Reaction: It specifies solutions against attacking nodes. A node can convince neighbor to forward the packets but stop afterwards, because of its overloaded, selfish or malicious behavior. The overloaded node uses the

maximum buffer space, CPU cycles, or network bandwidth to send data. Malicious node launches DOS attack when packet filtering. All schemes under this category can detect this bad behavior and respond to it.

Detection Features

To detect various harmful attacks present in the network, different features are there in MANET, Which will be useful to detect successfully. Some of the features are [21]:

Location: Location is very important feature to detect any type of attack. If the proper position of mobile nodes is known, then design of the network can be build very smoothly. Global Positioning System (GPS) device will help to maintain each node in the network, for easy implementation to the system. For cost reduction, certain nodes having GPS receiver can be arranged at specific positions in the network to get the exact position of the adjacent nodes. Using special antennas more location information can be collected, which will detect the direction for data receiving. The main hindrance of using GPS device or special antenna is that it will hype the cost of nodes and the network will become more expensive. Battery timing of mobile nodes will be decreased as in MANET nodes change their location regularly.

Time: Time feature is also helpful in malicious node detection. The normal routes are having less regular time per hop as related to the route having harmful node. All the nodes in the network should be maintained with synchronized clock for accurate calculation of the time difference between source and destination node. There is one more technique to calculate the time difference between the source and destination node, in which source node sends a unique Hello message to the stop node and note the sending time of the data. When the stop node collects that Hello message, it reverts back with a Hello-Reply message again. Average time of each hop is calculated by dividing the difference of sending and receiving time by two, excluding the handling time of source, destination and the adjacent nodes. Drawback for implementing a synchronized clock is a difficult, full of congestion and expensive for MANET. To determine the position and existence of malicious nodes with simple time difference methods are also a difficult part in MANET.

Hop Count: The hop count details are used for revelation parameter, as the malicious nodes mainly attract the network traffic by displaying diminished track. A path through normal nodes has greater hops as to the harmful path because hop count will be increased when the report shifts over the channel between normal nodes. Some techniques are helpful to find the existence of malicious node using hop count with accuracy and proper situation.

Average Time (single hop)＝Total hops÷ Total time or Distance

If the average hop time or distance is higher than the normal hop time, then route contains malicious nodes. This feature require synchronized clock or GPS device for accurate results.

Neighborhood: Neighboring nodes are the most helpful nodes while detecting malicious node within the network. Routing tables assemble and manage the data related to neighboring node while other schemes try to capture the attack by analyzing the data using Hello message. Such methods face issues in heavy traffic area, where each node contains more than one neighbors. This feature needs more memory, storage, and processing power to track the two hop neighboring nodes. Hello messages also increases the overall network traffic. Because of frequently changing nodes in MANET, such schemes will not work efficiently in networks, which will increase the false positive replies apparently.

Data Packets: On the basis of data packets received and sent, there are some intrusion detection schemes which can easily detect the harmful nodes in the network A routing table is managed by each node to keep the track record of neighboring node, to estimate their sate of work whether they are dropping, modifying or forward data to another node than destination node. By this information, trust rate of each adjacent node can be calculated easily. This is simple but effective technique and can work accordingly in larger area with high mobility factor.

Route Reply: Route Reply (RREP) is also used to detect harmful attacks. On receiving a request from source node for fresh route, the destination node sends RREP message to the source node. The malicious nodes always use such condition to launch the attack. RREPs are unicasted only so; the nodes that want to keep record of the RREPs have to be in the proper mode situation, which can affect the network efficiency.

Route Request*:* The most important part for on-demand routing in MANET is route request i.e. RREQ. It is also used with some other functions to detect the attacks like RREP does. RREQ goes to every node in the network. IDSs based on RREQ have simple calculations and needs fewer resources.

Limitations of Intrusion Detection Techniques

Some problems or issues arise when intrusions detection methods were applied on the network. Few of them are discussed below [21]:

Congestion: Some intrusion detection schemes uses special or control packets to analyze false nodes in the network. Topology changes frequently due to random motion of nodes, so there will be lots of special and control messages in the network to cause congestion. It will increase the adverse effect on the network achievements by dropping throughput and increase in delay and packet drop rate.

Routing Delay: It is that time duration which is consumed during path discovery and path verification process. It will take ample amount of time, if IDS takes extra capacity to establish path between source and destination. Therefore, network performance will be affected due to increasing delay rates.

Resource Overuse: Additional use of any resource for route finding and maintaining or transmitting data is termed as resource overuse. Mobile nodes have limited resources like memory, space capacity, processing power, and battery life etc. If detection schemes involve much info and calculations, then there will be more consumption of memory and the processing power which will give adverse effects to the network performance.

Special Hardware: It is the additional hardware that is used for routing and data transfer purposes. This is in the form of a GPS device, antennas or special nodes etc. By this overuse of assets and costing of the network will be elevated.

Mobility: Nodes can easily shift in MANET, due to their mobile nature. The detections schemes are mostly not able to work accordingly due to mobility of nodes in MANET. As in seconds of time durations nodes are changing their positions and by this detection method faces a lot difficulties to rescue the network from harmful attacks. FPR are also increased by increasing mobility rate.

Conclusion & Future scope

In this review research, we tried to check various security related issues in a dedicated mobile networks. In a nutshell we have discussed the essential characteristics of the mobile ad hoc networks. There is an increasing need for network users

to connect to the world anytime, anywhere, inspiring the use of the dedicated mobile network. Here, we target the harmful attacks present in the network to destroy the network's feature. The main concern of this paper is to find and protect the network from various attacking node. A detailed study about selected existing methods and techniques to identify the attacks in MANET is mention in the above sections. The detection methods mainly make use of on demand routing protocol, which has given better PDR, throughput with lesser delay rates. The performance is judged by many crucial factors like network environment, network scenario, traffic and mobility model etc. It is totally based on the existing network for selection of proper routing protocols, techniques and methodology to be followed. During the investigation, we found some points that could be explored in the future. The major focus of this document is to guide researchers in the territory of security in the area of mobile ad hoc networks. Advanced technology should include the function of prevention, detection and interaction mechanism at MANET.

Acknowledgements: This research paper is made possible through the help and support from everyone, including parents, teachers, family and friends. Specially, I would like to thank Prof. (Dr.) Sudhir Kumar Sharma for his valuable suggestions, guidance and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper. The product of this research paper would not be possible without all of them.

References

1. Sarika S, Pravin A, Vijayakumar A, Selvamani K (2016), Security Issues In Mobile Ad Hoc Networks, 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), Procedia Computer Science 92 (2016) 329 – 335, published by Elsevier.
2. Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi (2016), Secure Routing Protocols for Mobile Ad Hoc Networks, 978-1-4673-7689-1/16/ © IEEE.
3. Ms. PriyanksSogani and Dr. Aman Jain (2015), A Study on Security Issues in Mobile Ad Hoc Networks, International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 4, published by Academic Science, Special Issue March.
4. Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani (2008), A Survey of Secure Mobile Ad Hoc Routing Protocols, IEEE Communications Surveys & Tutorials, VOL. 10, NO.4, Fourth Quarter.
5. Antesar M. Shabut, Keshav Dahal, M. Shamim Kaiser, and M A Hossain (2017), Malicious Insider Threats in Tactical MANET: The Performance Analysis of DSR Routing Protocol, IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh.
6. Mahmoud Reda, Marianne A. Azer (2017), Correlation between Protocol Selection and Packet Drop Attack Severity in Ad Hoc Networks, 978-1-5386-4266-5/17/ Â © IEEE.
7. Balasubramanian Paramasivan, Maria Johan Viju Prakash, and Madasamy Kaliappan (2015), Development of a Secure Routing Protocol using Game Theory Model in Mobile Ad Hoc Networks , JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 17, NO.1, February.

8. Subramanian Ganesh and Ramachandran Amutha (2013), Efficient and Secure Routing Protocol forWireless Sensor Networks through SNR Based Dynamic Clustering Mechanisms, Journal of Communications And Networks, Vol. 15, NO.4, August.
9. Issa Khalil, Sameer Bataineh, Liana Qubajah and Abdallah Khreishah (2013), Distributed Secure Routing Protocol for Mobile Ad-Hoc Networks, 5th International Conference on Computer Science and Information Technology (CSIT) ISBN: 978-1-4673-5825-5.
10. A.L.Sandoval Orozco, J. Garc´ıaMatesanz, L. J. Garc´ıaVillalba, J. D. Marquez D´ıaz and T. H. Kim (2012), Security Issues inMobile Ad Hoc Networks, Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2012, Article ID 818054, doi:10.1155/2012/818054.
11. Ashish Kumar Khare, Dr. J. L. Rana and Dr. R. C.Jain (2017), Detection of Wormhole, Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology, I. J. Computer Network and Information Security, MECS, DOI: 10.5815/ijcnis.2017.07.04.
12. Neelam Janak Kumar Patel and Dr. Khushboo Tripathi (2018), Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method, Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099, IJSRSET.
13. Vikas Goyal and Geeta Arora (2017), a review Paper on Security Issues in Mobile Adhoc Networks, International Research Journal of Advanced Engineering and Science, Volume 2, Issue 1, pp. 203-207, ISSN: 2455-9024.15.
14. M.Jeevamaheswari, R. AnandhaJothi, V. Palanisamy. (2018). AODV Routing Protocol to Defence Against Packet Dropping Gray Hole Attack In MA NET, IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011, ISSN: 2395-602X.
15. Mohamed A. Al-Shora, Sayed A. Nouh, Ahmed R. Khalifa. (2018). Reliable Dynamic Source Routing (RDSR) Protocol with Link Failure Prediction for Mobile Ad Hoc Networks (MANET), Journal of Network Communications and Emerging Technologies, Volume 8, Issue 3, March.
16. Taku Noguchi, Mayuko Hayakawa. (2018). Black Hole Attack Prevention Method UsingMultiple RREPs in Mobile Ad Hoc Networks, 17th IEEE International Conference on Trust, Security and Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering.
17. Arif Sari. (2014). Security Approaches in IEEE 802.11 MANET, Int. J. Communications, Network and System Sciences, 2014, 7, 365-372, scientific research.
18. Jhum Swain, Binod Kumar Pattanayak and Bibudhendu Pati (2017), study and Analysis of Routing Issues in MANET, International Conference on Inventive Communication and Computational Technologies, (ICICCT).20
19. Vinay Rishiwal, Sandeep Kumar Agarwal, Mano Yadav (2016), Performance of AODV Protocol for H-MANETs, Symposium on Colossal Data Analysis and Networking (CDAN), 978-1-5090-0673-1/16, IEEE.
20. Versha Matre and Reena Karandikar. (2016). Multipath Routing Protocol for Mobile Adhoc Networks, 2016 Symposium on Colossal Data Analysis and Networking (CDAN), 978-1-5090-0669-4/16, IEEE.

21. Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, Muhammad Hanif Durad. (2015). Analysis of Detection Features for Wormhole Attacks in MANETs, International Workshop on Cyber Security and Digital Investigation (CSDI 2015), Procedia Computer Science 56 (2015) 384 – 390, Elsevier.
22. Vandana C.P, Dr. A. Francis Saviour Devaraj (2013). MLDW- Multi Layered Detection mechanism for Wormhole attack in AODV based MANET, International Journal of Security, Privacy and Trust Management (IJSPTM) Vol. 2, No. 3.
23. Rupinder Singh, Jatinder Singh, and Ravinder Singh (2016). WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks, Hindawi Publishing Corporation, Mobile Information Systems, Volume 2016, Article ID 8354930.
24. Anju J and Sminesh C N (2014). An Improved Clustering-based Approach for Wormhole Attack Detection in MANET, 3rd International Conference on Eco-friendly Computing and Communication Systems, 978-1-4799-7002-5/14 $31.00 © 2014 IEEE.
25. Manju Ojha and Rajendra Singh Kushwah (2015). Improving Quality of Service of Trust Based System against Wormhole Attack by Multi-Path Routing Method, International Conference on Soft Computing Techniques and Implementations- (lCSCTI) 978-1-4673-6792-9/15 IEEE.