JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.7, Special Issue.2, Jan 2019 E-ISSN: 2347-2693

A Survey On Network Layer Attack Detection And Isolation Techniques In MANET

[1*]R. Sujatha, [2]P. Srivaramangai

[1,2]Dept. of Computer Science, Marudu Pandiyar College, Thanjavur, India

*Corresponding Author: ksujathakathiravan@gmail.com,

Available online at: www.ijcseonline.org

Abstract— Mobile Ad Hoc Networks is an emerging trend through self configuring independent network environment consists of nodes and links. Due to this spontaneous configuring nature, it is more vulnerable to many attacks. Security is the vital concern in MANET. There are lot of attack strategies are vulnerable in the MANET. In this various attacks, the network layer attacks cause more vigorous. In network layer, the nodes are connected with the nodes in that range and the network formation and data transmission will be done through the multi hop wireless based routing scheme. The detection and mitigation of these attacks makes more complex when it deals with the n number of nodes and links. The detection and mitigation techniques are developed to isolate the attacks and not to make any impact to the legitimate nodes. This paper describes the network layer attacks and its detection and mitigation strategies with their performance. In this paper, the detection strategies are also compared with one another through the results provided from the references.

Keywords—: MANET, Attack Detection and Mitigation

I. INTRODUCTION

Mobile Ad Hoc Networks [1] [2] [4] [7] [11] [12] is the only promising network for the portable devices. It has more and more advanced characteristics and valuable features rather than the traditional networks. The MANET is self-configurable independent network, in which nodes connect and disconnect from the other nodes to form a network automatically and dynamically. The most promising characteristics of the MANETs are flexibility, distributed operation, addressing mobility, node to node connectivity, etc. Based on the node discovery, the routing of the data in the MANETs is done with the routing table. The nodes carry and forward the data to neighboring node in the routing path for the further data transmission so that it can be delivered to the particular destination. In multi-hop wireless networks, the in-between nodes in the sender and destination act as a relay agent to route the data traffic. As MANET [4] [5] is active and dynamic in nature so it is accessible to all the users it may be a legitimate user or the malicious node which reproduce the data or attack in the network.

Here the attacks need to detect and mitigate periodically or at the need of changes in the network. The attacks cause some more changes in the network. Thus the attack will makes data theft or collapse in the network when the data transmission. The various attack detection and mitigation techniques had developed to isolate the attacks in the networks. In this paper, the network layer attacks [12] can be described with the detection scheme and their performance issues and results. Thus the network layer attacks are explained with their design principle and the causes for the attacks also described. The data transmission may used for the network performance results with the parameters such as packet delay, network throughput and the reliability of data.

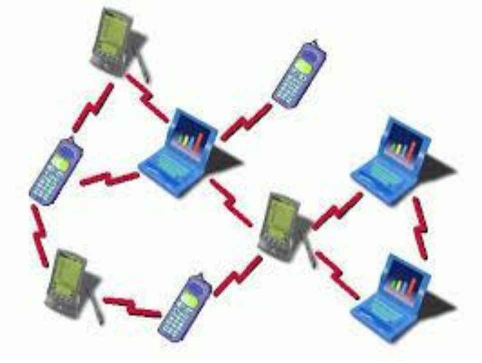

Fig 1 : MANET Structure

II. THEORETICAL BACKGROUND

The main background knowledge required for the discussion below is as follows: What is an attack? What are the kinds of attacks? What are the attacks which are affected in the layers of network? The attacks are happened through the network nodes inside or outside the network. Thus the attacks are making worse in the network data transmission or in the network structure. The attacks are done at the layers of the networks; it can be varied based on their behavior.

The dynamic mobile network [3] [4] consists of diverse nodes which can be a malicious node, whose intention is to attack the network and transmits the false information or false routing. The attacks can be majorly divided into two types. They are Active attacks and Passive attacks. Active Attack: In this the attacker tries to indulge into the system, pass infected code, or spoof the information, destroy or reproduce it, thus denying the normal functionality of the network. It is classified into external attack and internal attack. The intruder from the outside of the network will cause the damage to the network is meant as external attack while in the internal attack, the node act as a malicious and an entity of internal network that propagates the misspelled information. Passive attack affects network traffic through the analysis of routing i.e. identify the communicating entities, monitors the data transmission path between them, decrypt the affect possibly encrypted data, capture authentication credentials such as passwords, public key, private key, that is exchanged over the route link. From these credentials, the inferences are taken by the attackers regarding the confidentiality of data and thus steal the information without the legitimate user information.

A . Network Layer Attacks

The network layer attacks and its detection techniques are analyzed through the existing works proposed and experimented by the experts.

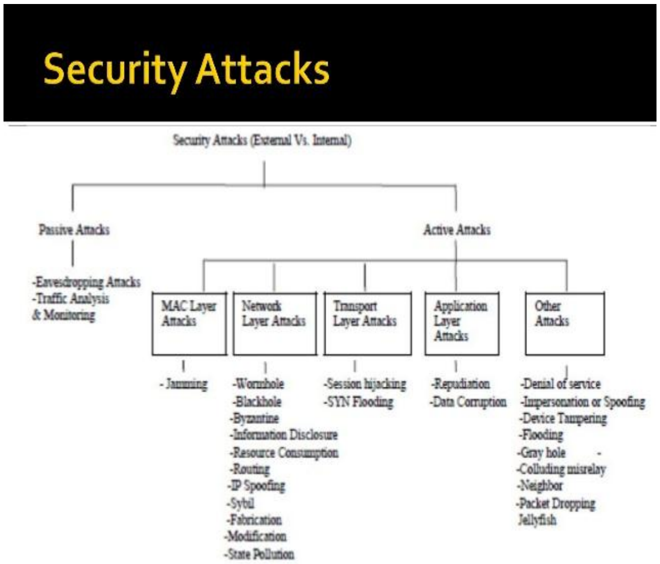

Fig . 2 Security attacks in MANET

a. Black Hole Attacks

A black hole attack [3] [4] is one of the types of network layer attack where the malicious node under duress obtains the route with finest sequence number and less hop count between the source and the destination.

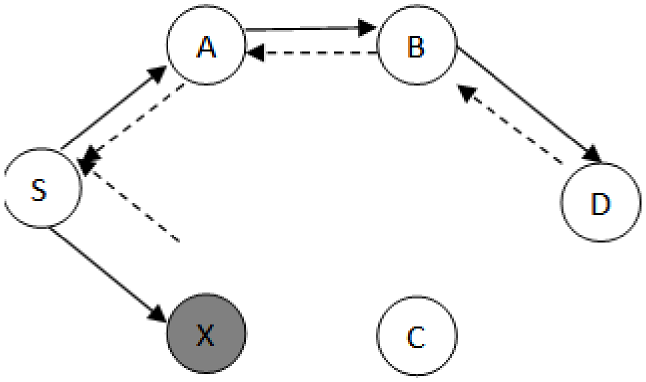

Fig. 3 Black Hole Attacks Illustration -nation and subsequently overhears or drops all data packets.

In Fig .3, the black hole attacks clearly illustrated with the malicious node and legitimate user nodes. Here the Source Node S sends RREQ signal to the neighbor nodes A and X. The malicious node X which acts as a black hole here. It sends the response signal as shortest path and drops the data which obtained from the source node.

b. Worm Hole Attacks

Worm Hole attacks [4] [5] [10] are as much like the type of denial of service attacks in the packet transmission. The nature of this attack is most vulnerable and impulsive in MANET.

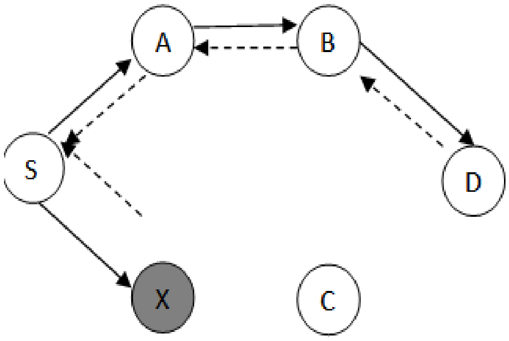

Fig. 4 Worm Hole Attack Illustration

In wormhole attack, malicious node receives data packer at one point in the network and tunnels them to another node which is malicious too. The tunnel exists between two or more malicious nodes is referred to as a wormhole.

Wormhole attacks are most vigorous threats to MANET routing protocols. Attackers use wormholes in the network to make their nodes appear more attractive so that more data is routed through their nodes. When the wormhole attacks are used by attacker in routing protocol such as DSR and AODV, the attack could prevent the discovery of any routes other than through the wormhole. If there is no defense mechanism are introduced in the network along with routing protocols, than existing routing protocols are not suitable to discover valid routes.

c. Sink Hole Attacks:

Sink Hole Attacks is a most vulnerable attack as insider routing attacks. It compromises the nodes in the wireless networks as legitimate attractive nodes with respect to the routing algorithm. Sinkhole attacks are difficult to detect and mitigate because the routing information identified from the node is complex to verify.

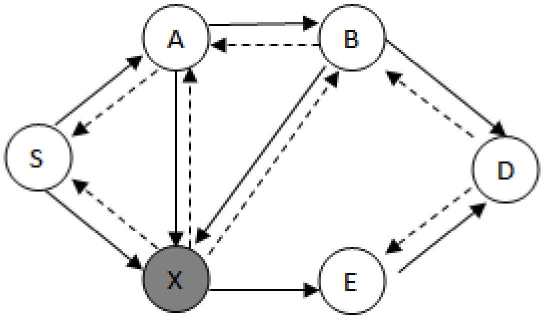

Fig .5 Sinkhole Attack Illustration

It is most occurs in the process of data gathering and shortest routing in the data communication. In this above figure.5, the malicious node X occurs as both data gathering and routing path. The Source node S tries to send the data to the destination D through the shortest path. It sends the RREQ signal to the A and X. The node X which sends response signal to the source node with false routing details as it will be the shortest path in the network to send data to the destination needed from the source.

B. Previous Works Survey

In [3], author surveys the detection of both black hole and gray hole attacks how its degrades the performance of the network data communication and the different defense mechanism that are available to detect and mitigate the black hole, worm hole and sink hole attacks. In this work, they defined the both proactive and reactive routing techniques and its design principles. The Denial of Service attacks is the most vulnerable attacks in the MANET, here to analyze these attacks, in [6] Alsumayt and Haggerty surveys the attack vulnerability in the MANET and also its performance degradation. They proposed an ideal and novel system to mitigate the DOS attacks and it also helps to design a methodology to detect this attack with certainty in MANETs. In [7], here the characteristics of MANET with the challenges and the opportunities in achieving security models, such as confidentiality and integrity. They provide a wide survey of wormhole attack types and various detection techniques and at last qualitative comparison of wormhole detection methods. In [8], the authors proposed a new hybrid technique called WRHT: Wormhole Resistant Hybrid Technique, which is works like the methods such as watchdog and Delphi schemes. Its most striking feature of this proposed technique consists of is capacity to defend against almost all categories of wormhole attacks without depending on any accessories. ash based Scheme [9] Weichao Wang et al. designed a hash based method to obtain the node behavioural proofs which contains the data traffic information within the routing path .The scheme is based on auditing technique for prevention of the packet drop attack. The Sink Hole attacks are considered as a most vulnerable attack in the network layer. The detection and mitigation techniques were proposed to isolate the attacks without degrading the performance of the legitimate nodes. The detection techniques are varying based on the vulnerability and nature of the network. Here A.Salehi et.al [13] proposed an algorithm for detection of Sinkhole Attack in WSN through the consistency of data. The detection and mitigation can be achieved through the two different approaches such as centralized approach using geostatistical hazard model and distributed monitoring approach. This can be experimented and validated the correctness and efficiency through the simulation in existing [14].

II. CONCLUSION

In MANET, the attack detection and mitigation techniques are developed continuously to protect the network performance degradation and the evolution can comes under the improvements in the performance of this isolation of attacks. Here the network layer attacks such as Black Hole, Worm Hole attacks and Sink Hole attacks in routing are analyzed with the existing works. In future, the new technique can be proposed and the results will also be compared with the existing results.

REFERENCES

[1]. Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao , "*A survey of black hole attacks in wireless mobile ad hoc networks* ", Human-centric Computing and Information Sciences 2011.

[2]. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "*An Overview of Mobile Ad Hoc Networks: Applications and Challenges*".

[3]. Rajes Chowdari and Srinivas K, "*A Survey on detection of Blackhole and Grayhole Attacks in Mobile Ad-hoc Networks*", International Research Journal of Engineering and Technology, Vol. 04, Issue No.05, May 2017 pp. 1375-1378.

[4]. Jain, S., & Hemrajani, N. 2013, "*Detection and mitigation techniques of black hole attack in MANET: An Overview*",

International Journal of Science and Research (IJSR), India Online ISSN, 2319-7064.

[5]. Divya R and Maheswari D, "*Study of Various Security Attacks and in Network Layer and the Mitigation Techniques for MANET*", International Journal of Advanced Research in Computer and Communication Engineering", Vol.5, Issue No.2, February 2016, pp.404-410.

[6]. Alsumayt A and Haggerty J, "*A Survey of the mitigation methods against DOS attacks on MANETs*", Science and Information Conference, UK, August 2014.

[7]. Mudgal R and Gupta R, "*Study of various wormhole attack detection techniques in mobile ad hoc networks*", International Conference on Electrical, Electronics and Optimization Techniques, Published in IEEE, March 2016.

[8]. Rupinder, Jatinder and Ravinder Singh, "*WRHT: AHybrid Technique for Detection of wormhole attacks in WSNs*", Research article on Mobile Information Systems, Vol.2016 – 13pps, Nov 2016.

[9]. Wang W, Bhargava B, Linderman M, "*Defending against Collaborative Packet Drop Attacks on MANET*".

[10]. Goyal, P., Parmar, V., & Rishi, R., "*Manet: vulnerabilities, challenges, attacks, application*", IJCEM International Journal of Computational Engineering & Management, 11(2011), 32-37.

[11]. Kejun Liu, Jing Deng "*An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs*" IEEE transactions on mobile computing, vol. 6, no. 5, may 2007.

[12]. P.Rathiga, Dr. S. Sathappan "*Hybrid Detection of Black hole and Gray hole attacks in MANET*", 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions, 2016.

[13]. Ahmad Salehi, M.A.Razzaque, Parisa Naraei, Ali Farrokhtala, "*Detection of Sinkhole Attacks in wireless sensor networks", IEEE Conf. on Space Science and Communication*", September 2013.

[14]. H.Shafiei, A.Khonsari, and P.Mousavi, "*Detection and Mitigation of Sinkhole Attacks in wireless sensor networks*", Journal of Computer and System Sciences, Vol.80, Issue 3, pp.644-653, May 2014.

[15]. R.Sujatha, Dr.P.Srivaramangai," *Enhancing security in Manets Communication Issues and Mechanisms*", International Journal of Computer Techniques – Vol. 4 – Issues 3 (79-83) May – June 2017, ISSN: 2394 – 2231.

Authors Profile

Mrs R.Sujatha pursued Bachelor of Science & Master of Science from Bharathidasan University in year 2006, Bachelor of Education from Tamilnadu Teacher Education University in year 2011 and Master of Philosophy from Tamil University in year 2013. She is currently pursuing Ph.D. Her main research work focuses on Network Security and IoT . She has published more than 18 research papers in international journals, conferences & Workshops. Her areas of interest include Computer Networks, Internet of Thing, Grid Mobile Computing.

Dr.P.Srivaramangai received her Ph.D Degree from Mother Teresa University, Kodaikanal in the year 2012. She received her M.Phil Degree from Manonmaniam University, Tirunelveli in the year 2003. She received his M.C.A Degree from Bharathidasan University, Trichy in the year 1996. She is working as Associate-Professor, PG and Research Department of Computer Science, Marudupandiyar College of Arts & Science, Thanjavur, Tamilnadu, India. She has above 30 years of experience in academic field. She published 25 papers in National & International journals so far. Her areas of interest include Computer Networks, Internet of Thing, Grid Computing, Cloud Computing and Mobile Computing.