ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(14), DOI: 10.17485/ijst/2016/v9i14/84433, April 2016* ISSN (Online) : 0974-5645

Study on Reliable and Secure Routing Protocols on Manet

K. Vijayakumar[1]*and K. Somasundaram[2]

[1]Department of Computer Science Engineering, Karpagam University, Coimbatore – 641021, Tamil Nadu, India; vijay_kollati@yahoo.co.in

[2]Department of Computer Science and Engineering, Vel Tech High Tech Dr. RR Dr. SR Engineering College, Chennai - 600062, Tamil Nadu, India; soms72@.yahoo.com

Abstract

Objectives: This survey article intent presents knowledge into the security execution issues related to steering in wireless networking like MANET's (Mobile Ad hoc Networks). **Findings:** The mobile adhoc networks are exposed to attacks at all the layers especially at the network layer. This study specially provides a set of solutions for the issues of various attacks like attacks on modifications, impersonation attacks, fabrication and rushing attacks. A few methodologies are analysed for prevention, detection and reaction on various attacks by malicious nodes. The study of this article has examined the methodologies meant for fathoming the implementation issues like, changes in topology, vitality utilization of stations, delay, throughput, transmit time, packet transmission ratio, systems or nodes security and administration. **Conclusion:** This article presents a comparison table specifying that every protocol provides security only to a limited access. Thus, there is still a prerequisite of more secured belief that can deal with the diverse asking for necessities like reliable protocols for security issues of MANET.

Keywords: Attacks, Detection, Malicious Nodes, Network Layer, Prevention, Protocols, Security, Throughput

1. Introduction

The security plays an important role when considered for communication networks of wired and wireless. The mobile adhoc networks laying its face down to dissimilar security attacks due to lack of decentralized administration. The achievement of mobile adhoc network (MANET) mainly depends on confidence of the users in security aspects. The severity of the attack depends on midway distance of the malicious nodes between the nodes, dropping of packets, misrouting of packets, providing false information etc. Together the scalability and mobility of the nodes shows the impact on the routing protocols with respect to security issues. All routing protocol requires protected data transmission. The various security desires of mobile adhoc networks are analogous like infrastructure less wireless networks or wired networks. On the other hand, the MANET's characteristics introduce various challenges and opportunities to achieve secure goals[9,12,15], namely confidentiality, integrity, authentication, access control, availability and non-repudiation which are defined as follows:

Authentication: Authentication[1] safeguards the communication or data transmission which is carried no more than by the endorsed nodes. The suspicious node which is demonstrating as a authorised node in the region of the network which does not hold proper authentication and that can badly distress the transfer of data between the nodes.

Availability: Availability is defined as providing or processing the various services even the attacks are in existence. It is anxious to state that the various network

* *Author for correspondence*

services should be offered each and every time they are required. The systems confirming the availability in MANET's must take necessary care of numerous attacks like services denial attacks, energy consuming attacks, and also malfunction of nodes.

Confidentiality: Confidentiality[1,12] is used to safeguards that the intended party only is being provided with the information. The remaining nodes which are participating during transmission except the sender, receiver can only read the information. By applying data encryption techniques we can attain high security.

Integrity: The non variation of the data's originality while transmission by any other malicious node in the network can be confirmed and stated by using Integrity.

Non-Repudiation: This feature non disclaimer guarantees that any node that sends and receives data cannot reject a transmitted message[15]. This factor is also used in support to identify and separate the node which is compromised in the network.

In addition to the previous specified problems there are certain other problems also need to be considered to provide security like:

Collaboration and Fairness
Location Confidentiality
Traffic diversion avoidance

2. Security Attacks on Manets

In communication networks where there is no infrastructure, security inspection is a great deal as every hub is allowed to pass through in several heading such that the concentrated protection in such systems is no more available. Assaults on such type of network where there is mobility, are comprehensively partitioned into two noteworthy classifications:

Active Attacks: In this kind of attacks[4,15] the attackers try to agitate the original functionality of the transmitting and communicating devices in the network. This task is carried by evaluating the information and changing the packets which contain the information, denial of neither services[13] nor changing the path desired for routing by modifying the route specifying path, count of hops in a path etc. These kinds of active attacks can easily be identified and detected when compared with the other opposite attacks called Inactive (Passive) attacks.

Passive Attacks: These passive attacks[4,15] can be stated as more dangerous when compared to active attacks because it will not change or vary the normal behaviour of network whereas the attackers attempt to pay attention silently or reclaims the important information available with data packets transmitted. It is very difficult to identify this behaviour of passive attack. These kinds of passive assaults[26] are broadly divided into four main categories is shown in. Figure 1.

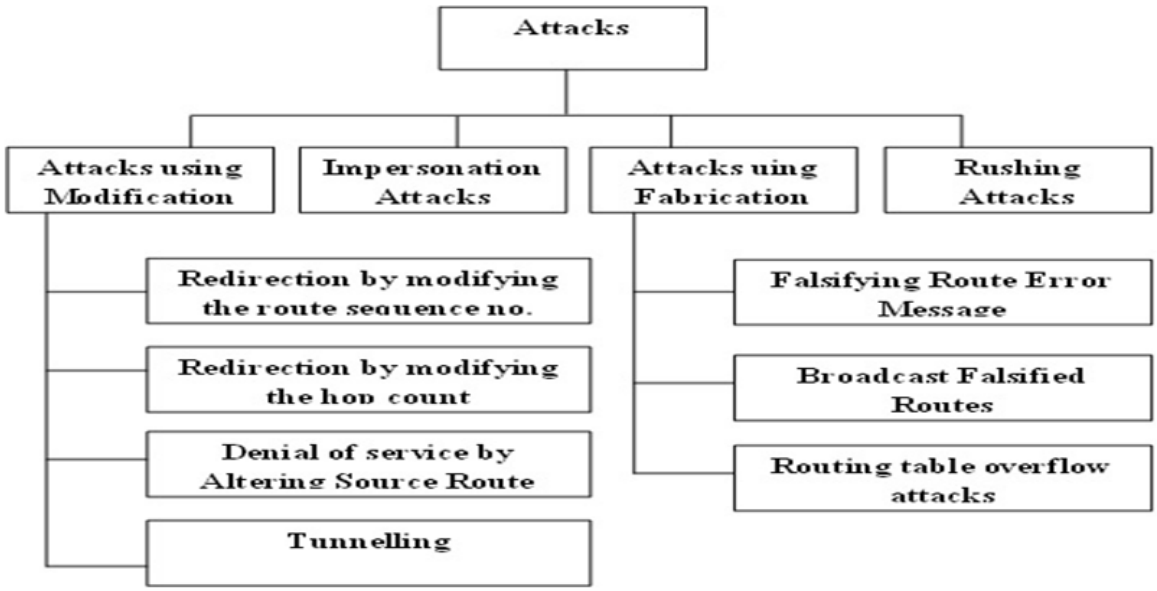

Figure 1. Various Types of Attacks on MANET.

2.1 Attacks using Modification

Redirection with the help of altering the route sequence number: To determine the superlative route between the sources to the destination, the stations should continually depends on various parameters like sequence number, delay, hop count etc. These parameters should be low in value which specifies the chosen path is the best. In this kind of attack, the traffic in the network is under misleading by the suspicious station by varying the count of hops between the nodes to a least assessment than the earlier least value.

Hop count alteration by redirecting: In these attacks the hop count parameter is changed to a smaller value and the packet traffic is diverted towards the malicious node which leads to a false path.

Source route alteration and causing attacks by DoS (Denial of Service): The attacks by denial of service are occurred by the entire demolition of the routing function by denial of service. In this the attacker affects in such a way that it neither drops the network traffic nor it redirects the data packets to an unknown destination or mislead to a lengthy path to destination to create unwanted delay in transmission.

Tunneling: These are another type of attacks where more number of nodes may co-ordinated to encapsulate and then the messages are switched over among them through active routing paths of data. By this event there is a chance for a single or more than one node to short circuit the regular stream of data flow by providing a false count for the set of connections which is guarded by two colliding attackers.

2.2 Attacks by Impersonation

Impersonation attacks can be caused by "*Spoofing*". In this kind of attacks, malicious node will alter the IP or MAC address for all the data packets departing from the node and the address of one node can also be used by another node. With the help of spoofing, the malicious node be able to modify the network topology or separate some nodes from the remaining network.

2.3 Attacks Caused by Fabrication

Fabricating route error message: These are the attacks in routing protocol like on-demand, which is further exceptional, which utilises link preservation to reclaim the damaged path. At whatever point a node alters its present location, the closest node proliferates mistake information to alternate nodes expressing that this specific way is no more accessible. By sending this kind of error information, any station can be effortlessly left.

Broadcasting erroneous routes: In this category of incursions, the attackers accomplish the path information from the header of data packet and modify the routing link. This will modify the path accumulation of nearby node.

Attacks by overflow of Routing table: In this type of assaults, where attacker performs to develop paths to other than active links. When the sufficient paths have been developed, new paths can be no more registered in the routing cache.

2.4 Rushing Attacks

These categories of incursion are also takes place in routing protocol like on-demand. In this a request packet for link establishment is send to determine the link to the sink node. This activity is taken as advantage by nodes to perform rushing attacks[4] by sending the RREQ message more regularly when compared with remaining stations such that, the path together with the adversary is identified.

3. Security Routing Protocols of Manet

There are different security conventions for MANET's which can be for the most part characterized into two noteworthy classifications namely prevention and reaction upon detection.

Prevention: In this category, the attacking stations are blocked in order not to start any further movements by the protocols involved in routing. This method requires encoding techniques to validate the integrity, confidentiality, non-repudiation of routing information.

Reaction upon Detection: Detecting attacks and Reaction upon detection attacks procedure as the name implies will find any malignant node or movement of any suspicious

station in the wired or wireless communicating network and take necessary action to continue the appropriate route in transmission of information in the network.

Based on the survey done on various protocols the secure routing protocols[26] can be categorised as shown in Figure 2.

Instantly, the various routing protocols that concerned in prevention of attacks schema are given in detail as:

3.1. Prevention of Attacks

3.1.1 Preventing by using Asymmetric Cryptosystem

ARAN: An On-demand secure routing protocol, ARAN (Authenticated Routing for Ad-hoc Network) is based on the cryptographic certificates. ARAN utilizes a preparatory cryptographic declaration process took after by end to end course verification procedure to acquire secure path establishment.

This routing standard is a safe directing on-interest directing convention taking into account the cryptographic declarations. This convention

- In the preliminary certification process, the certificates are issued by a confidential affirmation system, which conveys its public key to each and every hub within the system. Each and every node in the system is important to contain a public key and its address is to be affirmed prior to taking part in the communication and connecting to the network.
- The main aim of this end-to-end authentication is to ensure the route discovery for reaching the intended destination. The objective is that the source need to check such that the destination intended was come to or not. A digitally marked RDP (Resource Discovery packet) starts broadcasting by the source hub. This packet incorporates various parameters like address of destination node, N_s a nonce, endorsement of the starting hub, and current time. The current time and the Nonce are available to counteract repeat assaults and to distinguish looping and record its mark on the packet. All the succeeding middle hubs will evacuate the mark of the past hub, check it and affix their mark on the packet. Similarly, along the reply packet (REP) every hub annexes its mark before sending it to the following hop. All the routes whether active or not are being tracked by the nodes in order to maintain the route. Therefore if any inactive or broken node receives a data, a blunder message indicating is created and sent to the source hub.

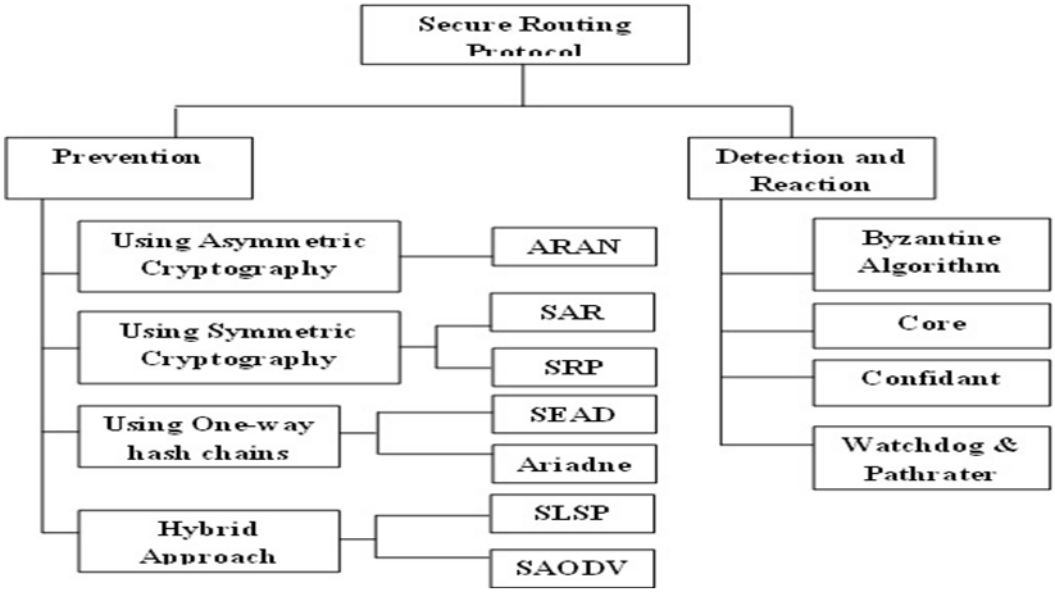

Figure 2. Secure Routing Protocols.

3.1.2 Preventing by Using Symmetric Cryptosystem

SAR: SAR (Security Aware mobile Ad-hoc Routing) protocol uses the metrics for security to obtain routing. A security parameter is included within the RREQ data packet in SAR. During the message sending or receiving, nodes are required to have secret keys for decrypting[3]. If any route is available with the required security parameter a packet RREP is transmitted between the intermediate station or the sink node to the source node. And a shortest route is being marked for data forwarding in case of different route is traced.

Secure Routing Protocol: This protocol uses symmetric cryptography which is an additional routing protocol for providing secure called Secure Routing Protocol (SRP) which relays on route querying method. In this among the source and destination node, a Security Association (SA) is needed. This Security Association SA generates a key which is normally used to perform the data encryption as well as decryption with the help of these two nodes. The SRP header is included with the base header and is shown in Table 1. The packet RREQ specifies the output of a key hashed function, QID a query identifier and QSEQ a query sequence number. The shared key, basic routing protocol header and the IP header is taken by the key hash function.

Table 1. SRP Packet header

IP HEADER	
BASIC ROUTING PROTOCOL HEADER	
TYPE	RESERVED
QUERY IDENTIFIER (QID)	
SEQUENCE NUMBER OF A QUERY (QSEQ)	
MESSAGE AUTHENTICATION CODE (MAC)	

The routing tables are being updated by the in-between hubs on transmitting the query to the neighbour hubs. In the event the query is dropped when their table of routing has similar QID of the receiving node.

At the point when the receiver is achieved, the receiver station will check for protection measurements by assessing the message authentication code (MAC)-key hash function. The secret key by validating, for the source node it makes reply packet containing of route from source to destination, QID, QSEQ. In the wake of getting the reply packet, MAC is once again calculated by the source node. Between the sender and the receiver we have many routes. By using the route error message, in this protocol route support is also additionally finished.

3.1.3 Preventing by using One-Way Hash Chain

SEAD: Secure Efficient Ad-hoc Distance Vector Routing (SEAD) is based on Destination sequence distance vector DSDV protocol which is a proactive and secured routing protocol. The protocol SEAD is designed against the modification and security attacks like Denial of Service and attacks by unwanted resource consumption. In this protocol, the data packet authenticity is been checked by making use of hash chain method where the hash chain value is taken for update the routing for transmitting. Whenever an update of routing is received by a node, each message entry authentication is verified. This protocol SEAD eliminates looping by making use of destination sequence number. The protocol SEAD protocol validates update message of routing for the source by avoiding loops which is being done with any one of the following two mechanisms:

The SEAD convention likewise validates the avoiding so as to wellspring of directing overhaul message circles which is being finished with any of the accompanying two systems:

- To employ broadcast authentication mechanisms, in the adhoc networks between the nodes a clock synchronization is being used.
- A shared secret key is provided between the node pair.

Authentication of a routing update message between the nodes i.e MAC (Message Authentication Code) is provided by a secret key shared between the pair of nodes.

Ariadne: This protocol Ariadne is also one of the routing protocols for security on-demand constructed with the help of DSR for ad-hoc networks using symmetric cryptography. This Ariadne protocol uses shared key for authentication (MAC) between the nodes. This protocol Ariadne working is stated in 3 ways as: At the point when a hub (source hub) needs to communicate with whatever other hub, it sends RREQ, a message for route request which contains the source address, destination address, an identifier to finds the present route disclosure, a measure of time called TESLA time interim representing

to the normal entry time of the request to the destination hub and a hash chain. At the point when RREQ is gotten, the intermediate hub checks the TESLA time interim legitimacy. A one way hash facility is used in order to check the authentication. In the event that the information packet is a legal packet then the hub attaches its own particular location in the rundown of hubs, by replacing the hash chain with another one comprising of its location in addition to the old one, and adds a MAC of the entire packet to the MAC list. Finally, the hub which is so called destination will verifies each and every step of the route by comparing the received hash and calculated MAC hash.

3.1.4 Hybrid Approach

SLSP: The SLSP (Secure Link State Routing Protocol) is utilized to safeguard the revelation and the dispersion of link state information. This convention utilizes asymmetric key to provide high security. Initially the hubs that participate are distinguished based on the IP addresses of their interfaces. Secure Link State Routing Protocol can be normally given in three steps. They are:

- **Public Key Distribution (PKD):** In this protocol the central server is not used for key distribution. The public key distribution (PKD) is normally carried over between the nodes that are available within its own surrounding area.
- **Neighbour discovery:** The neighbour nodes discovery process is done by the process that periodically the information about the Link state of node is broadcasted with the help of Neighbour Lookup Protocol (NLP). A packet with Hello message that contains MAC address of sender and the network IP address is broadcasted in the network. This kind of messages was also signed. The malicious node or any discrepancies in the network are recognised by the help of NLP.
- **Link State Updates (LSU):** The packets of LSU are recognized with the help of initiated nodes IP address. A sequence number of 32-bit is present in the LSU packet which is periodically updated. In this protocol the LSU of the intermediate nodes will authenticate the connected signature by means of a public key which is formerly reserved at the time of pubic key distribution phase. The nodes traversed field used in LSU is set to hashed hops traversed, the TTL is decremented and at last the packet is again broadcasted. These SLSP nodes are going to maintain a list of information like apriority ranking of their proximity nodes which depends traffic control rate in order to maintain the secure of the packet against denial of service attacks. For the lowest rate generated LSU packets high priorities are used. This behaviour facilitates the neighbours of determining the malfunctioning nodes that overflow higher rate control packets tie up the success nature of the assault.

SAODV: This Secure Ad-hoc On-demand Distance Vector Routing Protocoll *(*SAODV) protocol is depended on demand routing protocol AODV[2]. This protocol works with the help of asymmetric cryptography and also by using hash chaining. The RREQ packet which is shown in Table 2 is digitally signed by the node when it desires to send a message, and transmits to the neighbour nodes. At the point when the RREQ packet is gotten, intermediate nodes authenticates before overhauling or making an opposite route to the host by using cryptographic techniques.

Table 2. SAODV Protocol Header

TYPE LENGTH	HASH FUNCTION	MAX HOP COUNT
TOP HASH		
SIGNATURE		
HASH		

The hop count values are being certified in SAODV by using Hash chains. A seed; a random value is developed whenever a station wants to forward a RREP or RREQ packet. It marks a Maximum Hop Count given to the TTL (Time to live) value in the IP header. The seed is defined as the signature extension of the Hash range. The Top Hash range is set to the hashed seed and the Max Hop Count periods. At whatever point a neighbour node gets a RREQ or a RREP it confirms the count of hop by hashing Max Hop Count - Hop Count times the Hash field and check whether the resultant worth is same as Top Hash value. When the above said both values are dissimilar from each other, then the node will drops the data packet and a message showing error will be given by the nodes for the broken links.

3.2 Detection and Reaction

The various protocols that are designed for Detection and Reaction representation are:

3.2.1 Byzantine Algorithm

This Byzantine algorithm is specifically implemented to safeguard the network from Byzantine[2,15] collapse which includes change of packets, discarding data packets, incursion made by self-interested or malignant nodes. There are three stages[26] in defining Byzantine procedure comprise as shown in Figure 3.

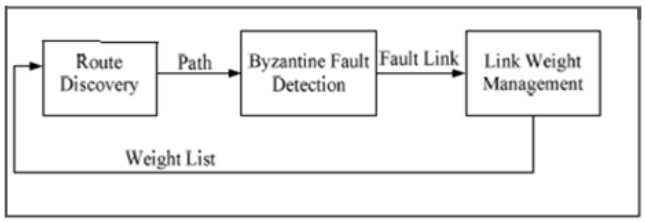

Figure 3. Three phases of Byzantine algorithm.

Route Discovery: Whenever a source hub needs to forward the data, it imparts link request data which contains address of source, address of destination, a weight list, a sequence number and private key for confirmation to its acquaintance. On acquiring the RREQ information the hub on the node in transition manipulates its node list for the entry of RREQ. In the event that there is no option, it checks the secret key for validation and includes its list and re-imparts it to different entities.

A route reply message (RREP) is generated on verifying the secret key when the sink node reaches. On accepting the RREP message, source hub approves the private key. It additionally coordinates the internal connection and available route. On the off chance that the received route is superior to anything available route, then modify this path in its route table.

Fault Detection: Fault detection process specifies, every transitional hub mentioned as a probe node forwards acknowledgement or acquaintance to sender hub for each and every message which it receives. If more quantity of unacknowledged messages moves beyond the verge value, enrol of fault is done on the route.

Link Weight Management: The protocol at this phase, manipulates the weight or load of the routes. At the fault detection stage if a path is determined as a faulty path, then it is being coupled with its related weight. At the route revelation stage path with negligible weight worth will be considered as enhanced way.

3.2.2 Core

In this algorithm it uses a method to uphold entity to associate all the nodes in MANET which functions upon the cooperative behaviours of the entities. It uses the methods of Watchdog and Reputation Table to determine the collaborative or malicious entities. The related reputation or ratings of the transitional nodes are maintained in a reputation table blocks. The block of Watchdog manipulates the function and offers the Reputation value. CORE mechanism contains of a source hub and a set of transition hubs. In this, at whatever point a transition hub denies co-working with the source hub, this CORE convention will constrain the dissent of move hub. This may take to lessening of transitional hub from the system.

3.2.3 Confidant

Confidant protocol is used to determine the non-supportive stations. The Confidant protocol comprise of various blocks like the monitor, path manager, trust manager and reputation system. The passive feedbacks for each message which it sends are considered and being monitored by the monitor block. The transition of alarm signals is concerned by the trust manager block. When a station locates that a host is non-functioning, it forwards information in the form of alarm. This kind of messages is shared among the nodes that are stated as associates. Alarms message from other stations are given considerably a smaller amount weightage. The reputation system block holds a chart of station and the related evaluations. Assessments are changed in light of a rate capacity that makes employments of modest weights if a alarm is managed for a getting misbehaving station and higher weights for direct data. The path manager block manages all link data in concern with accumulation, removal, and changing of route based on the acknowledged message it accepted from the reputation system. The path which contains the identified malicious node is eliminated, if the rating goes under a certain threshold value by calling the path manager block.

3.2.4 Watchdog and Pathrater

The protocol which is specified under watchdog and pathrater[17] is used to identify the nodes which are malicious and which will refuse in packets forwarding where as they are admitted to exchange the packets in the initial stage. The significant function of Watchdog is to investigate whether the data packets are being exchanged or not by the next station available in the link. If the next station is not exchanging the packet then it is noticed as the malicious characters. The main aim of pathrater is to estimate and identify the trusted route from the outcome watchdog generates. Whenever a node decides to send a packet to its neighbour node in the pathway, it first verifies that the neighbouring node will transmit or not and also verifies that the proximity node should not alter the contents in the packet before forwarding it. Hence forth any node that behaves like malicious node like deny of service or altering the data packet, then this Watchdog protocol will enhance its rating under failure where this failure ranking is very supportive in identifying the trusted route between source and destination.

4. Comparison of Various Secure Routing Protocols

The below Table 3 is specified based on various protocols studied, and a comparison[8] table is made between different protocols.

The Table 3 represent that a several tasks is carried for attacks by rushing , DoS and modifying routing table attacks whereas to prevent tunnelling attacks still more a lot of security protocols are needed. The routing protocol in aspects of security is capable of handling only restricted attacks. For e.g. ARAN and SAR convention can offer security against surging and directing altering routing table assaults, where as they are not reasonable for security against Denial-of-Service and assaults by tunnelling. In the same way, CORE provides security against Denial-of-Service attacks. The security for tunnelling attacks can be provided by Watchdog and Pathrater.

5. Attack Taxonomies in Manet

In MANETS there is a chance for different types of attacks where few kinds of attacks are applicable for general network, other applies to connectionless network and few are specific for mobile adhoc networks. The various attacks for security are broadly open based on different criteria[15], namely the province of the attackers, or the methods applied in assaults. The various security attacks in MANET and in the remaining networks can be broadly briefed based on the following strategies like Active or passive, External or Internal, various protocol

Table 3. Routing protocols comparison based on security aspects

Name of protocol	Type	Chances of attacks			
		Rushing attack	Denial of Service	Modifying routing table	Attacks by Tunnelling
ARAN (Authenticated Routing for Adhoc Networks)	On demand routing protocol	positive	negative	positive	negative
SAR (Secure aware Adhoc Routing)	On demand routing protocol	positive	negative	positive	negative
SRP (Secure Routing Protocol)	On demand routing protocol	positive	positive	positive	negative
SEAD (Secure Efficient Adhoc Distance vector routing)	Table Driven routing protocol	positive	positive	positive	negative
Ariadne	On demand routing protocol	positive	positive	positive	negative
SLSP (Secure Link State routing Protocol)	Table Driven routing protocol	positive	positive	positive	negative
SAODV(Secure Ad-hoc On-demand Distance Vector Routing Protocol)	On demand routing protocol	positive	negative	positive	negative
CONFIDANT	On demand routing protocol	positive	negative	negative	positive
BYZANTINE	On demand routing protocol	positive	positive	positive	negative
WATCHDOG & PATHRATER	On demand routing protocol	negative	negative	negative	positive

Table 4. Different security Attacks on Internet layered model

Name of Layer	Type of Attack
Physical layer	congestion, interceptions, eavesdropping
Data Link Layer	Traffic analysis, monitoring, disruption MAC (802.11) WEP weakness
Network layer	Black Hole, Wormhole, Byzantine, Flooding attacks, Consumption of resource, location disclosure attacks
Transport Layer	Session hijacking, SYN flooding
Application Layer	Repudiation, data corruption
Multi- layer attacks	Denial of Service, Masquerade, Replay, Man-in-the-middle.

layer[15], Stealthy or Non-stealthy, Cryptographic or Non-cryptographic etc. The Table 4 shows the security attacks at various layers[2,9,15] of the Internet model.

Active Attacks vs. Passive Attacks: The various attacks of mobile adhoc networks (MANET's) are broadly divided keen on two main groups, specifically active attacks and passive attacks[9]. In the passive attacks the data is switched in the network without interrupting the communication process while in an active attack contains packet disruption, alteration, or false modification, thereby disturbing the original behaviour of a MANET. The different illustrations of passive assaults are traffic investigation, eavesdropping and traffic observing and the active assaults jamming, impersonating, modification, denial of service (DoS), and message replay.

Internal Attacks vs. External Attacks: Another form of attacks[10] can also be categorised into external attacks and internal attacks[9], related to the environment of the assaults. Some articles specify attacks as outsider and insider attacks. Externals assaults are kept up by stations that don't fit in with nature of the system. Internal assaults are from bargained stations, which are truly part of the system. Internal assaults are less demanding when related with external assaults subsequent to the insider knows important and mystery data, and holds special permit privileges.

Attacks on Different Layers of the Internet Model: Further, the attacks are broadly divided by affording to five layers[2,15] of the layered model of Internet. The above Table 2 specifies a grouping of several security Attacks on Internet layered model. Certain attacks can be launched at various layers.

Stealthy vs. Non-Stealthy Attacks: Particular security attacks[13] use stealth, whereby the attackers try to conceal their activities from either a individual who is observing the system or an intrusion detection system[9,15] (IDS). Be that as it may, different assaults, for example, DoS can't be made stealthy.

Cryptography vs. Non-Cryptography Related Attacks: Certain attacks are non-cryptography associated, and rest are cryptographic primitive attacks. The Table 5 shows various cryptographic primitive attacks[3] with examples.

Table 5. Attacks based on cryptographic techniques

Cryptographic technique Attacks	Example
Pseudorandom number attack	Nonce, timestamp, Initialization Vector (IV)
Digital signature attack	RSA Signature, Elgamal signature, Digital Signature Standard (DSS)
Hash Collision Attack	SHA-0, MD4, MD5, HAVAl-128, RIPEMD

6. Conclusion

In this article, we have portrayed the distinctive security targets, security attacks and supporting security for diverse existing directing system necessities. In this study, an examination chart is given which specifies that every safe convention works beneath different restrictions that give security against constrained attacks. One of the protocols can achieve all security objectives.

Thusly, there is still a prerequisite of more secured convention that can deal with the distinctive asking for necessities of MANET. This section presents dominant part of the attack taxonomies in brief that has been considered as the preparatory piece of study in the introductory stages of the proposed research work. The work gives the essential thoughts regarding the capability of attacks and vulnerabilities in MANET that could help for comprehension the antagonistic part of the study.

7. References

1. Sumathi A, Vinayaga Sundaram B. An ANN Approach in Ensuring CIA Triangle using Energy based Secured Protocol E-AODV for Enhancing the Performance in MANETS. Indian Journal of Science and Technology. 2015 December; 8(34). Doi: 10.17485/ijst/2015/v8i34/IPL0821.
2. Joseph Ch, Kishoreraja C, Radhika Baskar, Reji M. Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios. Indian Journal of Science and Technology. 2015 November; 8(29). Doi: 10.17485/ijst/2015/v8i29/84653.
3. Vijaya Kumar K, Somasundaram K. A Symmetric Multiple Random Keys (SMRK) Model Cryptographic Algorithm. International Journal of Innovative Research in Computer and Communication Engineering. 2015 November; 3(11), 10896-903.
4. Wilson Prakash S, Sankaranarayanan S. Solution To Prohibit Rushing Attack In Mobile Ad-Hoc Network. International Journal on Applications in Information and Communication Engineering. 2015 September; 1(9):1-5.
5. Joseph Ch, Kishoreraja C, Radhika Baskar, Reji M. Performance Metrics of Wormhole Detection using Path Tracing Algorithm. Indian Journal of Science and Technology. 2015 August; 8(17):63541.
6. Anchugam CV, Thangadurai K. Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization - simulation Analysis. Indian Journal of Science and Technology. 2015 July; 8(13). Doi: 10.17485/ijst/2015/v8i13/58200.
7. Thenral B, Thirunadana Sikamani K. AMRA: Angle based Multicast Routing Algorithm for Wireless Mesh Networks. Indian Journal of Science and Technology. 2015 July; 8(13):59451.
8. Anand V, Sairam N. Methodologies for Addressing the Performance Issues of Routing in Mobile Ad hoc Networks: A Review. Indian Journal of Science and Technology. 2015 July; 8(15). Doi: 10.17485/ijst/2015/v8i15/70511.
9. Gomathi K, Parvathavarthini B. An extensive analysis of manet attacks using special characteristics. Indian Journal of Computer Science and Engineering (IJCSE). 2015 Jun-Jul; 6(3):110-13.
10. Dom Ali, Reza Seyed, Kheytkhah Esmail. Secure Challenges in Mobile Adhoc Networks - A survey. International Journal of Computer Science and engineering Survey. 2015 February; 6(1):15-29.
11. Pradeep Reddy CH, Jagadeesh Gopal, Arun Kumar S. Efficient Bandwidth Utilization with Congestion Control for Wireless Mesh Networks. Indian Journal of Science and Technology, 2014 November; 7(11):1780-87.
12. Santoshi K, Vijaya Kumar K. An Empirical Model of Malicious Node detection and Prevention with Data rating. International Journal of Engineering Trends and Technology (IJETT). November 2014; 17(2):56-59.
13. Jain Shikha. Security Threats in MANETS: A Review. International Journal on Information Theory. 2014 April; 3(2):37-50.
14. Subburaj V, Chitra K. Multi Hop Secure Adhoc Network to Eradicate Cooperative Diversity. Indian Journal of Science and Technology. 2014 February; 7(2):135-41.
15. Godwin Ponsam J, Srinivasan R. A Survey on MANET Security Challenges, Attacks and its Counter measures. International Journal of Emerging Trends & Technology in Computer Science. 2014 January-February; 3(1):274-79.
16. Abbas S, Merabti M, Jones DL, Kifayat K. Lightweight Sybil Attack Detection in MANETs. IEEE Systems Journal. 2013 April; 7(2):236-48.
17. Anitha D, Punithavalli M. A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS. International Journal of Computer Science and Mobile Computing. 2013 March; 2(3):112-19.
18. Shakshuki EM, Kang N, Sheltami TR. EAACK - A Secure Intrusion-Detection System for MANETs. IEEE Transactions on Industrial Electronics. 2013 March; 60(3):1089-98.
19. Liu W, Nishiyama H, Ansari N, Yang J, Kato N. Cluster based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks. IEEE Transactions on Parallel and Distributed Systems, 2013 Feb; 24(2):239-49.
20. Hinds Alex, Ngulube Michael, Zhu Shaoying, Hussain-Al-Aqrabi. A Review of Routing Protocols for Mobile Ad-hoc Networks (MANETS). International Journal of Information Education and Technology. 2013 Feb; 3(1):184-91.
21. Ayday E, Fekri F. An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks. IEEE Transactions on Mobile Computing. 2012 September; 11(9):1514-31.
22. Guan Q, Yu FR, Jiang S. Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications. IEEE Transactions on vehicular technology. 2012 July; 61(6):2674-85.
23. Gagandeep, Aashima, Pawan Kumar. Analysis of Different Security Attacks in MANETs on Protocol Stack A - Review. International Journal of Engineering and Advanced Technology (IJEAT). 2012 June; 1(5):269-75.
24. Dhurandher, SK, Obaidat MS, Verma K, Gupta P, Dhurandher P. FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems. IEEE Systems Journal. 2011 June; 5(2):176-88.
25. Yu FR, Tang H, Mason PC, Wang F. A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks, IEEE Transactions on Network and Service Management. 2010 December; 7(4):258-67.
26. Tomar Parul, Suri PK, Soni MK. A Comparative Study for Secure Routing in MANET, International Journal of Computer Applications (0975-8887). 2010 July. 4(5):17-22.
27. Nakayama H, Kurosawa S, Jamalipour A. A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks. IEEE Transactions on Vehicular Technology. 2009 June; 58(5):2471-81.
28. Krutika K. Chhajed, Ali MS. Distributed Security System for Mobile Ad-Hoc Computer Networks. International Journal of Computer Science & Communication Networks. 2015; 5(3):184-91.