IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Special Issue 2, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

An Effective Strategy for Black Hole Nodes in WSN, Affording A Reliable Way of Sending Data from Source to Destination Node Through A Fixed Data Transmission

Mrs. A. Rukmani[1], Dr. C. Jayanthi[2], Mrs. D. Annalakshmi[3]

Research Scholar, PG & Research Department of Computer Science, Government Arts College (Auto), Karur, Tamil Nadu, India[1,3]

Assistant Professor, PG & Research Department of Computer Science,Government Arts College (Auto), Karur, Tamil Nadu, India[2]

ABSTRACT - Wireless sensor networks are used in far places to cover the network, based on environmental condition that may be in fixed topology or random. Difficulty arises in recharging or replacing the batteries of sensor nodes which are so far to make the ad hoc networks. If two nodes are in out of range, then there is no direct link between them to communicate, but the data can be sent between them using the multi hoping property. Various attacks that are possible in Wireless Sensor Networks are passive attacks and active attacks. Wireless Sensor Network is liable on several attacks, in which Black hole is verycomplex to detect and isolate. An intruder captures the set of nodes in the networks and reprograms them to block the transmitted packets which are transmitted to the base station. The reprogrammed nodes are called black hole nodes and the region that holds such nodes are black hole region. So the information which entered into the black hole region is captured and that causes a long delay in delivery of packets. Black hole is a malicious attack which traps sensor protocols that are routing it. In this Optimal Segregation RoutingProtocol (OSRP) is used to exploits a malicious node for discovering routes. When a route request is broadcasted by a source node, different nodes are deception by the destination. If the attacker node involves the selected path, then the traffic drops the packet in selective manner. Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR) is considered for the performance crisis. This also effect on hierarchical routing protocols,which will create a relation reliable and efficient.

KEYWORDS: passive attacks, active attack, Black hole, Optimal Segregation Routing Protocol (OSRP), packet delivery ratio and packet loss ratio.

I. INTRODUCTION

Wireless sensor network communication between different nodes is achieved via electromagnetic waves and the communication medium is wireless. Also, the range of transmission depends on the energy / power and the level of topography in the transparent region. Since the sensor nodes are moving within the mobile sensor network and are located in an open environment, attackers have many opportunities to be attacked. When sensor nodes are managed remotely, they are unattended. As such, security is essential for wireless sensor networks. They are vulnerable black hole attacks and malicious intrusions. There are also issues with mobile sensor network security attacks that need to be resolved. The mobile sensor node infrastructure will allow a temporary network of decentralized nodes to exist, allowing attackers to attack any node and from any direction.

The security mechanisms and algorithms that cause this situation should not be complicated. Mobile sensor nodes exist in mobile sensor networks and mobility. Creating dynamic attributes of topology this result. It is very important that the protocol be related to security goals, and they need to design security performance to avoid various security attacks. In wired internet, the core protocols designed was failed for wireless architectures. The unmodified standard TCP performs poorly in wireless environment, because of its inability to differentiate packet losses that caused by network congestion from those attributed to transmission errors was found in many studies. So,

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

that security mechanism is not suitable for new security measures that require wireless sensor networks. Opportunities and increased delays for collisions with dense deployments of sensor networks are frequent. Messages hidden from passive attackers are the most important issue in wireless sensor networks. The WSN needs to protect the channel from the attacker, so sensitive data can be communicated through sensor nodes such as key distribution.

II. TYPES OF ATTACKS

a. Passive Attacks

Dropping and monitoring data transmission passive attacks can be intercepted by attackers. Methods are not intended to damage or otherwise affect other nodes must be suitable for passive attacks. This includes monitoring passive attacks, listening to the data stream, and not modifying the data stream. Passive attacks do not harm the network directly, because they cannot modify the data and attacks on privacy are passive attacks.

b. Active Attacks

This is a malicious node in which the node in the network can get damaged by creating a network disruption. Information or data flow changes that are bogus can form an active attack. Attackers can passively modify or reverse data or information, do not rely on active attacks, it can also take all control over network communication. Examples of active attacks are relays, black holes, overwhelming, interference, wormholes, hollow floods, caves, spoofing, data modification, floods, etc. In this type of attack, the routing attack is because the attacker's target routing protocol and the performance of the contents of the routing table are severely affected.

A common example is that a malicious node can mistakenly share routing information with erroneous outbound data caused by this peer. This type of attack is difficult to achieve because the attacker seeks to collect data on the type and amount of data transmitted, the configuration of the node and its location information.

III. PROBLEM STATEMENT

In a black hole attack, an attacker can physically capture and re-program a set of nodes in the network. These nodes can launch different attacks on the network, which can result in information loss with higher energy costs. Subsequently, the information entered in the black hole area was leaked, but the information did not reach its destination. A black hole attack may have leaked its confidential information in case of an attack, and in the case of a mixed anomaly, or the target may have been delayed. This creates high end-to-end latency and reduces packet transfer rates and network throughput. As a result, the information cannot reach the target node in the required time.

IV. AIM AND OBJECTIVES

The WSN black hole detection mechanism is based on a wireless sensor network with low resource requirements and high detection accuracy. Designing adaptive approaches based on existing routing protocols of wireless sensor network to withstand black hole attack and isolate the attackers. Design a lightweight solution that does not consume the already limited processing power and battery power of WSN nodes. To design a new routing protocol to improve its efficiency against the black hole attack to prevent the information security and to reduce the energy when transmit data. To increase the packet delivery ratio, reduce the routing overhead and avoid the denial of service and other attack using the proposed digital security. This method improves security factors for dynamic routing topology analysis.

V. RELATED WORK

1. Author/ Year/ Method - Soundaran, et.al/ 2020/ mm, Wave Statistical Spatial Channel Model (SSCM). The proposed work is energy preserving secure measure based on the network connectivity aims to detect the wormhole attack. Drawback is, it doesn't control the packet flow and carriers that increase their capacity to meet the growing demand for sufficient bandwidth.

2. Author/ Year/ Method - Aliady, - W. A., et,al./ 2019/ secured AODV protocol. In proposed work worm hole attack that is a harmful and easily deployed attack that targets the routing layer. Drawback is, the existing outbound constraint attributes are identified by communication between adjacent nodes. Its more time consume and energy.

3. Author/ Year/ Method - Anastasia Tsiota et.al./ 2019/multi-tier heterogeneous wireless network. The

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

performance bounds on the coverage probability of random multi-tier HWNs with joint jamming in proposed work. Drawback is packet losses and difficult to identity misbehavior node and request.

4. Author/ Year/ Method - Longpeng Li et.al./ 2019/ secure random key distribution scheme. The proposed work detects and revocation of malicious nodes and the parameter s to help prevent the replication attack. Its drawback is high voting threshold for replication detection, optimizing the upper bounds to ensure the connectivity of network.

5. Author/ Year/ Method - Yanpeng Guan et.al,/ 2018/ False Data Injection Attack Detection Mechanism. Resilient attack detection estimators are delicately constructed to provide locally reliable state estimations and detect the false data injection attack is the work. Drawback is, it identifies the limited some attack in the WSN. A malicious node that evaluates the time difference between the values (averages) held by regular nodes.

6. Author/ Year/ Method -Ying Liu et.al.,/2018/ secure diffusion least mean squares (S-dLMS). The proposed work that mean-square senses is analyzed, and then an adaptive rule is suggested to select the threshold for detection. Its drawback is the data averaged performance of the whole network decreases a delivery ratio.

7. Author/ Year/ Method - Haomeng Xie et.al/ 2018/ security data collection. The proposed works provide an overview of WSNs and classify the attacks in WSNs based on protocol stack layers. Drawback is, it doesn't consider directions towards trustworthy and effective security measurement in WSNs.

8. Author/ Year/ Method -Yanpeng Guan and Xiaohua Ge et.al., / 2017/ homogeneous Markov chain. The proposed to achieve secure consensus estimation distributed attack for target tracking. Its drawback is, low tracking accuracy, particularly when there exist malicious attacks on sensor measurement channels.

9. Author/ Year/ Method - Huseyin Ugur Yildiz et.al., / 2017/ Linear Programming (LP). The impact of critical node elimination attacks on WSNsis the proposed work. Drawback is, it considers shorten network elimination attacks on WSNs. It not supports large network.

VI. IMPLEMENTATION OF THE PROPOSED METHOD

The proposed method utilizes digital chain and secret sharing method to guarantee the availability, confidentiality, authenticity and reliability of information. To detect black hole nodes in the route discovery process, the nodes authenticate each other by providing a digital security method. The source of node S wants to check its routing table to see if the path to destination node D is already available and find the route of destination node d. Upon routing to the destination, node S broadcasts a RREQ packet and sends it to the adjacent node.

VII. PROPOSED ARCHITECTURE DIAGRAM

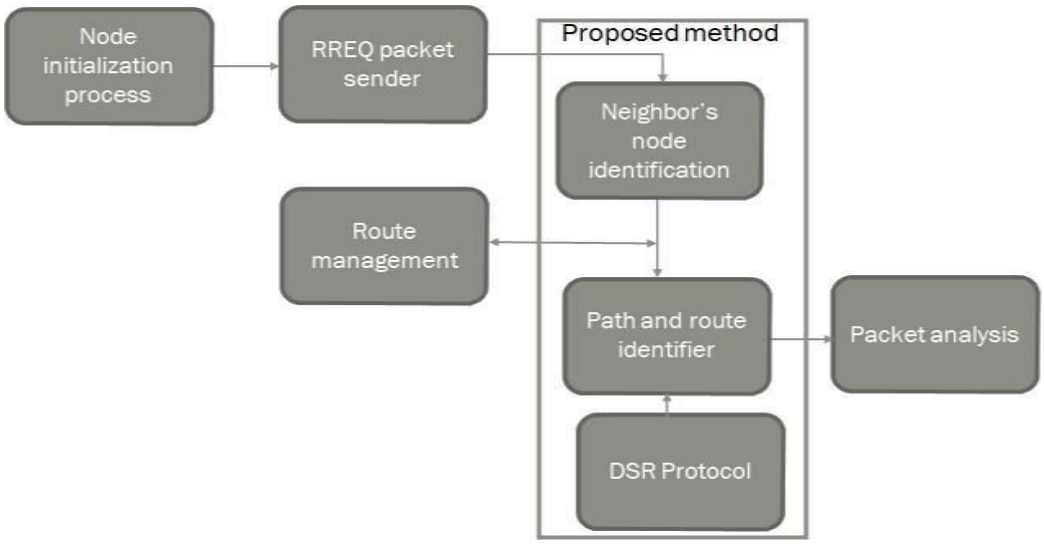

Fig. 1: Proposed Architecture Model

When the route request – RREQ packetreaches the intermediate node, then the RREQ is scanned and the

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

destination address is checked. After the route discovery process, the node enters theauthentication phase where it authenticates with the neighbors of the route. Try all the nodes on the chosen route to verify their adjacency by issuinga suggestion. The route discovery phase is extended and the information issigned by the Dynamic Source Routing – DSR protocol to ensure their authentication. The DSR's extended route discovery process consists of a route discovery process that follows the authentication phase. Once the route is established between the source and destination, the nodes forming the routeenter the authentication phase. The ID of the next hop node requested by the source node. The time it takes to process the RREQ packet and the locationof the node is an ideal parameter to determine the relative security levelof the node against black hole attacks. The protocol uses a cached route thatis separate from the availability of the cached route to the source node when affected by a black hole node.

VIII. RESULT ANALYSIS

The network analysis parameters areuse to prove the proposed methodperformance the analysis parameters are,

- **Throughput** – Successfully transmitted rate of data per second within the network during the simulation.
- **End-to-End delay** – End to end delay (seconds) is that the time taken for a data packet to achieve the destination.
- **Delivery ratio** – It's a ratio of number of packets received by destination to number of packet sent by source.
- **Malicious node analysis** – It generates the routing message to route links andsupply incorrect link state information and also flood other nodes in the network with routing traffic.

IX. CONCLUSION

The proposed protocol method for detecting black hole nodes in WSN providesa reliable way of sending data from source to fixed data transmission to destination node. This digital security scheme ensures that black hole nodes do not participate insource-to- destination routing. In this method to detect the misbehavior node reduce the routing over head, time delay and black hole attack.

The proposal updates the inventory at random intervals to improve reliability. The reliability of data transmission methods can thereby ensure and improve the confidentiality of information. To allow the target node to validate the new routingprotocol scheme, enhancements areproposed to validate the routing data.

REFERENCES

1. Soundaran, Rajasoundaran, Palanisamy, N., PATAN, R., Nagasubramanian, G.,& Khan,M. (2020). Secure and ConcealedWatchdog Selection Scheme Using Masked Distributed SelectionApproach in Wireless Sensor Networks. IETCommunications. doi:10.1049/iet-com.2019.0494
2. Aliady, W. A., & Al-Ahmadi, S. A. (2019). Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks. IEEE Access, 7, 84132–84141.
3. Anastasia Tsiota, Dionysis Xenakis, Nikos Passas, Lazaros Merakos, (2019). On Jamming and Black Hole Attacks in Heterogeneous Wireless Networks. IEEE Transactions on Vehicular Technology, 68(11),10761 - 10774.
4. Li, L., Xu, G., Jiao, L., Li, X., Wang, H., Hu, J., gao, honghao. (2019). A Secure Random Key Distribution Scheme Against Node Replication Attacks in Industrial Wireless SensorSystems. IEEE Transactions on Industrial Informatics, 1–1.
5. Guan, Y., & Ge, X. (2018).
6. Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks. IEEE Transactions on Signal and Information Processing over Networks, 4(1), 48–59.
7. Liu, Y., & Li, C. (2018). Secure Distributed Estimation Over Wireless Sensor Networks Under Attacks. IEEE Transactions on Aerospace and Electronic Systems, 54(4), 1815–1831.
8. Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2018). Data Collection for Security Measurement in Wireless Sensor Networks: A Survey. IEEE Internet of Things Journal, 6(2), 2205 - 2224.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

9. Guan, Y., & Ge, X. (2017). Distributed Secure Estimation Over Wireless Sensor Networks Against Random Multichannel JammingAttacks. IEEE Access, 5, 10858–
10. 10870.
11. Yildiz, H. U., Tavli, B., Kahjogh, B. O., & Dogdu, E. (2017). The Impact of Incapacitation of Multiple Critical Sensor Nodes on Wireless SensorNetwork Lifetime. IEEE Wireless Communications Letters, 6(3), 306– 309.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details