INTERNATIONAL SCIENCE REVIEWS

AIU

No. 4 (2) 2021

Natural Sciences and Technologies series

ISSN: 2707-4862

ASTANA
INTERNATIONAL
UNIVERSITY

INTERNATIONAL SCIENCE REVIEWS
Natural Sciences and Technologies series

Has been published since 2020

№4 (2) 2021

Nur-Sultan

EDITOR-IN-CHIEF:

DEPUTY EDITOR-IN-CHIEF:

EDITORIAL BOARD:

Editorial address: 8, Kabanbay Batyr avenue, of.316, Nur-Sultan,
Kazakhstan, 010000
Tel.: (7172) 24-18-52 (ext. 316)
E-mail: natural-sciences@aiu.kz

International Sciense Reviews NST - 76153
International Science Reviews
Natural Sciences and Technologies series
Owner: Astana International University
Periodicity: quarterly
Circulation: 500 copies

CONTENT

Mardenov Y., Zhukabayeva T, Abdildaeva A., Sultangazieva A. DETECTING AND PREVENTING BLACK HOLE ATTACKS ON WIRELESS SENSOR NETWORKS…………………….……………………………………………………...……5

Серік Фараби, Тасболатұлы Нұрболат МЕТОДЫ ОЦЕНИВАНИЯ ВНЕДРЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ БИЗНЕС-ПРОЦЕССАМИ ПРЕДПРИЯТИЯ …………………………………………………………………..……..…..11

Леспекова А.А, Муканова А.С. МӘТІНДІ ТОНАЛДЫЛЫҚҚА АНЫҚТАУ ӘДІСТЕРІНЕ ШОЛУ………………………………………………………………………………..………21

МажитА., Муканова А.С. ИССЛЕДОВАНИЕ И АНАЛИЗ МЕТОДОЛОГИЙ УПРАВЛЕНИЯ IT-ПРОЕКТАМИ В ТЕЛЕКОММУНИКАЦИОННОЙ ОТРАСЛИ ……31

DETECTING AND PREVENTING BLACK HOLE ATTACKS ON WIRELESS SENSOR NETWORKS

Mardenov Y. [1,2], Zhukabayeva T[1,2]., Abdildaeva A. [1], Sultangazieva A. [1]

Astana International University[1]
L.N. Gumilyov Eurasian National University[2]

Annotation. The protection of wireless sensor networks (WSN) is an urgent problem, since network nodes have low computing power, limited battery power and are located in unprotected places, and information is transmitted over wireless channels, any network disruption can lead to undesirable consequences. One of the common attacks against WSN is the Black hole attack. In this attack, the malicious host uses its routing technique to be able to advance in search of the fastest route to the host of the site or to the packet it wants to identify. This study analyzes the methods of protection in WSN against Black hole attacks. A method is shown of how a malicious node affects nodes in its transmission range.

Keywords: Black hole attack, WSN, attack detection.

I. Introduction

The latest advances in networking, semiconductor physics and materials science have enabled the widespread development and deployment of wireless sensor networks (WSS). BSS are formed by a large number of network nodes [1], called motes, - miniature autonomous devices capable of collecting information from the territory within a certain range and transmitting it to other devices. Each such device contains a data collection module (temperature, pressure, illumination, etc.) and an autonomous power source. Also, each motorcycle is equipped with a radio transceiver or other wireless communication device, that is, data is transmitted over the network via a radio channel. To accumulate all the collected information, the network contains a powerful node (sink, base station) connected to a stationary power source. Data is collected in this sink according to a specific routing algorithm. Combined into a wireless network, all nodes form a distributed self-organizing system for collecting and transmitting information. The advantages of systems based on sensor networks are the ability to deploy in hard-to-reach places, wireless communication, self-organization (the ability to redistribute routes in the event of failure of some nodes). Despite discoveries in the field of research in wireless sensor networks (WSN), there are already a large number of current problems in which these networks can be applied. [2] WSN security is one of the important ones. Inadequate physical protection makes them susceptible to interception, compromise and hacking. As a result, any encrypted data contained on these networks can be used by intruders to carry out attacks from the network, compromising the confidentiality of information. In addition, since there is a transmission in communication systems "over the air" by means of radio waves, it is possible to carry out a wide class of attacks, starting with passive listening and ending with active [3], for example, Sybil,

Hello flood, Wormhole, DOS, Black hole attacks, etc. Old security mechanisms are not suitable due to lack of processing power, limited memory and power [4]. This article discusses the Black hole attack; as a result of this type of attack, more than 90% of the information transmitted to the sink can be lost [5].

II. Black hole attack

Black hole attacks are one such attack in WSN. This attack is carried out by an external attacker on a subset of sensor nodes in the network [6]. This is an active type of attack where an attacking node claims to have the shortest route to any desired node on the network, even if it does not have any route to it; therefore, all packets will go through it, and this allows the black hole node to forward or drop packets during data transfer. Regular nodes trust any response to the requests they send, and the black hole node takes advantage of this and continues to answer any request, claiming that it has the shortest path to the desired node. Usually, nodes begin the discovery phase to find a path to a destination node. The source node sends the request to the destination node, any node that receives this request checks to see if it has a new path to the destination node. When the black hole node receives this request, it immediately sends a response to the broadcaster, claiming it has the freshest and shortest path to the destination node. The originating node considers it to be the answer because there is no mechanism to verify that the request is from a normal node or from a black hole node. The source node starts forwarding packets to the black hole node in the hope of delivering those packets to the destination node, then the black hole node starts to discard those forwarded packets. [7]

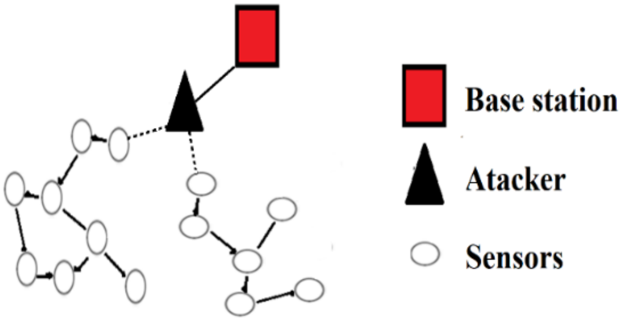

Figure-1 Black hole attack in the WSN

The attack can be organized in two ways [8].

- The first method is for an attacker to place a new node in the network area, with the help of which an attack is later organized. Impacts of this kind are relatively easy to detect and localize using standard FSS mechanisms.
- The second method is more dangerous when one of the legal nodes that are already participating in information exchange is hacked.

The attacker-controlled node removes all packets transmitted to it by other nodes for transit. In addition, a hacked node v0 can propagate information through the network that it is the closest node to the sink s, as a result of which the self-organizing network, which is the SSN, changes routing, and the other nodes that are closer to v0 than to s transmit their packets for onward transmission to s.

In [10] the developed scheme depends on the use of a fake identifier to decorate a black hole node. The originating node starts by sending a decoy request that contains an identifier that is not on the network. The black hole node will respond to this decoy RREQ due to its normal behavior, which responds to any RREQ on the network, reassuring that it has a better path. The developed scheme is implemented in DSR, so they modified the RREQ and RREP headers to identify the node of the black hole in the path. A warning is sent to neighboring nodes when a black hole node is detected. The origin node continues to check if there is a drop below a certain threshold; Then he starts bullying again. The limitations of this scheme are that it increases the size of control packets (RREQ and RREP), which leads to increased overhead in addition to black hole alerts, which can be used by an intelligent black hole to isolate nodes into the network.

In [11], they developed a technique that relies on the use of a cooperative decoy detection scheme (CBDS). In CBDS, black hole detection is divided into three phases: decoy, backtrace, and reactive defense. During the decoy phase, the source node chooses one of its neighbors at random and sends a decoy request using its identifier. During the backtracking phase, a list of suspicious nodes is generated from the RREP of the RREQ decoy, then neighbors enter random mode to determine if there is an attacker node in the path. For every black hole node found on the network, a black hole alarm is sent to neighboring nodes. In the reactive protection phase, the source node checks if the PDR is below a certain threshold, then it starts the decoy phase again. The limitation of this method is that the nodes enter promiscuous mode, which is not acceptable for all nodes. Since some nodes do not want any unauthorized user to listen to their own broadcasts, being in random mode will also encourage passive attacks. An intelligent black hole node can use the black hole alarm function and start transmitting false black hole signals to isolate network nodes.

In [12], they analyzed the black hole attack and explained that the route from a malicious node must increase the sequence number of the destination for a specific target in order to resolve the source node. The authors analyze and propose a statistical baseline anomaly detection approach to detect a black hole attack, and on the destination side they receive RREP (Route Replys) according to the destination sequence number

In [13], the black hole attack is isolated by propagating a message about the separation of the attack. This helps to improve the Packet Delivery Ratio (PDR) with minimal latency. Simulations are performed based on parameters such as black hole attack detection rate (BHADR), black hole attack detection time (BHADT), false positive rate (FPR), PDR and latency. The relationship between nodes is identified based on independent probability distribution functions and a mutual probability function.

III. The proposed algorithm

This project is a simulation of black hole attack detection in wireless sensor networks that uses a routing protocol for low power lossy devices as the network layer.

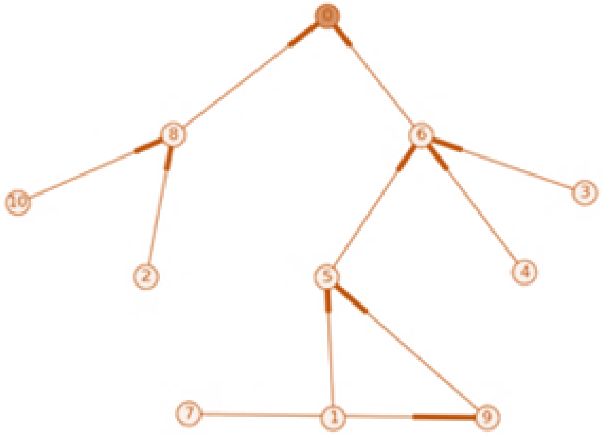

Figure-2 Wireless Sensor Network

This algorithm demonstrates that this type of attack can significantly affect the WSN through significant energy depletion.

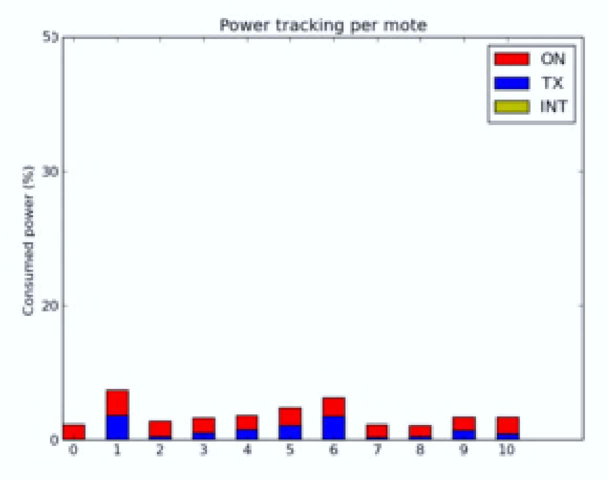

Figure-3 Tracking without active attack

Upon entering the WSN, thanks to the Contiki configuration constants set in the building block, the malicious node immediately starts sending DIS messages to its neighbors, then triggers DIO messages and resets the manual mode timers.

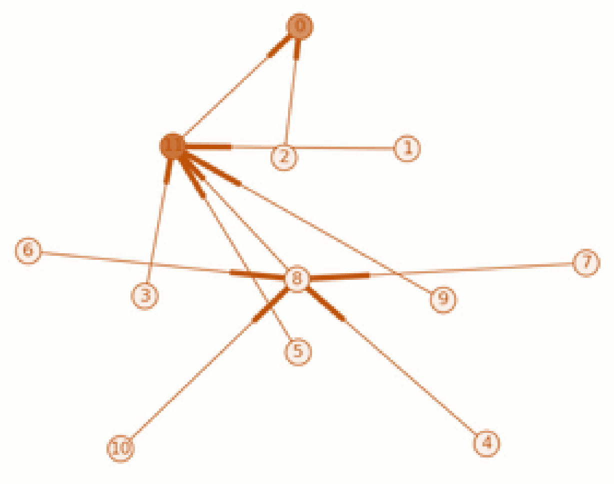

Figure-4 Black hole attack on WSN

As you can see, the malicious node (11) affects the nodes in its transmission range. We can now illustrate the effectiveness of the attack using this information to compare the power consumption in a simulation without (Figure-1) and with a malicious node (Figure-3).

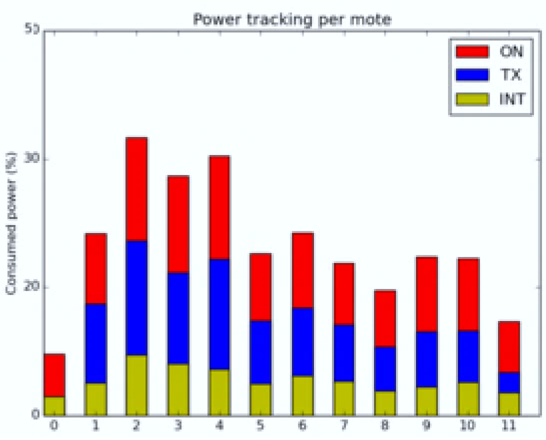

Figure-5 Tracking a Black Hole Attack

As you can easily see, nodes in the range of a malicious sensor are particularly susceptible to attacks in terms of turn on and receive times. However, these nodes are not affected by TX timing. This is because after receiving the DIS, the discarded nodes immediately send DIO due to the multicast nature of the DIS sent. Also, a way to perform a flood attack could be to unicast DIS to neighbors, activate DIO immediately in response, but not reset the manual timer.

Output

A black hole attack on a WSN can attract all kinds of traffic to a compromised host. Which leads to the launch of other attacks such as wormhole, eavesdropping. The consequences of which lead to the exhaustion of all network resources, dropping packets, modifying routing information

A mechanism for detecting the intrusion of black hole attacks is proposed. The approach is based on the exchange of control packets between sensor nodes and a base station. The simulation effects show that the recommended methodology has improved performance in IDS in terms of safety and energy consumption. As future work, sensory nodes can be modeled as black hole nodes along with a channel, and an efficient mechanism can be developed.

References

[1]. Umashankar Ghugar, Dr.Jayaram Pradhan, A Study on Black Hole Attack in Wireless Sensor Networks. Copyright, International Journal of Advance Computing Technique and Applications (IJACTA), ISSN : 2321-4546, Vol 5, Issue 1 2017

[2]. Miriam Carlos-Mancilla, Ernesto López-Mellado, and Mario Siller. Wireless Sensor Networks Formation: Approaches and Techniques. Hindawi Publishing Corporation Journal of Sensors. Volume 2016, Article ID 2081902, 18 pages. http://dx.doi.org/10.1155/2016/2081902

[3]. [4] A. Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In J. A. Clark, R. F. Paige, F. Polack, and P. J. Brooke, editors, SPC, volume 3934 of Lecture Notes in Computer Science, pages 104{118. Springer, 2006

[4]. Ефименко, М. С. Проблемы применения и безопасности в беспроводных сенсорных сетях / М. С. Ефименко, С. И. Клымив. — Текст : непосредственный // Актуальные вопросы технических наук : материалы V Междунар. науч. конф. (г. Санкт-Петербург, февраль 2019 г.). — Санкт-Петербург : Свое издательство, 2019. — С. 24-26. — URL: https://moluch.ru/conf/tech/archive/324/14789/ (дата обращения: 10.06.2020).

[5]. Dokurer S., Erten Y., Acar C. Performance analysis of ad-hoc networks under black hole attacks. Proc. of IEEE Int. Conf. SoutheastCon 2007. 2007, pp. 148–153.

[6]. Ms.B.R.Baviskar, Mr.V.N.Patil. BLACK HOLE ATTACKS MITIGATION AND PREVENTION IN WIRELESS SENSOR NETWORK. International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163. Volume 1 Issue 4 (May 2014) http://ijirae.com

[7]. Adwan Yasin and Mahmoud Abu Zant. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 9812135, 10 pages. https://doi.org/10.1155/2018/9812135

[8]. В.В. Шахов, А.Н. Юргенсон, О.Д. Соколова. МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ АТАКИ BLACK HOLE НА БЕСПРОВОДНЫЕ СЕТИ. Программные продукты и системы / Software & Systems 1 (30) 2017. Т. 30. № 1. С. 34–39

[9]. C. Karlof, D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures, Special Issue on Sensor Network Applications and Protocols", vol 1 (2-3), 2003,pp.1293 –1303

[10]. P.-C. Tsou, J.-M. Chang, Y.-H. Lin, H.-C. Chao, and J.-L. Chen, “Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs,” in Proceedings of the 13th International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity, ICACT 2011, pp. 755–760, Seoul, Republic of Korea, February 2011.

[11]. P. L. Chelani and S. T. Bagde, “Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme,” in Proceedings of the 2016 International Conference on Communication and Electronics Systems, ICCES 2016, Coimbatore, India, October 2016.

[12]. R.H.Jhaveri, S.J.Patel, D. Jinwala, “A novel approach for Greyhole and blackhole attacks in mobile ad hoc networks”, Second International Conference on Advanced Computing and Communication Technologies, IEEE Computer Society, 2012, pp. 556–560.

[13]. John Clement Sunder A* and A. Shanmugam, “Black Hole Attack Detection in Healthcare Wireless Sensor Networks Using Independent Component Analysis Machine Learnining Technique”, Current Signal Transduction Therapy (2018) 13: 1. https://doi.org/10.2174/1574362413666180705123733