International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 22 (2018) pp. 16117-16126

A Review of Security Challenges in Ad-Hoc Network

Radha Raman Chandan
Department of Computer Science, B.H.U, Varanasi, India.

Pramod Kumar Mishra
Department of Computer Science, B.H.U, Varanasi, India.

Abstract
Mobile Ad-Hoc Network is an infrastructure less wireless network consists of mobile nodes. MANET has been a great research topic because of various challenges associated with it. This paper goes through a brief study of security in MANET and the challenges associated with it. For developing a robust security mechanism, it is necessary to first understand the routing techniques and possible attacks on them. In this paper gives the details about possible various types of attacks and its detection & prevention mechanism, our main focus are on network layer attacks specific to MANET.

1. INTRODUCTION:

An ad-hoc network is a decentralized local area network. Ad-hoc network means a network which is built spontaneously without any pre-existing infrastructure. Ad-hoc networks are of mainly 3 types:

- Mobile Ad-Hoc Network (MANET) [24].
- Wireless Mesh Network
- Wireless Sensor Network

A mobile ad-hoc network (MANET) is a type of multi-hop wireless network and can be defined as a collection of wireless mobile devices that are self-configuring and self-organizing [3][5][8].

The devices in MANET can directly communicate with each other within their transmission range without needing any base station i.e. there is no need of any central coordination. So the MANET can also be defined as a decentralized network which means a network where there is no base station to coordinate the flow of messages.

In conventional networks, some extra devices are used to determine the routes for establishing the communication between nodes such as routers are used in wired networks and wireless networks use access points. But in MANET, each node is itself responsible for routing by forwarding RREQ packets or control messages. Each node in network behaves like a router by forwarding the packets that are not related to its own use.

MANET does not follow any pre-existing infrastructure, thus called as an infrastructure less network, because of which it becomes easy and cheap to setup the network.

High mobility and scalability are other features. All the nodes are free to move in to or out of the network any time. MANETs are considered as a wireless local area network that is built spontaneously as devices connect. Because there is no pre-defined structure of the network and nodes can easily move independently, it follows the dynamic topology.

The main objective behind the MANET is to make the networking possible at any place and at any time [2].

Packet radio network was the first wireless network system, also considered as first generation of MANET, which later got sponsored by Defence Advanced Research Project Agency (DARPA) in early 1970s. It was mainly based on CSMA and ALOHA for providing an infrastructure less packet-switched network. The second generation starts from early 1980's where a special attention is given to the cost and scalability of the network and the security threats. GloMo (Global Mobile Information System) and NTDR (Near Term Digital Radio) were the two main developments of this generation.

The first two generation of mobile ad-hoc network came into existence for different military scenarios. The main aim for both generations was same i.e. adding combat operations. Third generation of MANET is mostly dedicated to commercial use.

2. RELATED WORK

In this section, we review of security issue in wireless adhoc network. To provide secure MANET, many researchers has analyses the various attacks in MANET and also present set of various detection and prevention solutions of attacks in wireless adhoc network.

Lijun Qian: In this paper author has evaluated the performance of multipath routing under wormhole attack environment. Multipath routing is vulnerable to wormhole attack. Author has proposed the statistical analysis of multipath detection method (SAM) for wormhole attack. In variant topologies network and different node transmission range environment this approach successfully detects such malicious nodes. Statistical analysis of multipath also helps for Intrusion Detection system in wireless ad-hoc network [25].

Shams Qazi: In this paper author has discussed about different mode of wormhole attack in ad-hoc network. a attacker can easily launched the wormhole attack without knowledge of Ad-Hoc network. There are various ways to detect and prevent wormhole attack like requirement of special hardware device or building the strong assumption. Most existing secure routing protocol (especially AODV) works on fixed rate transmission here author has considered multi-rate transmission to enhanced security in DSR routing protocol against wormhole attack by the calculation of RTT. Enhanced protocol secure DSR routing against wormhole attack for multi-rate transmission .there are various delays in routing the packet here .Author considered the queuing delay and processing delay of various participating nodes to calculate the round trip time (RTT) among the neighbouring nodes. Author has implemented the security protocol on both mode (Fixed rate transmission and multi-rate transmission). In simulation result proposed protocol improves the performance of routing protocol against wormhole attack. Advantage of this enhanced protocol doesn't require any special hardware or any complex calculation [26].

Su M-Y. WARP: For defending the wormhole attack in adhoc routing author have proposed WARP routing protocol. To adopt link disconnection multi route among source and destination. WARP protocol is modified form AODV protocol. By implementing WARP routing protocol, every nodes of network keeps the information about no of times form the path among source to destination. If occurrence of links greater than threshold vale then it will marked route exceeded among two node and these two nodes may be wormhole affected nodes. All neighbouring node of these affected nodes cancelled all request for forming the route [27].

Seung Yi, Prasad Naldurg, and Robin Kravets: In this paper author has proposed new routing schemes known as security Aware Adhoc routing (SAODV) protocol. This algorithm improves the relevance of route discovery for adhoc routing protocol. Author proposed the security frame work under two tier classifications through routing protocol security matrices. They have simulated the result in NS-2 through new SAODV. They considered the attributes for simulation are traffic pattern, packet format and trust hierarchy. after the simulation the have found that SAODV sends a little control message of routing protocol but disadvantage is that overhead increases[28] .

Fan-Hsu n Tseng 1, Li-Der Chou 1 and Han-Ch ieh Chao: In this paper Author has survey the various solutions against blackhole attack and discuss the state-of-art routing techniques. Author has focused on various types of black hole in mobile adhoc network. Here they have divided the black hole attack in two categories like ordinary black hole attack and collaborative black hole attack. In single black hole attack only one malicious node utilize the routing where as in collaborative black hole attack multiple malicious nodes collaborative together to utilize routing information.to detect and prevent the collaborative black hole attack there are various cooperative prevention schemes [29].

Table1: *Analysis Collaborative Black Hole Attack Detection [29].*

Mechanism	Routing	Simulator	Defects	Result
Cross check & DRI Proposed[30]	AODV	No	No	No
Cross checking Using FREQ and FREP and DRI table [31].	AODV	-	Small Communication overhead (2 to 3 %) of RREQ.	Throughput up to 51%.
DCM [32].	AODV	NS-2	More overhead than AODV.	Detection rate is above than 98% & improvement in PDR.
Hash Based [33].	DSR	-	-	No simulation result.
Hash & MAC Based PRF Scheme [34].	AODV	NS-2	The malicious node able to forge Fake reply.	PDR is higher than 92%.
RIP & BBN [35].	AODV	-	-	No Simulation
BDSR [36].	DSR	QualNet	More overhead but lower than WD Approach	PDR Is always more than 91%.

3. CHALLENGES IN MOBILE AD-HOC NETWORK:

MANET is a lot different from the conventional networks. It provides a great deal of flexibility the topology, infrastructure, size and state of the network. This flexibility tends to be more challenging to be handled. Mobility of nodes, limited power and bandwidth, providing Quality of Service are some of the most obvious challenges associated with MANET [6].

a) **Mobility:** MANET provides freedom to the devices to easily move in any direction. It allows the nodes to create, enter or exit the network anytime anywhere. Mobility facilitates the devices; however, it makes it challenging to work with MANET. High mobility leads to the frequent link breakage which generates difficulty in routing as any node which is the part of transmission route may change its position or even leave the network any time.

b) **Power and Bandwidth:** Mobile devices come with limited power as it relies on batteries. They also face the problem of limited bandwidth. Because of it, MANET needs to have a very efficient routing algorithm for determining the optimal paths so that packets can be transmitted with minimum power and bandwidth consumption.

c) **Quality of Service:** QoS is the problem which makes the MANET more challenging area. MANET is a wireless network and in comparison, to wired links, wireless links experience more data loss, distortion, delays and variation in speed and capacity which makes it difficult to guarantee the quality of service. As MANET follows dynamic topology, it's very difficult to have accurate information about the state of network and devices and it becomes even more challenging to provide the QoS.

d) **Security:** For any network security is the main concern and it becomes more challenging when it comes to MANET. MANET allows anyone to move freely in or out of the network and devices communicate with each other in open space which exposes the network activities to the attackers

.

4. SECURITY THREATS IN AD-HOC NETWORK

Threats in ad hoc network are explained with the help of threat models that can be further classified in following categories [4]:

4.1 Ad-Hoc Network Routing Threats:

Routing threats are the most generic threats to a system. Here are most common requirements that a network system must hold:

- **Confidentiality -** Confidentiality guarantees that the information or routing data will not be accessed by an unauthorized node. Therefore, threat to confidentiality means that the routing information has been compromised.
- **Integrity-** All the nodes within the network should have correct routing information which can only be accomplished if they follow the correct routing procedure. If the routing data has been altered, updated or deleted, it means there is threat to integrity.
- **Availability-** If a node demands for the routing information it must get access to it, without any additional delay and regardless of the state of the network.
- **Authorization**- Only the authorized nodes are allowed to access the routing data whereas the unauthorized are not involved in the routing protocol. This property is one of the most important as it provide access control services to the nodes.
- **Dependability and reliability-** As Ad hoc networks was initially developed for emergency situations like war or natural disaster where the use of centralized network is not feasible therefore reliability is one of the important concern. Hence, emergency procedures are required so the protocols never fail in situation like heavy network load or routing table get filled due to memory constraints or any other constraints which leads to failure.
- **Accountability-** Each action should be lodged as it will be required for appropriate reaction against attacks as well as in case of non-repudiation.

There are two categories of threats

4.1.1. External Threats:

External attacks are accomplished by entities which are outside of the network or by nodes which are not authorized. These attacks generally threaten the lower layers i.e. physical and data link layer. As, in Ad hoc network the nodes inherit the mobile nature it is intrinsically difficult to secure this layer. These threats can be further classified in following categories based on their action:

Passive attacks-Passive eavesdropping is a technique where an unauthorized node silently listens the network traffic, even the route updates. It gathers the data and other information which can be used to threaten the network by interfering the topology, knowing the geographical location of the nodes and identifying the heavily used nodes.

Active attacks-Unlike passive, these attacks are designed to disrupt the network by sending signals or data. Denial of service attack is one of the major active attacks causing the communication channel to be blocked.

4.1.2. Internal Threats:

These threats are not easily detected as the nodes are integral part of the network and they are authorized within the ad hoc network i.e. they arise from the trusted sources. Based on their behavior they are categorized in four group- Failed nodes, badly failed nodes, selfish nodes and malicious nodes.

Failed nodes- A node is said to be a failed node if they are not able to perform an operation such as forwarding data packets or routing information.

Badly failed nodes- A node which does exhibit the properties of failed nodes along with it having an additional feature of sending the false information within the correct formatted packet is termed to be badly failed nodes.

Selfish nodes- These nodes participate in the network for their own benefit i.e. for enhancing their performance or for saving resources and if they find that their personal cost is involved they start behaving as the failed nodes. These nodes actually start dropping the packet which is almost difficult to detect by most of the routing protocols.

Malicious Nodes- Malicious nodes intentionally aim to interrupt the operation of routing protocol, by denying their services. They may accommodate feature of any of the failed nodes. It is highly menacing if it is the only node acting as a link through which the destination could be reached or if it is acting as a link between two networks.

5. ATTACKS IN MANET

MANETs are more susceptible to security attacks than any other conventional network. Features such as mobility and open communication are widely being exploited by attackers. It is necessary to understand the possible attacks in order to develop a robust solution as it is explained in previous section; attacks can be classified as active and passive attack or external and internal attacks**[13][14][15]**. Usually each attack targets a specific layer of network model. Some possible attacks at different network layers are as follows:

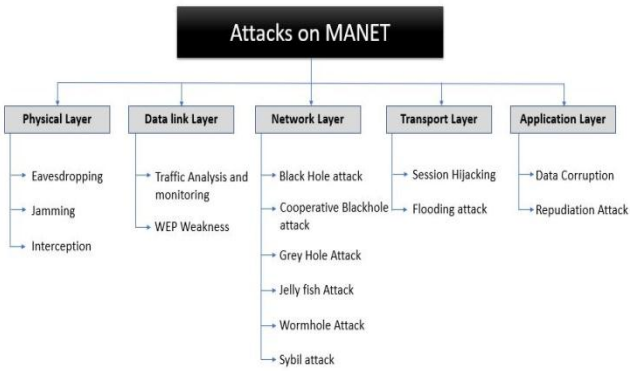

Figure 1: *Attacks on different layers of Ad Hoc Network*

Table 2: *Security Attacks and Solutions on each Layer in MANET [1][23][52].*

Layers	Attacks	Security Issues	Solution
Application layer	Data corruption and Repudiation.	Detecting and Preventions of Malicious Codes viruses and Worms.	Intrusion Detection System(IDS),Firewalls and Adequate security solution etc.
Transport layer	Session Hijacking, Traffic analysis, monitoring, SYN Flooding.	Authentication and securing end-to-end communication.	Adequate security solution use of public & Private key cryptography (SSL, TLS) etc.
Network layer	Grayhole,Wormhole, Jellyfish,Blackhole,Flooding,Resource consumption, location disclosure attacks	Protection of the Adhoc routing, IP spoofing and forwarding protocols	No such a effective solution for Source authentication and message integrity method to prevent the packet interception and routing message modification, there are some Securing routing ip spoofing protocols (e.g. IPsec, ESP, SAR, ARAN) to overcome the effect of blackhole attack, impersonation attacks, jelly fish attack and Wormhole attack etc.
Datalink layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP,WPA weakness	Protection of wireless MAC protocol securing node to node communication and providing link layer security support	No such a effective solution to Secure traffic analysis and traffic Monitoring, secure link layer protocol like LLSP, using WEP, WPA, WPA2etc.
Physical layer	Eavesdropping, Jamming, Interceptions	Preventing signal jamming denial-of-service attacks	To secure signal jamming by using Spread spectrum Mechanisms e.g. FHSS, DSSS etc.

5.1 Physical Layer Attacks [7]:

Eavesdropping: It is a technique of secretly capturing the data packets from the network without any consent of sender or receiver with the aim to steal the confidential information. It is a passive attack which simply means the capturing of data by the node other than the appropriate destination.

Eavesdropping is possible in MANET because all the channels are wireless and can be accessed by anyone.

Jamming: In this attack, a jammer transmits the radio signals to disrupt the flow of information. Jammer continuously emits the strong signals (random noise and pulse) which block the valid traffic in network. Jamming is an active DoS attack which prevents the destination to receive the proper information by making the packet lost or corrupted.

Interception: Attacker can easily intercept the data packets in MANET due to the communication in open space. Interception can either be active or passive. Attacker can get the access to routing messages and may examine or refine the packets before sending to next hop. Intruder can also transmit the fake messages to further nodes in the route.

5.2 Data Link Layer Attacks:

Traffic Analysis and monitoring: Traffic monitoring is the process of observing the network activities to gather the information such as states and location of nodes, network topology, traffic pattern, information about source and destination, etc. This information can further be analysed to extract the confidential data that can be used to lunch various potential attacks by a malicious node.

WEP Weakness: WEP is a security algorithm incorporated as a privacy component in the original IEEE 802.11 standard. It insures the integrity by using CRC32 checksum. It also provides data confidentiality with the use of stream cipher RC4. WEP has various flaws such as:

- WEP faces key management problem. Same key should not be used twice or for a long time even if you keep the key long enough, attacker can grab the frames to crack it.
- An attacker can easily perform the analytic attack and recover the key by analyzing relatively small amount of traffic because initialization vector is sent as plane text with RC4 encryption key.
- Initialization vector (IVs) is a 24-bit value that is used with secret key as a plane text. The problem is that the 802.11 protocol doesn't provide any specification to implement IVs.

5.3 Network Layer Attacks:

5.3.1 Black Hole attack: Black hole attack is analogous to the black hole (dead star) which absorbs the matter and energy in the similar way, a malicious node drops the data packets transmitting through it. This attack utilizes the drawback of route discovery phase of reactive routing protocols by sending a quick fake route reply message, challenging that it has the shortest and fastest route to reach the destination although it won't be having any path to the destination. In the following fig. the Source node(S) broadcast the route request packet to find the shortest and fastest way to reach the destination node (D). The Malicious node (M) on receiving the RREQ packet, immediately transmits the fake RREP packet to the source node in order to pretend that it has the shortest path to reach the destination. When source node receives this forged RREP packet it discards other RREP packet and start transmitting data packets which will be further dropped by the node M once it receives them[2].

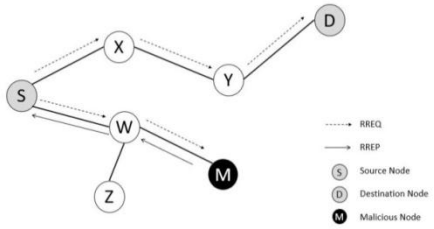

Figure 2: *Black Hole Attack*

Cooperative Black Hole attack: Cooperative black hole attack is the extension of black hole attack in which more than one node will be participating to disrupt the communication. In black hole attack if somehow, we are able to contact the immediate node occurring after the malicious node and find the answer of are queries that are whether it has a route to the malicious node and the route to the destination then we can easily judge whether the node is malicious or not. But, if the immediate node is also the malicious node then this security mechanism may compromise. For example, suppose the malicious node (M1) cooperates with another malicious node (M2) as shown in fig 3. Through some intrusion detection system it is predicted that the M1 is compromising the data packet, so to affirm this the source node(S) will transmit the route query packet to the next immediate node(which in this case is M2) and ask it whether it has any route to the node M1 and to the destination. As, M2 is participating with M1 it will reply "Yes" in both the cases hence, the network will compromise.

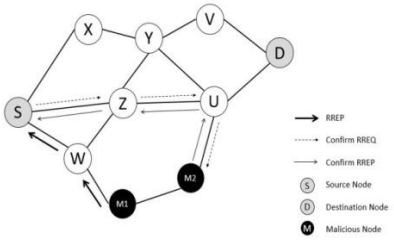

Figure 3: *Co-operative Black hole Attack*

5.3.2 Grey Hole Attack: Grey Hole attack also drops the data packet as the black hole does but, it has quite different behaviour. In this attack the malicious node behaves normally in the route discovery phase i.e. it doesn't perform any malevolent activity when route request or route reply packet are being transmitted through it but as soon as it receives the data packets it starts dropping them. The behaviour of Grey-hole attack can be characterised as:

1. The malicious node drops all the data packets which are passing through it.
2. It drops the data packets which are being transmitted from some specific source.
3. It drops only those data packets which are to be delivered to some specific destination.
4. Drops the data packets at some specific instance of time while behave normal at other instances.

Due to this unpredictable behaviour of Grey Hole attack it is quite hard to detect these attacks.

5.3.3 Jelly Fish Attack: Jellyfish is characterised as a passive attack in which instead of dropping the packets it either delays them or muddle the order of packets to degrade the quality of service (QoS). The main motive behind scrambling the packet is to degrade the network throughput and to drain the network performance. It's very difficult to detect this attack because it completely follows the routing protocols. This attack can have following features:

1. The attacker can store the packets in a buffer for some period of time and then transmit it; this will increase the networks latency.
2. The attacking node can capture the node and send them in scramble order. Since, the order of the packets received at the destination is mis-matched it causes delay to rearrange them.

5.3.4 Worm Hole Attack: Wormhole attack is one of the most intense and sophisticated attacks on MANET. A wormhole can be defined as a route between two conspiring attackers. This route fakes to be shorter than the original one within the network which causes the failure of routing mechanism. This route can be established by via a wired link or a high frequency link between two nodes. An attacker captures the packets at one location and transmits it to another. This node may selectively or completely drop the packets or re-distribute them back in the network. It can also disrupt the routing by tunnelling the routing control messages [16] [17]. Any kind of encryption cannot be helpful because attacker does not need to have the information of packet's content to perform the attack.

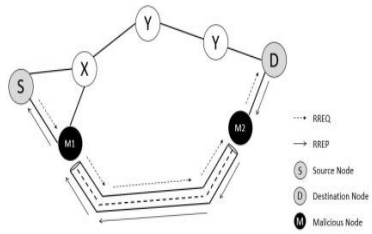

Figure 4: *Wormhole Attack*

5.3.5 Sybil Attack [9]: Sybil attack can be considered as a spoofing attack where a malicious node spoofs the identity of other legitimate nodes within the network. In this attack the node that steals the identity of legitimate node is called malicious node or Sybil attacker while the node whose identity was stolen is known to be Sybil node. Since, the Sybil attacker can have identities of multiple nodes it can easily misguide legitimate node and can receive all the messages that are originally being transmitted to the victimised node.

Different forms of Sybil attack can be represented in three dimensions:

Dimension I: Direct and Indirect Communication

Direct communication is the scenario where a legitimate node directly communicates with the Sybil node. Malicious node gets all the packets and information from this Sybil node without any concern of sender. All the messages sent by the Sybil node that the legitimate node receives are also actually sent by the malicious node. In indirect communication, one or more malicious nodes come in between the sender and Sybil node and sender and pretend that they are passing all the received packet to the Sybil node but actually they are not.

Dimension II: Fabricated and Stolen Identity

A Sybil attacker can either fabricate new arbitrary identities whose identification is compatible with the identification of valid nodes or it can steal the identity of a legitimate node and can assign it to Sybil node.

Dimension III: Simultaneous and Non-Simultaneous:

In simultaneous use of all the identities, attacker cycles through the identities so frequently that they seem to be used at the same time. In non-simultaneous use, attacker uses the same number of identities one after another over a period of time.

5.4 Transport Layer Attacks:

5.4.1 Session Hijacking: In this attack the attacker basically hijacks the session by declaring itself as an authenticated user. Since, a user is only authenticated at the beginning of the session; the attacker may take benefit of this and hijack the session. The attacker actually spoofs the IP address of the user's machine and determines its sequence number after which it generates a high traffic for the victim node; through which it get the full control over the session. The session hijacking is further classified in three groups:

Active Session Hijacking: In this attack, it takes full control over the session by completely dropping the connection between the server and client. In active session hijacking the attacker drops the connection by performing Denial of service attack at any of the one end and completely obsoleting it from the session. After which it communicates with the server by predicting itself to be the authenticated user.

Passive Session Hijacking: It is almost analogous to the Active session hijacking the only difference is instead obsoleting the user from the session; it monitors the traffic between them.

Hybrid Session Hijacking: The Hybrid session hijacking is the combination of active and passive session hijacking. In this attack, the attacker first listen the traffic until it finds

something useful from it and finally performing the attack by replacing itself with the client.

5.4.2 Flooding attack: Flooding attack is basically made with the intension to degrade the network performance. In this attack the attacker either aims to squander the resources such as battery power and computational unit, or it aims to exhausts the resources such as bandwidth by flooding the network with useless packets. For example, a malicious node can repetitively broadcast a route request packet for the node which actually doesn't exist in the network. Since, the destination node does not exist the packet will be aimlessly flooded within the network, increasing the network traffic as well as consuming the bandwidth and battery power. Flooding attack may also lead to Denial of Service if they are not timely-checked.

5.5 Application Layer Attacks:

5.5.1 Data Corruption: Application layer is the closest layer to the end users and thus provides the opportunity to perform widest range of attacks. Networks are being widely spread by malicious code. This layer provides the widest surface to attackers to perform various types of malicious codes on the nodes in network which results in data corruption or sometimes failure of the entire application. These malicious codes can be viruses, worms, Trojan horse etc. They do not affect only the application or programs but may harm the operating system too.

Viruses are the malicious programs which attach itself to an executable file or program and infect the system or data when user runs that file. It can easily be spread by sharing or mailing those files but cannot harm the system until the user run or open that file.

Worm is a subclass of virus which has the ability to replicate itself and it can send itself to others without any human intervention by using information transport feature of the system. Because of replicating itself, it may also consume a very large amount of system memory. These abilities make it more dangerous.

Trojan horse is more than just a malicious code. It's seems to be a useful software received from a legitimate source when downloaded. When you open or run it then only it makes damage to the system and its effects may vary. It neither replicates itself nor infects the files. They can delete the files, destroy the information and even can provide the access to your system to the attackers by creating the backdoor.

5.5.2 Repudiation Attack: In repudiation attack, a malicious or selfish node denies its participation in data transmission by manipulating the entries stored in the log files. Installing firewalls and end-to-end encryption is not enough to solve this problem. Digital signature is one of the techniques that can be used to ensure nonrepudiation.

Table 3: *Summary of Various Attacks and Proposed Mechanism* [51].

Attacks	Brief Explanation	Methods Recommended	Routing Protocol
Black-hole Attack	In this attack ,attacker drops all forwarded packets	1. Path based techniques to detect and prevent the attack [38]. 2. Two stage approach, in first stage detection of suspected nodes and in second stage isolation of malicious nodes [39]. 3. Verification of control message sent by malicious node and detection of attacks [40]	1.DSR Ad-Hoc Routing Protocol 2.AODV, DSR Ad-Hoc Routing Protocol 3. OLSR Ad Hoc Routing Protocol
Wormhole Attack	Attacker replays the packet	1. Cooperative approach Among the multiple nodes to detect & Prevent [41]. 2. Detection & prevention by Digital Signature [42].	1. Any Ad-Hoc routing protocol(AODV,DSR, OLSR) 2.Combined with Ad-Hoc, OLSR
Sink-hole Attack	Malicious node attracts the hole network traffic towards itself after that it can modify or altered the received packets	1. To prevent attack there are three variable (Image Ratio, Sequence Number and Route Add Ratio) implementation [43]. 2. Trust based algorithm to detect and prevent sinkhole attack [45]	1. DSR protocol. 2. On-demand multipart routing protocol.
Flooding Attack	In this attack, attacker floods the network with fake traffic to disturb	1. To controls the attack by introducing a variable RREQ_RATELIMIT ,it limit the number of packets sent into the Network 2. This attack is prevent by delaying the RREP(Route Reply) from destination to the source . Due to this number of packets sent in the network will be reducing [49]. 3. A probabilistic flooding Algorithm used to prevent this attack [50].	1. AODV Ad Hoc Routing Protocol [48]. 2. DSR protocol 3. Any Ad-Hoc routing protocol(AODV,DSR,OLSR)

Masquerade Attack	The attacker accepts the identity of Extra node in the Ad-Hoc network.	Secure public key cryptography Authentication based on the trust model [46].	Any Ad-Hoc routing protocol(AODV,DSR,OLSR)
Route Fabrication	Attacker inserted False routing messages into the network. .	To prevents the route fabrication attack author uses a soft computing and fuzzy logic approach to establish a trust among the nodes[47] .	AODV protocol for the implementation.

6. CONCLUSION AND FUTURE WORK:

From all the above study, we came to know that MANET is facing a lot of challenges specially the security challenges and there no such robust system which can handle this. Even the routing protocols are not sufficient. Security in MANET and network layer issues needs a serious attention. As network layer is not only facing the conventional attacks but also the MANET specific attacks which are not easy to be handled in an open communication environment with existing protocols. Such security mechanism should be developed that can provide the detection & Prevention from malicious nodes while holding all the properties of MANET at the same time.

REFERENCES:

[1] I.Ilyas,"The hand books of Ad hoc Wireless Networks-II series" CRC Press LLC, USA.

[2] B.Kushwaha, P.K. Mishra. Article: Comprehensive Analysis of Ad Hoc Network Routing Protocols. International Journal of Computer Applications 139(3):1-5, April 2016. Published by Foundation of Computer Science (FCS), NY, and USA.

[3] A. Hinds, Michael Ngulube, Shaoying Zhu and Hussain Al-Aqrabi, "A Review of Routing Protocols for mobile Ad-Hoc NETworks (MANET)", International Journal of Information and Education Technology, vol. 3, no. 1, February 2013.

[4] Po-Wah Yau and Chris J. Mitchell," Security Vulnerabilities in Ad Hoc Networks", Mobile VCE Research Group, Information Security Group, Royal Holloway, University of London Egham, Surrey TW20 0EX, UK.

[5] L Raja,S. S. Baboo," An Overview of MANET: Applications, Attacks and Challenges", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue1, January 2014 pg-408-417.

[6] V.Jayalakshmi,T. Abdul Razak, "A Study on Issues and Challenges in Mobile Ad hoc Networks", International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, Issue 9, September 2015.

[7] Aditi, J. K. Singh," Analysis of various security attacks in Mobile Ad Hoc Network", International Research Journal of Engineering and Technology (IRJET), vol.3, issue 7, July 2016.

[8] S. S. Dhenakaran, A. Parvathavarthini, "An overview of Routing Protocols in Mobile Ad-Hoc Network", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, issue 2, February 2013.

[9] S. Sinha, Aditi Paul, Sarit Pal, "The Sybil attack in mobile Ad Hoc Network: Analysis and Detection", Pacific Academy of Higher Education and Research University, Udaipur, India.

[10] A.Bhattacharyya, A.Banerjee, "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques", Department of Computer Science & Engineering, Institute Of Engineering & Management, Saltlake.

[11] C.Sivarammurthy, B.S.Manoj,"Adhoc wireless networks-II edition", Pearson education of India.

[12] Elizabeth M. Royer, Charles E. Perkins," An Implementation Study of the AODV Routing Protocol" IEEE 2000, vol no.7803-6596-8/00.

[13] Jin Taek Kim, Jeong-Ho Kho, Chang-Young Lee, Do-Won Lee, Cheol-Soo Bang, Geuk Lee," A Safe AODV Security Routing Protocol" -International Conference on Convergence and Hybrid Information Technology 2008, IEEE 2008,vol no. 978-0-7695-3328-5/08.

[14] Lidong Zhou Zygmunt J. Haas,"Securing Ad Hoc Networks" IEEE network, special issue on network security, November/December, 1999.

[15] B.Kannhavong, H.Nakayama, Y. Nemoto, N. Kato and A. Jamalipour. A Survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, page 86, 2009

[16] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: ADefense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc. of IEEE Inforcom, 2002.

[17] Ali Ghaffari "Vulnerability and Security of Mobile Ad hoc Networks" proceeding of the 6th WSEAS international conference on simulation, modeling and Optimization, Lisbon, Portugal, September 22-24, 2006.

[18] Toby Xu, Ying Cai," Location safety protection in ad hoc networks", published by Elsevier B.V.-vol no. 1570-8705.

[19] Ying Dong, Tat Wing Chimb, Victor O.K. Li, S.M. Yiu b, C.K. Hui,"ARMR: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks" 2009 Elsevier B.V.-vol .no. 1570-8705.

[20] Patrick P. C. Lee, IEEE, Vishal Misra, and Dan Rubenstein, "Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks", IEEE 2007-vol.no. 1063-6692.

[21] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani," A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE 2008, vol.no-1553-877X/08.

[22] Fei Xing, and Wenye Wang," On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures" -IEEE 2010, vol.no.-1545-5971/10.

[23] E. Gajendran, B.Sarvesan "A Literature Survey on Security Challenges in Mobile Ad Hoc Networks"IJCA,Volume 84,December 2013.

[24] Radha Raman, B.Kushwaha, "Performance Evaluation of AODV, DSDV, OLSR Routing Protocols Using NS-3 Simulator", IJCNIS, Vol.10, No.7, DOI: 10.5815/ijcnis.2018.07.07.

[25] L.Qian a, N. Song, Xiangfang Li b," Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statisticalanalysis approach", 2005 Elsevier, doi:10.1016/j.jnca.2005.07.003.

[26] S.Qazi n, Raad Raad, Yi Mu," Securing DSR against wormhole attacks in multirate ad hoc networks" Elsevier Ltd.http://dx.doi.org/10.1016/j.jnca.2012.12.019.

[27] Su M-Y. "WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks". Computers and Security 2010; 29(2):208–24.

[28] Seung Yi, Prasad N., R. Kravets" A Security-Aware Routing Protocol for Wireless AdHoc Networks", University of Illinois at Urbana-Champaign.

[29] Fan-Hsun Tseng et al," A survey of black hole attacks in wireless mobile ad hoc networks". Human-centric Computing and Information Sciences 2011,http://www.hcis-journal.com/content/1/1/4.

[30] Ramaswamy S, Fu H, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". International Conference on Wireless Networks, Las Vegas, Nevada,USA, 23-26 June 2003.

[31] Weerasinghe H, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: SimulationImplementation and Evaluation", December 2007, Jeju-Island,Korea

[32] Yu CW, "A Distributed and Cooperative Black Hole Node Detection and EliminationMechanism for Ad Hoc Network". PAKDD workshops, Nanjing, China, 22-25 May 2007.

[33] Wang W., Bhargava B.,"Defending against Collaborative Packet Drop Attacks on MANETs. International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009,New York, USA, 27 September 2009.

[34] Min Z,"Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks",International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 16-17 May 2009.

[35] Vishnu K.A, "Detection and Removal of Cooperative Black/Grayhole attack in Mobile Ad Hoc Networks".International Journal of Computer Applications. doi: 10.5120/445-679.

[36] Tsou P-C,"Developing a BDSR Scheme to Avoid Black Hole Attack Basedon Proactive and Reactive Architecture in MANETs".International Conference on AdvancedCommunication Technology, Phoenix Park, Korea, and 13-16 Feb. 2011.

[37] P Agrawal, Ghosh RK.Cooperative Black and Gray Hole Attacks in Mobile Ad hoc Networks. International Conference on Ubiquitous Information Management and Communication, Suwon,Korea, 2008.

[38] J.CAI, P. YI, Jialin et al, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", IEEE International Conference on Advanced Information Networking and Applications (AINA),Perth, Australia, April 20-23, 2010, pp.775-780.

[39] M. Zeshan, S. Khan, A.R. Cheema, Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks",(FITME '08), Leicestershire, UK, Nov. 20. 2008, pp.568-572.

[40] P. Moradiya, S.Sampalli, "Detection and Prevention of Routing Intrusions in Mobile Ad Hoc Networks", 2010 IEEE (EUC), Hong Kong, Dec. 11-13, 2010,pp.542-547.

[41] G. Lee, D. Kim,J.Seo, "An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks", (ISA 2008), April 24-26, 2008, pp.220-225.

[42] P.Sharma, A.Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", (ICCSN), May 27-29 2011, pp.307-311.

[43] B.J.Culpepper, H. Chris Tseng, "Sinkhole Intrusion Indicators in DSR MANETs", Broad Nets 2004, San Jose, USA, Oct. 25-29, 2004, pp. 681- 688.

[44] D.Sheela, "A Non-Cryptographic Method of Sink Hole Attack Detection n Wireless Sensor Networks", (ICRTIT),Chennai, India, June 3-5, 2011, pp.527-532.

[45] T.Thumthawatworn,T.Yeophantong,P.Sirikriengkrai, "Adaptive Sinkhole Detection on Wireless Ad Hoc Networks", IEEE Conference, 2006, USA, 4-11 March 2006,pp.1-10.

[46] E.Ngai, M.Lyu,"Trust and Clustering-Based Authentication Services in Mobile Ad Hoc Networks", Proceedings of International Conference on Distributed Computing Systems, March 23-24, 2004, pp. 582- 587.

[47] H. Hallani,"Trust Assessment in Wireless Ad-hoc Networks", Wireless Days, 2008 (WD '08). Dubai, Nov. 24-27, 2008, pp.1-5.

[48] J. Kataria, P.S. Dhekne, "A Scheme to Control Flooding of Fake Route Requests in Ad-hoc Networks", (CODEC-06).University of Calcutta, December 18-20, 2006, pp. 198-201..

[49] S.Ahmad,I.Awaan, "Performance Analysis of DSR & Extended DSR Protocols",AICMS 08),May 13-15, 2008, pp.191-196.

[50] Y. Sasson,D.Cavin, A. Schiper, "Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks", 2003 IEEE Wireless Communications and Networking, (WCNC 2003), vol.2, March 2003, pp.1124-1130.

[51] H Kayarkar "A survey on security issues in ad hoc routing protocols and their mitigation techniques", arXiv preprint arXiv: 1203.3729, 2012 - arxiv.org.

[52] E.Gajendran, S.Vijayan Article: A Literature Survey on Security Challenges in Mobile Ad Hoc Networks. International Journal of Computer Applications 84(1):1-5, December 2013.