International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209705 Volume 8, Issue 4, July – August (2021)

RESEARCH ARTICLE

Wormhole Detection Using Encrypted Node IDs and Hop Counts in the Event Report of Statistical En-Route Filtering

Ga-Hyeon An
Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea.
angachi576@skku.edu

Tae-Ho Cho
Department of Computer Science and Engineering, Sungkyunkwan University, Suwon, Republic of Korea.
thcho@skku.edu

Received: 01 July 2021 / Revised: 05 August 2021 / Accepted: 13 August 2021 / Published: 28 August 2021

Abstract – Wireless Sensor Network (WSN), there are low capacity, low cost, tiny sensor nodes, and sinks. Sensor nodes detect an event occurring in its surroundings and send data about the event to the sink. Sensor nodes have a limited transmission range and computational power. Since the wireless sensor network operates with limited resources than the ad hoc network, it is difficult to apply the defense method as it is, so research on a new defense method is needed. In a WSN, sensor nodes manage, monitor, and collect data for a specific environmental and physical application, and the collected data is transmitted to and used by a base station. Base stations are connected via the Internet and share data with users. Since the sensor node is composed of low power and low capacity, it is mainly used in an unattended environment, so it is easily exposed to various attacks and can be damaged. This type of network makes it difficult to detect wormhole attacks when they occur along with other attacks like false report injection attacks and Sybil attacks. Therefore, to prevent this, in this study, the hop count and the encrypted node ID are added in the report generation process of the statistical en-route filtering technique to detect wormhole attacks even when a wormhole attack occurs along with a false report injection attack to improve security.

Index Terms – Wormhole Attack, Statistical En-Route Filtering, Wireless Sensor Network, Hop Counts, Encrypted Node IDs.

1. INTRODUCTION

As shown in Figure 1, the WSN is consists of low-capacity, low-cost, intelligent, and tiny sensor nodes and sink [1]. Sensor nodes detect event data occurring around it and send a message to the sink. The WSN is mainly used in unmanned environments and has applications in the military, traffic, fire, health, GPS location, and more [2].

In WSN, sensor nodes are used to collect data by using wireless communication to monitor specific environments and physical applications with limited transmission range and limited computational power using small sensor nodes. Also, many applications deploy and use sensor nodes in an unattended environment, so the lifespan of the node can be determined by the battery life, so it uses low energy [3]. As such, the sensor node uses low power, low cost, and low capacity, and is deployed in an open environment such as an unattended environment, so it can be subjected to various attacks by attackers [4, 5]. Also, the types of attacks that occur at the OSI layer are different. Table 1 shows each attack occurring at the OSI layer [6].

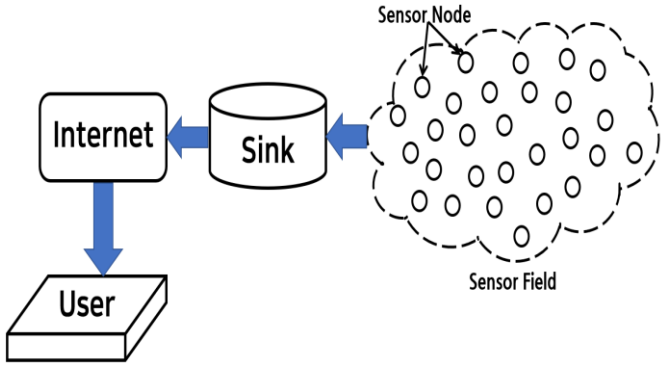


Figure 1 Wireless Sensor Network

Layers	Attacks
Physical Layer	Replay attack, Interference
Data Link Layer	Collision, Exhaustion, Denial of sleep
Network Layer	Selective forwarding attack, Sinkholes, Sybil attacks, Node replication attacks, Wormholes, Flooding, Hello flooding attack,

RESEARCH ARTICLE

	Attacks against privacy, Blackholes
Transport Layer	Injects false messages, Flooding(SYN Flood), Content attack
Application Layer	Data Aggregation, Distortion

Table 1 OSI Layer Specific Attacks

Attack	Description
Selective Forwarding Attack [7]	An attack in which a compromised node acts like a black hole and rejects and removes specific messages.
Sinkhole Attack [4]	An attacker can cause other attacks, such as selective forwarding attacks, as attacks that attract almost all traffic in a specific area around the attacker through a compromised node.
Sybil Attack [8]	This refers to a form of attack that creates one action that behaves as if it were the action of several people to achieve a specific purpose.
False Report Injection Attack [5]	This uses compromised nodes to generate a report on events that did not occur. It is an attack that can cause energy depletion of intermediate nodes in the process of delivering reports to a base station and may confuse the user when the reports arrived at the base station.
Wormhole Attack [4]	Two or more compromised nodes broadcast to neighboring nodes that they can move with a path shorter than the original path by generating another path. After that, attacks such as selective forwarding, deletion, and eavesdropping can be performed within it.
Spoofing Attack [9]	This occurs when an attacker believes the information came from a node that it did not transmit and can root a user or device on the system.
Blackhole Attack [10]	This occurs when an attacker captures a set of network nodes and reprograms them to block received packets instead of forwarding them to the base station.

Table 2 Attack Type

As described in Table 2, since the wireless sensor network is similar to the ad-hoc wireless network, the attack is also similar [3]. However, sensor nodes in wireless sensor networks are much more limited than in ad-hoc networks. Also, additional security requirements such as Data Confidence [11], Data Authentication and Integrity [12], Data Availability [13] are also required as well as general network requirements. Therefore, it is difficult to directly replace the defense technology of the ad-hoc network, and new defense techniques appropriate for the wireless sensor networks are needed [14].

Among the above-mentioned attacks, the wormhole attack becomes difficult to detect if they occur with other attacks, such as the Sybil attack and false report injection attack. To detect a false report injection attack, proper authentication of the message is required, and a statistical en-route filtering technique can be used as a defense technique against this. However, since the statistical en-route filtering technique only considers the integrity of the report content, it is still vulnerable to wormhole attacks such as selective forwarding, deletion, and eavesdropping [15].

In this study, when events occur within the wireless sensor network, the sensor nodes around the generated event detect the event, generate a detected event report, and forward it to the base station. In the process of transmitting a report, a wormhole attack may occur in which the report is transmitted through a different path than the original path. Therefore, a wormhole attack is detected by adding the hop count and the encrypted node ID into the report content during the report generation process of the statistical en-route filtering technique. In addition, we propose a wormhole attack detection technique that can improve security so that it can detect both false report injection attacks and wormhole attacks that occur together.

This paper proceeds as described below. Chapter 2 introduces wormhole attacks and the defense methods of the existing wormhole attack and introduces the statistical en-route filtering technique that is the basis of the proposed technique. Chapter 3 describes the assumptions and operation process of the proposed technique. Chapter 4 shows the result of comparing the performance of the proposed method with the existing method, and Chapter 5 describes future work. Finally, Section 6 describes the conclusion.

2. RELATED WORK

The basic data security requirements for a wireless sensor network are primarily the same as for an ad-hoc network,

RESEARCH ARTICLE

which is confidential, reliable, and available data. However, defense techniques used in the ad-hoc network cannot be directly applied due to limited resources, as previously mentioned [2].

2.1. Statistical En-Route Filtering

As shown in Figure 2, en route filtering-based technologies are divided into cryptography and classification based on probability of filtering based on encryption and filtering probability. Classification based on cryptography can be divided into symmetric cryptography based techniques and asymmetric cryptography based techniques based on cryptography again [2].

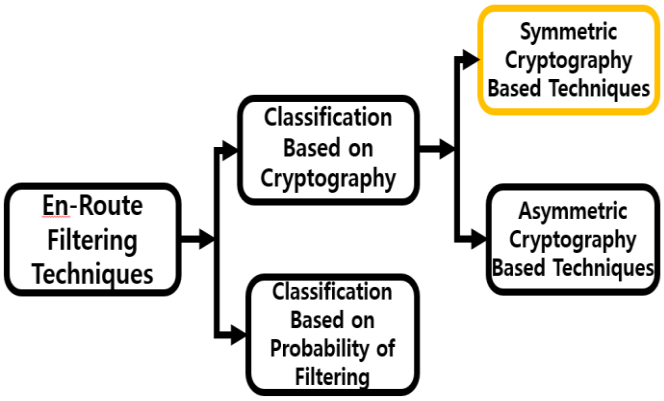


Figure 2 En-Route Filtering Techniques

The symmetric cryptography based techniques are again classified as Figure 3. [2].

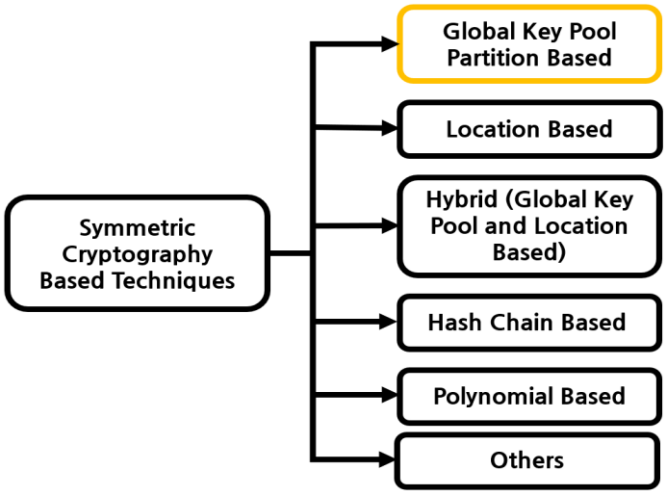


Figure 3 Symmetric Cryptography Based Techniques

Among various en-route filtering technologies, Statistical En-Route Filtering (SEF) [2] based on Global Key Pool Partition is used to detect false report injection attacks. It consists of a total of four steps: a pre-key distribution step, a report generation step, a report intermediate node filtering step, and a base station filtering step.

In the pre-key distribution step, the key is distributed using the Global Key pool as shown in Figure 4. The Global Key Pool has N keys $\{K_i, 0 \le i \le N-1\}$, which are divided into n nonoverlapping partitions $\{N_i, 0 \le i \le n-1\}$, and each partition has m keys $(n \times m = N)$ [5]. Each key has an index, and when a node is assigned each key, the node is assigned a key from a randomly selected partition. This is used to generate MAC (Message Authentication Code) on each node when an event occurs [5].

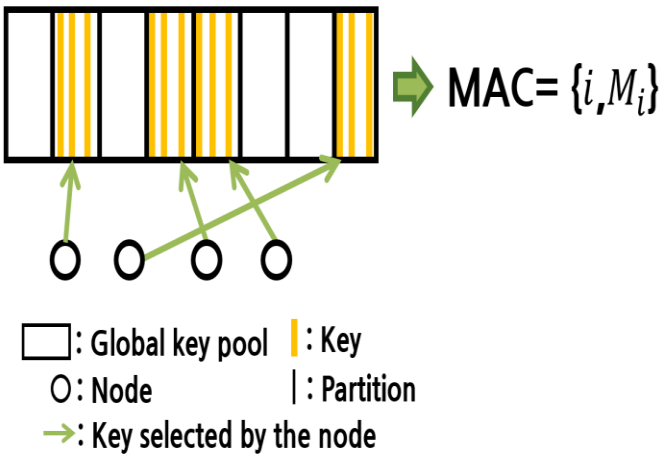


Figure 4 The Pre-Key Distribution Step

Figure 5 describes the operation process of the SEF after the pre-key distribution step of electing a CoS (Center of Stimulus) node when events occur. The CoS nodes collect the MACs of the surrounding sensor nodes which detect the occurrence of events, generate event reports, and transmit reports to the sink through the intermediate node.

The conditions for checking the report in the intermediate node filtering step of the report are as follows. The CoS node classified MACs collected from neighboring nodes are based on key partitions. At this time, the MAC created with the key to the same partition is defined as one category and is represented by a security Threshold (Threshold: T) $(T \le n)$. K_{i_j} is the $j\ th$ key of the $i\ th$ key partitions, i_j is the index of node, and M_{i_j} is the MAC of node [5].

Operations in en-route filtering [5]:

1) Check if $T\ \{i_j, M_{i_j}\}$ exists in the report, and if not remove the report.
2) If T indexes belong to a specific partition of $\{i_j, 1 \le j \le T\}$ key T, it is transmitted to the next node, otherwise it is removed.

RESEARCH ARTICLE

3) When M is calculated using one $K \in \{K_{i_j}, 1 \leq j \leq T\}$ key, if it is the same as M_{i_j}, the report is transmitted to the next node, otherwise it is removed.

4) If the key does not exist in the $\{K_{i_j}, 1 \leq j \leq T\}$ condition, the report is transmitted to the next node.

In the final step of SEF, the base station stores the global key pool, then checks all MAC and unique indexes present in the report, and if they are different, the report is removed.

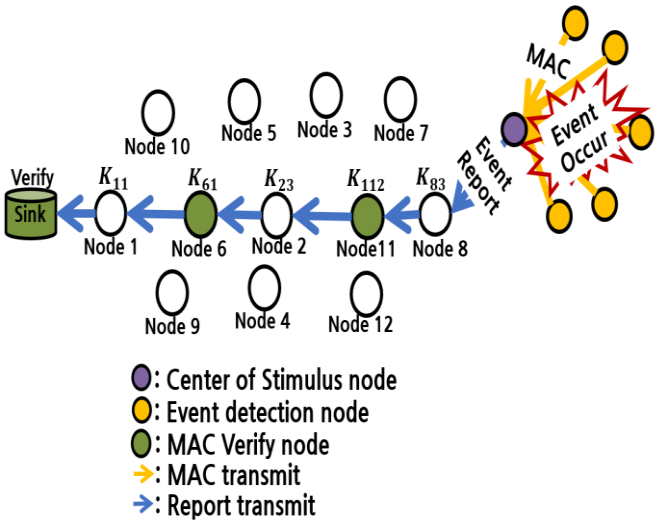


Figure 5 Statistical En-Route Filtering Operation Process

2.2. Wormhole Attack

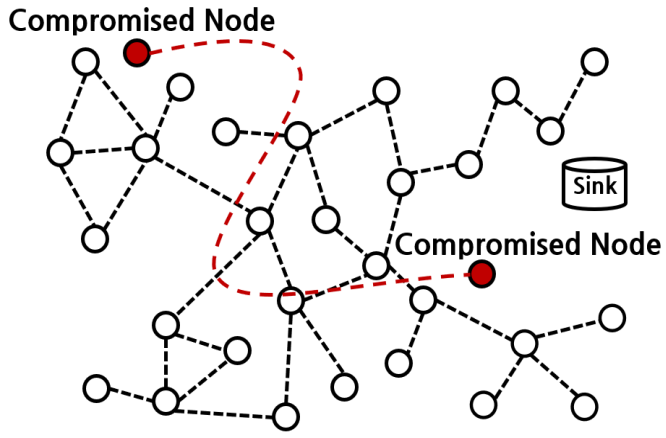


Figure 6 Wormhole Attack

As shown in Figure 6, an attack that includes compromised nodes in the sensor network by an attacker and generally operates in pairs of two or more nodes is called a wormhole attack. Pairs of attack nodes send and receive data packets or messages through tunnels that are only connected. In the case of a tunneled distance that is further than the original radio transmission scope of a single hop, attack node broadcasts to neighboring nodes that it can move faster than the original path, and then moves to a different path or data packets or messages may not reach the base station. Wormhole attacks can occur even if an attacker does not have an encryption key, and legitimate nodes do not see attack nodes or other tunneled paths, making them easier to attack but harder to detect. Moreover, this is even harder to detect attack when attacks like selective forwarding, deletion, and eavesdropping occur together within a wormhole attack [4].

2.3. Type of Wormhole Attack

1. Packet encapsulation type: An attacker launches an attack using two malicious nodes. One malicious node is close to a source node and the other is close to a sink, creating the tunnel between them. The malicious node encapsulates the data packet in the form of a malicious packet and instructs it to tunnel to the other end. When request packets are generated from a source node, the malicious node acts like the shortest path, tunneling to the other end without asking for another path, thus achieving the fastest path discovery. This type of wormhole attack compromises throughput, packet forwarding speed, and network integrity [16].
2. Out of band channel type: The attacker uses a high-quality bandwidth or a wired connection with a specific frequency for the malicious node. Channels can achieve using wired connections or long-range and directional wireless channels. Intermediate nodes are not included in this connection. Therefore, it provides the fastest response time. Because the malicious node serves as the endpoint of the shortest path, a fast response time can be achieved when searching for a path [17].
3. High transmission power type: An attacker only needs one attack node with high transmission capacity to create another shortest path and can communicate with a sensor node at a distance. Malicious nodes broadcast requests at high power levels when they receive RREQ. When a node receives a high-power broadcast, it broadcasts the RREQ back to the target node. If an attacker uses this method, they are more likely to be in the established path between the base stations without the help of other malicious nodes in the network [18].
4. Packet relay type: This type can be attacked using one or more nodes compromised by the attacker. A malicious node is an attack that convinces a neighbor that it is a legitimate node [19].
5. Protocol deviation type: In this type, the routing protocol for communication is distorted, and malicious nodes try to lure network traffic. The attacker forwards the packet

RESEARCH ARTICLE

to the sink without back-off so that it can be included in the path to the sink [20].

2.4. Existing Wormhole Attack Defense Techniques

Various wormhole attack detection methods exist in ad-hoc wireless networks [21]. The method of providing a directional antenna to a node uses the node's antenna area to establish a connection between nodes [22]. Packet leashes use geographic and temporal leashes to provide information through packets that control the transmission scope called leashes. A geographic leash specifies the distance between the receiver and sender. A receiving node that receives the packet calculates the transmission time and distance [23]. The receiver can detect whether a packet has passed a wormhole attack through data analysis [24]. However, the two methods described above are difficult to apply to WSN using low-capacity and small sensor nodes because they are premised on using a special device attached to the sensor node [25]. The LITEWORP method selects a guard node that exists simultaneously within the scope of two adjacent nodes in the path. The guard node continuously monitors the traffic of two adjacent nodes and checks whether packets other than the existing packets are forwarded [26]. LITEWORP works without any special devices. However, since the guard node has to monitor all data transmitted to two adjacent nodes, it can incur a huge overhead to the node in terms of energy and processing. Therefore, it may not be suitable for sensor networks [26, 27]. In the AOMDV routing protocol, the sender node checks if there is a route through which two nodes in the routing table can communicate, and if there is a route, it provides routing information. On the other hand, if the route does not exist, it broadcasts an RREQ and sets the route. After that, all routes are kept in the routing table of source nodes [28].

2.5. WODEM

WODEM (WOrmhole Attack DEfense Mechanism) [26, 29] is a method that can detect wormhole attacks while meeting the limited part of sensor networks. WODEM selects one of the sensor nodes and only installs a location awareness program (GPS) and a long-lasting battery on this node. A couple of detector nodes exchanges newly defined control packet and compares their distance with the number of hops passed [29]. If the maximum distance is less than the actual distance for that number of hops, a wormhole attack can be detected along the path. WODEM is divided into Detector Scanning step, Wormhole Detection step, and Neighbor List Recovery step [26, 29].

In the detector scanning step, as shown in Figure 7, one detector node of a pair of detector nodes scans the other detector node and measures the channel features. Prevent control packets from passing through wormholes using channels separate from normal communication channels on the network to maintain scan secret [26]. Therefore, all detector nodes in the scan step are tuned to different channels. In the wormhole detection step, the number of detected hops and the actual hop count are compared with a pair of detector nodes to determine whether there is a wormhole. If a wormhole is detected at this stage, it moves on to the neighbor-list repair step.

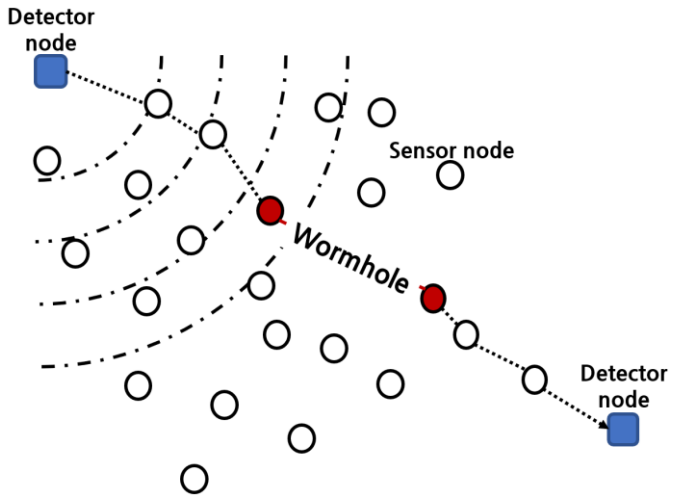


Figure 7 WODEM Operation Process

In the neighbor-list repair step, a pair of detector nodes find two sensor nodes with detected wormholes in the path and removes them from the neighbor list. In WODEM, the Detector Scanning step and the Neighbor-list repair step are repeatedly operated until no more wormholes are detected.

WODEM is cost-effective because it does not require a special device and only the node selected as the detector node needs a location recognition device and a long-lasting battery. In addition, sensor nodes other than detector nodes do not require additional processing, so they are energy efficient.

3. PORPOSED MODELLING

As mentioned earlier, wormhole attacks become difficult to detect when they occur together with another attack such as Sybil attack and false report injection attack. Among them, we want to detect wormholes based on reports of the SEF that can detect false report injection attacks. However, for SEF, it's hard to find a wormhole attack because only data integrity is considered. Therefore, it is possible to detect a wormhole attack by adding additional data into the event reports of the statistical en-route filtering technique.

3.1. Assumptions

The assumptions of this proposed method are below:

1. The routing protocol from the CoS node to the sink uses a minimum hop count.

RESEARCH ARTICLE

2. The base station knows the minimum hop counts in the path from every node to the base station and all node information.
3. The report uses Shortest Path Routing.
4. Every node has only one child node.
5. The hop count increases by 1 using Count each time the report passes an intermediate node.
6. Each time an intermediate node passes, the node's ID is encrypted.

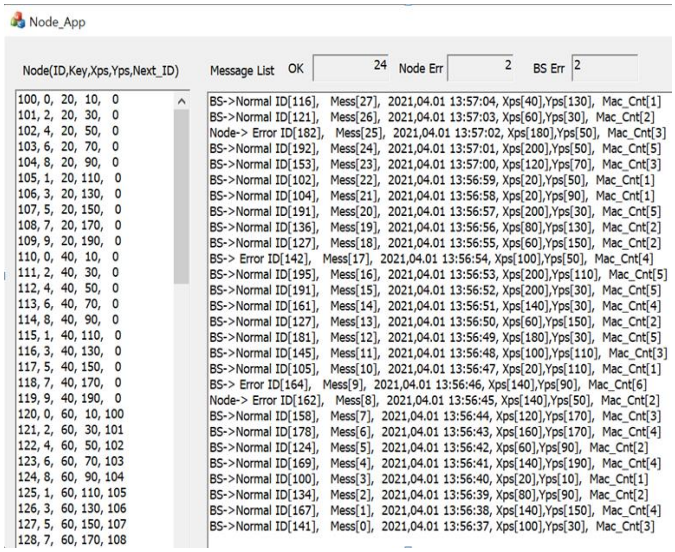


Figure 8 Proposed Technique Simulation

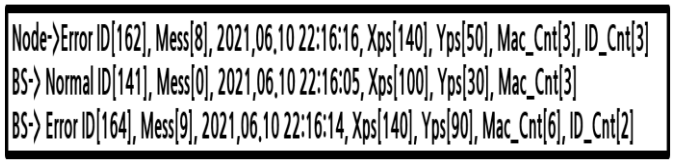


Figure 9 Proposed Technique Simulation Message

Definition	Explanation
BS->Normal	When the report is delivered to the base station without a wormhole
Node->Error	When a wormhole is detected in a node
BS->Error	When the base station detects a wormhole
ID[162]	Node ID number
Mess[8]	Event generation message number
2021,06,10 22:16:13	Event generation time
Xps[140], Yps[50]	The location of the node that detected the wormhole
Mac_Cnt[3]	Hop Count
ID_Cnt[3]	Node ID Count

Table 3 Proposed Techniques Simulation Message Definition

3.2. Proposed Technique

The wormhole attack detection method proposed in this study is constructed in the second step of SEF, the report generation process. When a sensor node detects an event that occurred in the sensor field, the CoS node collects the MAC from the node that detected the event and generates an event report. Subsequently, when the report is transmitted to the sink using intermediate nodes, hop count and encrypted node ID are added to the report in the format shown in Figure 10. L is generated event location, t is generated event time, E is generated event content, i is Key Index, and $node\ ID$ is the encrypted node ID.

$$L, t, E, i, MAC, hop\ count, node\ ID$$

Figure 10 Event Report Format

If the event report passes through a wormhole, as the report moves to a different path from the original path as shown in Figure 11, the hop counts, the number of encrypted node IDs, and the encrypted node ID information in the report are different. Therefore, hop count is additionally verified when verifying the MAC in the intermediate node filtering step of the SEF. At this time, since all nodes have only one child node, the verification node can know its parent node when verifying the hop counts. In addition, if we trace the parent node that sent the report to the verification node, we can know the original normal path and the hop counts in the normal path. Therefore, if the hop count in the normal path and the hop count in the report is different, intermediate nodes will remove the report.

In the case of node IDs, each node ID is encrypted whenever a report is transmitted through an intermediate node and finally decrypted by the base station. If the hop count in the report is changed due to an attack such as selective forwarding, deletion, or eavesdropping that may be caused by a wormhole attack, it is not easy to find the wormhole attacks through only the hop count. Therefore, when the base station decrypts the encrypted node ID in the event report, it compares the number of decrypted node IDs and the hop count, if they are different, it is regarded as having passed the wormhole and the report is removed. If the number of decrypted node IDs and the hop counts are the same, the base station knows the node information exists in the path for transmitting the report from all nodes to a base station. Therefore, check decrypted node

RESEARCH ARTICLE

ID information in the event report, compared the node ID of the normal path with the node ID that exists in the report, and if they are different, finally remove the report from the base station. The operation method of the proposed method is shown in Figure 12.

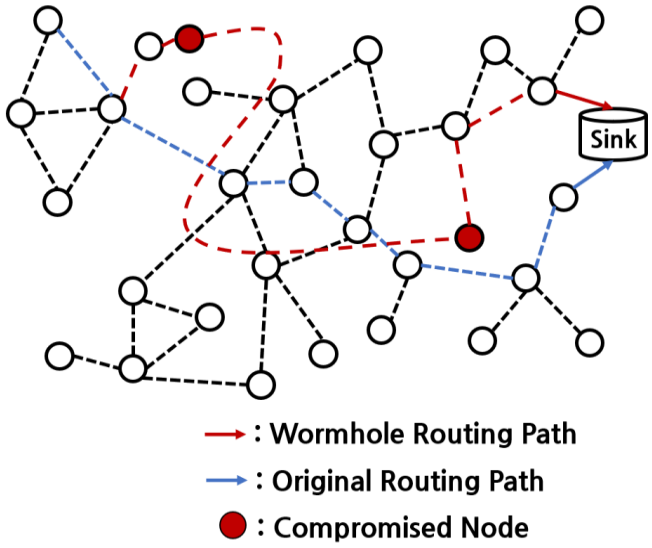


Figure 11 Report Routing Path

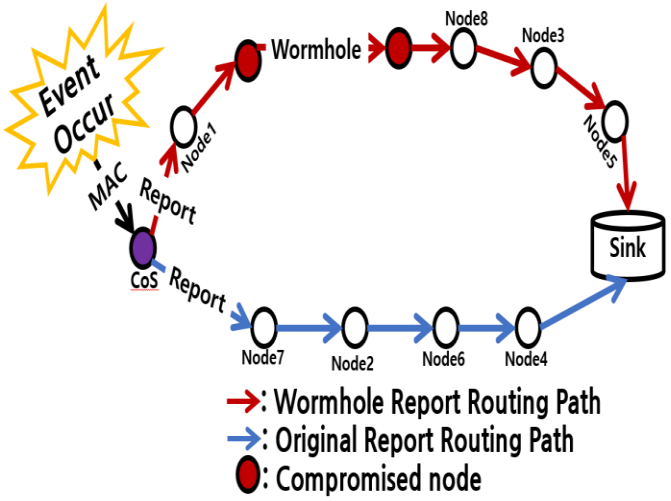


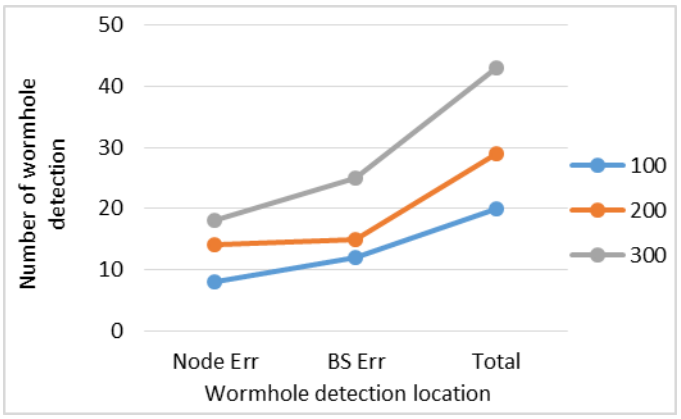
Figure 12 Proposed Techniques Operation Process

4. RESULTS AND DISCUSSIONS

The following describes the simulation environment: The event occur randomly, 100 nodes are fixedly placed in a sensor field of $200 \times 200m^2$. MAC is 32bits, the key is 16 bits, ID is 24 bits.

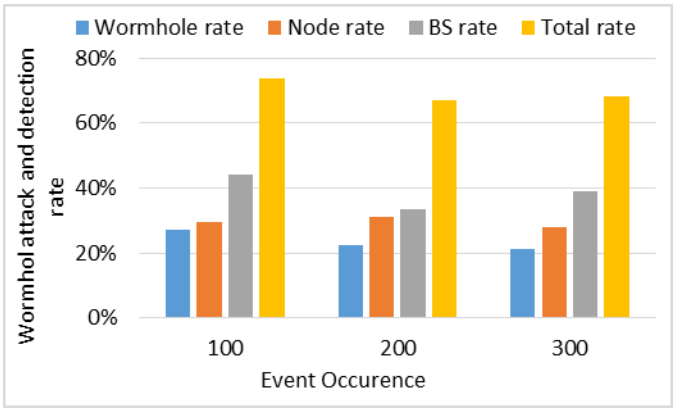
4.1. Adding Only Hop Count to the Event Report

The results when comparing 100 to 300 event occurrences are the same as in Graph 1.



Graph 1 Wormhole Attack Detected Through Event Report with Hop Count Added

Graph 2 is a graph showing the result values for wormhole attacks and detections that occurred in 100 to 300 events as a percentage. The blue graph shows the wormhole attacks, the orange graph shows the wormhole attacks detected at the node, the gray graph shows the wormhole attacks detected at the base station, and the yellow graph shows the total sum of the wormhole attacks detected at the node and the base station as a percentage.



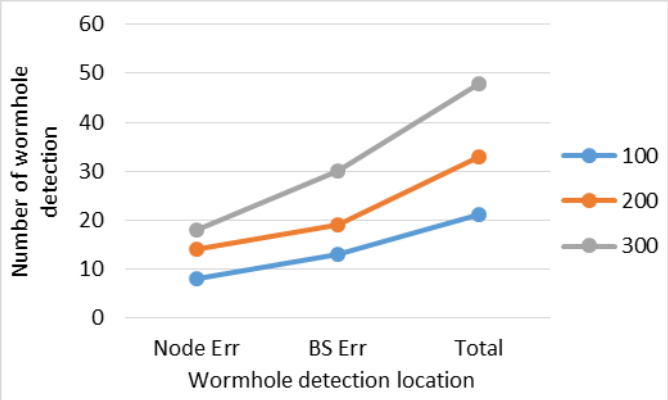
Graph 2 Wormhole Attack and Detection Rate According to the Number of Event Occurrences When the Hop Count is Added

The average of each item for 100–300 event occurrence times in Graph 2 is as follows. The average wormhole attack rate is 23.1%, the average of the wormhole attacks detected in the node is 29.61%, the average of the wormhole attacks detected in the base station is 38.7%, and the average of the total sum of the wormhole attacks detected by the node and the base station is 69.7%.

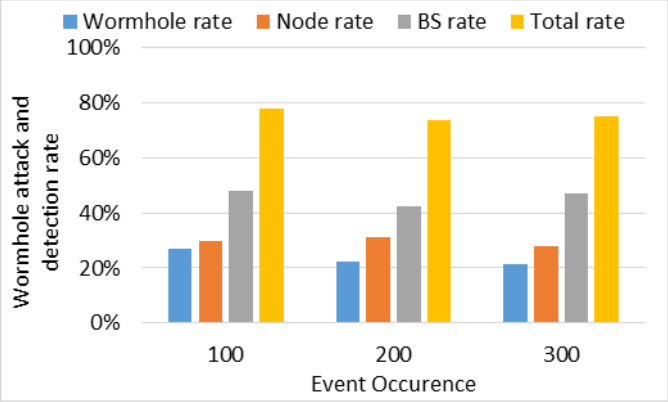
4.2. Proposed Technique Result

The results when comparing 100 to 300 event occurrences are the same as in Graph 3.

RESEARCH ARTICLE



Graph 3 Wormhole Attack Detected Through the Event Report of the Proposed Technique



Graph 4 Wormhole Attack and Detection Rates According to the Number of Events in the Proposed Technique

The average of each item for 100–300 event occurrence times in Graph 4 is as follows. The average wormhole attack rate is 23.1%, the average of the wormhole attacks detected in the node is 29.61%, the average of the wormhole attacks detected in the base station is 45.74%, and the average of the total sum of the wormhole attacks detected by the node and the base station is 75.3%.

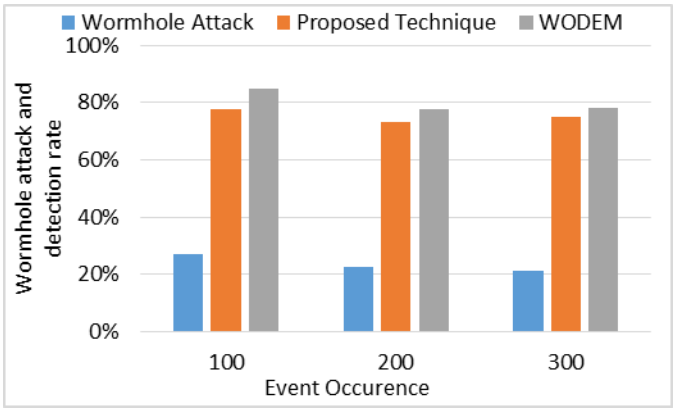
Compared to the proposed technique, the ratio of wormhole attacks detected at nodes is the same, but the proportion of wormhole attacks detected at the base station and the total number of wormhole attacks detected at the node and base station were approximately 7% and 5.6% higher, respectively.

The reason for this result is that the encrypted node ID does not perform the decryption process when verifying the hop count on the intermediate node, but only the encryption process. After that, the decryption process is executed only at the base station. The comparison of the two wormhole detection techniques results in an increase in the wormhole attack detection rate at the base station, increasing in the total wormhole attack detection rate.

4.3. Proposed Technique and WODEM

Three pairs of detector nodes in WODEM were tested at 100 to 300 event occurrence counts.

Graph 5 shows the result values for wormhole attacks and detections that occurred in 100 to 300 events as a percentage. The blue graph shows the wormhole attacks, the orange graph shows the wormhole attacks detected by the proposed technique, and the green graph shows the wormhole attack rate detected by the WODEM.



Graph 5 Wormhole Attack and Detection Rates According to the Number of Event Occurrences of WODEM and the Proposed Technique

The average of each item for 100–300 event occurrence times in Graph 5 is as follows. The average wormhole attack rate was 23.1%, the average of wormhole attacks detected in the proposed technique was 75.3%, and the average of wormhole attacks detected in WODEM was 80.3%. Thus, WODEM showed a detection rate about 5% higher than the proposed technique. However, since the proposed technique is based on SEF, it can detect not only wormhole attacks but also wormhole attacks and false report injection attacks occurring at the same time. Therefore, although WODEM has slightly better security in terms of the detection rate of wormhole attacks, it can be expected to improve security for the proposed technique when it occurs simultaneously with a false report injection attack.

5. FUTURE WORK

The proposed technique and WODEM [29] are similar in that they detect wormhole attacks using the hop count. However, when WODEM detects a wormhole between a pair of detector nodes, it immediately removes the node from the neighbor node list and repeats the process until no wormhole is detected. When wormhole attacks are detected, the process for detecting other wormhole attacks is not repeated except for the detected wormhole attack. In other words, in WODEM, there is a process for the defense of deleting a node from the neighbor node list after wormhole detection, but in the

RESEARCH ARTICLE

proposed technique, there is only a detection process and no defense process. Since the proposed method is based on SEF, the base station has information on all nodes. Therefore, after the last step of SEF, the base station broadcasts the node information where the wormhole attack occurred to all sensor nodes in the sensor field. Afterward, additional research is needed on the process of defending after detecting a wormhole attack so that when the nodes send a report in the sensor field, it excludes the path of the node where the wormhole attack was detected.

6. CONCLUSION

In this study, the hop count and the encrypted node ID were added to the event report based on SEF to detect wormhole attacks. Because the proposed method operates based on SEF, the contents of the MAC and the hop count in the report are verified during the intermediate node filtering process. Therefore, if the intermediate node detects a wormhole attack using the hop count, it is possible to prevent selective forwarding, deletion, and eavesdropping attacks that may occur due to a wormhole attack in advance. If the intermediate node fails to detect wormhole attacks or the hop counts are changed by the wormhole attack, the base station can finally find the wormhole attacks through the node ID encrypted in the report. In addition, it's possible to detect when wormhole and false report injection attacks occur simultaneously, thereby increasing security to a high level.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2021R1A2C2005480).

REFERENCES

[1] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," in IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002, doi: 10.1109/MCOM.2002.1024422.

[2] Kumar, A., Pais, A.R. En-Route Filtering Techniques in Wireless Sensor Networks: A Survey. Wireless Pers Commun 96, 697–739 (2017).

[3] Tubaishat, Malik, and Sanjay Madria. "Sensor networks: an overview." IEEE potentials 22.2 (2003): 20-23.

[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003., 2003, pp. 113-127, doi: 10.1109/SNPA.2003.1203362.

[5] Fan Ye, Haiyun Luo, Songwu Lu and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," IEEE INFOCOM 2004, 2004, pp. 2446-2457 vol.4, doi: 10.1109/INFCOM.2004.1354666.

[6] Sastry, Anitha S., Shazia Sulthana, and S. Vagdevi. "Security threats in wireless sensor networks in each layer." International Journal of Advanced Networking and Applications 4.4 (2013): 1657.

[7] S. Kaplantzis, A. Shilton, N. Mani and Y. A. Sekercioglu, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines," 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, 2007, pp. 335-340, doi: 10.1109/ISSNIP.2007.4496866.

[8] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," Third International Symposium on Information Processing in Sensor Networks, 2004. IPSN 2004, 2004, pp. 259-268, doi: 10.1109/IPSN.2004.239019.

[9] Jindal, Keshav, Surjeet Dalal, and Kamal Kumar Sharma. "Analyzing spoofing attacks in wireless networks." 2014 Fourth International Conference on Advanced Computing & Communication Technologies. IEEE, 2014.

[10] Wazid, Mohammad, et al. "Detection and prevention mechanism for blackhole attack in wireless sensor network." 2013 International Conference on Communication and Signal Processing. IEEE, 2013.

[11] Walters, John Paul, et al. "Wireless sensor network security: A survey." Security in distributed, grid, mobile, and pervasive computing. Auerbach Publications, 2007. 367-409.

[12] Carman, David W., Peter S. Kruus, and Brian J. Matt. "Constraints and approaches for distributed sensor network security (final)." DARPA Project report,(Cryptographic Technologies Group, Trusted Information System, NAI Labs) 1.1 (2000): 1-39.

[13] Dener, Murat. "Security analysis in wireless sensor networks." International Journal of Distributed Sensor Networks 10.10 (2014): 303501.

[14] Rehana, Jinat. "Security of wireless sensor network." Seminar on Internetworking. 2009.

[15] Jeba, S. Annlin, and B. Paramasivan. "False data injection attack and its countermeasures in wireless sensor networks." European Journal of Scientific Research 82.2 (2012): 248-257.

[16] Goyal, Minalini, and Maitreyee Dutta. "Intrusion Detection of Wormhole Attack in IoT: A Review." 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET). IEEE, 2018.

[17] Khan, Zubair Ahmed, and M. Hasan Islam. "Wormhole attack: A new detection technique." 2012 International Conference on Emerging Technologies. IEEE, 2012.

[18] Khandare, Pravin, Yogesh Sharma, and S. R. Sakhare. "Countermeasures for selective forwarding and wormhole attack in WSN." 2017 International Conference on Inventive Systems and Control (ICISC). IEEE, 2017.

[19] Maidamwar, Priya, and Nekita Chavhan. "Wormhole Attack in Wireless Sensor Network." (2012).

[20] Meghdadi, Majid, Suat Ozdemir, and Inan Güler. "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks." IETE technical review 28.2 (2011): 89-102.

[21] Umashankar Ghugar, Jayaram Pradhan. (2019). A Review on Wormhole Attacks in Wireless Sensor Networks. International Journal of Information Communication Technology and Digital Convergence, 4(1), 32-45.

[22] L. Hu, D. Evans, Using Directional Antennas to Prevent Wormhole Attacks, 14 Proceedings of the 11th Network and Distr ibuted System Security Symposium, pp. (2003) .

[23] Ghugar, Umashankar, and Jayaram Pradhan. "Survey of wormhole attack in wireless sensor networks." Computer Science and Information Technologies 2.1 (2021): 33-42.

[24] Maidamwar, Priya, and Nekita Chavhan. "Wormhole Attack in Wireless Sensor Network." (2012).

[25] Y. C. Hu, A. Perrig, D. B. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks, inProc. of IEEE -INFOCOM, (2003), pp. 1976 -1986, vol.3

[26] Kim, Frank Stajano Hyoung Joong, and Jong-Suk Chae Seong-Dong Kim. "Ubiquitous Convergence Technology."

[27] I . Khalil, S. Bagchi, N . B. Shroff, LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multi hop Wireless Networks , Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05) .

[28] Amish, Parmar, and V. B. Vaghela. "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol." Procedia computer science 79 (2016): 700-707.

RESEARCH ARTICLE

[29] Yun JH., Kim IH., Lim JH., Seo SW. (2007) WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks. In: Stajano F., Kim H.J., Chae JS., Kim SD. (eds) Ubiquitous Convergence Technology. ICUCT 2006. Lecture Notes in Computer Science, vol 4412. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-71789-8_21.

Authors

Ga Hyeon An received his B.S degree in the Department of Electronic Communication Engineering from Dealim University, in February 2021. His research interests include wireless sensor network, IoT, machine learning and deep learning.

Tae Ho Cho received his Ph.D. in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Computing at Sungkyunkwan University, Korea. His research interests include wireless sensor networks, intelligent systems, modeling and simulation, and enterprise resource planning.

How to cite this article:

Ga-Hyeon An, Tae-Ho Cho, "Wormhole Detection Using Encrypted Node IDs and Hop Counts in the Event Report of Statistical En-Route Filtering", International Journal of Computer Networks and Applications (IJCNA), 8(4), PP: 390-399, 2021, DOI: 10.22247/ijcna/2021/209705.