С.Сейфуллин атындағы Қазақ агротехникалық университетінің Ғылым жаршысы (пәнаралық) = Вестник науки Казахского агротехнического университета им. С.Сейфуллина (междисциплинарный). - 2020. - №4 (107). – Р.106-115.

DETECTING WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS

Zhukabayeva T.K.*,associate professor*
Mardenov E.M.*,PhD students*
Gumilyov L.N.,Eurasian National University
Kazakhstan, Nur-Sultan,A. PushkinAve, 11,
emardenov@gmail.com

Abstract.

Wireless sensor networks (WSN), consisting of wireless sensors and control devices and methods of self-organization using intelligent algorithms, demonstrate broad prospects. WSNs are subject to numerous types of threats and attacks. One of which is a wormhole attack. This article provides an overview of wormhole attack detection methods in WSN, as well as a new optimized method for detecting this attack. The detection method is based on the removal of the edges of the wormhole and causes significant changes in the length of the shortest paths between network nodes.The accuracy of the proposed algorithm is not affected by the number of wormholes

Key words: WSN, wormhole, security attacks, defense mechanism, special network,malicious node, sensor nodes, string topology, anchor node, directional antenna.

Introduction

The sensor network is a special type of network, although it has some common things with a computer network. Typically, several security requirements are required to protect a network. These requirements should be considered while developing a security protocol, including confidentiality, integrity and reliability. An effective security protocol should provide services to meet these requirements.

There are many attacks available in WSN that are mainly divided into two parts. The first part is an attack on the security mechanism, and the other is the routing mechanism. Here are some of them being mentioned: Sybil attack, Black hole attack, Hello Flood attack, Funnel attack, Denial of service, Gray hole Attack, Wormhole attack

A wormhole attack is one of the serious attacks that can be smoothly resolved in networks, but it is difficult to observe. This review document is a threat monitoring experiment and focuses on some other method of detecting wormhole attacks in WSN. [1]

A typical Wormhole attack requires two or more attackers — malicious nodes — which have better communication resources than conventional sensor nodes. An attacker creates a low latency connection (i.e., a high throughput tunnel) between two or more attackers on a network. Attackers promote these tunnels as high-quality routes to the base station. Consequently, neighboring sensor nodes use these tunnels in their communication paths, transferring their data under the control of opponents. Once the tunnel is established, the attacker collects data packets at one end of the tunnel, sends them using the tunnel (wired or wireless), and repeats them at the other end.Wormhole attacks can cause serious damage to the WSN by interrupting or changing the information flow to the base station. In addition, if attackers do not modify or manufacture data packets, cryptographic solutions alone cannot detect Wormhole attacks [2]. A typical Wormhole attack is shown in Figure 1. A typical Wormhole attack requires two or more malicious nodes that have better communication resources than conventional sensor nodes. An attacker creates a high throughput tunnel between two or more attackers on a network. Attackers promote these tunnels as high-quality routes to the base station. Consequently, neighboring sensor nodes use these tunnels in their communication paths, transferring their data under the control of opponents. Once the tunnel is established, the attacker collects data packets at one end of the tunnel, sends them using the tunnel, and repeats them at the other end.

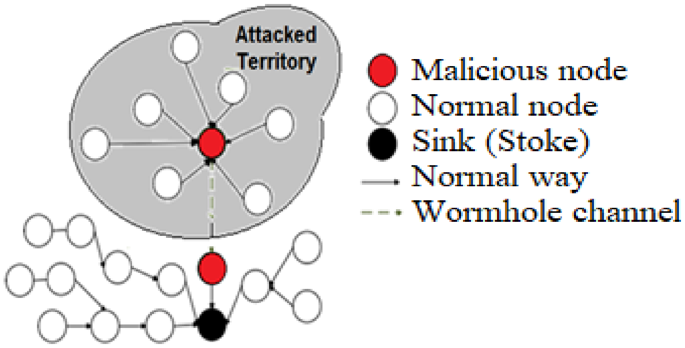

Figure-1. «Wormhole» attack

Approaches wormhole attack detection

At WSN, over the past few years, several researchers have been working to detect wormhole attacks.

Wormhole Attack Types

Wormhole attacks can be classified based on the implementation method used to launch it and the number of nodes involved in creating the wormhole. Types of Wormhole Attacks:

A. Wormhole using packet encapsulation [3], [4], [17]

In encapsulation-based wormhole attacks, there are several nodes between two malicious nodes, and data packets are encapsulated between them. Since encapsulated data packets are sent between malicious nodes, the actual number of hops does not increase during the crawl. Consequently, routing protocols that use a hop counter to select a path are particularly susceptible to encapsulation-based wormhole attacks.

In the work [5] “Packaged leashes”, in accordance with the concept of geographical and temporary leashes. The information provided to packets that controls the transmission distance is called Leashes. The distance of the sender and receiver is determined by geographic location. When receiving nodes receive packets, it calculates the distance and time of transmission. In this technique, the position of the node is not so important, and the time factor plays an important role. He can access the calculation of time and its comparison with an accuracy of the order of a nanosecond. In each packet, the allowed time interval is indicated in the s field, which is compared by the receiver, and the transmission distance of the packet is simply determined by the product of the speed of light and the transmission time. In the case of a large time difference, this indicates the presence of a wormhole.

In [6], the authors suggested that two nodes of the graph are connected by a tunnel, since they are neighbors. RREQ (Route Request) and Topology Management (TCM) messages are transmitted between these nodes in the graph through tunnels. Using additional tunnel nodes, these nodes have the shortest path. Once the connection is established, the attacker selects each other as multi-point relays (MRPs). As a result, several topological control messages and data packets leak through the tunnel. As a result, false topology information is spread across networks. The performance of secure multi-hop wireless systems using the ns-2 simulation and routing protocol can effectively protect against wormhole attacks and provide low latency.

In [7], the author proposed a digital study to detect wormhole attacks in WSN. WSN is explained that adds generation and protects the flow of evidence about the characteristics of the sensor nodes in the network. A group of detective nodes is distributed across networks to control the topology and datagram passing through the sensor nodes. The monitoring node and the base station node together form different WSNs, called the monitoring network. Frequency bands are used to establish communication between observers and the base station, but this is not supported by the sensor node. The detection sensitivity of the sensor assembly is less than that of the observer.

B. A wormhole using a high quality / out-of-band channel [3], [4], [17]

In this mode, a wormhole attack is launched using high-quality single-span out-of-band communication (called a tunnel) between malicious nodes. This tunnel can be achieved, for example, using a straight wired communication line or a long-range directional wireless communication line. This attack mode is harder to launch than the packet encapsulation method, since it requires special hardware capabilities.

Delay transition indication has been implemented (DelPHI) to identify wormhole attacks [8]. It is also a work on the same principle of comparing track travel time and predicted distance. This process works in two stages, firstly, it is the collection of the route path by the recipients, and the senders include DREQ packets similar to SAM concepts and sign it before sending. Upon receipt of the packet, the recipient must include its ID and increase the number of transitions by 1. Information about the minimum delay and the number of transitions is used for minimal detection. The second step uses “Travel Time - Travel Time” (RTT) for the time difference between the information sent and the confirmation received. In this process, the transition delay value (DPH) is calculated as RTT / 2h, where h is the number of transitions to a certain sequential value.

In [9], author proposed a method that provides secure data transfer using the concept of neighbor analysis to detect wormhole attacks in MANET. This method analyzes neighboring nodes, so that it checks the reliability of nodes for transmitting data on the network, in accordance with this method, the node sends a request to its neighboring nodes and supports a request and response system. Here, the node maintains a table for tracking latency. If the node does not receive response time, this means that attacks are happening on the network. The entire node from source to destination is analyzed to detect wormhole attacks using the AODV protocol in MANET.

C. Wormhole utilizing high power transmission capabilities [3], [4], [17]

In this type of wormhole attack, there is only one malicious node in the network that can transmit high power, and this node can communicate with other ordinary nodes over a long distance. When a malicious node receives RREQ, it sends the request at a high level of power. Any node that hears high power transmission relays the RREQ to its destination. Using this method, a malicious node increases the likelihood of being on routes established between the source and destination, even without the participation of another malicious node. This attack can be mitigated if each sensor node is able to accurately measure the level of the received signal.

A two-stage mechanism was used to detect wormhole attacks [10]. The first steps consist of two methods. In the first method, no de and its next node are identified using Round-trip-Time (RTT), and in the second method, a list of them is compiled, and if the destination node is not in this list, then it is undoubtedly complete in nature. In the second step of the mechanism, after detecting doubts about the full link, the attack ends with the RTS / CTS method. The paper demonstrates the possibility of fingerprinting on the radio of wireless sensor nodes, the technique of radio printing [11]. It starts by receiving a radio signal from a fingerprint reader, and then the signal is converted to digital form. The signal transmission is positioned, and its characteristics are described. The fingerprint character set is later used to identify the device.

In [12], the authors used the AODV and DSR routing protocol. If doubt is found in any node, then information about the trust margin is used to identify the node, regardless of whether the node is susceptible to wormhole attack or not. In this model, each node controls its neighboring node based on its packet drop pattern.

In [13], the authors proposed a technique based on the hash compression function (HCF). It is mainly used for a secure hash function to calculate the value of the hash function field for route requests (RREQ) over networks. It uses the AODV routing protocol. According to the authors. The source node starts the route discovery process to search for the destination node. Then, the source node calculates the hash function based compression function (HCF) and calculates the value of the hash function field with the route request (RREQ), and it goes to the neighboring node. If the value of the neighboring node matches the value of the destination node. In this situation, the destination node receives a No Route Request (RREQ). Finally, the destination node implements the concept of hash-based compression (HCF).

D. Wormhole Using Packet Relay [3], [4]

An attack on a wormhole based on packet relay can be launched by one or more malicious nodes. In this type of attack, a malicious node relays the data packets of two remote sensor nodes to convince them that they are neighbors. This type of attack is also called a “play-based attack" in the literature.

In [14], the authors proposed localization based on a system that is vulnerable to wormhole attacks, how they manipulate the localization method to prevent attack wormhole, and a “safe location based distance consistency” scheme was implemented, it works to detect, accurately locate and trapping wormhole attacks

In [15], the authors propose that security becomes centralized in MANET. MANET applications have been deployed in various fields. A wormhole attack is one of the serious attacks that can be smoothly resolved in networks, but it is difficult to observe. This is possible even if the attacker does not negotiate in any situation, and the rest of the communication gives security, novelty, authenticity and confidence.

E. Wormhole using protocol distortion [3], [4], [17]

In this wormhole attack mode, one malicious node tries to attract network traffic, distorting the routing protocol. Routing protocols based on the “shortest delay” instead of the “least hop” are at risk of wormhole attacks using protocol distortion. This type of wormhole is harmless in itself, and is also called a “swift attack” in the literature.

In [16], the authors suggested that attackers could record the location of packets in the WSN, send them to another location, and transfer them back to the network. When he found the roots, is there a wormhole detection process that considers the difference between a neighboring node and another node? If the difference is greater than that of the destination node, detect wormholes.

Several approaches to detecting wormholes and their countermeasures in WSN have been presented above.

Model description

Above is an analysis of a method for detecting wormhole attacks in WSNs, most of which are for hardware protection or for specific security nodes on networks.

The presented algorithm uses only information about network connections in order to find infected nodes by a wormhole. The detection method is based on the assumption that the removal of the wormhole edges causes significant changes in the length of the shortest paths between some nodes in the network, while the other shortest paths remain unchanged. To track changes, the broadest searches are started on some selected nodes, called “root nodes”, while other sensors and their environs are iteratively isolated.

First, the search occurs in width in a distributed manner. The source node may send an outgoing signal or packet containing its depth (0). Then the receiving nodes add 1 to the depth and forward the modified packet, etc. After each node determines its distance, it can send it to the source node on the route indicated by the now completed spanning tree. You can use this function to make the algorithm almost completely decentralized. Although the root nodes must perform some additional, not trivial calculations. The algorithm is presented in figure-2.

This algorithm has been tested in Python 3.6. The code contains a repository for randomly generating a network of wireless sensors in a 2D plane, inserting a wormhole into the network, and a detection algorithm to identify the affected sensors. The algorithm uses only network formation to search and isolate nodes under the wormhole. The idea is based on the assumption that removing the entire edge of the wormhole causes significant changes in the length of the shortest paths between some of the nodes in the network, while the other shortest paths remain unchanged. In order to track changes, a search is started on several selected nodes. The first breadth-first search may be performed in a distributed manner. The source cannot send a start signal or packet increasing its depth (0). Then the receiving nodes add 1 to the depth and forward the modified packet, etc. After each node determines its distance, they can send it to the source node on the route indicated by the now completed spanning tree. This feature can be used to make the algorithm almost completely decentralized. Although, the nodes should do some additional, but trivial calculations (Fig-2).

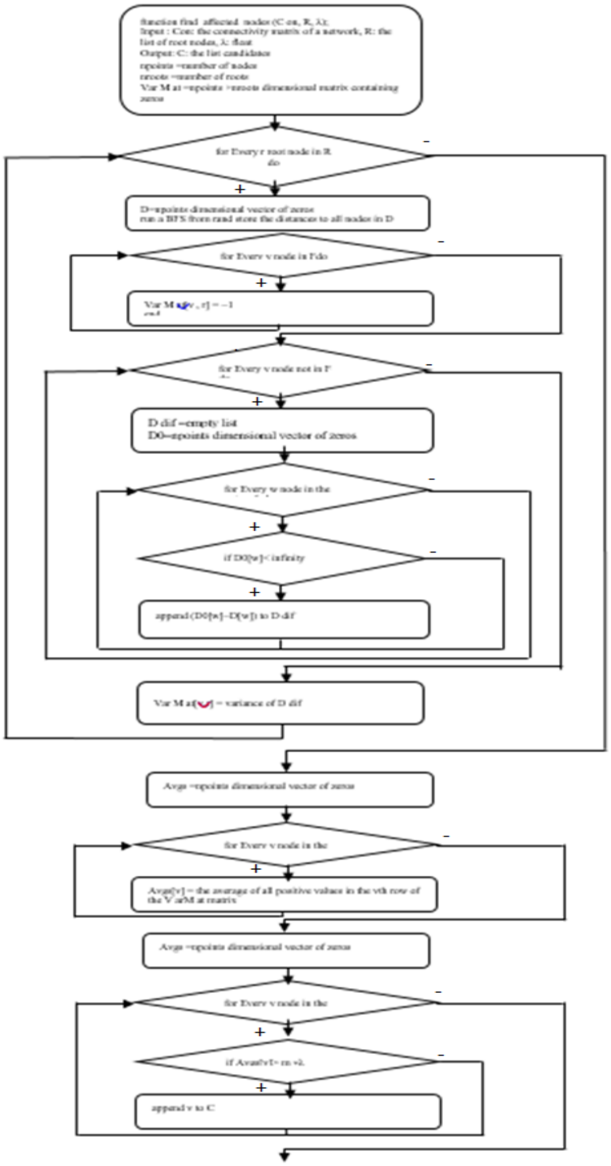
function find affected nodes (C on, R, λ);
Input : Con: the connectivity matrix of a network, R: the list of root nodes, λ: float
Output: C: the list candidates
npoints =number of nodes
nroots =number of roots
Var M at =npoints ×nroots dimensional matrix containing zeros
for Every r root node in R do
D=npoints dimensional vector of zeros
run a BFS from rand store the distances to all nodes in D
for Every v node in Γdo
Var M at[v , r] = −1
end
for Every v node not in Γ do
D dif =empty list
D0=npoints dimensional vector of zeros
for Every w node in the
if D0[w]< infinity
append (D0[w]−D[w]) to D dif
Var M at[v,r] = variance of D dif
Avgs =npoints dimensional vector of zeros
for Every v node in the
Avgs[v] = the average of all positive values in the vth row of the V arM at matrix
Avgs =npoints dimensional vector of zeros
for Every v node in the
if Avgs[v]> m +λ
append v to C
+
-

Figure-2-Operational algorithm

Results

In the last section, many modern techniques have been introduced to address the problem of wormhole attacks. However, all of these methods have limitations. Many of them depend on special equipment or special protective units. Some methods are based on the assumption that the wormhole inserts only one false edge into the network. Others are exceptionally reliable for wormholes that introduce large full bipartite subgraphs.

The following is a detailed description of this approach. The algorithm uses only network connection information to find and isolate nodes under a wormhole attack. This method is based on the assumption that the removal of the edges of the wormhole causes significant changes in the lengths of the shortest paths between some nodes in the network, while the other shortest paths remain unchanged. To track changes, a breadth-first search is then started from some selected nodes, called “root nodes”, while other sensors and their environs are iteratively isolated.

When the program starts, it deploys a wireless sensor network with random deployment and a communication model with a quasi-single disk graph in the 10x10 region. The number of sensors is 400, and the communication radius of the nodes is 1.2. Enemy radios have a radius of 0.6, and they are located at a distance of at least 6 jumps between them. k and th (lambda) are the parameters of the algorithm.Make_plot = True visualizes results.

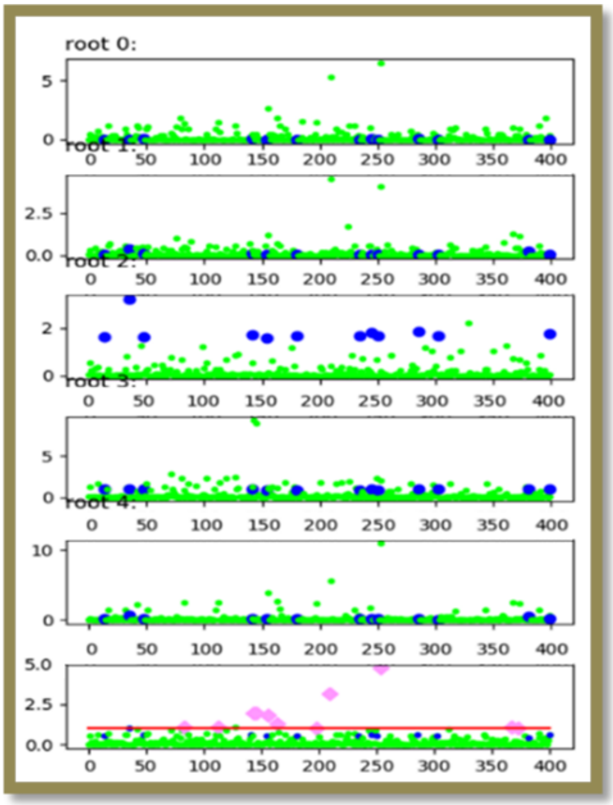

Figure - 3 Classification results for various root nodes

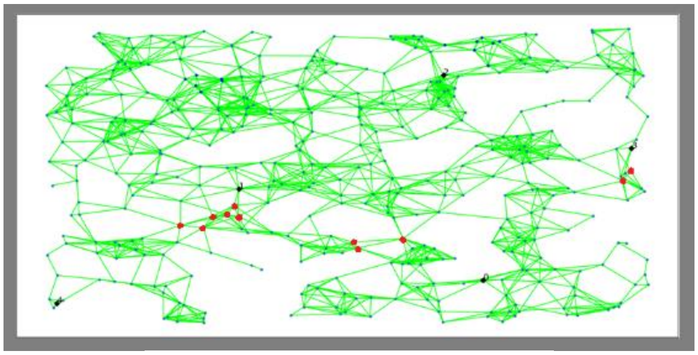

Figure-4 Network Diagram

Makeplot=False, the output is a simple matrix of confusion

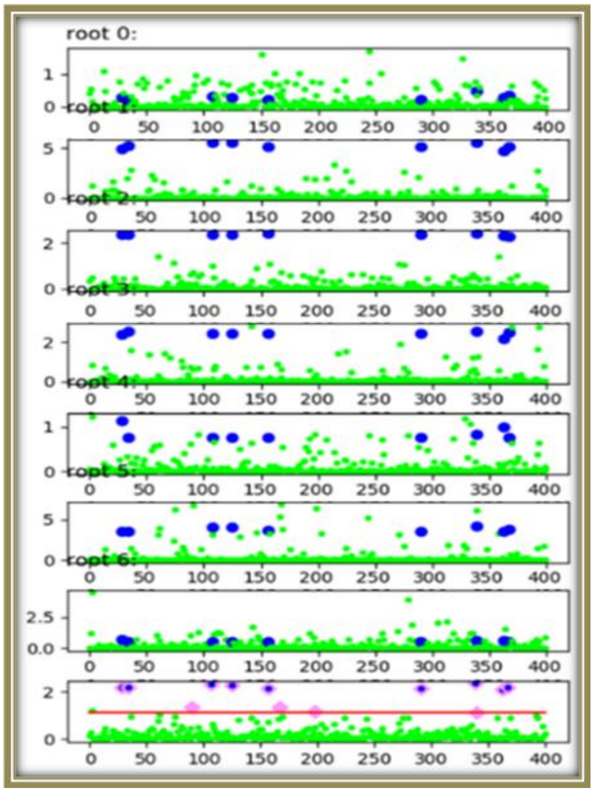

Figure-5 Classification results for various root nodes

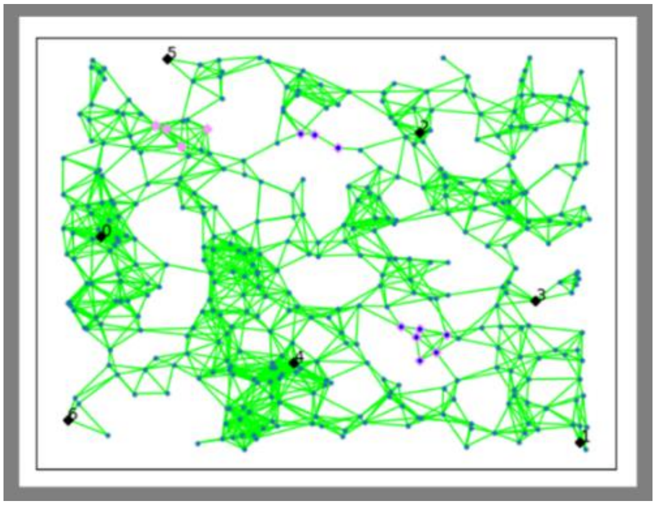

Figure-6 Network Diagram

Figure 3, 5 shows the classification results for different root nodes, and Figure 4, 6 shows a network diagram in which the wormhole nodes and the predicted wormhole nodes are colored blue and red, respectively.

In order to demonstrate how the value of λs affects the result, run several times with different values

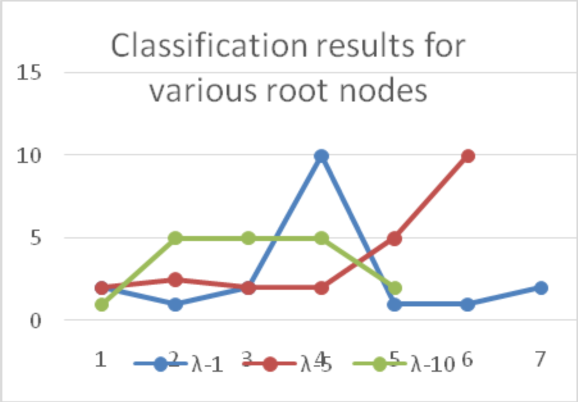

Figure-7 Classification visualization results for various rootnodes

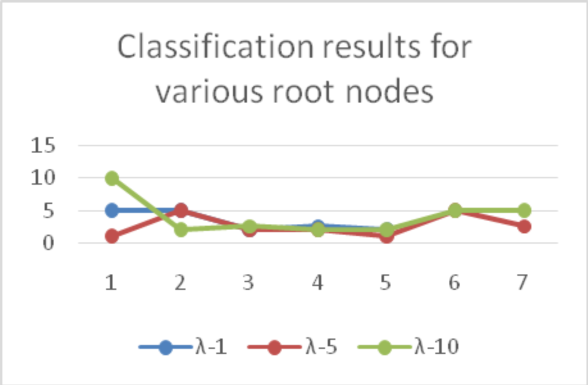

Figure-8 Classification results for various root nodes of the confusion matrix

The longer the wormhole path, the more damage, and easier to detect. During the simulation, wormholes were created so that the distance between two sets of wormhole nodes in the source network was at least 7. Tests performed with λ = 1.5.10 and created 30 networks with 400 nodes for each deployment model, communication model and network density. Experiments have shown how the algorithm performs under these conditions by measuring the average number of false positives and the average number of reviews for these test cases. The results are shown in Figures 7 and 8. Tests show the effectiveness of the algorithm. The number of false positives is relatively low, especially for a perturbed grid and for random placement with an average degree of 10 or more.

Conclusion

Wormhole attacks have been identified as attacks that can be powerful and can cause serious damage to the network, even if authentication and encryption are required for communications. This attack cannot be taken lightly. Methodologies for detecting and protecting against these attacks have been proposed mainly for special and sensor networks. Very few researchers have been able to test their security system using a true FSU. Also, some results showed a low detection frequency, high network load and high .

The tested approach does not rely on special equipment, information about the network before the attack, but uses only information about connecting to the network. In addition, the accuracy of the proposed algorithm is not affected by the number of wormholes. Testing the effectiveness of the algorithm using tests communication cost

in scenarios with different communication models, deployment methods and network density. The future solution must be verified in a real sensor network. Thanks to this check, it will be easy to check whether the solutions in the real wireless sensor network are consistent.

References

1. Vinayak gupta, Brijesh kumar singh, parmesh war lal bhanwariya "An Introduction to security issues in wireless sensor networks" Journal of environment al science, computer science and engineering and technology (JECET); November 2013;vol.2 No.4,pp.1276-1285.

2. Md. Safiqul Islam, Rasib Hayat Khan, Dewan Muhammad Bar ry. A hierarchical intrusion detection system in wireless sensor networks // international journal of computer science and network security. 2010. Vol. 10. No 8.

3. M. Tubaishat and S. Madria, Sensor networks: an overview, IEEE Potentials, vol. 22, pp. 20-23, (2003).

4. Nishant Sharma and Upinderpal Singh, Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks, International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 2, February 2014, pp.29 – 33

5. L. Hu, D. Evans, Using Directional Antennas to Prevent Wormhole Attacks, 14 Proceedings of the 11th Network and Distributed System Security Symposium, (2003).

6. K. S. Win., Analysis of Detecting Wormhole Attack in Wireless Networks, World Academy of Science, Engineering and Technology, 48, pp. 422-428, (2008).

7. M.S. Sankaran, S. Poddar, P.S. Das, S. Selvakumar, A Novel Security Model SaW: Security against Wormhole attack in Wireless Sensor Networks. In Proceedings of International Conference on PDCN, (2009).

8. H.S. Chiu and K. Lui, DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks. In Proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, (2006).

9. C.P.Vandana, A.F.S. Devraj, MLDW-a Multilayered Detection mechanism for Wormhole attack in AODV based MANET , International Journal of Security, Privacy and Trust Management. Vol. 2 (3), June (2013).

10. S. Ö zdemir, M. Meghdadi, Ý . Güler, A time and trust-based wormhole detection algorithm for wireless sensor networks. In 3rd Information Security and Cryptology Conference (ISC'08), pp. 139-142, (2008).

11. K.B. Rasmussen and S. Capkun, Implications of radio fingerprinting on the security of sensor networks, Third International Conference on Security and Privacy in Communication Networks and the Workshops, pp. 331-340, Sep, (2007).

12. H. Vu, A. Kulkarni, K. Sarac, N. Mittal, WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks. In Proceedings of International Conference on Wireless Algorithms Systems and Applications, LNCS 5258, pp. 491-502, (2008).

13. N.Choudhary and S.Agrawal, Analysis of Worm-Hole Attack in MANET using AODV Routing Protocol, SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE), vol. 1 (10) 2014, pp. 1-6.

14. D.B. Roy, R.Chaki, N.Chaki, A New Cluster-based Wormhole Intrusion Detection algorithm for Mobile Adhoc Networks, International Journal of Network Security & Its Applications (IJNSA), vol. 1 (1), April, (2009).

15. Z. Zhao, B. Wei, X. Dong, L.Yao, F.Gao, Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis”,International Conference on Information Engineering(ICIE), (2010).

16. B. Prasannajit, Venkatesh, S. Anupama, K. Vindhykumari, S.R. Subhashini, G. Vinitha, An approach towards Detection of Wormhole Attack in Sensor Networks, First International Conference on Integrated Intelligent Computing (ICIIC), (2010), pp.283-289.

17. Ghugar, Umashankar & Pradhan, Jayaram. (2019). A Review on Wormhole Attacks in Wireless Sensor Networks.

18. M. A. Patel and M. M. Patel, "Wormhole Attack Detection in Wireless Sensor Network," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, (2018), pp. 269-274, doi: 10.1109/ICIRCA.2018.8597366.

ОБНАРУЖЕНИЕ WORMHOLE АТАК В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Жукабаева Т.К ассоциированный профессор
Марденов Е.М., докторант
Евразийский национальный университет имени Л.Н. Гумилев
Казахстан,г.Нур-Султан,ул.А.Пушкина 11, emardenov@gmail.com

Аннотация. БССподвержены многочисленным типам угроз и атак. Одна из них - wormhole атака. В этой статье представлен обзор методов обнаружения wormholeатак в БСС, а также новый оптимизированный метод обнаружения этой атаки. Метод обнаружения основан на удалении краев червоточины и вызывает значительные изменения длины кратчайших путей между узлами сети. На точность предложенного алгоритма не влияет количество червоточин.

Чем длиннее путь wormholeатаки, тем больше повреждений и легче обнаружить. Алгоритм работает в этих условиях, измеряя среднее количество ложных срабатываний и среднее количество отзывов для этих тестовых случаев. Тесты показывают эффективность алгоритма. Количество ложных срабатываний относительно невелико, особенно для нарушенной сетки и случайного размещения.

Ключевые слова: БСС, червоточина, атаки безопасности, механизм защиты, специальная сеть, вредоносный узел, сенсорные узлы, строчная топология, узел привязки, направленная антенна.

СЫМСЫЗ СЕНСОРЛЫҚ ЖЕЛІЛЕРДЕ WORMHOLE ШАБУЫЛДАРЫН АНЫҚТАУ

Жукабаева Т.К., доцент
Марденов Е.М., докторант
Л.Н. Гумилев атындағы Еуразия алтын университеті
Қазақстан, Нұр-Сұлтан қ., А.Пушкин көшесі 11, emardenov@gmail.com

Аңдатпа. Сымсыз сенсорлы желілер, көптеген қатерлер мен шабуылдарға ұшырайды. Оның бірі - wormholeұңғымасына шабуыл. Бұл мақалада WSN-де wormholeсаңылауларын анықтау әдістеріне шолу, сондай-ақ осы шабуылды анықтауға арналған оңтайландырылған жаңа әдіс ұсынылған. Анықтау әдісі wormholeсаңылауының шеттерін алуға негізделген және желілік түйіндер арасындағы ең қысқа жолдардың ұзындығында айтарлықтай өзгерістер тудырады. Ұсынылған алгоритмнің дәлдігіне wormholeтесіктерінің саны әсер етпейді.

Wormholeтесік жолы неғұрлым ұзағырақ болса, соғұрлым зақым көп болады және оны анықтау оңайырақ болады. Біз алгоритмнің осы жағдайларда қалай жұмыс істейтінін байқадық, жалған позитивтердің орташа санын және осы тестілік жағдайларға арналған шолулардың орташа санын өлшедік. Тесттер алгоритмнің тиімділігін көрсетеді. Жалған позитивтер саны салыстырмалы түрде аз, әсіресе бұзылған тор үшін және кездейсоқ орналастыру үшін.

Кілт сөздер: Сымсыз сенсорлы желілер, wormholeсаңылауы, қауіпсіздік шабуылдары, қорғаныс механизмі, арнайы желі, зиянды түйін, сенсор түйіндері, жол топологиясы, якорь түйіні, бағытталған антенна.

DETECTING WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS

Zhukabayeva, T.K. associate professor
Mardenov E.M., doctoral student
Eurasian National University named after L.N. Gumilyov
Kazakhstan, Nur-Sultan, A. Pushkin Ave.11, emardenov@gmail.com

Abstract. WSNs are subject to numerous types of threats and attacks. One of which is a wormhole attack. This article provides an overview of wormhole attack detection methods in WSN, as well as a new optimized method for detecting this attack. The detection method is based on the removal of the edges of the wormhole and causes significant changes in the length of the shortest paths between network nodes. The accuracy of the proposed algorithm is not affected by the number of wormholes.

The longer the wormhole path, the more damage, and easier to detect. Experiments have shown how the algorithm performs under these conditions by measuring the average number of false positives and the average number of reviews for these test cases. Tests show the effectiveness of the algorithm. The number of false positives is relatively low, especially for a perturbed grid and for random placement.

Key words: WSN, wormhole, security attacks, defense mechanism, special network,malicious node, sensor nodes, string topology, anchor node, directional antenna.