Trust based Intrusion Detection System for MANET

Adline Jancy Y
Department of ECE
Sri Ramakrishna Engineering College
Coimbatore, India
adlinjan@gmail.com

Gomathy B
Department of CSE
PSG Institute of Technology and Applied Research, Coimbatore, India
bgomramesh@gmail.com

Vijayakumar K
Department of ECE
Sri Ramakrishna Engineering College
Coimbatore, India
vijayakumar.k@srec.ac.in

Benston Jose *S*
Department of CSE
St. Peter's Institute of Higher Education and Research
Chennai, India
benstonjose.csa@spiher.ac.in

2025 International Conference on Next Generation Computing Systems (ICNGCS) | 979-8-3315-9116-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICNGCS64900.2025.11182737

***Abstract*— Wireless Sensor Networks (WSNs) are exposed to a number of network attacks. Blackhole attacks are those in which an attacker takes control of the nodes and modifies the programming of a set of nodes such that packets are stopped rather being forwarded to the base station. In response to a route request message, a node acts as a gray hole node, selectively discarding and forwarding data after finding the shortest route to the destination node. The system sends packets to their destination via the AODV protocol. As a result, data entered in the attack area is intercepted and cannot reach its destination, resulting in reduced throughput and end-to-end delays. The system employs the IDS AODV technology to enhance performance, allowing us to effectively reduce assaults on integrated MANET-Internet connection.**

Keywords--Blackhole Attack, Gray Hole Attack, Ad hoc On Demand Vector, MANET

I. INTRODUCTION

Wireless sensor applications rely on vital information sharing between nodes, security in wireless sensor networks (WSNs) is critical. There have been a lot of security issues brought up because of the network's open rollout. By targeting the various protocol layers in WSN, the attackers disrupt the security system. A local area network (LAN) that connects devices directly without any infrastructure is known as an ad-hoc network. The individual network nodes forward packets to every node in the network. A group of nodes or other wireless devices that communicate directly with each other to exchange information form ad hoc networks. With an automated mobile node linking each other via a wireless environment devoid of permanent infrastructure in an Ad-hoc network.

A mobile ad hoc network (MANET) is characterized by a mobile node that can move in any direction and that uses radio links to self-configure, self-maintain, and self-organize itself within the network without the support of fixed infrastructure like centralized servers, routers, base stations, or fixed links. Because there is no central coordinator in the network, each node that participates in network communication is responsible for acting as a router during communication. All nodes are therefore provided with a routing mechanism to move a data packet from its source to its destination. Nodes are powered by a battery with a limited capacity, and they all experience high energy consumption, particularly while participating in data transfer for several sources and destinations.

Without a fixed infrastructure, Ad-hoc network are group of wirelessly connected mobile nodes which a self-configured, self-healing network. As the network infrastructure changes over a period, MANET nodes are free to change its location at random. By routing traffic to other nodes in the network, each node acts as a router. This is a simple, quick-to-implement circumstance that prevents a more streamlined fixed-line network from being employed in other scenarios such as battlefields, emergency disaster relief, and conferences.

The network layer is sent packets from the source to the destination by finding the best route—that is, the path with the lowest cost and shortest route from the source to the destination. The network layer attacks is to disrupt the chosen route by the routing protocols between the source and the destination.

A node uses Ad hoc On-Demand Distance Vector (AODV) Routing protocol to search a route to a destination and Routes remain connected as long as the source transmits. Routes are loop-free and updated sequence numbers. AODV reacts to network topological changes and the attacked nodes. The HELLO messages that support route maintenance are range-limited, and limits network overhead.

When it comes to route discovery, the conventional AODV routing protocol has security problems. To reach its target, the data must be sent via a secure channel.

In order to facilitate, the proposed process can identify both Black hole attack and Gray hole attack in the network layer of MANET. Black Hole Attack is a DoS attack that the sender sends a Route Request (RERQ) package to create a path when the malicious body responds to the sender using the Route Reply (RERP) message. The sender node accepts it as a legitimate route and continues on that path; additionally, it will ignore another RERP message delivered through the original destination node, and through the malicious node, the sender node will transmit packets. After then, a malicious node discards every packet. The NS2 simulator was used to carry out the attack in this paper's analysis of the black hole and gray hole.

In this paper, a simulation-based trust parameter analysis of an assault in a Mobile Adhoc Network is undertaken. In the absence of an attack, packet drop reduced and throughput and PDR rise as network traffic increases. Similar to this, PDR and throughput drop as the number of black and gray holes rises. Black hole and gray hole attacks reduce the average latency, which is influenced by the

Gray hole attack scenarios is compared in the table, with an intrusion detection system (IDS). A Black hole attack provides a 0% packet delivery ratio since the throughput and end-to-end delay are both zero. This shows the disruption of all data is by the Black Hole attack. However, all 1,238 packets are successfully received when IDS is used with AODV, causing 100% delivery at a throughput of 51.23 kbps and an end-to-end delay of 29.65 ms.

A Gray hole attack resulting in a 71.79% packet delivery ratio, a throughput of 25.75 kbps, and an end-to-end delay of 8.962 ms, as only 2,819 of the 3,927 packets generated are received. Through increasing the packet delivery ratio to 76.94%, throughput to 27.60 kbps, and slightly increasing the delay to 9.577 ms, the IDS helps to prevent this attack as well. There is also a decrease in packet drops from 1,181 to 979.

Black hole attacks are more severe and completely make communication breakdown. IDS system increases the network performance by detecting and removing malicious node. Gray hole attacks still have packet drops even with IDS and this table1 indicates the way IDS works to promote network security and efficiency.

V. CONCLUSION

In this paper, a simulation-based trust parameter analysis of an intrusion in a Mobile Adhoc Network is undertaken. In this paper, a simulation-based trust parameter analysis of an assault in a Mobile Adhoc Network is undertaken. In the absence of an attack, packet drop reduced and throughput and PDR rise as network traffic increases. Similar to this, PDR and throughput drop as the number of black and gray holes rises. Black hole and gray hole attacks reduce the average latency, which is influenced by the attacker's proximity to the sending node in all simulations. In every case that has been investigated and examined, the network parameter degrades with the black hole attack. Under no attack conditions, throughput and PDR improve as network traffic increases, while packet drop decreases. Additionally, it has been discovered that the greater the attacker is to the source, the bigger the impact. PDR and throughput drop as the number of black and gray holes rises. The average delay is affected by the attacker's proximity to the sending node in all simulations, and it is reduced with black and gray hole attacks. This occurs as a result of the black hole transmitting the RREP with the highest destination sequence number before looking up a route in its routing table. Finally, it is concluded that these trust parameters are definitely produced high performance in the attacker nodes detection.

[1] Sravanthi Godala, Rama Prasad V. Vaddella, “A Study on Intrusion Detection System in Wireless Sensor Networks”, International Journal of Communication Networks and Information Security, Vol. 12, No. 1, April 2020.

[2] Ishmanov, F. Mallik, S.A,Kim, S.W,B.Begalove ,“Trust Management System in Wireless Sensor Networks: Design and Research Challenges”, Trans emerge. Telecommunication technology-2013.

[3] Y.Adline Jancy, B.Gomathy, A.Benuel Sathish Raj, “A Secure Ant Colony based Trust Computation Model in Wireless Sensor Networks”, Journal of Physics: Conference Series, 2021.

[4] Jian Wang, Shuai Jiang, S, and AbrahamO. Fapojuwo, “A Protocol Layer Trust-Based Intrusion Detection Scheme for Wireless Sensor Networks”. Journal of Sensors, May 2017.

[5] R.Sugumar, A.Rengarajan and C.Jayakumar, “Trust based Authentication Technique for Cluster based Vehicular Ad hoc Networks(VANET)”, Wireless Networks 2018.

[6] Harsimran Kaur and Mani Sahore, “A Survey on Wireless Sensor Network Security Using AI Methods” International Journal of Latest Trends in Engineering and Technology Vol.(7)Issue(4), pp.234-239.

[7] Sherin Hijazi , Mahmoud Moshref and Saleh Al-Sharaeh “Enhanced AODV Protocol for Detection and Prevention of Blackhole Attack in Mobile Ad Hoc Network” International journal of computers & technology, February 2017.

[8] Luo, W., Ma, W., Gao, Q., “A dynamic trust management system for wireless sensor networks.” Secure Communication Network- 2016.

[9] Heta Changela and Amit Lathigara, “Algorithm to Detect and Overcome the Black Hole Attack in MANETs”, International Journal of Computer Applications, August 2015.

[10] R Ramya, S Sharmila Devi, Y Adline Jancy, : An Overlook on Security Challenges in Industry 4.0, Intelligent Analytics for Industry 4.0 Applications, 2023.

[11]Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, Karl Levitt, “A specification-based intrusion detection system for AODV” Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, Pages 125 – 134, 2003.

[12] Kalnoor, G., and Gowrishankar, S. "Minimizing energy consumption for intrusion detection model in wireless sensor network." In Applications of Artificial Intelligence and Machine Learning, pp. 527–537, Springer, Singapore, 2021.

[13] Singh, N., Virmani, D., and Gao, X. Z. "A fuzzy logic-based method to avert intrusions in wireless sensor networks using WSN-DS dataset." International Journal of Computational Intelligence and Applications, vol. 19, no. 3, article 2050018, 2020.

[14] Smys, S., Abul Basar, and Haoxiang Wang. "Hybrid Intrusion Detection System for Internet of Things(IoT)." Journal of ISMAC 2, no. 04 (2020): 190-199.

[15] G. Vetrichelvi, Dr. G. Mohankumar, “ A Detailed Survey On Attacks And Intrusion Detection in MANETs”, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 7, July – 2013.