Volume 4, Issue 4, October 2017 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

A Survey on Security Issue in MANET

Khushboo Kushwaha
M. Tech. Research Scholar
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email: khushboo.kushwaha118@gmail.com

Deepak Agrawal
Head of the Department
Department of Computer Science and Engineering
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email:deepakagrawal@takshshila.org

ABSTRACT

The progression in the field of web because of remote systems administration advances. It offers ascend to numerous new applications. In the past of couple of decades, we have seen the progression in remote systems. The rising abilities of cell phones have given another bearing to the web, which diminishes the cost and enable us to utilize foundation remote systems and framework less remote systems (i.e. Portable Ad Hoc Wireless Network). With so many applications that MANETs gives us, there are still a few difficulties that have to overcome.

MANETs being researched by many different organizations and institutes. MANETs utilize the customary TCP/IP structure to provide end-to-end correspondence between hubs. One fascinating exploration range in MANET is directing. Steering in the MANETs is a challenging task and has gotten a huge measure of consideration from explores. Because of absence of a characterized focal expert, securitizing the steering procedure turns into a testing errand in this manner leaving MANETs powerless against assaults, which brings about crumbling in the execution attributes and also brings up a difficult issue check about the unwavering quality of such systems.. In this paper, we give the historical backdrop of MANET, challenges (issues) include in MANET and its a few applications and a diagram of an extensive variety of directing conventions proposed. We likewise give an execution correlation of all directing conventions and propose which conventions may perform best in huge systems. And furthermore the known directing assaults and the proposed counter measures to these assaults in different works.

Keywords:—*MANET, Routing, Routing Protocols, Security, Attacks.*

I. INTRODUCTION

Opposed to the foundation remote systems where every client straightforwardly speaks with an entrance point or base station, a portable specially appointed system, or MANET is a sort of remote impromptu system. It is a self-designing system of portable switches associated by remote connections with no entrance point. Each cell phone in a system is self-governing. The cell phones are allowed to move heedlessly and sort out themselves discretionarily. At the end of the day, specially appointed system don't depend on any settled framework (i.e. the portable specially appointed system is framework less remote system. The Communication in MANET is happen by utilizing multi-bounce ways. Hubs in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, breaking of communication link is very frequent, as nodes are free to move to anywhere. The density of

nodes and the number of nodes are depending on the applications in which we are using MANET.

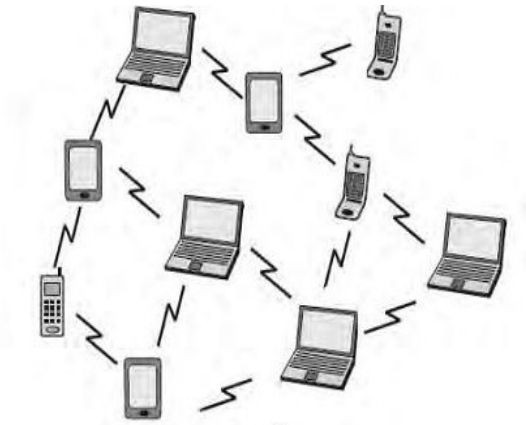

Figure 1: Mobile Ad Hoc Network

II. HISTORY

We can described the life cycle of portable impromptu system into in the first place, second and third generation. Present ad hoc network are considered the third age [2][3]. The original of impromptu system can be followed back to 1970"s. In 1970"s, these are called Packet Radio Network (PRNET) [4]. The Defense Advanced Research Project Agency (DARPA) initiated research of using parcel changed radio correspondence to give solid correspondence between computers and urbanized PRNET. Fundamentally PRNET utilizes the mix of Areal Location of Hazardous Atmospheres (ALOHA) and Carrier Sense Multiple Access (CSMA) for numerous entrance and distance vector routing [5][2][3].The PRNET is then evolved into the Survivable Adaptive Radio Network (SURAN) in the early 1980"s. SURAN provides some benefits by improving the radio performance (making them smaller, cheaper and power thrifty). This SURAN also provides resilience to electronic attacks. Around the same time, United State Department of Defiance (DOD) continued funding for programs such Globe Mobile Information System (GloMo) and Near Term Digital Radio (NTDR). GloMo make use of CSMA/CA and TDMA molds, and provide self- organizing and self-healing network (i.e. ATM over wireless, Satellite Communication Network). The NTDR make use of clustering and link state routing and organized an ad hoc network. NTDR is worn by US Army. This is the only "real" ad hoc network in use. By the growing interest in the ad hoc networks, a various other great developments takes place in 1990"s.The functioning group of MANET is born in Internet Engineering Task Force (IETF) who worked to standardized routing protocols for MANET and gives rise to the development of various mobile devices like PDA"s palmtops, notebooks, etc. Meanwhile the Development of Standard IEEE 802.11 (i.e. WLAN"s) benefited the ad hoc network. Some other standards are also developed that provide benefits to the MANET like Bluetooth and HIPERLAN.

III. MANET CHALLENGES

Regardless of the variety of applications and the long history of mobile ad hoc network, there are still some issues and design challenges that we have to overcome [6]. This is the reason MANET is one of the elementary research field. MANET is a wireless network of mobile nodes, it's a self-organized network. Every device can communicate with every other device i.e. it is also multi hop network.

The scalability is required in MANET as it is used in military communications, because the network grows according to the need, so each mobile device must be capable to handle the intensification of network and to accomplish the task.

MANET is a infrastructure less network, there is no central administration. Each device can communicate with every other device, hence it becomes difficult to detect and manage the faults. In MANET, the mobile devices can move randomly. The use

of this dynamic topology results in route changes, frequent network partitions and possibly packet losses[1].

Each node in the network is autonomous; hence have the equipment for radio interface with different transmission receiving capabilities these results in asymmetric links. MANET uses no router in between.

In network every node acts as a router and can forward packets of data to other nodes to provide information partaking among the mobile nodes. Difficult chore to implement ad hoc addressing scheme, the MAC address of the device is used in the stand alone ad hoc network. However every application is based on TCP/IP and UDP/IP.

IV. ROUTING IN MANET:

Routing is the process of information exchange from one host to the other host in a network."[4]. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc.

4.1 Different Strategies:

Routing protocol for ad-hoc network can be categorized in three strategies.

a) Flat Vs Hierarchical architecture.
b) Pro-active Vs Re-active routing protocol.
c) Hybrid protocols.

4.1.a Flat Vs. Hierarchical Architecture:

Hierarchical network architecture topology consists of multiple layers where top layers are more seen as master of their lower layer nodes. There are cluster of nodes and one gateway node among all clusters has a duty to communicate with the gateway node in other cluster. In this schema there Is a clear distribution of task. Burden of storage of network topology's on gateway nodes, where communicating Different control message is dependent on cluster nodes. But this architecture breaks down when there is single node failure (Gateway node). Gateway nodes become Very critical for successful operation of network. Examples include Zone-based Hierarchical Link State (ZHLS) routing protocol[6]. Where in flat architecture there is no layering of responsibility. Each and every node does follow the same routing algorithm as any other node in the network.

4.1.b. Proactive VsReactive routing protocol in MANET:

4.1.b.1 Proactive Routing Protocol:

In proactive routing scheme every node continuously maintains complete routing information of the network. This is achieved by flooding network periodically with network status information to find out any possible change in network topology. Current routing protocol like Link State Routing (LSR) protocol (open shortest path first) and the Distance Vector Routing Protocol (Bellman-Ford algorithm) are not suitable to be used in mobile environment. Destination Sequenced Distance Vector Routing protocol(DSDV) and Wireless routing protocols were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm. Examples of Proactive Routing Protocols are: [7].

a) Global State Routing(GSR).
b) Hierarchical State Routing (HSR).
c) Destination Sequenced Distance Vector Routing(DSDV).

4.1.b.2 Reactive Routing Protocol:

Every node in this routing protocol maintains information of only active paths to the destination nodes. A route search is needed for every new destination therefore

the communication overhead is reduced at the expense of delay to search the route. Rapidly changing wireless network topology may break active route and cause subsequent route search[6].

Examples of reactive protocols are:

a) Ad hoc On-demand Distance Vector Routing(AODV).
b) Dynamic Source Routing (DSR).
c) Location Aided Routing(LAR).
d) Temporally Ordered Routing Algorithm (TORA).

4.1.c. Hybrid routing protocols in MANET:

There exist a number of routing protocols of globally reactive and locally proactive states. Hybrid routing algorithm is ideal for Zone Based Routing Protocol (ZRP).

V. REACTIVE ROUTING PROTOCOLS:

Reactive routing protocols are more popular set of routing algorithms for mobile computation because of their low bandwidth consumption.

5.1 AODV:

AODV stands for Ad-hoc On Demand Distance Vector. AODV is distance vector type routing where it does not involve nodes to maintain routes to destination that are not on active path. As long as end points are valid AODV does not play its part. Different route messages like Route Request, Route Replies and Route Errors are used to discover and maintain links. UDP/IP is used to receive and get messages.. AODV uses a destination sequence number for each route created by destination node for any request to the nodes. A route with maximum sequence number is selected. To find a new route the source node sends Route Request message to the network till destination is reached or a node with fresh route is found. Then Route Reply is sent back to the source node. The nodes on active route communicate with each other by passing hello messages periodically to its immediate neighbor. If a node does not receive a reply then it deletes the node from its list and sends Route Error to all the members in the active members in the route. AODV does not allow unidirectional link [3]. Finally the animator in any simulation has to be discussed. NAM is used inNS2.

5.2 DSR:

This is an On-demand source routing protocol. In DSR the route paths are discovered after source sends a packet to a destination node in the ad-hoc network. The source node initially does not have a path to the destination when the first packet is sent. The DSR has two functions first is route discovery and the second is route maintenance [5,8].

5.2.1 Different DSR Algorithms:

a) Route discovery.
b) Route maintenance.

Assumptions:

a) X, Y, Z, V and W form ad-hoc network.
b) X is the source node.
c) Z is the destination node.

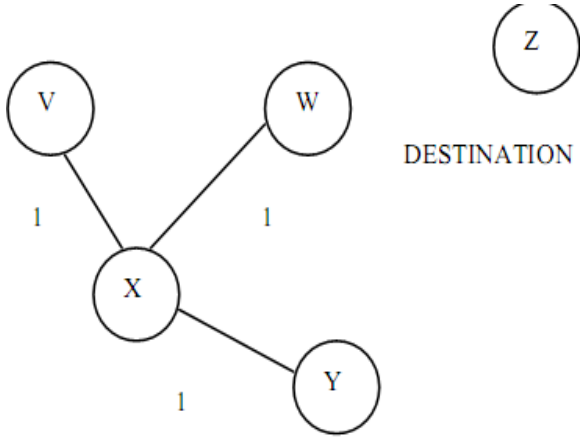

Figure 2: DSR Algorithm Routing Process

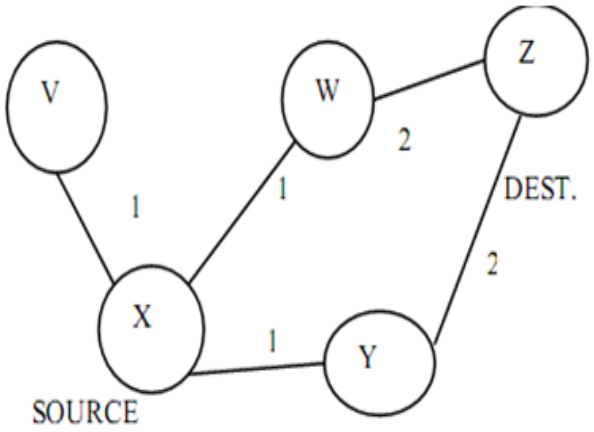

Figure 3: Showing Re-Broadcasting by Nodes V, W, Y.

5.2.2 DSR Watchdogs:

The main function of watchdog is to detect misbehaving nodes. The advantage of this method is that it detects failures not only at link level but also at the forwarding level. This algorithm works good with source routing protocols since the hop-by-hop nature of DSR. Without DSR, the watchdog would not know about a message lost due to a broken link.

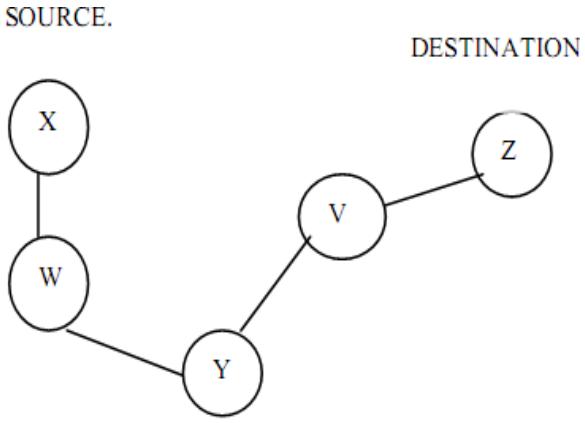

Figure 4: Watchdog Reference

5.2.3 The DSR with Pathrater:

Pathrater decides the route of packets from one node to another in an Ad-hoc network. Pathrater usesknowledge of misbehaving nodes reported by watchdog and also the link reliability data that it is going to maintain for route selection. Each node maintains another node's rating information, termed as metric, depending upon the packet dropping and packet sending to other nodes successfully. The exact path the packet has traversed has to be known by pathrater hence it should be implemented on top of source routing protocol.

5.2.4 Different caching techniques in DSR:

Each mobile host participating in the ad hoc network maintains a route cache in which it caches the source route that it has learned. There are several techniques for a node to learn & store about the route, some of them are as follows.

a) Running network interface in promiscuous mode.

b) Reading the route information from data packets.

c) Reading the routing information from Route Discovery packets.

d) Reading the broken route information from Error packets.

5.3 Location Aided Routing(LAR):

LAR uses the basic flooding algorithm that is defined in DSR with the exception that it uses location information of a particular node to limit the flooding in the network. The location information can be gathered using the Global Positioning System (GPS). Sometimes the GPS might only give the approximate location of a node. Even then the LAR protocol can be used. Using the location information, LAR calculates the expected zone of a particular node.

5.3.1 Expected Zone:

In a MANET, the nodes will be moving. So, the expected zone is the zone in which a particular node is expected to be at that particular instance of time. For example, if

node D is at a location L at time t0 and node D is moving with a speed v. Then at time t1, node D is expected to be in a circular region with radius v (t1-t0) from the location L. If a node S wants to calculate the expected zone of node D, node S should know the location of node D at time t0 and the speed at which the node D is moving. Without knowing any one of these details, node S cannot calculate the expected zone of node D and hence assumes the entire ad hoc network to be the expected zone. The speed can be the average speed, maximum speed or any other measure related to the speed.

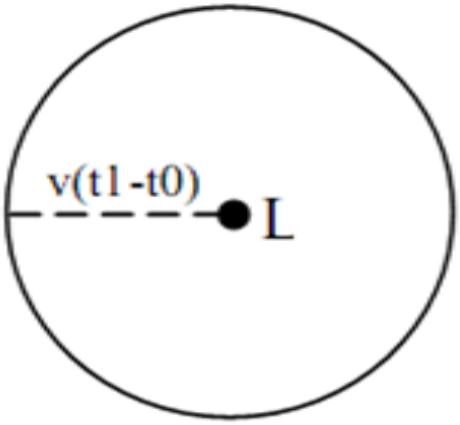

Figure 5. Expected Zone

5.3.2 Request Zone:

LAR limits flooding using the request zone i.e., in LAR, a node forwards a packet if it is in the request zone and discards the packet if it is not in the request zone. For example, if node S needs to find a route to node D. Then node S calculates the request zone and broadcasts the values of the zone along with the packet. A node that is receiving the packet that is sent by S only broadcasts the packet again if it is in the request zone and it is not the intended destination node. A request zone should include the expected zone of the destination and may include other regions because, if a sending node S is not in the expected zone of destination node D, then the request zone should include both S and expected zone of D as follows.

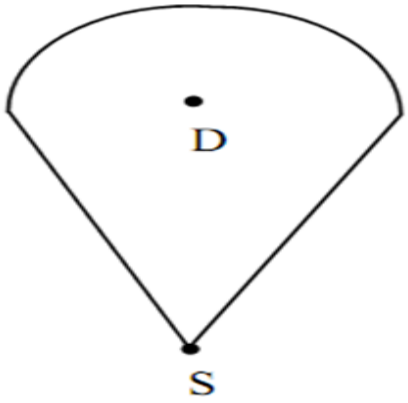

Figure 6: Request Zone [12]

But if none of the other nodes through which the packets have to travel are not in the request zone as above then you may need to expand the request zone.

VI. PROACTIVE ROUTING PROTOCOLS

In proactive routing protocols, each node maintains routing information to every other node (or nodes located in a specific part) in the network. The routing information is usually kept in a number of different tables.

6.1 Destination-sequenced distance vector (DSDV):

The DSDV algorithm [27] is a modification of DBF [3,9], which guarantees loop free routes. It provides a single path to a destination, which is selected using the distance vector shortest path routing algorithm. In order to reduce the amount of overhead transmitted through the network, two types of update packets are used. These are referred to as a "full dump" and "incremental" packets. The full dump packet carries all the available routing information and the incremental packet carries only the information changed since the last full dump. The incremental update messages are sent more frequently than the full dump packets. However, DSDV still introduces large amounts of overhead to the network due to the requirement of the periodic update messages, and the overhead grows according

to OðN2 Þ. Therefore the protocol will not scale in large network since a large portion of the network bandwidth is used in the updating procedures.

6.2 Global state routing (GSR):

The GSR protocol [5] is based on the traditional Link State algorithm. However, GSR has improved the way information is disseminated in Link State algorithm by restricting the update messages between intermediate nodes only. In GSR, each node maintains a link state table based on the up-to-date information received from neighboring nodes, and periodically exchanges its link state information with neighboring nodes only. This has significantly reduced the number of control message transmitted through the network. However, the size of update messages is relatively large, and as the size of the network grows they will get even larger. Therefore, a considerable amount of bandwidth is consumed by these update messages.

6.3 Hierarchical state routing (HSR):

HSR[26] is also based on the traditional Link State algorithm. However, unlike the other link state based algorithm described so far, HSR maintains a hierarchical addressing and topology map. Clustering algorithm such as CGSR can be used to organize the nodes with close proximity into clusters. Each cluster has three types of nodes: a cluster-head node which acts as a local coordinator for each node, Gateway nodes which are nodes that lie in two different clusters, and internal nodes that are all the other nodes in each cluster. All nodes have a unique ID, which is typically the MAC address for each node.

The nodes within each cluster broadcast their link information to each other. In HSR, each node also has a hierarchical ID (HID), which is a sequence of the MAC addresses from the top hierarchy to the source node. For example (see Figure 3) the HID of node 8 is h2; 2; 8i. The HID can be used to send a packet from any source to any destination in the network.

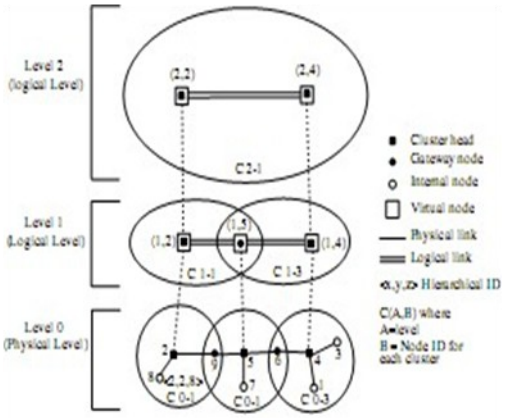

Figure 7: An Example of HSR Topology

VII. Routing Attacks in Manets

All of the steering conventions in MANETs rely upon dynamic participation of hubs to give routing between the hubs and to set up and work the system. The fundamental presumption in such a setup is, to the point that all hubs are well acting and reliable. But in an occasion where at least one of the hubs turn malignant, security assaults can be propelled which may disturb directing operations or make a DOS (Denial of Service)[20] condition in the system. Because of dynamic, disseminated infrastructure less nature of MANETs, and absence of concentrated specialist, the impromptu systems are defenseless against different sorts of assaults. The difficulties to be looked by MANETs are well beyond to those to be faced by the traditional wireless systems. The openness of the remote channel to both the veritable client and assailant make the MANET helpless to both passive eavesdroppers and in addition dynamic malevolent aggressors. The restricted power reinforcement and constrained computational ability of the individual hubs blocks the usage of complex security

calculations and key trade instruments. There is dependably a plausibility of a real trusted hub to be traded off by the assailants and in this manner used to dispatch assaults on the system. Hub portability makes the system topology dynamic forcing frequent networking reconfiguration which creates more chances for attacks. The attacks on MANETs can be categorized as active or passive. In passive attacks the attacker does not send any message, but just listens to the channel. Passive attacks are non-disruptive but are information seeking, which may be critical in the operation of a protocol. Active attacks may either be directed to disrupt the normal operation of a specific node or target the operation of the whole network. A passive attacker listens to the channel and packets containing secret information (e.g., IP addresses, location of nodes, etc.) may be stolen, which violates confidentiality paradigm. In a wireless environment it is normally impossible to detect this attack, as it does not produce any new traffic in the network. The action of an active attacker includes; injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes which violates availability, integrity, authentication, and non repudiation paradigm. Contrary to the passive attacks, active attacks can be detected and eventually avoided by the legitimate nodes that participate in an ad hoc network[21].

VIII. CONCLUSION

MANETs is an emerging technological field and hence is an active area of research. Because of ease of deployment and defined infrastructure less feature these networks find applications in a variety of scenarios ranging from emergency operations and disaster relief to military service and task forces. Providing security in such scenarios is critical. A number of challenges like the Invisible Node Attack remain in the area of routing security of MANETs. Although researchers have composed effective security steering, hopeful methodologies like Fellowship-TEAM-SMRITI [44, 55, 56], CREQ-CREP approach [45] and so forth., which can give a superior tradeoff amongst security and execution, significantly more is yet to be finished. Future research endeavors ought to be centered not just around enhancing the adequacy of the security plots yet in addition on limiting the cost to make them reasonable for a MANET domain. There is increasing use of remote devises. Offers of mobile laptop will beat offers of desktop PCs Receptive protocols are dynamic research area in the field of specially appointed portable system. There are still loads of reenactments to be done in this promising field.

REFERENCE:

[1] G. Aggelou, R. Tafazolli, RDMAR: a bandwidth-efficient routing protocol for mobile ad hoc networks, in: ACM International Workshop on Wireless Mobile Multimedia (WoWMoM), 2015, pp.26–33.

[2] S. Basagni, I. Chlamtac, V.R. Syrotivk, B.A. Woodward, A distance effect algorithm for mobility (DREAM), in: Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom98), Dallas, TX, 2016.

[3] Eichler, Stephan U., “Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC”, Oct. 2016, IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS).

[4] B. Bellur, R.G. Ogier, F.L Templin, Topology broadcast based on reverse-path forwarding routing protocol (tbrpf) in:

[5] Internet Draft, draft-ietf-manet-tbrpf- 06.txt, work in progress, 2015.

[6] T.W. Chen, M. Gerla, Global state routing: a new routing scheme for ad-hoc wireless networks, in: Proceedings of the IEEE ICC,2014.

[7] C.-C. Chiang, Routing in clustered multihop mobile wireless networks with fading channel, in: Proceedings of IEEE SICON, April 2016, pp.197–211.

[8] M.S. Corson, A. Ephremides, A distributed routing algorithm for mobile wireless networks, ACM/ Baltzer Wireless Networks 1 (1) 2015)61–81.

[9] S. Das, C. Perkins, E. Royer, Ad hoc on demand distance vector (AODV) routing, Internet Draft, draft-ietf-manet- aodv-11.txt, work in progress,2014.

[10] R. Dube, C. Rais, K. Wang, S. Tripathi, Signal stability based adaptive routing (ssa) for ad hoc mobile networks, IEEE Personal Communication 4 (1) (2015)36–45.

* * * * *