Understanding the MANET Security Using Various Algorithms and Types

Ningthoujam Chidananda Singh[1], Dr.Avinash Sharma[2]

[1]Research Scholar of Computer Science Department, Mewar University, Gangrar, Chittorgarh-312 901, Rajasthan, India, chidanandaningthoujam@gmail.com
[2]Professor of Computer Science and Engineering Department, Maharishi Markandeshwar (Deemed to be University), Mullana -133307, Harayana, India
asharma@mmumullana.org

Abstract

Ad hoc networks are used in wireless equipment and are the primary networks that those machines use for their connection. The network is also known as MANET, an acronym for Mobile Ad Hoc Networks. These are used to establish a network system in wireless electronically operated equipment like mobile phones, laptops, etc. Networks like these are capable of maintaining themselves, are fully dynamic and temporary, but on the negative part, they are very much prone to various security attacks. Security has always been a major problem for wireless networks like that of the ad hoc and other similar networks, because they are an open medium, and are less dependent on related algorithms. As much as we depend on these kinds of networks, we must also keep in mind that there is a high risk of malfunctioning in such networks. There are frequent attacks that take place and put the network at great risk. It also puts your data to risk as well. But that doesn't stop any of us from using the technology and the network that comes with it for almost the entire day. Our lives are incomplete without the technology of any or all kinds and here, we are going to discuss one of the most important aspects of technology – the wireless network. In the following article, we will discuss the working and efficiency of the defense mechanism that is being used to fight the security issues in the network. We will also discuss the simulation that has been used and the results that it has produced, which will support the efficiency and effectiveness of the new and modified algorithm.

1. INTRODUCTION

If we read the history of the Internet and other related cellular networks, we will learn that if the protection of any particular network has not been properly designed since its inception, it is more likely that the loopholes will be exploited by malicious users.The security aspect in such networks is not very easy to obtain because of the complexity in network arrangements and the fast-changing nature of such networks[1], [2].

The security aspect in these networks is read and understood at different stages. In the following article, we will discuss the mechanisms related to the security and the nature of the network that is being scrutinized.

We understand that not everyone who wants to know about these kinds of networks and their aspects is well aware of the technical aspects of the same. Therefore, we have made an effort to give you all the necessary information in very simple and understandable words and language[3].

2. THREATS IN AD HOC NETWORKS

Threats in Ad Hoc network can be distinguished on two major levels:

- Basic mechanisms- Attacks on the Ad Hoc network's basic structures, such as routing. To forestall these attacks, we need security mechanisms that are for the most part dependent on cryptographic algorithms.

ISSN: 2233-7857 IJFGCN

- Security mechanisms- Attack on the key management isn't a concern confined to Ad Hoc networks and also the security mechanisms. Nonetheless, despite the very peculiarity of the ad hoc network, the solution needs special attention.

3. THE VULNERABILITY OF THE BASIC MECHANISMS

Unlike the (conventional) wire line network nodes, you cannot assume that the nodes of the ad hoc networks are secured securely in locked cabinets. Therefore they're at high risk of being caught and compromised. The ad hoc networks are vulnerable to attacks that range from eavesdropping to active interference due to all communications being performed over the air. [4].

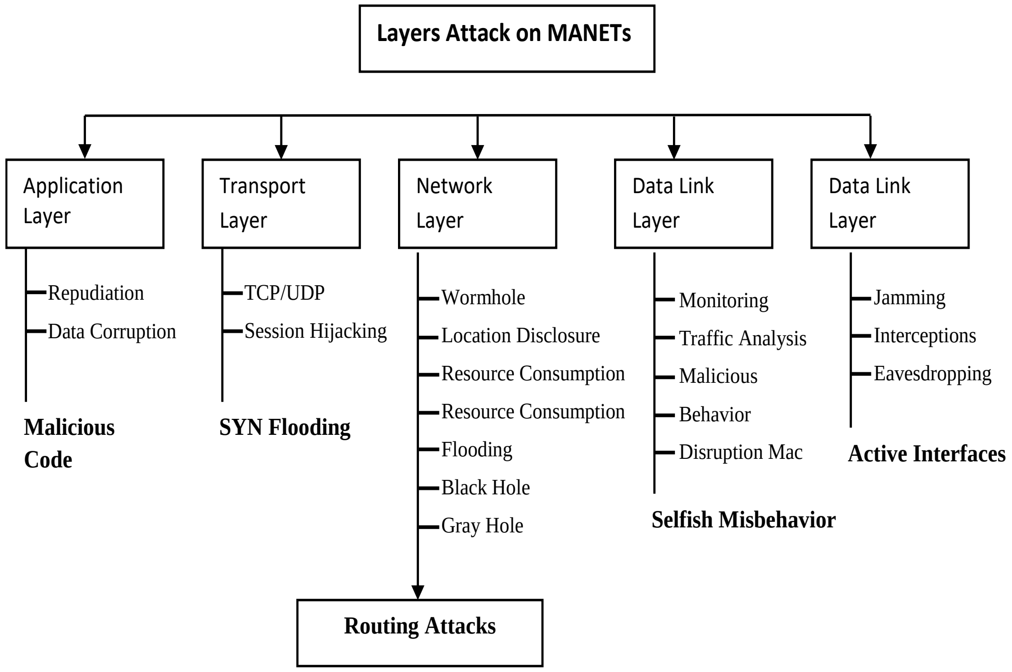
Another problem with the algorithms is that they were thinking they were cooperative. Nodes are expected to cooperate in mechanisms and networks and to function efficiently. Unless the nodes do not obey the rules, the communication channel allocation could turn out to be unequal and the network output will be seriously impaired. For ad hoc networks, routing mechanisms are more vulnerable than in traditional networks, because each system in an ad hoc network functions as a relay [5].

4. THE VULNERABILITY OF THE SECURITY MECHANISMS

In virtually any network, the basic security mechanism asks the user to make use of appropriate cryptographic keys. A good cryptographic design is meant to reduce complex problems to the management and safe-keeping of a small number of cryptographic keys[6]. The achievement of this goal becomes difficult in an ad hoc network because of the lack of guarantee in connectivity and the movement of nodes.

Another problem is to know who to trust. If there is a device that is equipped with a tamper-resistant security module, there is no way to make sure that the module has not been replaced by a fake one. There must be an authority to scrutinize the manufacturer, but can we also trust this authority?

Not only these, but any kind of mechanisms, systems, protocols, or networks are also vulnerable to a large number of attacks and malfunctioning. The systems are based on pure trust and that is exactly what the malicious users play with to tamper with your network and device[7].

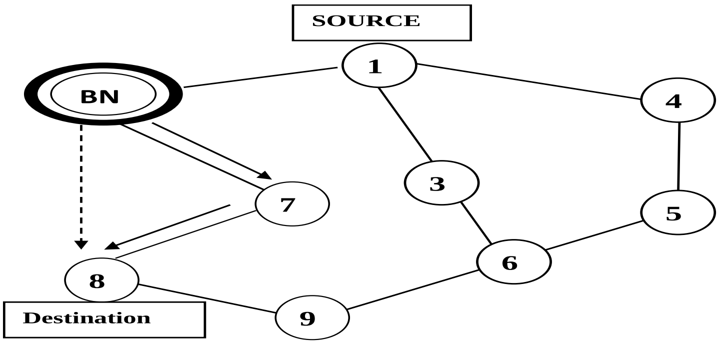


The attacker of the black hole is supposed to enter a group to be eligible to remove the data packets from the network as a whole. This type of vicious attack removes all or some data packs that were received, rather than forwarding them further. This also makes the delivery rate of data packets extremely slow[7]. There are two types of black hole attacks: (i) an attack of a single black hole, performed via an existing node in the network, and (ii) a black hole attack of more than one node. It combines multiple nodes, turns all of them into black holes, and then performs the attack.

The node that is responsible for the execution of the black hole attack waits for a request for a route. When the request arrives the invader node answers positively to the request without considering or looking at its routing list or without considering a route leading to the destination. While sending the route reply, it makes the reply shorter than the size of the other nodes[2]. The node that sends the actual route reply is cheated on by the invader node by tampering with the number of sequences and the number of hops.

When the framework begins imparting data sign unremarkably, parcel conveyance size connection is filtered. On the off chance that the parcel conveyance greatness connection is on the head of an edge limit, at that point, no malevolent hubs are blessing and the strategy ends. However, if parcel conveyance greatness connection drop is recognized, a lure RREQ is sent and the reaction is sought after. If there is no reaction, at that point the parcel conveyance size connection drop may be because of wasteful directing, and in this manner, CBDS is ended. be that as it may, if the sending hub gets an RREP reaction to the trap RREQ, turn around following project is activated and check parcels and review messages are sent to prove malevolent hub discovery[8]. On affirmation of vindictive hub, flexibly hub refreshes its rundown of the malignant hub with this new section and communicates a caution signal inside the system for all the hubs to take action accordingly. When all the hubs have refreshed their rundown of malevolent hubs, the recognized hub is boycotted and extra correspondence to the hub is stopped. In a self-assertively sent hub geography gracefully hub picks the helpful trap address haphazardly from its one jump neighbor hubs and sends the snare RREQ.

The node that sends the route request assumes that it has found the best route when it receives this route reply. Hence, this node is believed to be a short and appropriate path to send data packets[9]. Due to this, a black hole is created and each node, which is now called the black hole, either extracts or throws away the data packets instead of sending them.



Black hole attack method

What is the proposed algorithm?

(i) Data Routing Information (DRI)- In this system, two bits of information, that is additional, is sent out with the data packets around the network by the nodes. The first one to send a reply to that information is prioritized. Every participant node is expected to maintain their personal DRI tables. In this particular table, the two bits are 01 and 1. Here, the bit marked one is considered to be true and the bit marked as 0 is considered to be false. Appropriate conclusions are drawn out from the bits as and when they are received in the network.

While we wait for authors and researchers to discover and implement more plans to secure out the Internet and other cellular networks, we must also keep in mind that finding one solution won't be the end of all problems. When we are over finding solutions for the black hole attacks, malicious users will find a way to invent another vicious attack, more hazardous than the previous one[10]. And while all of us put our brains to work finding another protocol to rectify that attacks, there will be an emergence of another one. The process of problems and finding their solutions is a continuous and never-ending process.

We can hope that as the technology of the world advances, we will find better solutions to the problems, and our authors are still working to make this possible.

5. CONCLUSION

This algorithm has not only been modified and launched but also checked by regular testing and implementing the protocol in a simulator. This trial has proved that this new and modified algorithm is effective and efficient and is capable of curing the problems related to security in such networks. There is also another security attack called the "grey hole attack", which can also be prevented by using the AODV protocol[10]. This can be considered as one of the most important modifications of algorithms in the history of cellular networks.

To date, AODV is a good solution for handling malicious nodes. But as technology will further develop, there will be more problems coming our way. Almost all users of electronic devices are dependent on such networks; therefore, the need to make it more secure and easy to use is very high. It is great how tediously the authors are working to find and modify new algorithms and to make the network more secure for the users[1]

Under perfect conditions, the start to finish delay is demonstrated to be high (appeared in blue). When under lack of sleep assault this worth declines (as appeared by the green bar). Application of CBDS changes the start to finish defer an incentive to bring it closer to the perfect condition esteems. The perfect chart increments at first until malignant hub proportion of 3 and afterward bit by bit diminishes. At noxious hub proportion 3, we notice that the estimation of start to finish delay after the execution of CBDS is still lower than before the usage[11], [12]. These remaining parts of the region of future improvement to chip away at these exemptions and improve the effectiveness of CBDS conspire.

We hope this article was useful to you in understanding the various aspects of ad hoc networks and their security. We know that as technology develops, it brings more and more flaws and loopholes with it. But that shouldn’t stop us from developing with the world. Researchers and developers are always working on how to make the networking space a safe one for all of us, and it is best to invest our faith in them and live a tech-savvy life!

REFERENCES

1. A. Hinds, M. Ngulube, S. Zhu, and H. Al-Aqrabi, “A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET),” *Int. J. Inf. Educ. Technol.*, 2013, doi: 10.7763/ijiet.2013.v3.223.
2. H. Deng, W. Li, and D. P. Agrawal, “Routing security in wireless ad hoc networks,” *IEEE Commun. Mag.*, 2002, doi: 10.1109/MCOM.2002.1039859.
3. F. Kargl, S. Schlott, A. Klenk, A. Geiss, and M. Weber, “Securing ad hoc routing protocols,” in *Conference Proceedings of the EUROMICRO*, 2004, doi: 10.1145/570681.570682.
4. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks,” *IEEE Wirel. Commun.*, 2007, doi: 10.1109/MWC.2007.4396947.
5. P. Michiardi and R. Molva, “Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks,” 2002.
6. M. G. Zapata, “Secure ad hoc on-demand distance vector routing,” *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, 2002, doi: 10.1145/581291.581312.
7. K. El Defrawy and G. Tsudik, “ALARM: Anonymous location-aided routing in suspicious MANETs,” *IEEE Trans. Mob. Comput.*, 2011, doi: 10.1109/TMC.2010.256.
8. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions,” *IEEE Wireless Communications*. 2004, doi: 10.1109/MWC.2004.1269716.
9. A. Dorri and S. R. Kamel, “Security Challenges in Mobile Ad Hoc Networks: A Survey,” *Int. J. Comput. Sci. Eng. Surv.*, 2015, doi: 10.5121/ijcses.2015.6102.
10. P. Goyal, S. Batra, and A. Singh, “A Literature Review of Security Attack in Mobile Ad-hoc Networks,” *Int. J. Comput. Appl.*, 2010, doi: 10.5120/1439-1947.
11. P. Joshi, “Security issues in routing protocols in MANETs at network layer,” in *Procedia Computer Science*, 2011, doi: 10.1016/j.procs.2010.12.156.
12. P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT urban scenarios,” *IEEE Sens. J.*, 2013, doi: 10.1109/JSEN.2013.2272099.