Security for Mobile and Adhoc Network

Manzoor Ahmad Lone, Mohammad Mazhar Afzal

Abstract: ***A MANET is a distributed infrastructure-less network and in major cases it is concerned about the individual level of security solutions, since the MANET is a kind of decentralized type of network and to implement the centralized security control on it will not be an efficient way to secure the MANET networks though it will be the wastage of time and resources as well. When there is no centralized security in any network it always becomes vulnerable for the different attacks and can provide any way for the attacker to intrude into the Network or in the particular device. MANET is designed using the number of other small portable devices, although this system does not use any router, so that the centralized security could have work to protect the same network. But in this Network there is no router only the single Portable device is responsible for the attacks. It is really very hard and complicated to maintain this kind of network where it is defined that each end device will provide the security on its own, since there are the number of challenges when the security is concerned. In this paper we give the overview of the security in MANET and in case if there is any attack how the Network can be protected with theuse of the different security and protection technique. Attackers are always updated with the new and efficient ways how any network can be breached and thus it makes them intelligent to attack on any network. No matter security, engineers are always working to check the loopholes in their own system and trying to protect their networks butthe hackers to attack the network are inventing number of ways. When any network is being attacked by the attackers, the important data can be compromised. Data is very important asset for any industry and when the same valuable data is breached this can lead any organisation into serious issues. MANET does not use the strong centralized security system but there are always the best possible solutions which can be used to make sure that MANET can be used to make sure that of the attacker try to attack this Network he will find it much complicated to attack and intrude into the network hence will lead the attacker for the unsuccessful attack. This is very important to keep in consideration that before using any model of the network the security of the network should always keep in priority because more the secure Network is more efficient it will be.***

Keywords: MANET, Security, Attack

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are the fastest emerging networks that are growing with the technology. MANET is a network in which the different nodes are mobile. The mobility leads the insecurity in the same network and it gives the roam for the users that there are threats of insecurity in using the MANETs. In an Ad hoc network the mobile nodes are connected through the wireless links. Mobile Ad-hoc Networks can be established freely there is no restriction anytime and anywhere it can be established but with this advantage there is a disadvantage as well. MANET has opened the door for the researchers for self-organizing network, there is no need for the pre establishment of the Network and no centralized Network needs to be established before the MANET network can be established. MANET is actually based on WLAN technologies where in there is no previous predefined structure. MANET is self-configuring network which is added by different mobile hosts but those devices must support the wireless communication options. Security in Mobile Ad hoc Networks is very important and plays the vital role because this makes the MANET eligible that there will be no issue with the basic functionality of the network. As we know whenever we face any kind of security related issue on our networks it always disrupts the network to work smoothly.

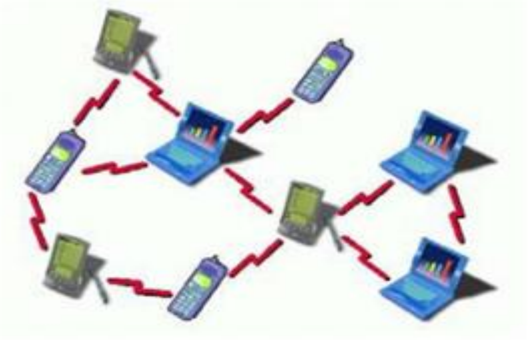

Figure 1: Mobile Ad hoc Network

As the MANETs are self-organizing network and each node acts as router, server and client as well. MANETs lack the centralized system thus the it is easy for the attackers and the hackers to eavesdrop and gain the access to the valuable information and data which is very important for the industries. When there is no physical connection it is very easy for the hacker to enter into the network then attack on the important data and can get the access to the whole information then leave the Network smoothly as no physical connection is between the nodes.The hackers can easily delete the important data, inject the false packets this violates the goals of the secure Network system or integrity and the authentication of the network and this can lead the data theft, the nodes can also launch the attack with in as the nodes are not defined under any centralized security protocol. Securing the MANETs plays an important role as number of organizations would prefer this network to avoid the physical mess but who knows anything can happen anytime, so to protect this network ad to deploy the best security techniques which can help the nodes to be safe from any attack from outside. This becomes the primary responsibly of a consultant or the researcher to secure the network by using the end to end security methods,

Revised Manuscript Received on May 30, 2020.
* Correspondence Author

Manzoor Ahmad Lone*, Department of Computer Science & Engineering, Glocal University Saharanpur, UP, India. Email: mailmanzoorlone@gmail.com

Dr Mohammad Mazhar Afzal, HOD Department of Computer Science & Engineering, Glocal University Saharanpur, UP, India. Email: hod.cse@theglocaluniversity.in

so that the important data will not be compromised and there is no roam for the hackers to hack into the system and learn from the one attack and use the previous attack to perform the bigger attacks on the network and steal the important details.

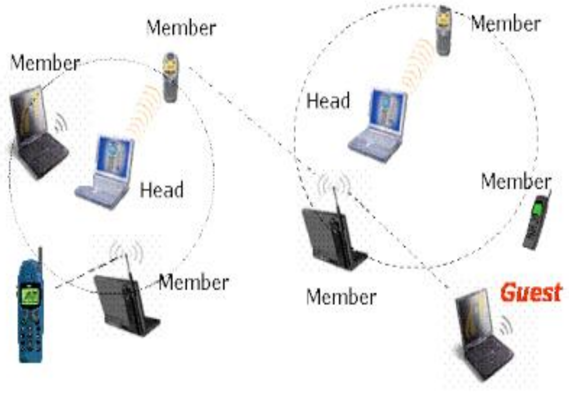

Figure 2: Self-Organized Network

Though MANET offers the best advantages over the WLAN and there are number of challenges in this field and Internet with the proper internet connectivity is the main source of service. Since the MANET is a network of distributed nodes, so the control of the Network is distributed among all the nodes of the of the Network and each node have the value and the control as there is no specific priority to any node in this scenario each node has the ability to act as the router, server or the client this is only because MANET is not a centralized system. In aura security is the biggest challenge and to implement the security with in this network seems difficult that is why the measures should be taken to implement the best possible security techniques.

MANET security involves routing protocols, the proper authentication and encryption apart from this key establishment is also included in the process. When we involve any measure in the security line up we tend to choose the best and the optimal step in order to make sure that this step will not be improper source in terms of security in MANETs. In past we have seen that the number of attacks in such type of Networks and it can be crashed easily if there is no proper security and after implementing the security techniques and possible solutions still there were the loopholes in the system and this lead data theft in the system that is why it is very important to provide the authority to the expert who is good in terms of security this is the way how this network could be secure. As the normal person with no skills in the security will not be able to meet the expectations.

In order to meet the expectations from the security end with the network this should be the priority that before we work or exchange the sensitive information in this network it should be secured and should be checked once if it is ok to exchange the data between the nodes of this network.

There could be different possible attack on this network but we broadly classify the attack on the Mobile Ad hoc Network that is Passive attack and Active attack.

I. Passive Attack: This attack is carried out by the hackers in order to steal the sensitive information from the targeted networks. Attackers always try to include themselves into the network and they try to be the part of the network. Attackers usually do not disturb the network in initial stage they let the network to function normally so that it becomes very hard to identify them when the nest is already being spread by the attackers.

II. Active Attacks: Active attackers always temper the traffic by creating the different scenarios like the network congestion, false routing information etc. Due to the active participation of the attackers they can be identified using the proper algorithms. Fabrication of messages is also the part of active attack.

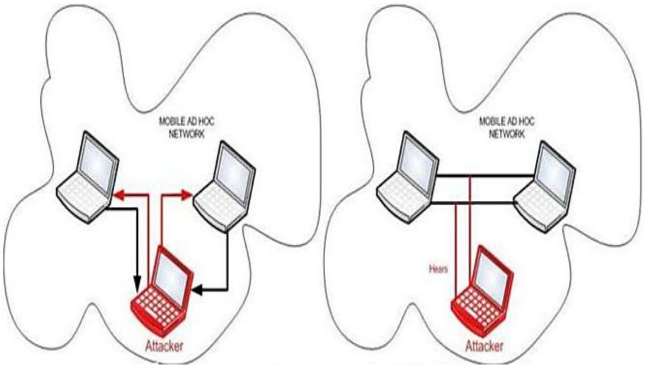

Figure 3: Active and Passive Attack in MANETs.

Passive and Active Attack is the main category of the attacks carried out on the MANETs. There are other attacks as will which we call as the sub category and those attacks are also being used by the attackers in order to steal the information which is very important, when the sensitive information is being stolen by the hackers they can make lot of money on this stolen information. The main aim of the hackers is to make the money. The attacks which can be carried on the MANETs are as: worm hole attack, Byzantine attack, Denial ofservice and modification of messages can be used to attack the network.

Number of researchers has already provided the solutions that how any network can be saved from these attacks and if those techniques can be followed then there is very less possibility of the attack. Security expert should be always up to date to protect the network and must be well aware about the latest updated tools for the penetration testing.

Correspondence Author

II. LITERATURE REVIEW

In order to under the better about the MANETs and how MANETs can be protected and secured, so for that several ways of information have been consulted, in this section I will outline the review of the literature in order to set the basics of discussing the enormous security options of MANETs.

Priyanka Goyal, SahilBatra, Ajit Singh provide an excellent overview and deemed about the security attacks and how the methods can be used, so that it will be trustworthy for the users to use this kind of network. On the other hand, Gagandeep, Aashima, Pawan Kumar discussed Analysis of Different Security Attacks in MANETs and what are the impacts of the different attacks and how those attacks can create the issue in the network and how hard it will become for the person to again make the smooth functioning of the network. In this article they discussed about the different Vulnerabilities of MANETs and the security attacks on the MANETs.

However,Mamatha.T provided the standard about the network security in MANETs where in different cryptographic methods have been discussed so that there will be proper data integrity and properauthentication in MANETs.

III. CONCLUSION

This paper inspects the security issues in the MANETs and the main category of the attacks and few other attacks as them which provide the opportunity for the attackers to attack. This paper highlights some issue and security threats which have been faced by some industries in the form of attacks. The paper throws the light on how the sensitive data is being theft by the people who are making money by attacking the different networks keeping in mind that the sensitive data will be compromised and those attackers will get highly paid out of it. The different authors have provided the different view point on how to prevent the network from being the victim of such attacks. This all is possible by using number of authentication techniques and the different cryptographic algorithms to achieve the proper authentication and the data integrity during the exchange of the data.

By using the number of methods in the MANETs which provide the clear message that the network is safe to use. As the technology is growing the MANET is being considered also the important topic and important area where more research will be done and there is a dearth need for the same and this way MANET will be trustworthy.

REFRENCES

1. K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007.
2. H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, “Self-Securing Ad Hoc Wireless Networks,” in proceedings of the 2002 IEEE Symposium on Computers and Communications, Italy, July 2002.
3. FahadSamad, Qassen Abu Ahmed, AsadullahShaikh and Abdul Aziz, “JAM: Mitigating Jellyfish Attack in Wireless Ad hoc Networks”, B.S. Chowdharyet.al.(Eds.): IMTIC2012, CCIS281, PP, 432-144.2012.
4. ZaibaIshrat, Security issues, challenges & solution in MANET in IJCST Vol 2, Issue 4, oct-nov 2011.
5. Kirti Gupta, Dr. Pradeep Kumar Mittal, An Overview of Security in MANET International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7, Issue6).

AUTHORS PROFILE

Manzoor Ahmad Lone, research scholar in CS having Strong belief in ethics, sincerity and smart work. Lonereceived his Bachelors Degree in Computer Applications (BCA) from University of Kashmir India,Masters Computer Applications(MCA) from University of Kashmir India and Masters of Philosophy in Computer Science (M.Phil) from Glocal University Camps Saharanpur UPIndia.His research Interests include Data Science, Network Security, Cloud Security, Security in IOT’s and Adhoc Networks.

Dr. MohammadMazharAfzal, is an Associate Professor and head of the Computer Science Department at Glocal University, where he has been since 2015. From 2008 to 2013 he served at a Government University at KSA. After completing his Masters in Computer Science in Year 1997 he served at Department of Computer Science Maulana Azad college, Aurangabad for nearly a decade. He received his PhD from Dr. Babasaheb Ambedkar Marathawada University Aurangabad (MS). His research interests span both Internet Governance and Network Security. Much of his work has been on improving the understanding, design, and performance of Security systems and various cryptographic techniques. In the networking arena, he has worked on characterizing the Internet and the World Wide Web. In addition he is always keen on improving and imparting modern methods of teaching and imparting knowledge. He also served various academic bodies at different capacities. Additionally he is also working as Director (IQAC) at Glocal University.