International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)

ISSN: 0976-1353 Volume 29 Issue 7 – Aug 2022.

DETECTION AND PREVENTION OF GREYHOLE ATTACK IN MANET USING AODV ROUTING PROTOCOL

Mrs.M.Sahila M.E
Department of Electronics and Communication Engineering,
Bharath Niketan Engineering College
Aundipatty,Tamilnadu 625536

G.Ravivarman
Department of Electronics and Communication Engineering,
Bharath Niketan Engineering College
Aundipatty,Tamilnadu 625536

Abstract: Communication is considered an essential part of our life. A different medium was used to exchange information, but advances in technology resulted in different network settings. One of the most suitable in the wireless field is wireless sensor network (WSN). These networks are created by self-organizing nodes that operate in a radio environment. Because communication is faster, they are limited to many attacks that operate at different layers. For communication to be effective, some security measure must be in place in the network if it has secure communication. In this article we describe various attacks operating at different layers, one of the common network layer attacks called Blackhole Attack with its mitigation technique using Intrusion Detection System (IDS) through ns2 network simulator was also discussed.

Keywords:WSN, IDS, through ns2 network simulator

.

I. INTRODUCTION

A wireless sensor network (WSN) is a distributed, autonomous network that consists of nodes (sensor nodes) arranged in a certain environment. These sensor nodes monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants, in various areas [1]. A sensor node is a small and simple device with limited computing resources. They are randomly and slowly arranged in the sensed environment [2]. Wireless sensor networks are widely used in various applications such as area monitoring, forest fire monitoring, military surveillance, health care, and water quality management. WSN has a number of security issues. There are some limitations in WSNs such as limited lifetime, required low power consumption and less storage [3] [4]. Based on these limitations and due to the noisy climate in which they are arranged, WSN are highly affected and vulnerable to many types of attacks [5]. An intrusion detection system (IDS) is a system that monitors system or network activities against some malicious activities and informs the master station. The system is generally divided into two categories: IDS exploits and IDS anomalies. When IDS is misused, the malicious activity is evaluated by comparing new data with a previously stored signature in the system database. Abnormal activities in the IDS anomaly are detected from a predefined normal profile [5]. Several schemes have been proposed for intrusion detection in WSNs. In [6], a malicious node is detected using the signal strength, and if the strength conflicts with the geographic location of the originator, the message transmission is considered suspicious. Rule-based intrusion detection schemes are used in [7][8]. In a rule-based scheme, an intrusion is detected by a set of rules that are defined before the detection phase. These rules are applied to data obtained from network behavior. If the data meets the rule, it is considered normal, otherwise it is considered malicious. An alarm is triggered when an intruder is detected. Various multipath routing techniques have also been proposed in routing. The aim of this technique is to provide the best redundancy path with high energy efficiency.

II. LITERATURE REVIEW

Royer E. M, Toh C.K, emphasized that, in order to ensure the security between two communicating nodes, a protocol must enable the destination node to identify the source of a given message, and the source node must be able to authenticate the legal destination node.

Yu Y, Guo L, Wang X, Liu C, a secure routing protocol with payment mechanism that prevents node selfishness for mobile ad hoc networks is proposed. A source node can securely send a confidential message to the destination node through a number of intermediate nodes. In addition, all messages transmitted between nodes should be verified and protected in the protocol.

Wei C.H., Hwang M.S., Augustin Y. H. C, presents a reputation-based routing scheme for hierarchical ad hoc networks and the cluster head, acting as the reputation manager for updating reputation information. Thus, the malicious nodes would be isolated for safeguard routing security.

Ramaswamy S, Fu H, Sreekant Aradhya M, Dixon J, Nygard K., a mechanism is proposed to defend cooperative black hole attack. Each node observes the data forwarding nature of its neighboring node. This information is recorded in a DRI (Data Routing Information) table. Each node maintains an additional DRI table. Panicker and Jisha proposed various attacks in the MANET, particularly in network layer especially black hole attack, which is reduced by three mechanisms like TOGBAD, SAR protocol, and DPRAODV protocol [5] based reduction. It has some cons like protocol functionality, route distance, and network overload. To overcome this drawback, we introduced the new approach for black-hole detection algorithm to detect the maliciously behaving nodes and produce the cost-effective and ensure QoS guarantee by proactive alleviation procedure.

Wu et al. proposed survey on attacks and countermeasures in MANET to achieve security goals, such as access control, authentication, availability, confidentiality, integrity, and non-repudiation [6]. It also provides the MANET-IDS (Intrusion Detection Systems) to prevent attacks. Through this survey, we analyze the various ad hoc networks countermeasures in terms of packet delivery ratio and QoS guarantee such as network support, availability, and time consumption of the specific nodes on the networks.

Bhattacharyya et al. proposed DATA traffic attacks and CONTROL traffic attacks to preserve the networks with respect to the RREQ and RREP methods. Thus network layer DATA traffic attacks are reduced by the proactive alleviation procedure.

Gagandeep and Kumar proposed the various types of attacks under protocol stack and routing. Security issues associated with mobile ad hoc network attacks were classified based on the active and passive attacks. In particular, the active attacks like timing attacks are reduced based on the rushing attacks against on-demand routing protocols. These procedures are helpful to us to reduce the timing attacks like the ad hoc networks.

Su M.Y., Chiang K.L., Liao W.C, anti-black-hole mechanism is discussed. Every node is subjected to an estimation of the suspicious value. The suspicious value is found based on the amount of abnormality in RREQ and RREP packets of the node. When the suspicious value exceeds a threshold value, the node is identified as a black hole and the Intrusion Detection System (IDS) will blacklist the node and the time of identification. Thus the cooperative black hole nodes can be identified. The drawback is that the mobile nodes have to maintain training data and regular updates.

Lo N.W, CBDAODV mechanism is proposed. A source node will accept at least two RREP packets from different replying nodes. Thus by utilizing another routing path, the source node itself can evaluate the reliability of the currently selected

route and make a rerouting decision once it suspects the reliability of currently selected route. Through another route, a confirmation control packet which consists of the name of the second malicious node to which the first malicious node sends the data packets is sent. On receiving the packet, the destination node will reply to indicate the existence of the route between the destination and the malicious node. If the reply packet indicates that no path exists, the source node now switches its routing path to the alternate route and retransmits its data packets. Also the malicious nodes are put to observation, to identify whether the nodes regularly work in cooperation with each other.

Tamilselvan L, Sankara Narayanan V, a solution is proposed by modifying the AODV protocol to avoid multiple black holes in the group. It maintains a fidelity table. Every participating node is given a fidelity level that tells the reliability of that node. Any node having value as 0 is considered as malicious node and is eliminated from the network. The fidelity levels of the nodes along a route are increased on every successful transmission of the data; otherwise the fidelity level of the nodes is decreased. The processing delay in the network is high.

Mistry N. H, Jinwala D. C, Zaveri M. A, in this paper MOSAODV mechanism is presented, where a timer is set in the source node to collect all the RREP packets and those packets with exponentially high destination sequence number are discarded.

III. EXISTING SYSTEM

A routing protocol can take over an existing routing protocol, and we give the shortest path protocol as an example. Node A on the route selects the neighbor that is closer to the sink and has high confidence as the next hop. If there is no node among all neighbors closer to the sink that has confidence above the default threshold, it will notify the upstream node that there is no path from and to the sink. The top node, working in the same way, reselects another node from its neighbors closer to the sink until data is routed to the sink or there is conclusively no path to the sink.

Disadvantages of Existing System

- No Security
- More Memory Space Is Required
- Some Limitations

IV. PROPOSED SYSTEM

The existing mechanism has certain limitations. First, no communication will take place if no shared hops are present between the paths. Second, the time delay increases as the reception and processing of RREP packets by the source increases. Each node maintains an additional table, so more memory space is needed. The proposed method uses the watchdog technique for detection. When a node sends data, the selected watchdog monitors another node to verify that it is also sending data further. If a watchdog finds any node that does not forward data, that node is considered a malicious node. A simple technique used by a sentinel node to detect a malicious node in a network by eliminating route spoofing.

Advantages of Proposed System

- Eliminating the False Route Entry.
- High Security
- Less Memory Space Requirment

Figure 2. Data Flow Diagram

ISSN: 0976-1353 Volume 29 Issue 7 – Aug 2022.

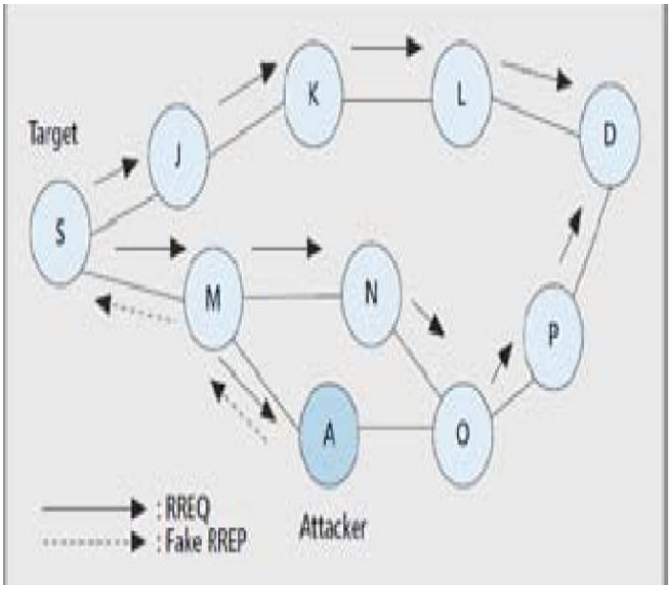


Figure 1 Architecture Diagram

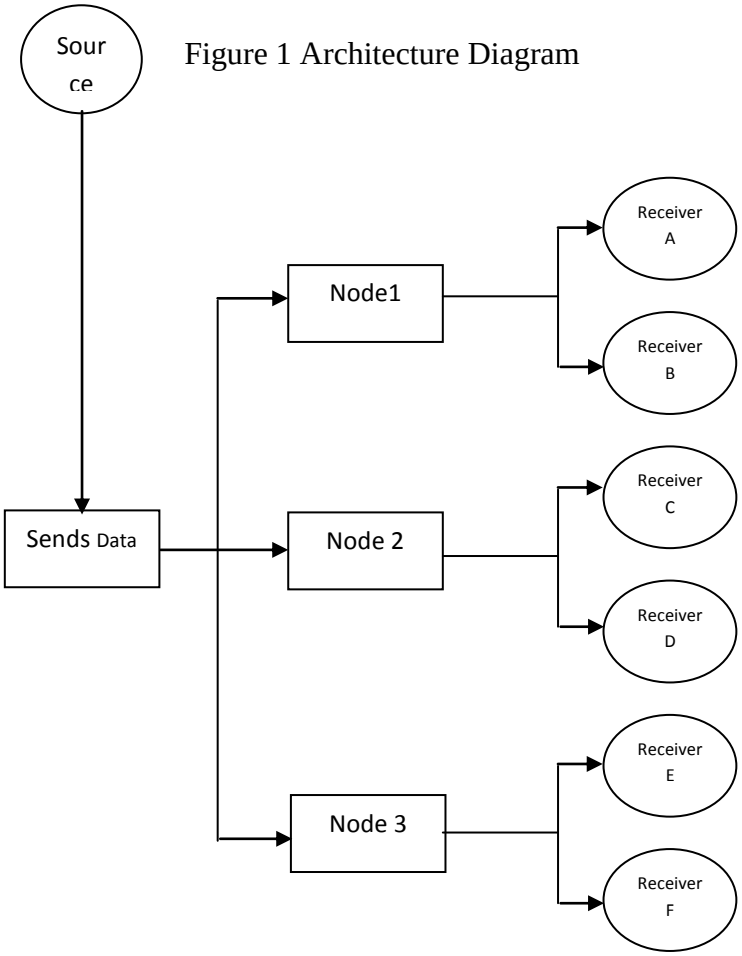


Figure 2 Data Flow Diagram

V. METHODOLOGY

Network Model

We believe that line-level security has been introduced through a common protocol based on cryptography. Therefore, we consider the link key to be secure as long as the adversary does not physically compromise either side of the link.

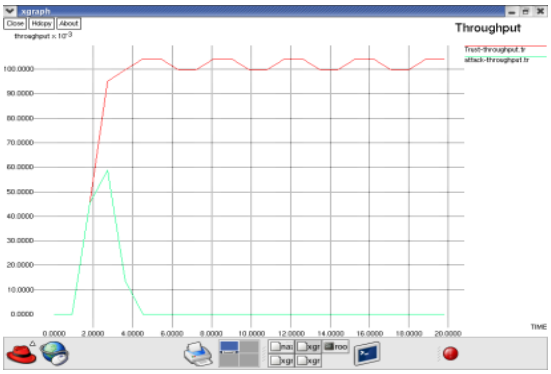


Figure 3 Graph

Graph Analysis

In this graph, it will show the existing and proposed throughput and the ratio of delays and losses. It will provide the final result of the final result of the existing proposed work in graphical representation.

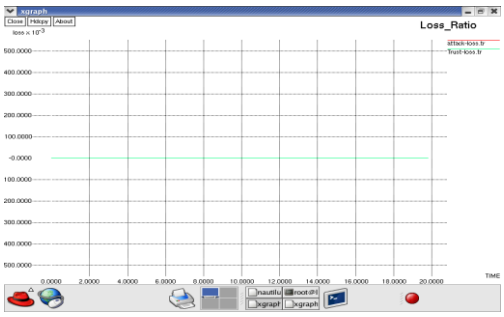
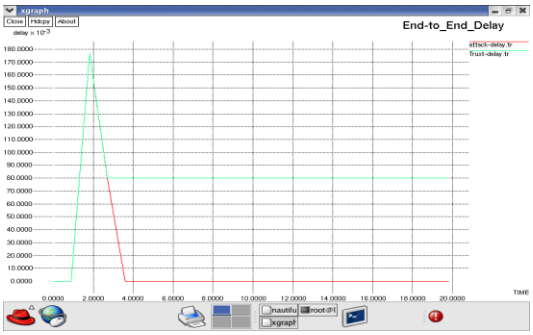
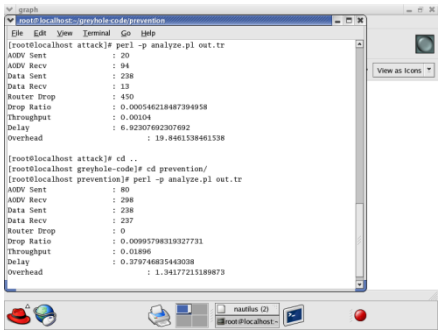


Figure 4 Loss Ratio



Result A Figure 5 End to End Dealy

It will give you AODV data bytes sent, AODV data bytes received, data sent, data received, router drop, drop ratio, throughput, delay and overhead.



VI. CONCLUSION

In this paper, we have presented an effective method for detecting black hole attack in a wireless sensor network. The watchdog technique is implemented in this work. The proposed model better improves the network performance by avoiding the malicious node from the network. Future work may focus on detecting other attacks and comparing with a black hole attack with a different routing protocol. They can be categorized based on how much they affect network performance. Detection of additional attacks and strategies to eliminate these attacks must be performed in future research.

REFERENCES

[1] M. Tiwari, K.Veer Arya, R. Choudhari, K. Sidharth Choudhary, "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", "2009 Fourth International Conference on Computer Sciences and Convergence Information Technology"

[2] E. Nam Huh and T. Hong Hai, "Lightweight Intrusion Detection for Wireless Sensor Networks"

[3] J. Du, J. Li, " A Study of Security Routing Protocol For Wireless Sensor Network", "2011 International Conference on Instrumentation, Measurement, Computer, Communication and Control"

[4] F. Bao, I. Ray Chen, M. Jeong Chang, and J.-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", "IEEE Transactions On Network And Service Management, June 2012"

[5] M. A. Rassam, M.A. Maarof and A. Zainal, "A Survey of Intrusion Detection Schemes in Wireless Sensor Networks", "American Journal of Applied Sciences, 2012" [6] W. Ribeiro Pires J´unior, T. H. de Paula Figueiredo H. Chi Wong, A. A.F. Loureiro, "Malicious Node Detection in Wireless Sensor Networks", "Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04),IEEE 2004"

[7] V. K. Jatav, M. Tripathi , M S Gaur and V. Laxmi, "Wireless Sensor Networks: Attack Models and Detection", "2012 IACSIT Hong Kong Conferences IPCSIT vol. 30 (2012) © (2012) IACSIT Press, Singapore"5, no. 1 (2010).