International Journal of Communication and Information Technology

E-ISSN: 2707-6628
P-ISSN: 2707-661X
IJCIT 2020; 1(2): 52-55
Received: 01-10-2020
Accepted: 02-11-2020

Paramjit
Research Scholar, Department of Computer Science and Engineering, OSGU Hisar, Haryana, India

Saurabh Charya
Dean and Associate Professor, Department of Computer Science and Engineering, OSGU Hisar, Haryana, India

Corresponding Author:
Paramjit
Research Scholar, Department of Computer Science and Engineering, OSGU Hisar, Haryana, India

Analysis of black hole attack mitigation techniques in wireless sensor networks

Paramjit and Saurabh Charya

DOI: https://doi.org/10.33545/2707661X.2020.v1.i2a.72

Abstract
Nodes in a Wireless Sensor Network (WSN) exchange data with one another using radio waves. Nodes in a WSN are usually represented as static components. Its use has been widespread for quite some time. Researchers have paid much attention to how much power sensor nodes in WSNs use. In WSN Due to computational and power constraints, wireless sensor network (WSN) security is paramount. One type of attack that threatens the safety of WSNs is called a black hole attack. When an adversary takes control of a subset of a network's nodes and modifies their code to prevent them from sending packets they receive or originate to the base station, this is known as a black hole attack. Therefore, everything that comes close to a black hole gets drawn in. Since the network is divided during a black hole attack, crucial occurrence data does not spread the base stations, reducing efficiency. In order to prevent black hole attacks, a number of methods created on secret allocation and multipath routing have been developed in the works. However, we show that these methods are ineffective and could render black hole attacks more effective. Use a Java simulator to assess the network's performance with and without a strategy that relies on many base stations to thwart black hole attacks, and then propose a method for doing so. The Java network simulator Net bean IDE was used for its implementation.

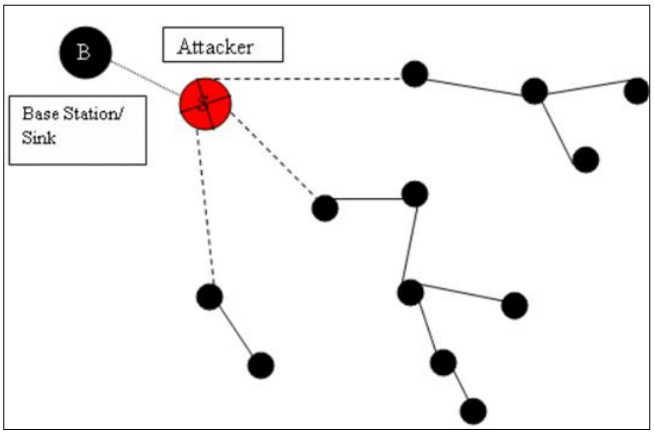
Keywords: WSN, blackhole attack, malicious node, multiple base station

Introduction
A Wireless Sensor Network (WSN) is a network of several individuals. These low-power sensors are wirelessly connected and share data collected from their surroundings. Every node has a sensor that can pick up light, pressure, heat, sound, temperature, etc. A sink node (or central node) receives data from all sensor nodes. To increase the network's coverage and scalability, sensor nodes perform various important activities, including computation, signal processing, and network self-configuration. Some of the features of wireless sensor networks include self-repair and self-organisation. In connection failure, self-healing sensor nodes can select an alternate course or route, and self-organising nodes can accept new members into the network without disrupting transmissions [1]. Node installation is unnecessary in a sensor network since nodes can be placed anywhere. Given that the sensor relies on an internal battery for power, the efficiency of a wireless sensor network is directly proportional to the rate of energy consumption.

Security issues related to WSN
Since Wireless Sensor Network sensor nodes are typically deployed in highly dynamic settings, WSN applications are inherently more vulnerable to security threats. The first steps in developing a comprehensive security strategy for a WSN involve identifying and analysing the threats specific to the networks' intended uses. Attacks that result in node capture and those likely to occur after a valid node has been captured are the primary focus of most studies [2]. Wireless sensor networks (WSN) are exposed to attack since the transmission medium is inherently broadcast. When considering the vast potential uses of wireless networks, it is essential that security be given top priority.

Black Hole Attack in WSN
A black hole attack occurs when a malicious node intercepts transmissions from its neighbouring nodes while the network is in use and then fails to transport the packets it has generated or those it has received from another source node.

These harmful nodes are known as black hole nodes, then the area they occupy is called black hole region [3].



Source: [4]

Fig 1: Occurrence of black hole attack in WSN

The small green circles in the above diagram represent the sensor nodes, while the larger red area represents the black hole. When the source node chooses a routing that includes the malicious node, traffic is routed through the adversary node, and the malicious node begins dropping packets at random. Here, the reformed nodes are called black hole nodes, and they serve as the entry site for various damaging attacks [5]. This type of attack occurs at the Network Layer of the OSI model. When it happens at the network layer, it disrupts normal operations and slows down the entire network, impacting key performance indicators, including packet loss, latency, and throughput.

Aim

The purpose of this research is to evaluate existing approaches for preventing Black Hole Attacks in WSNs and to propose a new effective approach to mitigate the black hole attack.

Objectives

- To efficiently reduce the impacts of black holes on data transmission, a novel method, including a distributed network of several base stations, is proposed.
- To evaluate how various wireless sensor network infrastructures cope with black hole attacks.
- To determine the cause of a black hole attack in WSNs.

Research question

1. In wireless sensor networks, what factors lead to black hole attacks?
2. What are the used techniques to mitigate the black hole attack in Wireless sensor networks?

Literature Review

Security flaws in WSNs can be broken down into three categories: Node, router, and data traffic. Constantly running a whole network is difficult because of environmental constraints, processing limitations, and short transmission distances. Using WSN's reliance on previous hops, attackers can insert rogue nodes into routes with relative ease.

To identify the BH attack, this method [6] suggests splitting the network into equal-sized chunks and giving each one a distinct identifier. The nodes are able to mutually identify one another and provide their present state of energy to the network and the BS via a localization technique. The node with the highest aggregate energy is known as the Cluster Head (CH). Some mobile agents help the system by monitoring the network; if they notice something out of the ordinary, they label the node as a BH node and alert both the Control Node (CH) and the Base Station (BS).

To protect against the BH attack, [7] suggests using a Control Packet (CP) with Extensive Extended Data Routing Information (EDRI). Node parameters can be found in the EDRI table. Data about the BH node, source, destination, and neighbour ID are included. The node's integrity can be expressed as a binary number. The CP stores the source node ID, neighbour node IDs, and a secure value created by a persistent random number generator (RN). Since a hostile node cannot broadcast the CP, it is effective for detecting a single BH assault. Next hop number (NHN), CP, and RNG drive the community attack mechanism. It contains three stages: Route finding, analysis, and removing cooperating BH nodes.

Guidelines for detecting black hole attacks in an intrusion detection system are proposed in [8], which is based on an analysis of the Mint Route protocol in Tiny OS. The rules-based approach for detecting intrusions. Concerns concerning the intrusion detection method's scalability are warranted, however, because the rules would often be built in code to solve a particular problem. An intrusion detection system for WSNs is also proposed by [9]. Mobile agents are used to monitor networks because of the system's emphasis on modularity and the simplicity with which new features may be added to the IDS.

To defend against BH attacks, an intrusion avoidance system-secure data transmission (IAS-SDT) solution [10] is based on AODV and AOMDV (multipath extension) with an assumed network topology. During route setting, a communication is disjointed and encoded using a homomorphic encoding technique. Each cluster is given a share of the identifiable paths. Each group receives only a small piece of the communication. If an enemy accidentally loses the pieces, they will be distributed along an alternate path until they all arrive [11] A detail method for preventing black holes that uses authorisation and cryptography built within the routing protocol. This is an important step toward a solution, but it depends on the nodes' cryptographic keys remaining secure. A secure routing strategy, which [12] contend reduces the impact of routing misconduct, is also proposed. This approach also employs cryptographic mechanisms to guarantee that recipients will reject erroneous route responses. Since sensor nodes are often very small and difficult for the network operator to get a hold of, relying solely on the secrecy of the cryptographic keys is not enough to ensure against black hole attacks. As a strategic measure against the BH and wormhole attack in the AODV, it is suggested in [13] that nodes along the path preserve a record of all RREP packets for a certain period of time together with their sequence numbers. Using the provided formula, we can determine the mean of the sequence values. Finally, the transmission paths with values higher than those calculated are activated.

This section is a detailed discussion of the methods used to prevent attacks on the research infrastructure. Notably, these methods do not account for the location of the BH node in the network about the total damage done by the attack, nor do they conduct a root-level DF examination of a BH attack.

The number of malicious nodes is typically described as being proportionate to the damage caused to the network in mitigation strategies. Our study proposes a novel method for a distributed network of several base stations. The given mitigation techniques are adequate for their intended purposes. Analysis of the attack is always necessary for developing cutting-edge countermeasures and overcoming vulnerability.

Methodology

Multiple Base station

Effective packet delivery to the BS is added critical than preventing data collection by an adversary in a WSN. Effective data encryption technologies and anonymity techniques can make data that a threat can deduce from captured packet(s) useless. Therefore, we prioritize delivering the packet(s) to the BS even in the case of black hole nodes. A innovative strategy is being deployed to ensure high packet delivery success by strategically placing many BSs to maximize the likelihood that packets from the SNs will get to at least one BS in the network. To handle the flood of enormous quantities of heterogeneous data from the network, numerous optimization algorithms remained devised for query allocation and base station location. Here, we suggest employing several BSs to improve data transmission despite black hole assaults.

Technical Explanation

Our method is based on the following assumptions and system model. SNs (N=1...n) are spread out randomly around the network. More powerful than SNs and linked to an alternative energy source, the network is made up of a collection of BSs denoted by the symbols (B=B1.....Bm). Connectivity between nodes is guaranteed by the WSN's high density so that respectively SN can deliver data packages to every BS. The BSs are considered to be hardwired to one another. By assuming an external adversary may hack the network's SNs and reprogram them to perform packet analysis on incoming data before deleting it rather than passing it to the BSs. A node that has been hacked SN is called a black hole node. The attacker can compromise multiple SNs in the network and produce multiple black holes. To further examine the captured packets, the compromised nodes can work together with additional cooperated nodes in their area or in added black hole areas by assuming that SNs in the black hole zone cannot carry out their environment-sensing functions.

Results

Net Beans, a Java network simulator, activates the AODV protocols in a virtual network environment. Using multiple based stations instead of using one base station, AODV protocols' performance is tested across a wide range of network characteristics.

Table 1: False and success black hole attack with a single base station

Total Routes	1
Failed	1
Fake success	0
Success	0

Source: [14]

Power efficiency in WSN is prioritised by choosing the closest base station as the starting point for the initial routing path. When a black hole attack is feasible, only routing activates across many base stations. To search for evidence of black holes, we will use a security method.

Table 2: False and success black hole attack with a multiple base station

Total Routes	8
Failed	1
Fake success	4
Success	3

Source: [14]

Discussion

The proposed method is compared with the below four methods of mitigating black hole attacks in WSN.

The RSA method is employed in MANET to protect the ZRP routing protocol from black hole attacks and to detect instances of multiple black hole attacks. The simulation findings reveal that ZRP is superior to DSR in terms of throughput, average end-to-end latency and packet delivery ratio, packet drop ratio, and detection time. Throughput is improved, average end-to-end delay is lowered, packet drop ratio is minimised, and multiple BHA is detected and prevented.

Using the redundant nature of the network's base stations, [15] devised a way to foil blackhole attacks. They propose that mobile agents are responsible for detecting anomalous behaviour and that only routing across several base stations should be triggered if there is a chance of a blackhole node in the network. Additionally, system performance was verified via simulation.

An Intrusion Detection System (IDS) based work was provided [16]. The exchange of packets between a sensor node and base station is the foundation of the blackhole attack detection concept. Therefore, the base station must act as the monitor node and look for the bad node. This technique takes advantage of a highly effective mechanism. They showed that an IDS based on an expert system can be used to find black hole attacks on wireless sensor networks. The architecture of such a system, which we refer to as ADIOS, was described in detail, along with recommendations for optimising its performance in a low-resource setting. Through simulations, we showed how to take advantage of a network's various nodes to alleviate the computational, memory, and power demands of individual nodes without compromising their capacity to detect attacks in a fast and accurate fashion.

The BHDP system was proposed by [17]. The network is protected from blackhole attacks thanks to the system's ability to identify them. The key benefit of their suggested technique is that the same packet may be delivered to different base stations without any modification. Blackhole attacks are identified using a variety of indicators, including delivery ratio, total packet drop, and others. It's possible that a sizable amount of storage space is needed for the rule base. When compared to the aforementioned methods, our proposed method has been found to be more effective at reducing the black hole attack in a WSN. In addition to being more secure than the aforementioned methods, it also improves network performance by blocking black hole attacks.

The black hole attack is caused by when a router occurs in an offline state; it goes undetected by the other routers in the network, which means that any packets sent to it will be lost. Similarly, if no host is assigned to a given IP address, that address is considered to be inactive. The missing address is used by attackers to send out blackhole attacks. Blackhole attacks can be conducted in the network if the firewall protecting the network is breached.

Conclusion

Relevant techniques for black hole attacks in WSNs are analysed in this research. Using a strategy involving multiple base stations, the harmful effects of a black hole attack on WSN can be significantly reduced. Data transmission to numerous base stations is initiated by the detection of anomalous behaviour in a subset of nodes. This paper which employing an encryption technique that repeatedly checks in on the fixed nodes in order to spot any deviations caused by the presence of black holes. These solutions are very efficient, and they only demand a small amount of network processing and message exchanges, which helps the SN conserve its power.

Reference

1. Suma S, Harsoor B. An approach to detect black hole attack for congestion control utilizing mobile nodes in wireless sensor network. Materials Today: Proceedings. 2022;56:2256-2260. DOI: 10.1016/j.matpr.2021.11.590
2. Kaur H, Singh A. Identification and mitigation of black hole attack in wireless sensor networks. International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE); c2016. DOI: 10.1109/icmete.2016.66
3. Gurung S, Chauhan S. A survey of black-hole attack mitigation techniques in manet: Merits, drawbacks, and suitability. Wireless Networks. 2019;26(3):1981-2011. DOI: 10.1007/s11276-019-01966-z
4. Security in Wireless Sensor Networks: A survey. In: Sensor Networks Security; c2016. p. 253-288. DOI: 10.1201/b13609-19
5. Malik A, Singh Y, Singh M, *et al.* Analysis of black-hole attack with its mitigation techniques in ad-hoc network. In: Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks; c2020. p. 211-232. DOI: 10.4018/978-1-7998-5068-7.ch011
6. Shree O, Ogwu FJ. A proposal for mitigating multiple black-hole attack in wireless mesh networks. Wireless Sensor Network. 2013;5(4):76-83. DOI: 10.4236/wsn.2013.54010
7. Weißbach M, Feldmann M. An approach for black-hole attack mitigation in disruption-tolerant ad-hoc smart-phone networks. Proceedings of the 13th Workshop on Challenged Networks; c2018. DOI: 10.1145/3264844.3264853
8. Gurung S, Chauhan S. Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in Manet. Wireless Networks. 2017;25(3):975-988. DOI: 10.1007/s11276-017-1639-2
9. Ariffin KA, Mokhtar RM, Rahman AH. Performance analysis on leach protocol in Wireless Sensor Network (WSN) under black hole attack. Advanced Science Letters. 2018;24(3):1791-1794. DOI: 10.1166/asl.2018.11160
10. Tiruvakadu DS, Pallapa V. Honeypot based black-hole attack confirmation in a Manet. International Journal of Wireless Information Networks. 2018;25(4):434-448. DOI: 10.1007/s10776-018-0415-2
11. Karakoç E, Çeken C. Black Hole attack prevention scheme using a block chain-block approach in SDN-enabled WSN. International Journal of Ad Hoc and Ubiquitous Computing. 2021;37(1):37. DOI: 10.1504/ijahuc.2021.115125
12. Shinde M, Mehetre DC. Black Hole and selective forwarding attack detection and prevention in WSN. International Conference on Computing, Communication, Control and Automation (ICCUBEA); c2017. DOI: 10.1109/iccubea.2017.8463929
13. Babriya K, Singh S. A review study on preventing and detecting technique of black hole attack in Manet. International Journal of Trend in Scientific Research and Development. 2017;1(4). DOI: 10.31142/ijtsrd129
14. Khan D, Jamil M. Study of detecting and overcoming black hole attacks in Manet: A Review. International Symposium on Wireless Systems and Networks (ISWSN); c2017. DOI: 10.1109/iswsn.2017.8250039
15. Mitigating black hole attacks in wireless sensor networks using node-resident expert systems. Wireless Telecommunications Symposium; c2014. DOI: 10.1109/wts.2014.6835013
16. Karuppiah AB, Dalfiah J, Yuvashri K, Rajaram S. An improvised hierarchical black hole detection algorithm in wireless sensor networks. International Conference on Innovation Information in Computing Technologies; c2015. DOI: 10.1109/iciict.2015.7396103
17. Kaur R, Kaur H. A reserve path based black hole detection and prevention algorithm in Wireless Sensor Network. Int J Comput Appl. 2017;178(7):30-35. DOI: 10.5120/ijca2017915839