A Survey on Various Routing Protocols and Attacks in Mobile Ad Hoc Network

Vibhu Singh
Master of Engineering,
Computer Science And Engineering
Maharana Pratap College Of technology
Gwalior, India.

Ram Naresh Sharma
Master of Engineering,
Computer Science And Engineering
Maharana Pratap College Of technology
Gwalior, India.

***Abstract*— Wireless communication has become an active research area today with a high level of penetration and uses in the daily life of mobile devices. Mobile MANET's are networks that do not support infrastructure and are limited to network nodes, without infrastructure, Due to the mobility of nodes and also the ability to dynamically join and exit the network. Security is a difficult task and an essential area for research into such a complex and dynamic environment. MANETS have several routing protocols for selecting the best route to transmit messages or information on the smallest and comparatively optimum base. The exchange of information between source and target mode is the most secure and shortest route for these routing based protocols. MANET nodes may be vulnerable to various types of attacks. The comprehensive analysis of routing protocols and attacks on the network has been performed in this paper.**

Keywords—Routing ProtocolOLSR, Mobile Ad Hoc Network, DSR, Attacks, Wormhole Attack, AODV.

I. INTRODUCTION

MANET consists of a series of dynamic and temporary wireless locations without an existing networking infrastructure, such as a baseline. For places that have trouble constructing infrastructure, including battlefields, physical communication networks in the areas of natural disasters, forests and oceans are unnecessary. This MANET node acts as a router for transmitting data packets from one device to another in addition to their host. The route between ad hoc nodes is a multi-hop in ad hoc networks; thus, For intermediate other nodes, network communications are used when direct communication is outside the target network. Ad Hoc is a simple local Wi-Fi mode since no access point is needed. Every host has a sender and receiver for direct communication. A normal network configuration for packets to forward from node to node is used in the routing protocol. [1].

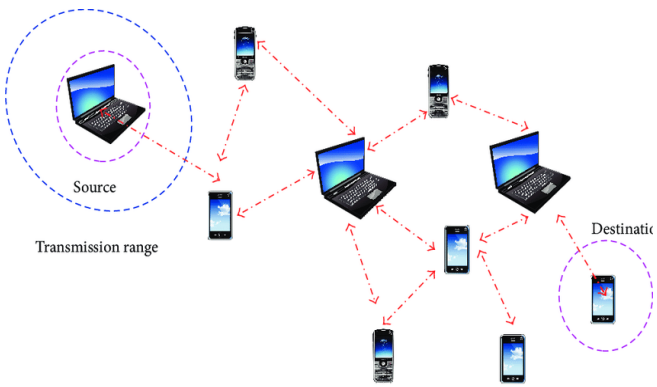

Fig.1. MANET Architecture

The MANET network node is an excursion specifying the route. A MANET network node is an ad-hoc node that constantly affects the MANET network through its evolved functions. As each node is a router free to move, it should be possible for nodes to send easily and efficiently data by the proper MANET network log.

II. SECURITY IN MANETS

There are several important criteria for MANET to ensure the security of the network:

A. Data verification

The receiving node tests the data for consistency or corruption after the authentication of the sender node.

B. Availability

This says that if it is under attack, the network will continue providing service. It uses different approaches without interfering with its process.

C. Authentication

Nodes to be sent should be specific target nodes that respond to the authenticated node message.

D. Integrity of data

The nodes should be valid destination nodes that counter the message transmitted by the authenticated node.

E. Privacy

Unauthorized nodes or users can not access or view the data and information. [10].

III. ROUTING PROTOCOLS

The way between origin and destination nodes is specified, maintained and managed by the routing process. This renders network routing a crucial activity. There are three types of ad hoc protocols for mobile networking, (On-demand) routing,(Constructive) table-driven protocols, and hybrid protocols that have a constructive value. All network target nodes are routed to constructive routing protocol with standard tables. Reactive routing protocols are used to search for roads On demand through the Internet when you ask to pass a packet, the road will be identified. Hybrid protocols are used to check the benefits and inconveniences of both approaches.

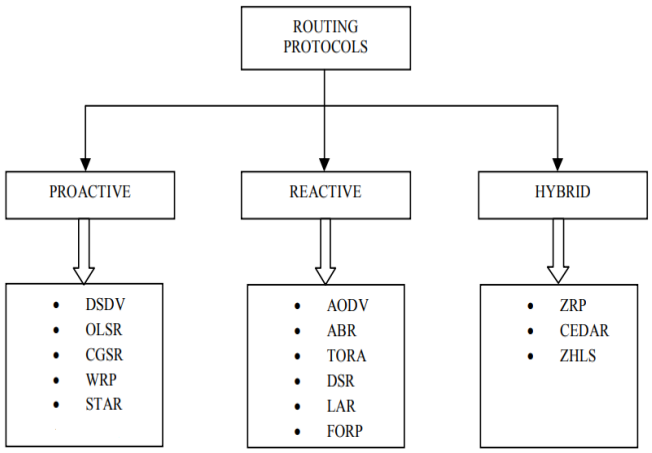

Fig.2. Routing protocol Types

A. Ad Hoc On-Demand Distance Vector AODV

ADV is intended for use which ad hoc networks of thousands or thousands of mobile nodes. The Ad-hOC Vector is designed to be used. The main goal of the protocol is to adapt to changing network connection conditions rapidly and dynamically, find routes to help avoid bandwidth loss and minimize the memory and process consumption of router nodes.

The AODV works on demand, so it is only searching for routes if a path discovery mechanism is necessary That node only has details on the next routing table hop, The message for which the destination must be sent. The next-hop will be verified on the router table and the message will be sent to the j node if k nodes send a message. If j is not the target node, then until a message is sent the cycle will be repeated. The process of discovery is done if the source does not hit the destination you want.

Figure 2 indicates RREQ and RREP in the AODV protocol. This route is hopped by hop from source to destination.

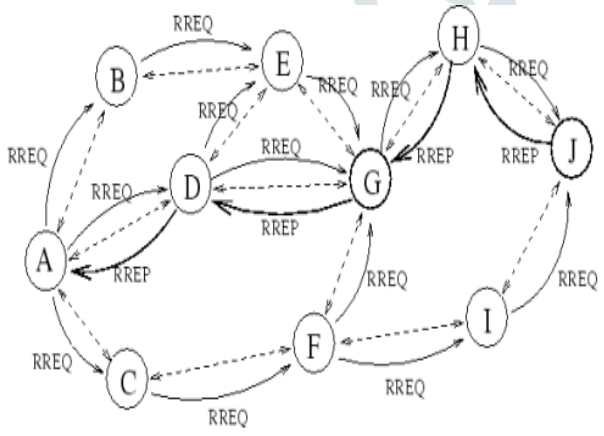

Fig.3. RREQ & RREP in AODV

1. Route Discovering

AODV uses messages such as route request(RREQ) and route reply(RREP) to create routes. If the originating node will send an unknown Node a data message, an RREQ will be sent via the Network. The nodes receiving the message update their routing tables, add a source entry and send the message to the RREQ node. If you have conventional an existing message, the message is discarded A RREQ node will send the source an RREP, whether it is the destination or not or whether the destination is known The nodes control the RREQ origin and broadcast recognition. The nodes update their route tables to provide a link to a node just sent to RREP, for the initial RREQ source, provided that an RREP message must be sent to sent to the source. When the source node receives RREP, a data packet is only redirected to the destination by the message sent to the RREP node.

2. Route Maintenance

Displacement of a node may refer to a connection failure, In that case, the error node sends a route error message (RERR) at the root and tells the route about link failure. If the route is used, the path position process is restarted. [2].

B. OLSR

Optimized Link State Routing Protocol Protocol, construction table protocol, chooses a group of neighbors as a multi-point relay in each node in the network. It includes the OLSR protocol. This MPR strategy is used to min overhead network control messages and create the way to any network target from the source node; only MPR nodes send overflow messages during the flood cycle. The type of messages defined in OLSR is HELLO, TC, MID, and HNA. Messages. HELLO, a message is used for the identification of neighbor nodes that have symmetrical and direct connections, specifying a list of neighboring 1-hop addresses and a list of neighboring 1-hop nodes chosen for the MPR. Each MPR node produces and transmits messages from Topology Control (TC) for its neighbors. Such messages are used to create topology data for each network node and to calculate the routing table for packets.

C. Dynamic Source Routing (DSR)

In addition, DSR is one of the few usable AODV routing protocols. DSR has a variety of AODV pathways. RREP, RREQ, and RRER packages are used to associate routes through Route Discovery and Route Maintenance DSR. One thing that varies from AODV is the collection of DSR routes based on the source node. A default messaging feature such as AODV does not have a DSR. For all network routing information, DSR is equipped with a Cache Memory function. The cache memory simplifies the network recovery process when the network topology suddenly changes. When topology changes, DSR no longer has to identify routes. The routing data route in the cache must only be recognized by means of DSR. The DSR route search mechanism is almost identical to AODV, That means, if the source node wants to send data, the RREQ packet is converted to its nearest node, without having information about the route it will be passed The sent RREQ package includes the address and destination of the sender. The RREQ packet nodes must store information about the route in memory of the cache. When a website has been identified, the node must send the RREP packet to its original route. The RREP packet is sent via the reverse section line generated by sending the RREQ packet. DSR protocol includes several routes and minimizes the road maintenance cycle which should normally be conducted continuously. Nonetheless, the protocol can not handle too much network responsibility by using the cache in route space [1].

D. Comparison of AODV, OLSR and DSR:

Protocol	Protocol Type	Control Message	Metric	Scalable
AODV	Reactive	PREQ, RREP, RERR	Shortest Path	Yes
OLSR	Proactive	HELLO, TC	Cost	No
DSR	Reactive	PREQ, RREP, RERR	Shortest Path	No

IV. ATTACKS IN MANET

It is indeed a difficult issue to secure wireless ad-hoc networks. In developing good security strategies the first step is to always consider the potential type of attacks. Secure communication in MANET is extremely necessary for the safe transmission of information. The existence of a central control system and a wireless communication channel makes MANET more vulnerable than a wired network to physical and/or cyber-attack. These attacks can be classified into two categories:

1. Attack External: It does not consist of network nodes. As a result, the routing information or services that are not available are congested.

2. Attack Internal: These are the nodes that are compromised within the network. The internal intrusion aims for identity theft and describes the network's contagious node as an actual node. Traffic between other nodes can be analyzed and you contribute to other network activities [3].

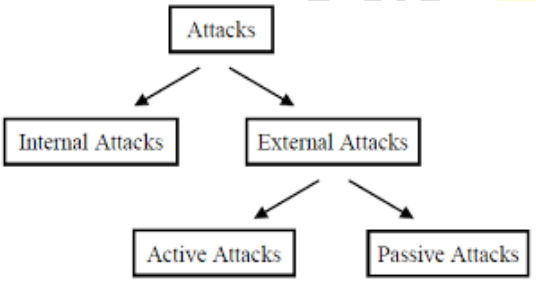

Fig.4. Types of Attacks

The attack classification may be done at the start of the attack. The classification could be as followed:

A. Blackhole attack

A zero metric for all stations around the attacker will be released, which will allow routing of the data packets. A bad node transmits false data routes that it can redirect data packets to a better node and other successful nodes. Instead of typically transmitting such packets, a malicious node loses all packets received (absorbs). An intruder listens in a flood based protocol to the demands of other nodes. Black holes apply to areas in the network that secretly discards (or drops) the visitors in or out of the web, without the source node being informed that the information did not reach their intended recipient. The source code. Certainly, black holes are invisible and can only be observed when travelers are monitored. Attackers embed themselves in the way of their original source-by-destination in a black hole attack with the help of sending a fake REP with the higher sequence number which makes it more accessible. The source then can be captured by malicious nodes to create a direction and reject all other directions. After that, the attacker honestly loses all of these packets when transmitting statistical packets to the destination and therefore can not even receive a whole piece of information. Attacks by the Black Hole are classified in class.:

i. Single Black hole attack

Only one node is act as a malicious node in a single region in a black hole attack. This is termed also a single Black Hole node attack.

ii. Black Hole Collaborative Attack

More than one node in the community acts as a malicious knot in a Black Hole Collaborative Attack. The Black Hole Attack has several malicious nodes.

B. Gray hole attack

The Grayhole attack is an expanded assault of a black hole and is unpredictable for the behavior of malicious nodes. Three forms of gray hole attacks occur: *f*

- The malicious node can only extract packets from a given source or meaning.
- Some time a node may be malicious, but later, it operates as other nodes. *f*
- Combining the two previous assaults.

Malicious Gray-hole node is participating in route discovery and is used as the shortest path to update the source route cache/routing table Source subsequently still considers malicious nodes to be The following packet hop node Malignant node takes all incoming packets, and unanticipatedly falls. The whole phenomenon produces resilience against the process of detection and avoidance as it is harder as nodes will partly drop packaging because of its malicious intent but also because of pressure, congestion or natural selfishness.

C. Wormhole attack

Two malicious nodes connected to the high bandwidth tunnel via a low latency communication channel, are required for attacking Wormhole. Those roads (tunnels) by attackers to the target are known as high quality. Therefore, neighboring nodes pursue these in their contact routes and their data are analyzed by opponents. The collection of packets activates packets to the opposite end (wired or wireless) by the tunnel. The attack in Wormhole is rendered by different techniques. To order for encapsulation to happen, A range of links between two malicious nodes is needed. The packets are encapsulated to order to prevent real jumps during the journey. Hop number for selecting routes is therefore used to use routing processes sensitive to this type of attack. For instance, If a malicious node is identified in the AODV Protocol RREQ, it is transferable into the nearby malicious Node and RREQ is sent to the next Node. The second node's neighbors then move through the second node and take valid paths at different times. Only one malicious node for high power transmission can be connected for Wormhole. for high power transmission. The other nodes obtained by the RREQ must be sent to the destination by transmitting the RREQ via a malicious node. This approach makes the malicious node more likely to be found in paths between source and destination.

D. Sybil attack

The attack by Sybil is brought about through the malicious node which creates false identities from further nodes, called Sybil nodes, and acts as a group of nodes. Sybil's identities either are obtained by theft another valid node or by creating a new identity. Different effect of the Sybil attacks: *f*

- Inequitable distribution among network nodes of resources, *f*
- Votes with false results (due to the presence of duplicate identities),
- Damage geographic routing schemes & node location (in various network locations), *f*
- The complexity of recognizing a node of bad behavior.

E. Jellyfish attack

The attacker node attempts to access the network with this type of attack. If a network node is accessed by the attacker, it starts to undergo unnecessary network delays, i.e. once a packet is received by the attacker node packets are sent after a delay that causes high end-to-end delays in the intruders and changes performance.

F. Denial of service

In that kind of attack, an attacker simultaneously sends millions of packets or useless traffic to a server and attempts to slow down the server or make the resources unavailables to the user.

G. Replay attack

In a MANET, due to frequent node mobility, the topology of the network is unstable. There will be no topology for the current network in a second. The malignant node reproduces and eventually injects old current control messets (TC messages in the OLSR protocol) into the network throughout the replay attack. Such messages are then obtained and updated according to this expired information in the routing tables of the nodes. This replay attack can be used to route recognition fraud, destructive operations or requested information from a repeated packet. [4].

V. Literature Survey

In this paper, we stared at[5] Two major Black Hole routing protocols, the AODV and the Optimized Link State Routing (OLSR) protocol. We used four metrics to determine how the black hole-attack affects the performances of routing protocols for comparing efficiency with percent performance, packet transmission levels, end-to-end delays, and pack-to-lost protocols.

This paper[6] discusses how to detect and avoid a wormhole attack using the AODV routing protocol in WLAN based ad-hoc mobile networks (MANET). During this attack, the mobile nodes of the attackers hold the packet at another stage on a network and transfer it to another node of mobile attackers. This study is conducted in a software Network Simulator (NS2). The AODv Routing Protocol is the basis for Mobile Adhoc WiMAX, which requires performance parameters such as the output, the delay and the packet transmission rates in order to evaluate the built-in Adhoc mobile system.

In this paper[7], we are proposing a new solution in a secure, protected MANET data transmission in the event of possible blackhole attacks based on the AOMDV protocol and homomorphic protection encryption framework. The network output proposed is stable, but malicious nodes that have been introduced into the network weaken AOMDV. The simulation results show the improved packet propagation and network efficiency in the case of blackhole knots in the proposed system.

This paper[8] provides a hybrid approach for the identification and prevention of wormholes in ad hoc mobile networks. AODVWP designed to use the technique of hybrid positioning based on dynamic wormhole detection and prevention, the adjacent node and the hop number process. The benefit of two different predefined methods is contained in this system.

We introduced in this paper[9] a technique called the EPPN for detecting and mitigating the effect of a wormhole attack. A simple hop count model builds on the EPPN technique. EPPN also uses the idea of a primary product number to aid in the identification of wormholes. A corresponding safety analysis shows the reliability of the system in the event of attacks by wormholes. A safety protocol to ensure malicious nodes in a MANET is therefore suggested, as anticipated.

In this paper[11], the technique for enhancing wormhole attack detection (SWAD) in the MANET is proposed. There is no criterion for the identification of the wormholes in this proposed technique. In order to identify the wormhole link the technology proposed uses two threshold values to equate them to the delayed end-to-end time of two nodes with the path of the suspected node, namely, the wormhole node. If the suspected node has high delays and less size, the source node detects the wormhole connection via the network. Finally, the results of the simulation show that the proposed ISWAD technique is capable of detecting any wormhole connections as well as enhancing performance in terms of throughput, delays in end-to-end, etc.

VI. Conclusion

MANET has become more common in examine as well as industry. Due to its ad hoc existence, this is simple to use because of the lack of fixed infrastructure, the flexibility of its modules, the lack of a central routing entity. Nonetheless, MANETs are vulnerable to a number of vulnerabilities, MANETs physical protection, including battery power, Nodes, and limited memory capacity. In this paper, For some security issues, we surveyed the different MANET attacks. Because in contrast with conventional networks, MANET has higher security needs. A robust security solution to counter attacks of this kind is important. To do so, evaluate the several malicious node actions in the communication channel to determine what they need to do.

References

[1] Ida Nurcahyani, Helmi Hartadi, Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET), International Symposium on Electronics and Smart Devices (ISESD), 2018.

[2] Joilson Alves Junior and Emilio C. G. Wille, “Routing in Vehicular Ad Hoc Networks: Main Characteristics and Tendencies,” Journal of Computer Networks and Communications, vol. 2018, Article ID 1302123, 10 pages, 2018. https://doi.org/10.1155/2018/1302123.

[3] Neeraj Arya ; Upendra Singh ; Sushma Singh," Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm", Computer, Communication and Control (IC4), 2015 International Conference on, 10-12 Sept. 2015, IEEE page(s) 1 – 5.

[4] Sbai, O., & Elboukhari, M. (2018). Classification of Mobile Ad Hoc Networks Attacks. 2018 IEEE 5th International Congress on Information Science and Technology (CiSt).doi:10.1109/cist.2018.8596391

[5] Nabou, A., Laanaoui, M. D., & Ouzzif, M. (2018). Evaluation of MANET Routing Protocols under Black Hole Attack Using AODV and OLSR in NS3. 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM). doi: 10.1109/wincom.2018.8629603

[6] Ghormare, S. N., Sorte, P. S., & Dorle, S. S. (2018). Detection and Prevention of Wormhole Attack in WiMAX Based Mobile Adhoc Network. 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). doi:10.1109/iceca.2018.8474705

[7] Elmahdi, E., Yoo, S.-M., & Sharshembiev, K. (2018). Securing data forwarding against blackhole attacks in mobile ad hoc networks. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).doi:10.1109/ccwc.2018.8301683

[8] Chouhan, A. S., Sharma, V., Singh, U., & Sharma, R. (2017). A modified AODV protocol to detect and prevent the wormhole usingh using hybrid technique. 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA).doi:10.1109/iceca.2017.8212740

[9] Sharma, S., & Sharma, R. M. (2017). EPPN: Extended Prime Product Number based wormhole DETECTION scheme for MANETs. 2017 11th International Conference on Intelligent Systems and Control (ISCO).doi:10.1109/isco.2017.7855991

[10] Kumar, S., Goyal, M., Goyal, D., & Poonia, R. C. (2017). Routing protocols and security issues in MANET. 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS). doi: 10.1109/ictus.2017.8286119.

[11] Selladevi.M 1 *, Latha Maheswari.T 2 , Duraisamy.S 3, Improved secure aware wormhole attack detection in mobile ad-hoc networks, International Journal of Engineering & Technology, 7 (4) (2018) 3472-3477.