Detection and removal of multiple black hole attacks through sending forged packet in MANETs

Kheeramani[1], Prof. Sangeeta Thakur[2]

[1]Student Master of Technology, Department of Electronics and Communication Engineering SIRDA Group of Institution H.P. Technical University Hamirpur India.
[2]Asst. Professor, Department of Electronics and Communication Engineering SIRDA Group of Institution H.P. India

---

Abstract A heterogeneous network is a Mobile Ad-hoc network. They have unique characteristics like as high mobility, multi-hop routing, an open platform, and no fixed infrastructure. An ad-hoc system is vulnerable to a variety of security threats. Authors discuss implementation of the AODV protocol extension, notably the sequence number variation technique, in this paper. The AODV demonstrated good AODV behaviour. The protected field of the RREQ and RREP packet formats was employed in the sequence number variation technique. In AODV, the SNV technique provides security against black-hole and gray-hole assaults. Simulations using the NS 2.35 simulator were used to conduct analyses based on PDR, throughput, and latency of the selected node. In comparison to a previously suggested methodology, the simulation outcomes show that the suggested technique enhances network performance in the presence of attackers.

Key Words: ***WSN, MANET, AODV ,Black hole attack , Sequence Number variation approach,NS2***.

1. INTRODUCTION

Because nodes are not required to be physically stationary, the utilization of wireless networks has skyrocketed [1]. MANETs are such infrastructure-free wireless networks in which nodes communicate with each other via multihop pathways [2]. Because to qualities like as dynamic topology, simple node deployment, distributed administration, MANETs have acquired appeal in a variety of sectors including military operations, natural calamities, maritime communications, automotive computing, distant-weather prediction. Given their popularity, MANETs' qualities expose them to a variety of problems.

Every node in a MANET is responsible for routing packets [3]. In MANET, routing protocols are grouped into two types: proactive routing protocols and reactive routing protocols. The proactive protocols generate per-defined pathways among network nodes, whereas the reactive protocols establish on-demand routes, that is, they are established only when communication enables is required. If no communication happens over the preset routes, network packets may be wasted. As a consequence, reactive routing techniques for such networks have grown in favour. Reactive routing systems, on the other hand, are vulnerable to a variety of attacks.

An adversary could use the fact that the nodes are routers to undertake a variety of malicious behaviors in order to stifle communication among them. Because traditional routing technologies lack security safeguards, typical legitimate nodes may fall under the sway of attackers and become compromised. Privacy protection is also a concern in infrastructure-free networks such as MANETs [4]. Several researchers have worked to develop answers to these varied problems [5]. Different secure routing strategies are designed to counteract the adversary's negative impacts in order to permit seamless communication in the presence of such adversary nodes. The cryptographic techniques are employed informally to achieve network confidentiality .The employment of a hashing algorithm is also employed to address privacy concerns in transmission of data among mobile nodes and cars . In addition, cluster management and classification-based strategies are employed to mitigate the negative consequences of a MANET's dynamic topology [6]. Furthermore, numerous safe routing systems have been suggested to accomplish quality-of-services (QoS) by solving the eligibility presented by DoS attacks.

The sequence number attack (also known as the grayhole or blackhole assault) is a DoS attack in which the attacker attempts to prevent the benign node from receiving data packets. Sequence number attacks generate packet forwarding errors throughout data transfer with the sole purpose of lowering network performance. During the initial phase, the adversary node makes an effort to join the route. The adversary accomplishes this by sending a forged route reply packet (RREP) claiming to have a faster path to the destination [7]. The adversary node does this by delivering an RREP packet with a fictitious destination sequence number, indicating that the route is relatively fresh. As a consequence, the source node believes that the adversary node transmitting the RREP has a more recent route to the destination. As a result, the adversary node begins packet dropping behaviour after joining the route between the sender and recipient.

This paper is organized as follows: Section II describes the literature survey of proposed work. Section III illustrates the proposed objectives and Section IV shows the experimental results obtained by using the proposed approach. Finally ,the paper concludes with Section V.

II.LITERATURE SURVEY

Umar et al.,(2018) offers Improved CBDS, a method for controlling and mitigating cooperative black hole/gray hole attacks in mobile ad-hoc networks that combines an RSA public key cryptosystem into a current CBDS. A comparable system was constructed with 50 connected devices using network simulator version 2 (NS2), in which some nodes function as black hole attackers & eavesdroppers, similar to CBDS. The sender-receiver connection was modeled using User Datagram Protocol (UDP), with the help of CBR , traffic was generated using constant packets over the UDP link. Following the evaluation, the improved CBDS exceeded the existing CBDS by 22.22 percent in terms of packet delivery ratio, 36.36 percent in routing overhead, 10% in E2E delay, enhanced network throughput[8].

Saptura et al.,(2020) The Improved Check Agent approach sends a checking agent to record nodes that are considered black okay in order to detect black hole assaults. The implementation will be put to the test on a ZigBee-based wireless networks. A mesh network topology is used, with every node having multiple routing tables[10].Throughput could be increased by 100 percent using the Enhanced Check Agent technique[9].

Amit Kumar et al., (2015) presented a interaction factor dependent analytic methodology in this study. Wormhole attacks are one sort of attack in which two or more nodes share bandwidth & interrupt communication. A wormhole-infected network is created, as well as a work style for reliable communication in the attacked network is suggested. To improve communication and discover a safe communication node, a system model is developed. The researchers also look at how to create a secure way in an attack-based mobile network. Ultimately, the suggested framework provided variable adaptive communication that was improved. As per the findings, the model's performance has increased in terms of communication throughput and loss reduction[11].

Juhi Biswas et al., (2014) In practical systems, the AODV has been enhanced to detect & avoid wormhole invasions. On enhanced AODV, the MANET and Wormhole Attack Detection and Prevention Algorithms are used. The node authentication mechanism is used to try and eliminate false positives in the system. Furthermore, simulation results demonstrated that node validation not only prevents false positives, but also aids in mapping the true location of the wormhole, effectively acting as a type of double validation attack detection. Without any additional equipment, the technology detects wormhole attacks[12].

Elmahdi et al.,(2018) Reliable data transmission is an issue, supposing that routes from a sender to a receiver have already been created. For security, the suggested method uses an adhoc on-demand multipath distance vector (AOMDV) protocol and a homomorphism encryption algorithm. The suggested scheme's performance is steady, but AOMDV's performance degrades when malicious nodes are introduced into the network. The presence of black hole nodes in our suggested architecture improves packet delivery ratio & network throughput[13].

Dhende et al.,(2017) For identification & eradication of black hole and grey hole attacks in MANTEs, studies suggested a secure AODV protocol (SAODV). To obtain the results for analysis, the suggested technique (SAODV) is simulated using NS-2 to the AODV protocol. To obtain the findings, the number of nodes is adjusted from 45 to 85 during the simulation. The following performance metrics were utilized to contrast SAODV to normal AODV: PDR (percent), Delay, Overhead, Throughput. In comparison to the normal AODV protocol, the overhead is reduced to 9.42 percent and the bandwidth is increased by 6%, according to the testing results[14].

Table I. Comparison Of Various Black Hole Attack Detection Method

Proposal Name	Proposal Name	Assumption	Philosophy
Modified AODV protocol to prevent black hole attack. Modified AODV protocol to prevent black hole attack.[15]	AODV	Multiple Black Hole	Single Black Hole node
New method for detection and prevention single black	AODV	Single Black Hole	Single Black Hole
Agent based Aodv protocol for	Agent based AODV	Multiple and Cooperative black hole	Single Black Hole
Detect and avoid black hole attack[18].	AODV, MIAODV	Multiple and Cooperative black hole	Single Black Hole attack
Rebroadcast routing protocol for black hole[20].	NCPR DSR	Single Black Hole	Single Black Hole
Prevention of black hole attack using Trust based computing[19] .	TAODV	Cooperative black hole nodes	Single Black Hole Attack

III.PROPOSED OBJECTIVES

Wireless communication is helpful in connecting nodes of mobile ad hoc networks. Because the connection is wireless, nodes are subject to attacks such as black holes, worm holes, denial of service, and so on. The purpose of this study is to keep an eye on black hole attacks and detect them. MANET security is critical to preventing the harm that various forms of assaults may do. The black hole assault is regarded as common network attacks, with goal of preventing any network connection. When a routing protocol is needed, it works for identifying smallest way among two nodes in the network those wanted to communicate. AODV protocol does not include a mechanism for identifying and preventing black-hole attacks. The goal of research is to improve AODV routing protocol with lightweight technique for detecting and preventing blackhole attacks in network. To find the malicious nodes, we used a sequence number variation technique. As a result, the network's efficiency is limited in terms of energy consumption, packet delivery ratio, and throughput.

Research Gap:

The existing scheme proposes to find malicious nodes in network by making use of forged packets. These are the packets in which address of non-existent destination is used

are for broadcasting process. The black hole nodes tend to reply even to the non-existent destination positively. This is the base for detecting malicious nodes in network.

The issue with this approach is that the broadcasting of the forged packets consumed large amount of energy from nodes. This approach, however is able to detect the malicious nodes, is energy-inefficient. Therefore, we need to work on the detection approach which is friendly with the resources of the nodes as well.

Objectives:

1. To implement the existing approach in NS2.35 and analyze its performance.

2. To detect the malicious nodes using the sequence number variation approach.

3. To implement the proposed approach in NS2.35.

4. To compare the proposed and existing approach based on packet delivery ratio, throughput and energy consumption of network.

Research Methodology:

The proposed method aims to detect malicious nodes in network using sequence number variation approach. Since, malicious nodes tend to reply back to source node with very high sequence number in route reply packet; their sequence numbers are abnormal as compared to normal replies. Hence, we can compare the abnormalities in the sequence numbers to detect these nodes; on the back of this method we name this as sequence number variation approach.

Initially, the source node will broadcast normal route request packets in network; these packets will have address of normal existing destination in the network. Once the request reaches destination node, it will forward route reply to source node over all the paths. These replies will be of dual nature when it comes to sequence numbers in the packets.

The replies from the normal nodes which have actual address to the destination node will have normal sequence number; the replies from the malicious nodes which do not have address to the destination node will have very high sequence number.

At source node, received sequence numbers will be compared with each other. If any abnormality is found, it will be marked as malicious node. As a prevention step, the source node will not send packets to these nodes in network. Source node, now, from other routes will choose the one that has nodes with highest remaining energy in the network. The selected path will be chosen to forward data to the base station.

IV.RESULTS

The proposed solution was created using NS2.35, an open-source framework for simulating sensor networks, MANETs and VANETs. The languages used in this toolkit include utility command language, C++, and awk scripts. The main scripting is always written in tcl and supplied as input to the simulator. The simulator generates two types of files: trace files and nam files. These documents keep track of information about network's nodes as well as data that are delivered.

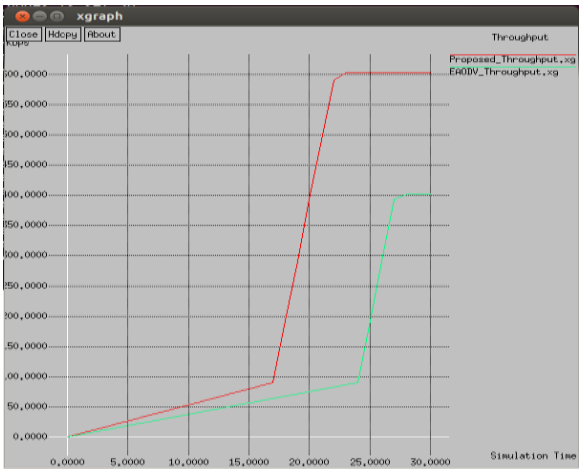

Figure 1: Throughput of the network

The above figure represents a graph for which X-axis shows simulation time and Y-axis shows throughput of the network. The throughput which is described as data obtained at destination node per unit time,

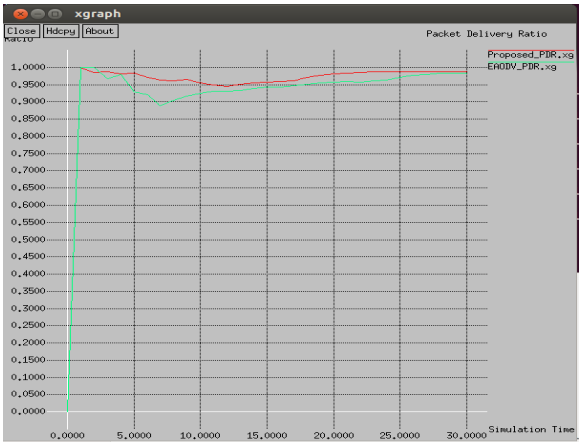

Figure 2: Packet Delivery Ratio in the network

Figure 2 is a graphical representation where X-axis and Y-axis shows simulation time and Packet Delivery Ratio of the network respectively.

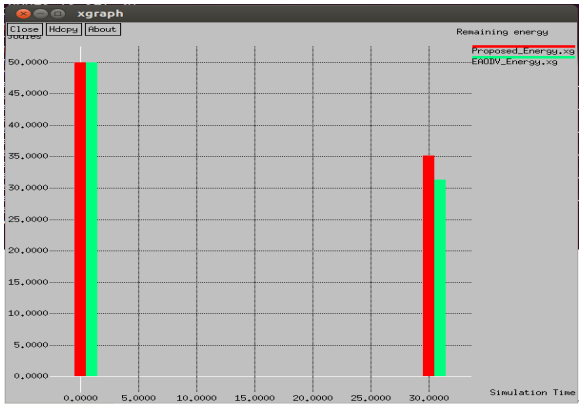

Figure 3: Remaining Energy

Figure 3 represents a graph having parameter Remaining Energy on Y-axis and simulation time on X-axis.

V.CONCLUSION

MANET nodes must rely on other nodes in order to communicate within the system. MANET's qualities are extremely valuable to enemies that seek to undermine network performance. The suggested approach wants to minimize attackers from accessing the channel, hence increasing packet delivery rate and thereby service quality. The bait demand and the prediction of the destination sequence number provide a double security check to establish the node's status as malicious. As a consequence, it is reasonable to conclude that the suggested technique is efficient in finding malicious nodes and preventing black hole attacks.

REFERENCES

[1]R. H. Jhaveri and N. M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," International Journal of Communication Systems, vol. 30, no. 7, 2017.

[2]A. D. Patel and R. H. Jhaveri, "Addressing packet forwarding misbehavior with two phase security scheme for AODV-based MANETs," International Journal of Computer Network and Information Security, vol. 8, no. 5, pp. 55–62, 2016.

[3]Z. Zhao, H. Hu, G.-J. Ahn, and R. Wu, "Risk-aware mitigation for MANET routing attacks," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 250–260, 2012.

[4]B. Li, Y. Huang, Z. Liu, J. Li, Z. Tian, and S.-M. Yiu, "HybridORAM: Practical oblivious cloud storage with constant bandwidth," Journal of Information Sciences, 2018.

[5]C. Gao, Q. Cheng, P. He, W. Susilo, and J. Li, "Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack," Information Sciences, vol. 444, pp. 72–88, 2018.

[6]Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphic proxy signature scheme," IEEE Access, vol. 6, pp. 12966–12972, 2018.

[7]A. D. Patel and K. Chawda, "Dual Security Against Grayhole Attack in MANETs," Advances in Intelligent Systems and Computing, vol. 309, no. 2, pp. 33–37, 2015.

[8]Umar, M., Sabo, A., & Tata, A., "Modified Cooperative Bait Detection Scheme for Detecting and Preventing Cooperative Blackhole and Eavesdropping Attacks in MANET", International Conference on Networking and Network Applications (NaNA),2018. [9]Saputra, R., Andika, J., & Alaydrus, M. , " Detection of Blackhole Attack in Wireless Sensor Network Using Enhanced Check Agent", Fifth International Conference on Informatics and Computing (ICIC),2020.

[10]J. Sun and X. Zhang, "Study of ZigBee Wireless Mesh Networks", in 2009 Ninth International Conference on Hybrid Intelligent Systems, 2009, pp. 264–267, 2009.

[11]Amit Kumar, Sayar Singh Shekhawat, "A Parameter Estimation Based Model for Worm Hole Preventive Route Optimization", IJCSMC, Vol. 4, Issue. 8, August 2015.

[12]Juhi Biswas, Ajay Gupta, Dayashankar Singh, "WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol"", 9th International Conference on Industrial and Information Systems (ICIIS), 2014.

[13]Elmahdi, E., Yoo, S.-M., & Sharshembiev, K., "Securing data forwarding against blackhole attacks in mobile ad hoc networks", IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC),2018.

[14]Dhende, S., Musale, S., Shirbahadurkar, S., & Najan, A., "SAODV: Black hole and gray hole attack detection protocol in MANETs", International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),2017.

[15]Ronima Sharma, Rajesh Shrivastava, "Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network", in IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[16] Iman Zangeneh, Sedigheh Navaezadeh, Abolfazl Jafari, "Presenting a New Method for Detection and Prevention of Single Black Holes Attack in AODV Protocol in Wireless Ad Hoc Network", in International Journal of Computer Applications Technology and Research Volume 2 Issue 6, 686 – 689, 2013.

[17]Roopal Lakhwani, Sakshi Suhane,Anand Motwani, "Agent based AODV Protocol to Detect and Remove Black Hole Attacks", in International Journal of Computer Applications (0975 8887) Volume 59 No.8, December 2012.

[18]Jaspinder Kaur,Birinder Singh, "Detect and Isolate Black Hole Attack in MANET using AODV Protocol", in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 2, February 2014.

[19]Ashish Sharma , Dinesh Bhuriya ,Upendra Singh "Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing", in International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014.

[20]Hafessa M Habeed,Selin.M., "A Secure Probabilistic Rebroadcast Routing Protocolbased on Neighbor Coverage in Mobile Adhoc Networks", in International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 September 2014.