Collective Study On Security Threats In MANET

Muhammad Zunnurain Hussain, Muhammad Zulkifl Hasan

Abstract: In this paper the authors will be discussing the security issues in MANET & the methods to protect it. Authors will be talk about related work in securing the network, different type of attacks, how to sense these sorts of attack, what are the features of MANET, then will be describing what the requirements for securing network are. Investigation had been done in past to maintain the network from attacks but due to the feature of MANET, inappropriate infrastructure and due to the disperse network quality it is open to attack. Authors will be tackling the defence against each attack. Solution has been suggested, So that the users can use proper authentication techniques and network resources can be properly utilized.

Keywords: Mobile Ad hoc Network MANET, Destination Sequence Distance Vector DSDV, Dynamic Source routing DSR, Ad-hoc on demand distance vector AOD , Truster Mobile Node TrMN, Associated Trusted Mobile Node (ATMn), Trusted Mobile Node (TdMN), Secure temporarily ordered routing Protocol STOP, Cluster based trust aware routing protocol (CBTRP), Intrusion detection system (IDS), Network intrusion detection systems (NIDS), System integrity verifiers (SIV), Log file monitors (LFM).

I. INTRODUCTION

MANETs consist of mobile nodes, which are interconnected by multiple paths or links. A node is randomly directed and organizes by mobile platforms of MANET. The function of node in network can be a router, client and server. Nodes can manage certain features like consumption of power, bandwidth etc. Security Threats in MANET is quite different as compared to conventional networks this is because of the fact that there is no central organization and administration. Non-wired links make the MANET inclined for attacks and hackers can easily access the confidential information, as it is wireless network. Hackers can edit, delete messages, files, and data and even inject virus in network and false information, which is against the network integrity and non-repudiation. The collective study advises the ways that can help in securing the network by placing authentication techniques and many more and future directions in securing the MANET. [2]

II. RELATED WORK

Dynamic research had been done and proposed for MANETs in the past [1]. The Research can be distributed in two parts: proactive and reactive. **In proactive routing**, every node had to maintain routing table, which is up to date as per topology.

In reactive routing, routes are controlled and discovered according to requirements they became inactive when not in use. While studying [3], the up to date routing information is available to each node while maintaining table driven routing protocols. Changes are subject to routing updates**.**

- *Muhammad Zunnurain Hussain, Department of Computer Science, SCET Lahore engrrhusain@gmail.com, Member, IAENG*
- *Muhammad Zulkifl Hasan, Computer Science Dept NUST, NIPCONS, engrrhasan@gmail.com, Member, IAENG*

In Destination Sequenced Distance Vector routing table, every node will keep a routing table that hold all possible destinations and number of hops available in network to them. It is table driven routing protocol based on Bellman ford algorithm.

In Dynamic Source Routing protocol DSR it is a non-wired mesh network routing protocol. The working of protocol is based on source routing where all the routing information is maintained on the mobile nodes having two processes route discovery and maintenance.

Ad-hoc on demand distance vector routing protocol is capable of doing unicast as well as multicast routing. It is a reactive routing protocol. It will direct a route to destination only on demand.

Trust based routing protocol [13], It is divided in two groups of nodes: one is Trusted Mobile Node (TdMN) & second is Truster Mobile Node (TrMN). TdMN are reliable and they are connected with one of the TdMNs which in internally connected and can be known as Associated Trusted Mobile Node (ATMn). Every mobile node uses routing protocol.

Here are following secure routing protocols and their findings given below, this table is drawn after reading [6]:

Protocols	Findings
SAODV	Protocol is able to tackle any sort of attacks like leveraging modification, fabrication or impersonation.
ARAN	Protocol operates on first available route, which is revealed not considering the value of hop count.
SAR	Authentication process guide to increase the operating cost of protocol.
SRP	Protocol has no requirement of defending the hop count in the routing information. Protocol is not capable to protect the infected nodes throwing unwanted information on the network, which can affect overall efficiency of the network.
ENDAIRA & ARIADNE	Considering the limited resources of MANET environment, ENDAIRA is better than ARIANDE.

Another type of routing protocol is STOP **Secure temporarily ordered routing Protocol** ,this protocol operates on less computational & memory problems, & transitational nodes must be having very less duty overall

and having no privilege to change any information during data transfer[12].

III. ROUTING ATTACKS IN MANET

The viral nodes can affect the MANET in certain ways to upset the normal functioning of the network like sending fake messages, wrong routing information and several other information to disrupt the normal network operation.

A. Flooding attacks

The attacker will use the network resources, bandwidth & power to interrupt & create trouble in maintaining the network performance.

B. Black Hole Attack

An infected node send the wrong routing information in the network stating that it is the best route and tends the other node to route data / packet through this infected node.

C. Link Spoofing Attacks

An infected node broadcast fake links with erroneous information of neighbours to create difficulty in routing operations [3].

D. Network partition

Network can be divided in to sub networks although there is path recognized between all of them but they cannot correspond properly with each other [10].

E. Selfishness

A node will not act as router for other nodes [10].

F. Sleep Deprivation

A node is required to use its battery [10].

G. Denial Of Service

A node is not authorized to send or receive any packet [10].

H. Grey hole attack

They can endorse the route as valid route with the target of creating difficulty in packets, so that they can be dropped with certain criteria [11].

I. Jellyfish attack

These attacks can meaninglessly create inconvenience in the communication like delaying of packets for certain time which causes the overall performance very poor [11].

J. Resource consumption attack

In these attacks, an infected node in the network deliberately gets through the resources of other nodes like battery and power, bandwidth etc [11].

K. Detour attack

In these attacks, Attackers usually change the path information so that it will create difficulty in the network and normal communication can be interrupted. The route information change up to certain level so that it will be shown so wage and attacker cannot get exact information about the information transferring [16].

L. Black mail attack

This attack occurs due to the requirement of authenticity & waiting for the permission of any node to change the information of other node during communication and upset the normal functioning of network [16].

Secure on Demand protocols mapped with vulnerable attacks are compared as below in table after reading [7].

Secure on Demand Routing Protocol	Category of Attacks they are Vulnerable to	Base Protocol
SAODV	Rushing.DoS,Wormhole	AODV
ARAN	Wormhole, Black hole,DoS, Rushing & Relay Attacks	AODV
SAR	Rushing,DoS,Wormhole	AODV/DSR
SRP	Rushing, Invisible Node Attacks, Wormhole,DoS	DSR
Ariadne	Rushing, Invisible Node Attack, Wormhole, DoS	DSR

IV. WAYS OF DETECTING ATTACKS IN MANET

A. Profile Based Detection Mechanism

It is also known as Behaviour-based detection. It creates a profile of a normal behaviour and tells us the variation in that profile accordingly. This profile can detect only the novel attacks in the system as there is no such mechanism to differentiate the real and fake activities going on in the network.

B. Specification based detection Mechanism

It defines set of rules that tells the exact operation of a program or protocols and monitors the execution of desired program or protocol with respect to the defined rules. After reading [1], proposed method was the cluster based trust aware routing protocol (CBTRP). He has presented CBTRP, which is reactive on demand source routing protocol. He has initiated a mechanism by which difference between real nodes and fake nodes can be easily achieved, and then he introduced clusters technique and trust between nodes and every hop through which proper communication can be possible. No UN trusted packet could be forwarded and received during process of CBTRP.

C. Intrusion detection system (IDS) Mechanism [14]

The system by which one can observe attacks in the network and behave according to the situation, how we can treat it the attack so that the network will be saved from future attack. It was further cut down in several goups :

Network intrusion detection systems (NIDS) , which obsereve the traffic in the network and suggest the ways to save the network from attacks.

System integrity verifiers (SIV) , it keeps an eye on the files in the system, possible changes in the system before or after applying certain security policies . for example , same sort of method is used in antivirus softwares to check and detect different viruses in the system before or after installing this package.

Log file monitors (LFM, a monitoring system which keeps on inspecting the system before and after the attacks . They check the system files in the same manner as IDS usually do [14].

V. PROTECTION AGAINST ATTACKS

A variety of attacks have effected on specific layers, researchers had proposed solutions for those cases. Authors will be relating all attacks, there effect on specific layers and what researchers had proposed against every attack [15].

Jamming which targets the physical & MAC layer, Researchers had proposed FHSS, DSSS as solution to this kind of attack.

In **Wormhole** attack targeting network layer, Researchers had proposed packet leashes as solution to these kinds of attacks.

In **Black hole** attack, targeting network layer and **Byzantine** also targets the network layer.

In **Resource Consumption** which targets the network layer, Researchers had proposed SEAD as solution to these kinds of attacks.

Information disclosure which targets the network layer, researchers have proposed SMT as solution to these kinds of attacks**.**

Location disclosure targets the network; researchers had proposed SRP, NDM as solution to this kind of attacks.

Routing attacks targets the network layer, Researchers had proposed SEAD ARAN ARI-ADNE as solution to this kind of attacks**. Repudiation** targets the application layer, Researchers had proposed ARAN as solution to this type of attack.

Denial of service(DOS) attacks targets the multi-layer, researchers had proposed SEAD and ARIADNE as solution to this kind of attacks. **Impersonation** type of attack targets multi-layer, researchers had proposed ARAN as solution to this kind of attack [15].

VI. REQUIREMENTS IN SECURING NETWORK

To secure a network from attacks and misuse, we must know the requirements for securing the network. The requirements are given below:

A. Availability

Certifies that the service should be available to the user in normal functioning of network. But will not be available during attacks.

B. Authenticity

Certifies that the communication between nodes is authentic and make sure that the wrong node should not be treated as original node.

C. Data Confidentiality

It is major security criteria for these networks. It authenticates that the information is not understand by wrong user other than the original one. It can be allowed on network by using cryptography.

D. Integrity

Shows the accuracy of message sent from one to another node. During the transmission process, it keep on examine that original information is not edited by any wrong user during the transfer of information from one node to another. For improving security and data integrity, we may add a hash to an encrypted message for error free transmission.

E. Non-repudiation

It certifies that the information is genuine. For example, if one node get wrong message over the network then it will delay the communication and broadcast this problem to all nodes on network. Digital Signature can be used to improve this issue. [4]

VII. FEATURES OF MANET

MANET has various features, which make this network more suitable for attacks, and problems, author elaborated this section after understanding paper [4]. These are given below:

A. Infrastructure less

It has no central infrastructure like servers, hardware that is important and need of a network to perform better. Because of the absence of the basic infrastructure it stops the use of hierarchical client connection as an alternate, node maintain unrestricted bond. To be specific, they consider the mutual roles in the network rather to depend on a single one. For example, any resolution to the security issues should depend on the mutual methods instead of regional one.

B. Wireless Links use

The utilization of wireless links tends wireless ad hoc network to infect through attacks. While in wired network attacker has to follow some physical access to the infrastructure or has to come through several lines of security like fire walls, gateways etc while in wireless network it can attack from any direction to affect the node or even network. In wireless ad hoc network, every node has to get ready for malicious attack, as there are no physical defence lines. There is MAC protocol IEEE 802.11, which will ensure the trusted communication between users to access the desired channel.

C. Multi-hop

Infrastructure less environment with no routers, gateways, clients/ host is routers at their own. The information on network will pass through multiple routes and nodes before reaching at the final destination. This feature is important regarding attacks because of non-trust full nodes.

D. Nodes movement autonomy

Mobile nodes are self-directed component, which can move at its own level. Which shows that the single node in the network at huge scale like in ad hoc network cannot be traced easily?

E. Amorphous

This aspect must be kept in mind while designing security of a network. Due to mobility of nodes, connectivity in wireless connection allows the nodes to accept and leave the network rapidly.

F. Power limitation

For a portable Ad hoc network, small batteries with limited power are provided. Designer has to consider this feature while making solutions. Attackers may focus on some nodes batteries to cause problems in their normal functioning so that they can cause some issues in network. This is called energy starvation attack.

G. Memory & Computation power limitation

Cryptography is the complex secure solution for these kinds of networks, designer has to take this feature in to account while making some final decision. Ad hoc networks have very concise memory and computational power to compute the tasks.

VIII. KEY MANAGEMENT

After going through [4], the key management system is a basic method for securing both networking function for example routing and the relevant services in MANET. Public Key Infrastructure (PKI) had been one of the most valuable tools for providing security to the dynamic networks. MANETs are infrastructure less character, so providing security in such conditions is challenging task. PKI has self-structured management system, so it will not trust on any other Certificate Authority (CA) or the management system. Public key management schemes can be compared after going through [8]. Like Self-Certificate the level of distribution is quite high while in PKIX it is comparatively low. In self-certificate, there is no requirement to build an infrastructure but in the case of PKIX already a standard one is working over the network. In self-certificate, we have to build a reliable path between local databases on the other hand PKIX connection depends purely based on available connection with servers. In self-certificate, the acknowledgement of certificate on the internet is low where as in PKIX it is high. User can cancel its certificate in the case of self-certificate, while only the issuer or the admin can cancel the certificate in the case of PKIX. In self-certificate the certificate validation has checked based on availability of trusted path between certificates in the local cache. while on the other hand PKIX, considering global mode it depends on the status updates from PKI. Validity of certificate in the case of self-certificate is local on the other hand, in PKIX, it is global. Self-certificate, support for mobility in the sense if one user leaves this MANET and join some other than he has to build a trust relationship before communication. On the other hand, in the case of PKIX users just have to update the certificate authority about mobility.

A. Dynamic key Management system

In this system, we will first use a special undisclosed key which between sender and receiver through some transitional node along the path considering the recent public key data. In the second step, each node moving in the direction will search for shortest path for neighbour near to it, which is encountered with an error or carry out any multiple keys between source and middle nodes. Third step, Trust relation between neighbours is updated by ensuring the behaviour of nodes and any attack details. Fourth step, each node creates a local certificate for creating trust relation with other nodes and can cancel the certificate if it is not valid. Fifth step is to combine all the existing data of PKI management with the current CR data for any real-time update. [9]

IX. REQUIRED CHARACTERISTICS FOR A THRIVING KEY MANAGEMENT SYSTEM

A. Distribution

As MANET has no infrastructure, the CAs should be spread over the nodes in the network.

B. Fault Tolerance

Main duty of the fault tolerance is to make sure that the network is working perfect although there are some malicious nodes in the network. Some of the cryptographic techniques can be used to see the behaviour of the network.

C. Availability

It is mostly used in combination with fault tolerance, but in MANET, it depends on the connectivity of the network. If there is, no malicious nodes in the network then wired network system might be available to the client for doing any task. While in MANET if there is any malicious node in the network client might not access the service due to the conflicting problem in connectivity of network.

D. Security

Act like a trust worthy for the entire network The certificate authority should ensure the faulty nodes security in the network. There must be some clear rules and criteria for attacking a system while it is working in normal mode because it might not be opposing the entire level of attacks in network. Researchers had proposed solution in [4] to secure the routing protocol that mostly depend on the authentication, and considering the presence of central CA, which is an issue in MANET. They have proposed two solutions for the key management in MANET, in which they have designed a method by making the local certificate authority, which maintains a database in which all the information is stored regarding network configuration. The basic function of this key management systems are as follows:

- They have created a public key generator, which can create the public and private key itself and manage through nodes.
- Then they have designed certificate-issuing authority, which issues the key according to matching the requirements.

For storing a certificate, they are managing a database in which the certificates are stored. Each node maintains two sort of certificate details. One is storing the basic information of certificate and second, the additional details and if any algorithm is used while implementing this will be stored at this point. In maintaining the authentication of keys, whenever a node want to get the public key of

another node it verifies the information in order to maintain the security of the system.
In the end, they have made Intrusion Detection System to make the network more secure.

X. Research Directions for Future

Because of the flexible nature of MANETs, they have very striking applications for military and disaster recovery management system. Mobile devices are becoming smaller in size and cheap in price because of this number of mobile devices increases day by day with great reliability. MANET will become part of our lives just like mobile does these days. Security is very hot issue these days that is why MANETs have introduced. Researchers had been working in the past in securing MANET and still there is need of more researches and efforts to be put on to make the MANET more secure and reliable for everyone. Author consideration is that, with the rapid increase in the use of MANETs more problems will be coming up that need to be sorted out properly. Previous methods were there but they were not for MANET, researchers had to design something new, as it requires new methods with the passage of time, because it is not conventional network. As MANET has its own Requirements and Characteristics, so it is important to see the application and the proposed solution as it varies from situation to situation. While reading through [5] writer considered some attacks and targets for a specific protocol considering specific features of MANET. Some solutions might fit in at some situation but it is not always happened because of the limited resources and capabilities of node in a network. New Researchers can develop and implement solutions keeping in mind the characteristics of the nodes in a network. Researchers should concentrate in making new solutions, which are suitable for MANET according to the specific need and desired features. [5] Researchers have given some new direction in which we can work and get better results, like Working in remote areas where human cannot reach easily. Where the battlefield or military operation is going on. In the agriculture field where research need to be done. Areas, which are affected by the will of GOD, like flood areas, earthquake affected portions. Certain type of important meetings, which need to be done on priority basis (in emergency). Fields like business, communication, education sector and research [16].

XI. Conclusion

In this paper, Authors have thoroughly studied different MANET security issues. As Researchers are working to reduce the issues, threats and problems in securing the MANET. They are also working on how to improve the defects in MANET like Bandwidth issues, power issues and security issues. Although Authors have explained some routing attacks and their counter measures in order to secure the network considering the previous challenges in maintaining the security over the network. Availability ensures the service of the network survivability regardless of the Denial of Service Attacks (DOS); it can be established on any layer of the ad hoc network. Authenticity ensures the error free communication between mobile node and peer node. Attacker can access the network and damage the files and other resources if there is no proper authentication. Integrity will make sure that the information has forwarded to destination without any error. Errors might arise due to malicious attacks to the network by the unauthorized person. Confidentiality will make sure that the important information has never broadcast to the unauthorized individual. Secret Information transmission requires confidentiality over the network to save it from attackers. Non-repudiation will make sure that real information has not rejected the sent message. These days Security is very hot issues any every company wants that his communication and information should be secured from any unauthorized access [3]. Researchers said that there is need of working in the area of packet dropping [16].

Acknowledgement

We would like to thank ALLAH Almighty for giving us strength to achieve this task up to the mark and then my mentors for their guidance, support in writing this collective study. In the end, I would like to thank my parents for motivating me in the right direction and my twin brother for helping me out in final review.

Reference

[1] H. Safa, H. Artail and D. Tabet, "A cluster-based trust-aware routing protocol for mobile ad hoc networks," Wirel.Netw., vol. 16, pp. 969-984, may, 2010.

[2] G. Raju and R. Akbani, "Mobile ad hoc networks security," Proceedings of Annual Review of Communications, vol. 58, pp. 635-628, 2005.

[3] S. Kannan, T. Maragatham, S. Karthik and V. Arunachalam, "A Study of Attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols," International Business Management, vol. 5, pp. 178-183, 2011.

[4] D. Djenouri, L. Khelladi and N. Badache, "A survey of security issues in mobile ad hoc networks," IEEE Communications Surveys, vol. 7, 2005.

[5] S. Şen, J. A. Clark and J. E. Tapiador, "Security Threats in Mobile Ad Hoc Networks," .

[6] A. Ahmed, A. Hanan, A. Shukor and M. Izzeldin, "MANET Security Schemes," .

[7] N. Balachandran, "Surveying Solutions to Securing On-Demand Routing Protocols in MANETs," ArXiv Preprint arXiv:1207.0758, 2012.

[8] J. Forné, J. Muoz, O. Esparza and F. Hinarejos, "Certificate status validation in mobile ad hoc networks," Wireless Communications, IEEE, vol. 16, pp. 55-62, 2009.

[9] M. Yu, M. Zhou and W. Su, "A secure routing protocol against byzantine attacks for MANETs in adversarial environments," IEEE Transactions on Vehicular Technology, vol. 58, pp. 449, 2009.

[10] Y. Li and J. Wei, "Guidelines on selecting intrusion detection methods in MANET," in The 21st Annual

Conference for Information Systems Educators (ISECON), Rhode Island, USA, 2004, pp. 4-7.

[11] V. Manoj, N. Raghavendiran, M. M. Aaqib and R. Vijayan, "An approach for detection of malicious node using fuzzy based trust levels in MANET," in Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief, 2011, pp. 477-480.

[12] S. Dabideen and J. Garcia-Luna-Aceves, "Secure routing in MANETs using local times," Wireless Networks, pp. 1-16, 2012.

[13] G. K. Patnaik and M. Gore, "Trustworthy path discovery in MANET--A message oriented cross-correlation approach," in Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on, 2011, pp. 170-177.

[14] V. Manchikalapudi, S. Yelisetti and R. K. Surapaneni, "Detecting misbehavior nodes and trust levels in manets," in Engineering Education: Innovative Practices and Future Trends (AICERA), 2012 IEEE International Conference on, 2012, pp. 1-4.

[15] L. Abusalah, A. Khokhar and M. Guizani, "A survey of secure mobile ad hoc routing protocols," Communications Surveys & Tutorials, IEEE, vol. 10, pp. 78-93, 2008.

[16] S. Joshi and D. K. Mishra, "A survey on threats in routing security in manet for trust management using SMC protocols," in Wireless and Optical Communications Networks (WOCN), 2012 Ninth International Conference on, 2012, pp. 1-6.