A METHOD OF IMPROVING ENERGY EFFICIENCY THROUGH GEOFENCING AND FALSE DATA BLOCKING IN CONTEXT-AWARE ARCHITECTURE FOR PROBABILISTIC VOTING-BASED FILTERING SCHEME OF WSNS

Su Man Nam[1] and Youn Kyoung Seo[2]

[1]DUDU Information Technologies, Republic of Korea
[2]Incheon Jae Neung University, Republic of Korea

ABSTRACT

In wireless sensor networks, sensor nodes have the disadvantage of being vulnerable to several attacks due to the use of wireless communication and constrained energy. Adversaries exploit vulnerable characteristics of these nodes to capture them and generate false positive and false negative attacks. These attacks result in false alarms in a base station and information loss in intermediate nodes. A context-aware architecture for a probabilistic voting-based filtering scheme (CAA-PVFS) identifies compromised nodes that cause the damage. Although this method immediately detects the compromised nodes using its CAA, its additional network use consumes unnecessary energy. In this paper, our proposed method configures geofencing for the compromised nodes and blocks the nodes using false data injection. The proposed method reduces the unnecessary energy of the additional network while maintaining security strength. Experimental results indicate that the proposed method offers energy savings of up to 17% while maintaining the security strength against the two attacks as compared to the existing method.

KEYWORDS

Wireless Sensor Network, Context-aware Architecture, Probabilistic Voting-based Filtering, False Positive Attack, False Negative Attack, Network Security.

1. INTRODUCTION

Wireless sensor networks (WSNs) are the subject of extensive research efforts in various fields such as environmental and habitat monitoring, and surveillance and tracking for military applications [1-5]. A WSN is composed of numerous sensor nodes and a base station in a sensor field. A sensor node uses a data collection module, a data process, and control module, a communication module, and a battery module to operate without interference [2, 4, 6-9]. The base station receives the data from the sensor node and provides information [8, 10, 11]. Although the sensor network operates in a large-scale environment without infrastructure, the sensor nodes are highly vulnerable to capture and compromise because of their constrained battery energy and operation resources [5, 10, 12-16].

In a WSN, adversaries can complete full control over it by reading its memory and influencing its program through fabricated messages [5, 10]. An adversary can capture a small number of nodes to attempt a false positive attack (FPA) [5, 10, 12, 17-19] and a false negative attack (FNA) [10, 17-19]. Figure 1 shows the false positive attack generated in a compromised node (*node1*) and

the false negative attack produced in the other node (*node2*). The compromised node (*node1*) injects false reports about non-existent event to drain the energy of intermediate nodes and generate false alarm in the base station. The other node (*node2*) inserts false message authentication codes (MACs) [10, 12, 20]into a legitimate report to drop it and to lose information.

A context-aware architecture for a probabilistic voting-based filtering scheme (CAA-PVFS) [10, 20] uses a different approach from existing several methods [5, 12, 17-19] to detect both these attacks. When false data occurs on a compromised node, the existing methods filter the data with high probability using their specific techniques in intermediate verification nodes. The CAA-PVFS, on the other hand, integrates its CAA and an existing method's filtering techniques to effectively identify a compromised node and improves security strength. In the CAA-PVFS, a sensor field includes a communication architecture (Comm-Arch) [10, 14] to collect all context information and to forward the collected information to its CAA. The CAA analyzes the collected information based on its knowledge base to detect the compromised node. Although the CAA-PVFS identifies the compromised node against the two attacks, the CAA-PVFS continues to transmit the false data of the node via the Comm-Arch after identifying it. Thus, this method affects the network lifetime through unnecessary energy consumption.

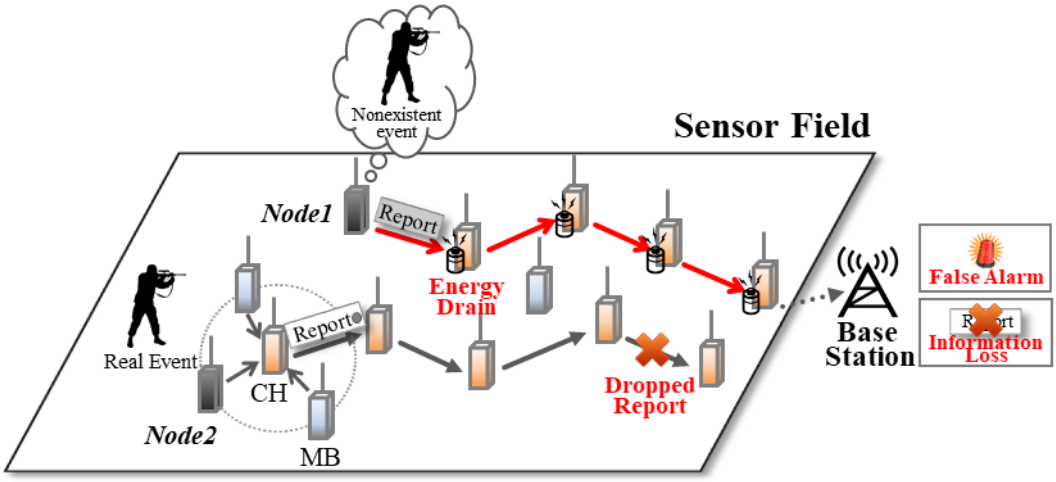

Figure 1. False positive and false negative attacks.

In this paper, we propose a method that configures geofencing after identifying compromised nodes by our CAA and blocks false data of the identified compromised nodes in the Comm-Arch's collection nodes. In our proposed method, the geofencing technology allows a false report to be removed in the compromised node's next node and the geofencing location to be appended in a legitimate report when the report passes through compromised area. The legitimate report is verified in the CAA and the base station. In addition, the data blocking technology prevents false data through the collection nodes of the Comm-Arch using their blacklist. Experimental results indicate that the proposed method improves energy efficiency while maintaining the security strength of the sensor network.

The main contributions of this paper are as follows:

- Compromised nodes' geofencing,
- False data blocking, and
- Improved energy efficiency of the entire network.

The rest of this paper is organized as follows: Section 2 introduces the existing method, discusses the problem statements. We offer a detailed description of the proposed method in Section 3. In Section 4, we present a performance evaluation of the proposed method. We draw conclusions and future works at the end of this paper.

2. BACKGROUND

In this section, we discuss the CAA-PVFS for detecting both false positive and false negative attacks, introduce the problem statements.

2.1. CAA-PVFS

In [10], the CAA-PVFS detects the false positive and negative attacks in the sensor network using its CAA. In the CAA-PVFS, the CAA is implemented in simulation models consistent with the structure and components of the sensor network. The CAA collects sensing data of the sensor network via Comm-Arch and detects abnormal behavior for identifying the compromised nodes through its knowledge base.

Figure 2 shows the procedure of the CAA-PVFS. The CAA-PVFS's sensor field consists of the PVFS-based WSN and the Comm-Arch. The PVFS detects false positive and negative attacks through a pre-defined threshold, which the number of fabricated MACs in a report. The sensor network is distributed with general sensor nodes, which are cluster-heads and members. The Comm-Arch's collection nodes are deployed with the sensor node in the sensor field. The collection node collects the sensing data from the cluster-heads and the members. It uses different frequencies to transmit the data to the CAA without interference of the sensor network. The CAA receives the collected data via the Comm-Arch and analyses the data.

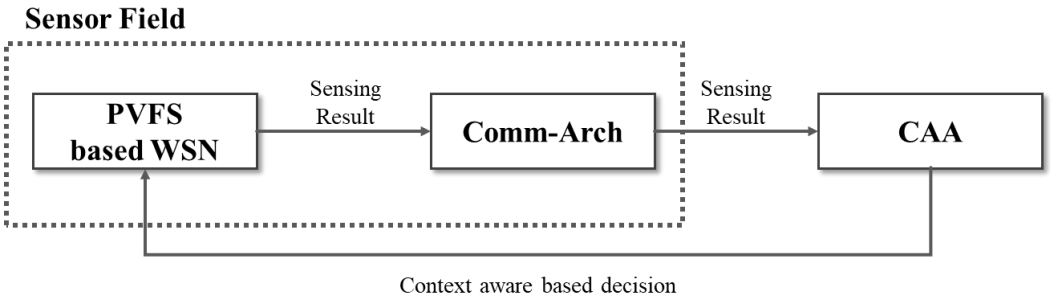

Figure 2. CAA-PVFS's procedure

CAA-PVFS consists of four stages:

- *Initialization and key assignment*: In the sensor network, sensor nodes (i.e., cluster-heads, members) are organized into the sensor field with keys. Each cluster-head forms a cluster with the members within one hop. The cluster-head chooses its verification nodes through probabilistic calculations. In the Comm-Arch, the collection nodes are arranged to gather data transmitted from the network.
- *Report generation*: As a real event occurs, an elected cluster-head forwards the event data to its members. Each member generates MACs and transmits them to the cluster-head. The cluster-head then generates a report including gathered MACs. In the Comm-Arch, the collection nodes gather the event data and the MACs while transmitting them.

- *En-route filtering*: As a verification node receives a report, it checks its keys to authenticate if the MAC is normal or false. If the number of authenticated fabricated MACs reaches the threshold, the node removes the report against the false positive attack; if the number of fabricated MACs is below the threshold, the report continues to be forwarded against the false negative attack. In the Comm-Arch, the collection node gathers reports transmitted among intermediate nodes.
- *Data verification in CAA*: The CAA effectively identifies the compromised node against false positive and negative attacks after gathering the gathered data. The CAA provides a final context-aware-based decision to the base station of the sensor network.

2.2. Problem Statement

The CAA-PVFS effectively identifies the compromised nodes and copes with the false positive and negative attacks through the Comm-Arch using the CAA. In the Comm-Arch, collection nodes gather event data, MACs, and reports from the sensor network and broadcast it to the CAA via multiple hops. Although the CAA-PVFS detects both attacks efficiently, the method is consistently transmitted with fabricated data from areas of compromised nodes. For example, we assume that one source collection node is 10 hops away from CAA and transmits a 36-byte report. In [10, 12, 14], an energy model of the sensor node consumes 16.25 μJ per byte to transmit and 12.5 μJ per byte to receive. The collection node consumes 28.75 μJ when sending and receiving 1 byte of the data. While the report arrives at the CAA, 10 intermediate nodes of a source consume 10,350 μJ (=28.75 μJ×36 bytes×10 hops). When event data, MACs, and reports are transmitted continuously in a compromised node, the Comm-Arch is greatly affected by high energy consumption. Thus, it is necessary to apply a geofencing technology in the sensor network and communication blocking in the Comm-Arch to reduce unnecessary energy consumption.

3. PROPOSED METHOD

In this section, we introduce the proposed method which configures geofencing for the compromised nodes and blocks the nodes' false data to reduce the needless energy of the Comm-Arch.

3.1. Overview

The proposed method configures geofencing of identified compromised nodes by the CAA and blocks false data of the compromised node using each collection node's blacklist.

Figure 3 shows an overview of our proposed method. In a cluster (Cluster 1), a compromised node is identified through an injection of the false positive attack. The compromised node reinjects another false report in the sensor network. When false data (i.e., event data, MACs, or reports) is transmitted continuously in a compromised node, the networks (i.e., WSN, Comm-Arch) are greatly affected by false data injection and high energy consumption without geofencing and data blocking technologies. As shown in Figure 3, our proposed method configures the geofencing in the sensor network and blocks false data by blacklist to reduce the unnecessary energy consumption in the entire network.

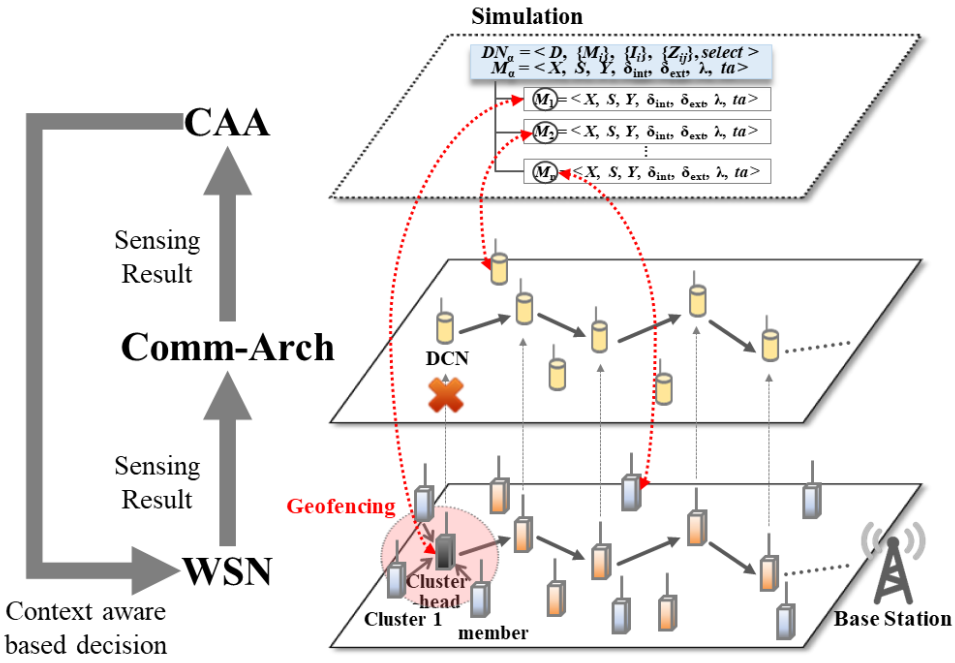

Figure 3. Overview of the proposed method

3.2. Detailed Procedure

Our proposed method newly adds the following functions based on the phases (initialization and key assignment, report generation, en-route filtering, and data verification) proposed in [10].

- Geofencing configuration: The proposed method configures the geofencing of the compromised nodes identified from the CAA.
- Data blocking: This method blocks fabricated data using the blacklist of the collection node in the configured geofencing.

Figure 4 shows an example of how the base station configures a geofencing in the sensor network. After our CAA verifies the false data, it notices an identification (ID) of a compromised node to the base station. The base station extracts a cluster location of the ID and storages the location of the compromised area. The station forwards the location information to neighbors of the compromised node. As shown in Figure 4, a cluster-head CH1 broadcasts this location information after it receives the alert information. Cluster-heads CH2 and CH3 receive the information and configure virtual perimeter in the sensor network. The base station also storages geofencing information of the compromised cluster after configuring the perimeter. In the Comm-Arch, when the cluster-heads forward the information, collection nodes receive it. After a collection node of the compromised cluster saves the information, the collection node immediately rejects fabricated data received from the compromised node.

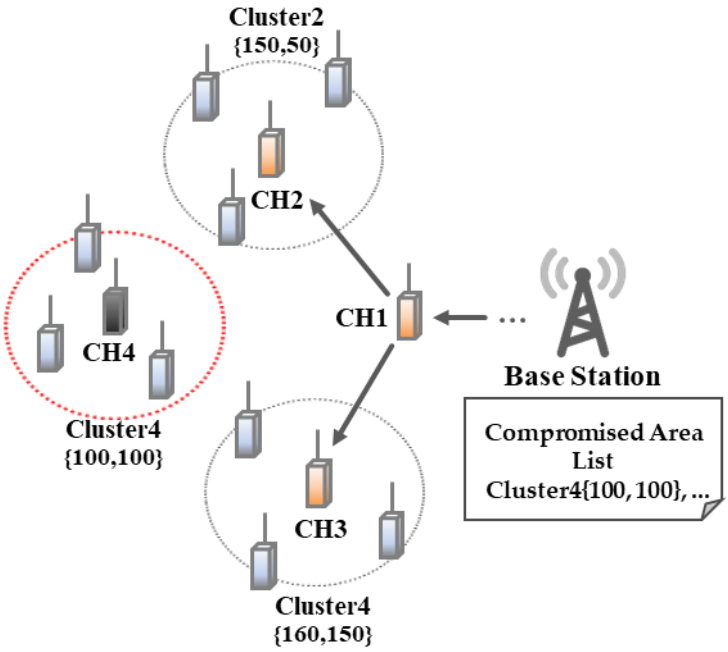

Figure 4. Geofencing configuration of the compromised cluster

Figure 5 demonstrates the geofencing of the compromised cluster in a sensor field. In the geofencing area, a cluster-head CH1 is a compromised node. The compromised node generates a false report about the non-existent event without the cooperation of its members. The CH1 broadcasts the false report to a CH4. The CH4 immediately drops the fabricated report after it receives the report of the compromised node. As soon as a collection node of the geofencing checks its blacklist, the collection node promptly also removes the report.

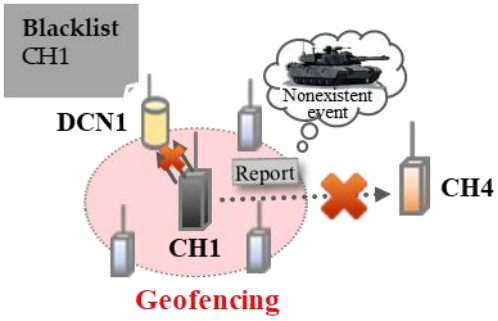

Figure 5. Geofencing's fabricateddata blocking

Figure 6 demonstrates the forwarding of two reports. One report bypasses the geofencing, and the other report is transmitted via the configured geofencing. This is a compromised member (MB1) in the geofencing area. The compromised node is identified through our CAA. A cluster-head CH2 generates a report and forwards it to a CH1. The CH1 broadcasts the report towards its collection node and a CH4. The collection node forwards the report to the CAA because the CH1 is normal. After receiving the report via geofencing, the CH4 appends the geofencing location in the report. The report with the appended location is finally verified in the base station and the CAA. On the other hand, a CH2 detours the geofencing and forwards the legitimate report to a

CH3. The CH3 transmits it to the CH4. The CH4 forwards the report to the next node without the extra action.

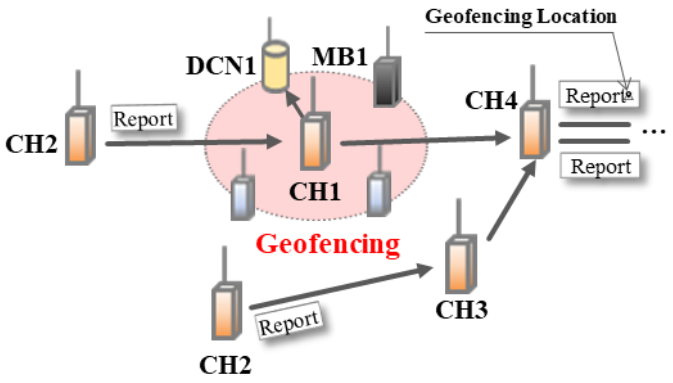

Figure 6. Geofencing location appending when a legitimate report passes through the geofencing.

Thus, our proposed method configures geofencing for the compromised nodes in the sensor network and blocks the nodes' false data to reduce the unnecessary energy consumption of the additional network.

4. SIMULATION RESULTS

We performed a simulation experiment to evaluate the proposed method and compare it to the CAA-PVFS. A sensor field, which is 1,000 × 1,000 ㎡ includes 100 cluster-heads and 900 members for the sensor network and 100 collection nodes for the Comm-Arch. All nodes were randomly and uniformly distributed in 100 × 100 m clusters. Each cluster includes one cluster-head, nine members, one collection node. These nodes are implemented through DEVS models. We used Fan et al.'s energy model for the sensor network [12]. Each cluster-head and members consumed 16.25 μJ per byte to transmit, 12.5 μJ per byte to receive, 15 μJ per byte to generate, and 75 μJ per MAC to verify. We also used Nam et al.'s energy model for the Comm-Arch [10]. Each collection-head consumed 19 μJ and 0.006 μJ per byte to compress and encrypt [21, 22]. The size of a report and key were 36 bytes and 8 bytes, respectively. The number of MACs is five to generate a report in a source cluster-head [17]. The base station was in the lower middle of the sensor field. We randomly generated the false positive and negative attacks in two clusters. Compromised nodes generate attacks according to a 10 percent false traffic ratio. In the simulation experiment, we randomly made 300 events. There was no packet loss in the experiment.

Figure 7 shows dropped attack count versus two types of the false positive attack and the false negative attack. Both the existing and the proposed methods have the same number of successful attacks from the compromised nodes because they can immediately detect them through their CAA. That is, both methods immediately identified the compromised nodes through the CAA after two attacks are generated. Therefore, the proposed method maintains the same security strength compared to the existing method.

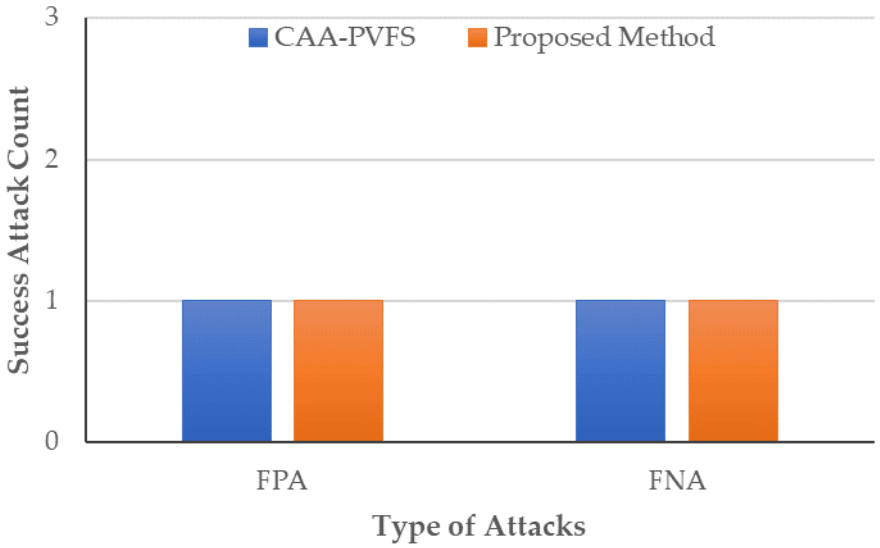

Figure 7. Dropped attack count versus two types of the attacks.

Figure 8 illustrates the energy consumption of the sensor network and the Comm-Arch versus the hop count. Overall, the proposed method consumes less energy in the entire hop counts as compared to the existing method. The hop count means the number of hops away from the base station. The proposed method consumed 18 percentage less energy between 1 and 5 hops compare to the existing method. Therefore, the proposed method consumes less unnecessary energy in these hops close to the base station.

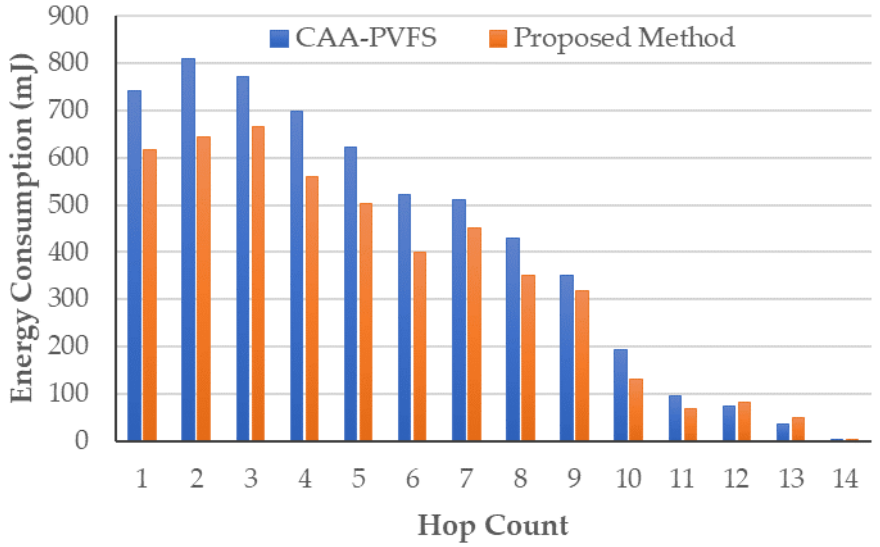

Figure 8. Energy consumption versus hop count.

Figure 9 shows the energy consumption of the entire network of the existing and the proposed methods. In the entire network (i.e., WSN, Comm-Arch), the proposed method consumed 4843.24 mJ and the existing method consumed 586.47 mJ. Thus, the proposed method saves about 17 percentage of energy compared to the existing method.

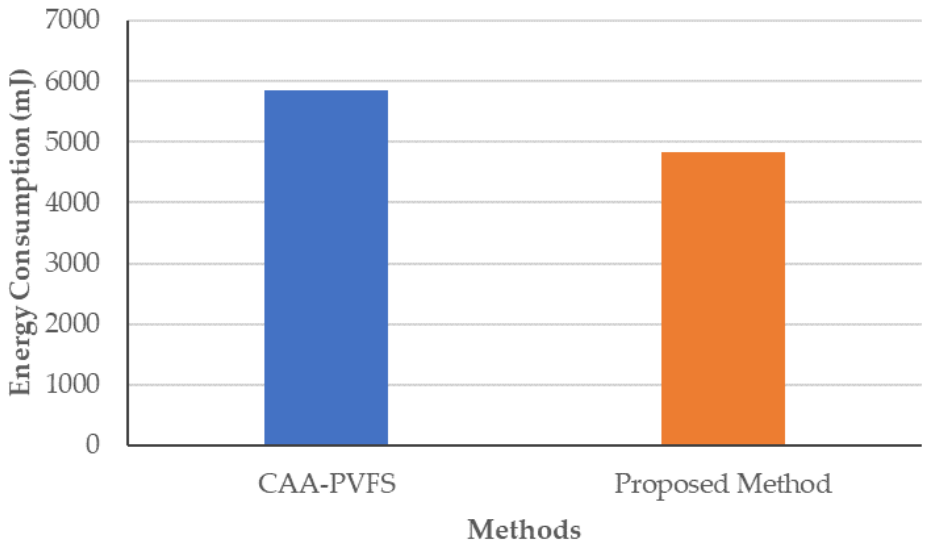

Figure 9. Energy Consumption versus methods.

5. RELATED WORKS

Several en-route filtering methods have been proposed to deal with false positive and negative attacks. In the PVFS [20], the first such technique, a CH and MBs in a cluster generate a report with their MACs. These MACs are randomly selected for attaching the report in the CH. Intermediate CHs of the source CH verify the report based on the correctness of the MACs. When the verification result at an intermediate CH is normal, the report is transmitted to the next CH. The PVFS is able to simultaneously detect both the false positive and the negative attacks with 80-90 percent probability within 10 hops. Akram *et al.* [23] presented a fuzzy adaptive selection of MACs in a report to improves the energy resource and the security level in the sensor network. This method can detect these two attacks within a short hop from the source CH. Lim *et al.* [24] proposed an automatic threshold reset scheme using a double fuzzy logic to achieve high en-route filtering probability. Nam *et al.* [25] provides proper security parameters using discrete event modeling and simulation in the PVFS-based sensor network.

Most of the existing en-route filtering methods for the two attacks focus on increasing false data by determining the effectiveness of the parameters of the PVFS. For example, Akram *et al.*'s method uses fuzzy logic to select the number of MACs of a report for improving the security strength. On the other hand, our proposed method provides geofencing of compromised nodes after detecting them through context awareness of the WSN rather than probability detection of false data.

6. CONCLUSIONS AND FUTURE WORKS

Wireless sensor networks have the disadvantage of being vulnerable to security due to the use of wireless communication and resource constraints of sensor nodes. Adversaries exploit certain limitations of these nodes to capture them. The compromised nodes result in unnecessary resource consumption and transmission interruptions through false positive and false negative attacks. In this paper, the proposed method configures geofencing for the compromised nodes in a sensor network and uses the blacklist of the collection nodes in a Comm-Arch. As a result, our

proposed method saved 17 percentage energy while maintaining the security strength of the entire network compared to the existing method. Our proposed method is unable to detect network layer attacks such as wormhole, sinkhole, sybil, etc. In future work, various types of attacks will be considered to increase the effectiveness of the proposed method. Recently proposed countermeasures will be adapted in the CAA in order to further improve energy efficiency and network security.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Akkaya, K. & Younis, M., (2005) "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks,* Vol. 3, No. 3, pp. 325-349.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E., (2002) "Wireless sensor networks: a survey," *Computer Networks,* Vol. 38, pp. 393–422.

[3] Singh, S. K., Singh, M. P., & Singh, D. K., (2010) "Routing Protocols in Wireless Sensor Networks - A Survey," *International Journal of Computer Science & Engineering Survey,* Vol. 1, No. 2, pp. 63-83.

[4] Akram, M. & Cho, T. H., (2016) "Energy efficient fuzzy adaptive selection of verification nodes in wireless sensor networks," *Ad Hoc Networks,* Vol. 47, pp. 16-25.

[5] Shahzad, M. K. & Cho, T. H., (2015) "Extending the network lifetime by pre-deterministic key distribution in CCEF in wireless sensor networks," *Wireless Networks,* Vol. 21, No. 8, pp. 2799-2809.

[6] Inc., M. "MICAz datasheet." http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf (accessed Oct. 1, 2017).

[7] Kim, J. M. & Cho, T. H., (2008) "A*-based key tree structure generation for group key management in wireless sensor networks," *Computer Communications,* Vol. 31, No. 10, pp. 2414-2419.

[8] Moon, S. Y. & Cho, T. H., (2014) "A routing path construction method for key dissemination messages in sensor networks," *ScientificWorldJournal,* Vol. 2014, p. 185156.

[9] Moon, S. Y. & Cho, T. H., (2012) "Key Index-Based Routing for Filtering False Event Reports in Wireless Sensor Networks," *IEICE Transactions on Communications,* Vol. E95.B, No. 9, pp. 2807-2814.

[10] Nam, S. M. & Cho, T. H., (2017) "Context-Aware Architecture for Probabilistic Voting-based Filtering Scheme in Sensor Networks," *IEEE Transactions on Mobile Computing,* Vol. 16, No. 10, pp. 2751-2763.

[11] Nam, S. M. & Kim, H.-J., (2021) "WSN-SES/MB: System Entity Structure and Model Base Framework for Large-Scale Wireless Sensor Networks," *Sensors,* Vol. 21, No. 2, p. 430.

[12] Fan, Y., Luo, H., Songwu, L., & Lixia, Z., (2005) "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications,* Vol. 23, No. 4, pp. 839-850.

[13] Nam, S. M. & Cho, T. H., (2015) "A fuzzy rule-based path configuration method for LEAP in sensor networks," *Ad Hoc Networks,* Vol. 31, pp. 63-79.

[14] Nam, S. M. & Cho, T. H., (2020) "Discrete event simulation–based energy efficient path determination scheme for probabilistic voting–based filtering scheme in sensor networks," *International Journal of Distributed Sensor Networks,* Vol. 16, No. 8.

[15] Kim, J. M., Han, Y. S., Lee, H. Y., & Cho, T. H., (2011) "Path renewal method in filtering based wireless sensor networks," *Sensors (Basel),* Vol. 11, No. 2, pp. 1396-404.

[16] Kim, J. M. & Lee, H. Y., (2020) "Node Density Loss Resilient Report Generation Method for the Statistical Filtering Based Sensor Networks," *IEICE Transactions on Information and Systems,* Vol. E103.D, No. 9, pp. 2007-2010.

[17] Li, F. & Wu, J., "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks," in *IWCMC '06: Proceedings of the 2006 international conference on Wireless communications and mobile computing*, 2016, pp. 27–32.

[18] Lee, H. Y. & Cho, T. H., (2011) "Optimized Fuzzy Adaptive Filtering for Ubiquitous Sensor Networks," *IEICE Transactions on Communications*, Vol. E94-B, No. 6, pp. 1648-1656.
[19] Lee, H. Y. & Cho, T. H., (2010) "A Scheme for Adaptively Countering Application Layer Security Attacks in Wireless Sensor Networks," *IEICE Transactions on Communications*, Vol. E93-B, No. 7, pp. 1881-1889.
[20] Li, F. & Wu, J., (2008) "PVFS: a probabilistic voting-based filtering scheme in wireless sensor networks," *International Journal of Security and Networks*, Vol. 3, No. 3, pp. 173-182.
[21] Ottoy, G., Hamelinckx, T., Preneel, B., De Strycker, L., & Goemaere, J.-P., "AES data encryption in a ZigBee network: Software or hardware?," in *International Conference on Security and Privacy in Mobile Information and Communication Systems*, 2010: Springer, pp. 163-173.
[22] Chen, F., Chandrakasan, A. P., & Stojanovic, V. M., (2012) "Design and Analysis of a Hardware-Efficient Compressed Sensing Architecture for Data Compression in Wireless Sensors," *IEEE Journal of Solid-State Circuits*, Vol. 47, No. 3, pp. 744-756.
[23] Akram, M. & Cho, T. H., "Fuzzy Adaptive Selection of Votes in Probabilistic Filtering Scheme in WSNs."
[24] Lim, S.-h. & Cho, T.-h., (2017) "Automatic Threshold Reset Scheme using a Double Fuzzy System for Improvement of Detection Rate in a Probabilistic Voting-based Filtering Scheme of WSNs," *International Journal of Computer Applications*, Vol. 176, No. 1, pp. 38-43.
[25] Nam, S. M. & Cho, T. H., "Discrete Event Modeling and Simulation of Probabilistic Voting-based Filtering to Find Proper Security Parameters in Wireless Sensor Networks," *International Journal of Computer Applications*, Vol. 975, p. 8887.

AUTHORS

Su Man Nam received the B.S. degree in Computer Information from Hanseo University, Korea, and M.S. and Ph.D. degree in Electrical and Computer Engineering from Sungkyunkwan University, Korea, in 2013 and 2017 respectively. Dr. Nam joined a researcher in the Department of Biomedical Informatics, Ajou University, Suwon, Korea, in 2018. He is currently a senior researcher in DuDu IT, Ltd., Seoul, Korea. He is interested in digital twin, modeling and simulation, WSN, and IoT.

Youn Kyoung Seo received the B.S. and M.S. degree in Computer Engineering from Kyungpook National University, Korea, in 2000 and 2002 respectively. She is currently in Ph.D. degree in Computer Engineering at Inha University, Korea and is currently a professor in Computer Information at Incheon Jae Neung University, Korea. She joined a senior researcher at Biomedical Knowledge Engineering Laboratory at Seoul National University, Korea, in 2009. She is interested in machine learning, deep learning and IoT.