A Survey On Security aspects of MANET Challenges, Issues, Attacks and Countermeasures

K.Santhosh kumar[#1] and R.Ramya [*2]

[1]*PG Scholar, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.*

E-mail: santhosh88mca@gmail.com

[2] *Assistant Professor, Department of Electronics and Communication Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.*

E-mail: ramya.psna@gmail.com

Abstract - Mobile Ad hoc Networks named as MANET is a cutting-edge advancement in the era of wireless technology and it is defined by collection of mobile nodes that are connecting together over a structure less wireless medium and it does not require any centralized control and also no need of dedicated routers for forwarding the packets instead of each node act as a router where the communication taken place. Nodes in the networks are roaming freely as it wants so it leads to dynamic topology moreover it has special feature called self-organization meaning that it can be deployed easily whenever and wherever required. Because of these unique characteristic, it offers plenty of applications as well as it also leads to security violations.Security is a prominent factor both in wired and wireless technologies and success of any application depends on how the security is implemented for that application. While communication each node should depends on other nodes that is expecting coordination form others to complete a particular task successfully in MANET but achieving such coordination is always impossible. In this paper we first discuss the challenges of MANET and turn to issues of MANET with respect security. Then we present various types of attacks, and how the attacks are executed by the way what are all the bit falls. Finally we discuss the security solutions in order to overcome these attacks.

Keywords: Mobile Ad hoc Network, Cooperation, Attacks and Security.

I.INTRODUCTION

In general there are two types of network in the communication era; Wired network and Wireless network and wireless network again classified into two category such that wireless with infrastructure and wireless without infrastructure. Mobile Ad Hoc Network comes under wireless network that has no existing infrastructure and it can be deployed quickly so that it is also called as self-organized network. Nodes in the networks are moving freely so as to dynamic topology and node can join and leave the network at any time. It is a distributed network so there is no central control for coordinating the nodes involving in the network [1] .Unlike traditional wired network, there is a dedicated router instead of each node act as a router for forwarding the packets. The figure 1 shows the architecture of wireless with infrastructure and figure2 shows the architecture of wireless without infrastructure called MANET. These unique characteristics offer plenty of application scenarios such that Mobile Conference, Home Networking, Emergency Services,

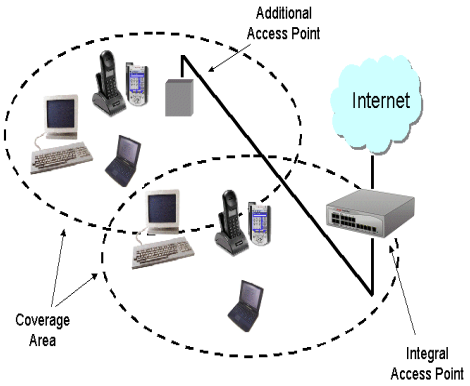
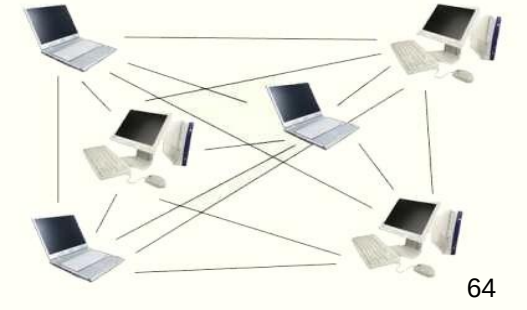


Figure1: Wireless with Infrastructure

Personal area network and Blue tooth and Automotive PC interactions Embedded Computing Applications [2]. Typically these applications are running on the top of MANET architecture and because of thadvancement



F Figure1: Wireless without Infrastructure in MANET

And unique feature; MANET of these applications has received tremendous attention nowadays. The rest of the paper is organized in the following manner, section II discusses the challenges involved in MANET, section III address the security issues, section IV discuss the security attacks and their operations and impact of those attacks, section V discusses the solutions for the security attacks and final section concludes the paper.

II.CHALLENGES IN MANET

MANET has distinct characteristic that leads to various challenges. The following section discusses the challenges in MANET.

A. Limited Battery Power

In general all the wireless mobile nodes are having limited battery power only. A node may consume its battery power when it finds an optimal route and also drain its energy due to attempting travel in invalid routes of the network [3].

B. Dynamic Topology of Networks

In wired network the topology of network may static whereas in MANET movement of nodes occurs frequently. It causes dynamic topology of network [2].

C. Shared Wireless Medium

There is no central control entity in MANET in order to control the nodes. Here every node has a right to access to other nodes without worrying about the access primitives until the security mechanism established. It leads to vulnerabilities [2].

D. Self-organized control of Nodes

Due to the lack of central control administration each node behaves them and move in the network as it wants. In the nodes point of view, they seem to free but in the security point of view it may affect and compromised with malicious nodes in the network [3].

E .Scalability

Number of nodes in the MANET may often increase because a new node may join or relieve from the network moreover the movement of nodes may also causes the scalability problem in MANET [4].

F. Lack of centralized Control

There is no central administration in MANET when compared with wired network. Due to the lack of such administration leads to various security attacks and degrade the network performance [4].

G. Routing

In wired network the routing of packets from source to destination is easily obtained because they predetermined one. But in case of MANET, achieving exact route is impossible one because we could not predict the routing in advance due to the movement of nodes [2].

H. Infrastructure less

The absence of infrastructure less may also affect the network performance because the lack of relationship among the mobile devices may severely suffer it leads to various attacks [2].

I. Memory Consumption

Typically all the mobile nodes are having limited storage capacity so it may not be support the high computation when developing the cryptography techniques to ensure the security [3].

J. Multi hop

There are no specialized routers and gateways in MANET when compared with wired network. Hence each node acts as a router in order to forward the packet from the source to the destination. In this situation a packet may have to travel more than one hop before reaching its desired destination so the trust worthiness of intermediate nodes may be unfeasible and it will affect the network [2].

III.SECURITY ISSUES

Security is one of the active research topics in MANET environment because of the following reasons first dynamic nature it leads network partition hence overall performance of the network is in question. Second wireless channel is accessible to all type of network users and malicious attackers. Third nodes in the environment are moving with relatively poor physical protection have non negligible probability of being compromised. Therefore, our attention not only focuses malicious attacks from outside a network, but also account the attacks launched from within the network by compromised nodes [5].Due to the dynamic nature of network, a new node can join and leave at any time hence we cannot predict the trust relationship among the nodes and that node may be a compromised one.

In MANET environment there may be number of nodes may participate depends on the applications where the nodes are participating so security mechanism should be capable to handle such large networks. As consequence, there is no clear line of defense in MANETs from the security design perspective. For any MANET environment the following security requirements are to be considered: Availability, Confidentiality, integrity, Authenticity and Non repudiation [6]. Availability ensures the survivability of network services even if denial of services (DoS) attacks is presented. Confidentiality confirms that certain information is never revealed to unauthorized parties for misbehave activities. Integrity guarantees that a message is being transferred is never corrupted that should be received as it is. Authentication enables a node to ensure the identity of the peer node with which it is communicating. Non repudiation ensures that the source of a message cannot deny having sent the message and the receiving from denying the reception of the messages.

IV.ATTACKS, OPERATIONS AND ITS IMPACT

As a consequence of challenges that discussed above, MANET is vulnerable to various kinds of attacks. Attack is nothing but an action will be carried by any node in order to harm the networks by the way performance of the network in question. Typically there are two types of attacks in MANET; internal and external attacks [6]. Internal attacks are launched by compromised nodes in the network and it is highly dangerous and we cannot predict such type of attack. On the other hand, external attack is launched by outside of the network and can be easily predicable. External attacks are classified into two category; passive attack and active attack. Passive attack aim is to obtain information from the system that is transferred and not try to affect the system at any way but active is opposite the affect the system resources and alter the system resources. The following table1 discusses the various major attacks and their operation followed by its impact in network.

Types of Attack		
Active attacks		
Attacks	**Operations**	**Impacts**
Flooding[7]	Broadcast lot of route request packets for a particular node ID who is not actually involve in the network	Bandwidth Consumption
Wormhole[8]	Creating own private network	Performance degrade
Black hole [9]	Creating fake route	Packet drops, Performance degrade
Replay[9]	Data is maliciously or fraudulently delayed or repeated	Invalid routing table entries
Byzantine[9]	Creating routing loops, forwarding packets to invalid paths and dropping packets	Lack of routing services
Sinkhole[10]	Offers extremely attractive link	Congestion
Link Spoofing[11]	Advertises itself that has a direct link	Interrupt the routing operations
Sybil[12]	Impersonates several other node using various malicious means	Misbehaving functionalities
Blackmail[13]	Generates false messages to put up the genuine nodes on the blacklist	Wastage of energy
Denial of Service[14]	Disabling the network or by overloading it with false messages	Performance degrade
Gray hole[15]	An adversary may behave like a genuine node	Overload, congestion
Selfish node[16]	Makes the packet to take long time to deliver across the network	Low throughput
Passive Attack		
Attack	**Operation**	**Impact**
Eavesdropping[17]	Secretly overhears the transmission of packets	Misbehaving functionalities
Syn flooding[9]	Sends a huge number of spoofed SYN packets to the destination node	SYN request may be dropped

Table 1: Various attacks, operations and its impact

V.SOLUTIONS FOR THE SECURITY THREATS

To overcome the security violations in MANET, various cryptographic methods and trust based mechanism are used at present. These all methods fight against the attacks in MANET. The following sections describe some of the proposed methods in MANET.

A. Key management:

In order to get the better understanding of key management authors are advised to read the [18-24] papers. Cryptography is the essential and fundamental security techniques in MANET [6]. If proper key management is utilized, the MANET environment becomes more secure. Public key cryptography has proven technique in MANET based on centralized certificate authority (CA) or distributed Certificate Authority. Centralized authority is based on trust third party but such pre-determination and assumptionis not possible it leads to MANET security into pitfalls. On the other hand distributed CA is based on secret sharing mechanism or Pretty Good Privacy (PGP) and it also complex one when the network density is high. Another technique is called symmetric cryptographic is based on single secret key which compromises of various techniques such as FeistelChiper, Data Encryption Standard (DES), Advanced Encryption Standard (AES) etc. Though this techniques has high computational, till affect by attacks.

B. Intrusion Detection Systems

It is simply named as IDS and is used to detect misbehaving, anomaly nodes in the network. IDS identifies the following two approaches namely statistical anomaly detection is used to ensure the high level of confidence whether that behavior is not genuine user behavior and rule-based anomaly detection consists of set of rules can be used to assess the intruder. The papers [25-27] proposed IDS based security mechanism for MANET for better understanding of the readers.

C. Trust based Mechanisms

The traditional security mechanisms that discussed earlier is suitable but providing demerits in terms of high computation power, huge memory and processing capabilities, keys used for security also pre-determined and depends on trusted third party hence the result is performance degradation in overall network's throughput, availability and robustness[]. In order to overcome this problem trust comes into existence. At present trust is getting more attention from the research communities due to its significant nature and benefits. Trust is defined as "one entity (truster) is willing to depend on another entity (trustee) [4]" or "the truster abandons control over the actions performed by the trustee [5]". According to the definition, nodes involving in the MANET should trust other nodes based on the trust evaluation before their communication begins.Generally trust is calculated based on direct and indirect observation of nodes. The papers [28-34] proposed trust based mechanisms for MANET.

VI.CONCLUSION

Security is one of the considerable factors in research avenues of MANET because it determines the success, reliability and robustness of deployment applications. Though today security mechanisms are providing security, many unpredictable and undiscovered attacks are exist. Advancement in security of research is till performing to find new threats and countermeasures in order to improve the overall MANET performance. At last we conclude the overall security of MANET is determined by the MANET weakest points.

VII.REFERENCES

[1] Sivagurunathan.S and Prathapchandran.K, "Trust based Security Schemes in Mobile Ad Hoc Networks- A Review", DOI 10.1109/ICICA.2014.67, IEEE Computer Society, pp. 291-295, 2014.

[2] PerkinsC, [Ad Hoc Networking], Addison-Wesley Professional,2008

[3] Siva Ram Murthy.C and Manoj B.S, [Ad Hoc Wireless Networks], Pearson, 2004[

[4] William Stallings, [Wireless Communications and Networks], Pearson, 2009

[5] S.Sivagurunathan, V Mohan and P Subathra, "Distributed Trust Based Authentication Scheme in A Clustered Environment Using Threshold Cryptography for Vehicular Ad Hoc Networks," International Journal of Business Data and Communication and Networking (IJBDCN), vol. 6 (2), 2010.

[6] William Stallings, [Network Security Essentials], Pearson, 2012.

[7] Neetu Singh Chouhan and ShwetaYadav, "Flooding Attacks Prevention in MANET", International Journal of Computer Technology and Electronics Engineering, Vol.1 (3).

[8] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, Vol.10 (4), 2010.

[9] Abhay Kumar Rai, Rajiv RanjanTewari and Saurabh Kant Upadhyay," Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, Vol. 4(3).

[10] AkankshaSaini, and Harish Kumar," Comparison between Various Black Hole Detection Techniques in MANET", National Conference on Computational Instrumentation, 2010.

[11] BounpadithKannhavong,HidehisaNakayama,YoshiakiNemoto, and Nei Kato "SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks",IEEE,2008.

[12] HimadriNathSaha ,Dr.Debika Bhattacharyya and Dr. P.K.Banerjee ,"Semi-Centralized Multi-AuthenticatedRSSI Based Solution to Sybil Attack", International Journal of Computer Science & Emerging Technologies"Vol.1(4), 2010.

[13] Dr Karim KONATE and Abdourahime GAYE A,"Proposal Mechanism Against the Attacks: Cooperative Blackhole Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network", International Journal of Future Generation Communication and Networking, Vol.4 (2), 2011.

[14] Sukla Banerjee," Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science, 2008.

[15] M. B. Mukesh Krishnan, P. Sheik Abdul Khader ,"Fuzzy Based Security Model to Detect Compromised and Selfish Nodes to Mobile AD HOC Network" , European Journal of Scientific Research, Vol.86(4),2012, pp.520-524.

[16] ImadAad,yJeanPierreHubaux,y and Edward W. Knightlyz," Denial of Service Resilience in Ad Hoc Networks", ACM,2004.

[17] K. Sivakumar and G. Selvaraj, "Overview of Various Attacks in MANET and Countermeasures for Attacks", International Journal of Computer Science and Management Research, Vol.2 (1), 2013.

[18] Keun-HoLee,Sang-Bum Han,Heyi-SookSuh,Chong-Sun Hwang and Sangkeun Lee, "Authentication Protocol Using Threshold Certificates in Hierarchical cluster based Ad Hoc Networks", Journal of Information Science and Engineering, 2006.

[19] Jason H.Li, Renato Levy and Miao Yu, Bobby Bhattacharjee,"A Scalable Key Management and Clustering Scheme for Ad Hoc Networks", International Conference on Scalable Information Systems, 2006

[20] PrantiaM.Potey and Naveeta Kant, "Authentication based Hop Count Clustering Algorithm in Mobile Ad Hoc Network", International Conference on Recent Trends in Information Technology and Computer Science (IRCTITCS), 2011.

[21] Lijun Liao and Mark Manulis "Tree-based group key agreement framework for mobile ad-hoc networks",Future Generation Computer Systems, vol(23),pp.787–803, 2007.

[22] Dijiang Huang and Deep Medhi , "A secure group key management scheme for hierarchical mobile ad hoc networks", Ad Hoc Networks, vol(6), pp.560–577,2008.

[23] Shushan Zhao, Robert Kent and AkshaiAggarwal , "A key management and secure routing integrated framework for Mobile Ad-hoc Networks" , Ad Hoc Networks, vol(11), pp. 1046–1061, 2013.

[24] Jianping pan, Lin Cai and Xuemin, "Promoting identity based key management in wireless ad hoc networks", Wireless Network Security, Springer, pp.83, 2009.

[25] TiranuchAvantvalee and Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Netwworks", Wireless Network Security, Springer, pp.159, 2009.

[26] Madhavi, S, " An Intrusion Detection System in Mobile AdHoc Networks", DOI.10.1109/ISA.2008.80, IEEE, 2008

[27] Atul Patel, RuchiKansara and PareshVirparia, "A Novel Architecture for Intrusion Detection in Mobile Ad Hoc Networks", International Journal of Advanced Computer Science and Applications, pp.68-71.

[28] Guojun Wang, Qiong Wang, Jiannong Cao and MinyiGuo, "AnEffective Trust Establishment Scheme for Authentication inMobile Ad Hoc Networks," IEEE, 2007.

[29] YannickLacharite, Dang QuanNguyen,Maoyu Wang and LouiseLamont, " A Trust-based Security Architecture for TacticalMANET," Crown,2008.

[30] Wei Gong, Zhiyang You, Danning Chen, Xibin Zhao, Ming Guand Kwok-Yan Lam, "Trust based Malicious Nodes Detection inMANET," IEEE,2009.

[31] WenjiaLi,James Parker and Anupam Joshi, " Security throughCollaboration and Trust in MANETs," Springer, 2010.

[32] Bhalaji N and Shanmugam A, "Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Ad Hoc Networks," Elsevier, 2012.

[33] Hui Xia, ZhipingJia, XinLi,LeiJu and Edwin H.M.Sha, " Trust Prediction and Trust based Source Routing in Mobile Ad Hoc Networks," Elsevier,2012.

[34] AsmaAdnane, Christophe Bidan, Rafael and Timoteo de Sousa Junior,"Trust based security for the OLSR RoutingProtocol,Elsevier, 2013.

