BLACKLIST MANAGEMENT USING A VERIFICATION REPORT TO IMPROVE THE ENERGY EFFICIENCY OF CFFS IN WSNS

JungSub Ahn[1] and TaeHo Cho[2]

[1&2] Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea

ABSTRACT

Recently, the applications scope of Wireless Sensor Networks (WSNs) has been broadened. WSN communication security is important because sensor nodes are vulnerable to various security attacks when deployed in an open environment. An adversary could exploit this vulnerability to inject false reports into the network. En-route filtering techniques have been researched to block false reports. The CFFS scheme filters the false report by collaboratively validating the report by clustering the nodes. However, CFFS is not considered effective against repetitive attacks. Repeated attacks have a significant impact on network lifetime. In this paper, we propose a method to detect repetitive attacks with cluster-based false data filtering and to identify the compromised nodes and quickly block them. The proposed scheme uses fuzzy logic to determine the distribution of additional keys according to the network conditions, thereby improving energy efficiency.

KEYWORDS

WSN Security, Fabricated Report Verification, WSN Lifetime Extension, Enhanced CFFS

1. INTRODUCTION

A wireless sensor network (WSN) is composed of low-cost sensor nodes. WSNs detect external environmental changes and communicate the event contents to the base station (BS) through cooperative communication between the nodes [1-3]. The BS provides information to the user through an external network such as the internet. WSNs are widely used for applications in the military, transportation, healthcare and disaster preparation sectors. The sensor node consists of a sensor for sensing, an analog to digital converters (ADCs) for converting physically sensed data into a digital signal, a microcontroller for data processing, memory for driving a TinyOS, a radio transceiver for data transmission and reception, and a battery as a power supply [4-5]. There are two ways to deploy nodes: direct deployment and deployment from an airplane [6]. When the node is deployed, the battery cannot be charged or replaced [7]. Therefore, sensor nodes can be defective due to battery depletion, environmental impact, hardware or software malfunction, and malicious attacks [8-9].

An adversary can compromise the node and capture important information such as key information of the node. These threats make them vulnerable to various security attacks such as false report insertion attacks and denial of service attacks.

DOI: 10.5121/ijwmn.2018.10404

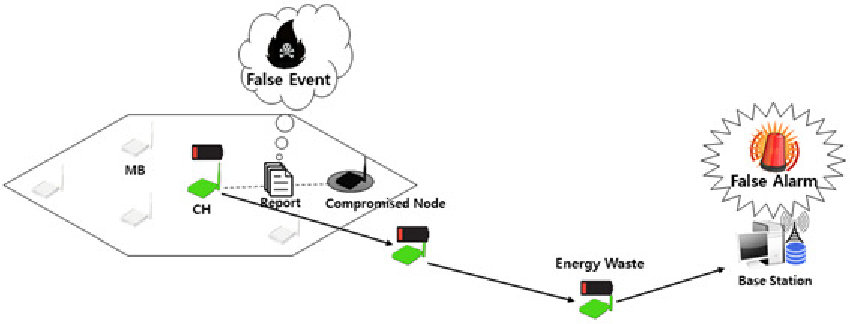


Figure 1. False Report Injection Attack

Figure 1 represents a false report injection attack. A false report injection attack occurs when an adversary generates a modulated event and injects a false report into the network [10-11]. Such an attack causes unnecessary energy consumption between nodes and a false alarm at the BS. Specifically, false alarms cause unnecessary additional response efforts. The sensor node has the greatest energy consumption for transmission and reception. Therefore, it is important to reduce the early detection of false reports to prolong the network lifetime. Many schemes have been proposed by applying an en-route filtering technique to defend against false report injection attacks [12-15]. A cluster-based false data filtering scheme (CFFS) occurs when the nodes are grouped into clusters of a tree structure and the report is filtered through the message authentication code (MAC) of the report [16]. This scheme has a high false report detection ratio but does not consider constantly generated data attacks. If an adversary continually injects false reports, the node consumes energy rapidly until the filtered node is identified. As a result, if the node is depleted of energy, the network becomes disabled.

In this paper, we propose a method to block compromised nodes using information on cluster characteristics and false reports in CFFS. This scheme is to defend against unnecessary energy consumption caused by continuous injection attacks. In Section 2 of this paper, we discuss cluster-based false data filtering and Section 3 explains the proposed method. Section 4 describes the experimental results. Finally, Section 5 presents conclusions and future research.

2. RELATED WORK

This session introduces the CFFS, which is the basis of the proposed scheme, to prevent false report attacks.

2.1. CFFS

Zhixiong et al. proposed a cluster-based False Data Filtering Scheme (CFFS) for early filtering of false reports [16]. CFFS is composed of nodes as clusters, which reduce the communication cost and improve network scalability and error detection accuracy. This structure is particularly useful for prolonging network life. CFFS consists of five steps: the pre-deployment phase, key distribution phase, report generation phase, report filtering phase, and BS verification phase. In CFFS, a cluster head node calculates its own burden value and allocates different numbers of keys to all upstream nodes by using the burden value in the key distribution step. If the member node senses an event, as shown in Figure 2(b), it generates a MAC using its own key and transmits it to the cluster head node. The cluster head node generates the report using the collected MAC. The generated report is transmitted to the BS.

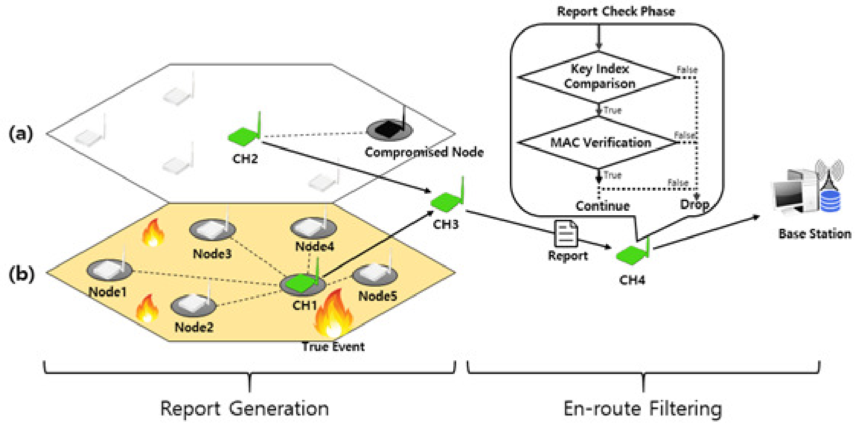


Figure 2. CFFS Overview

The verification process of the intermediate node is as follows.

1. If there are less than t $\{S_v, M_v\}$ tuples in R, CH_i drops R;
2. If the t node IDs $\{S_v, 1 \le v \le t\}$ does not belong to the same cluster, CH_j drops R;
3. If CH_i has one key $K \in \{K_v, 1 \le v \le t\}$, it re-computes $M = K(e)$ and checks whether the corresponding M_v is the same as M. It drops R if they are not the same.
4. If an in-cluster node S_u has one key $K \in \{K_v, 1 \le v \le t\}$, CH_j sends (e, S_v, M_v) to S_u. S_u verifies M_v as in step 3 and sends the result to CH_i.
5. If CH_i receives more than one failed verification results from in-cluster nodes during a time period η, it drops R.
6. Otherwise, CH_j sends R to its upstream node.

Figure 3. En-route Filtering Process

Figure 2 shows the report transmission process in CFFS. An adversary can compromise nodes and inject a false report as shown in Figure 2(a). However, false reports are filtered through report validation. If the node receives the report, the node conforms to verify that the included Key Index has been stored in the report. If the node has the same key index, the MAC verification process is performed, as shown in Figure 3. Finally, if the BS collects the report, the procedure is performed as shown in Figure 4.

1. If there are less than t $\{S_v, M_v\}$ tuples in R, the sink rejects R;
2. If t node IDs $\{S_v, 1 \le v \le t\}$ does not belong to the same cluster, the sink rejects R;
3. For every key $K \in \{K_v, 1 \le v \le t\}$, the sink computes $M = K(e)$ and checks whether the corresponding M_v is the same as M. If there is a mismatch, R is rejected. Only those with MACs that are all correct are accepted.

Figure 4. BS Filtering Process

3. PROPOSED METHOD

In this session, we describe the proposed scheme in detail. The overview in 3.1 represents the proposed scheme overview and 3.2 describes the assumptions for implementing the proposed method. In Section 3.3, we introduce the proposed method in detail.

3.1. Overview

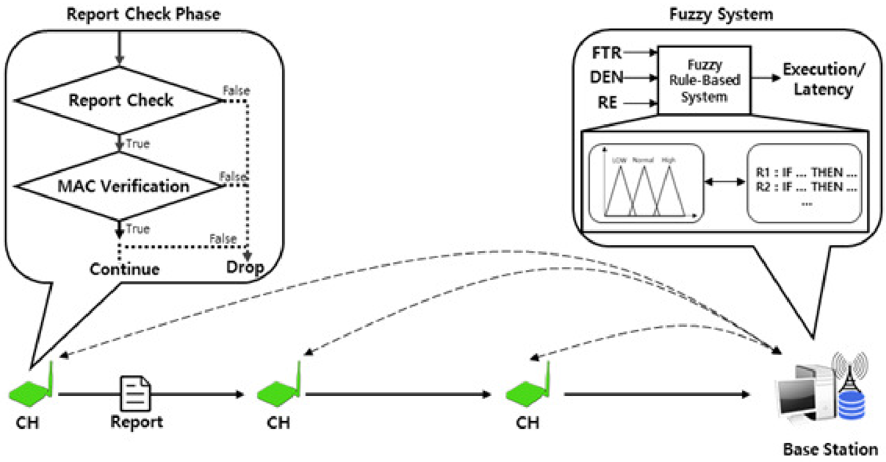


Figure 5. Proposed Scheme Overview

If the nodes beyond the security threshold are not compromised, false reports are filtered by intermediate node filtering or BS filtering in the CFFS scheme. In our method, when the report is dropped during the intermediate filtering process, as shown in Figure 5, the CH node extracts information about the report. The extracted information is transmitted to the BS and utilized in the fuzzy system function. The BS generates the node-blocked message and transmits it to the downstream node according to the result of the fuzzy system. When an intermediate node receives the message, it stores it in the memory. This information is used in the en-route filtering process to perform early filtering.

3.2. Assumption

The sensor nodes are deployed randomly and densely. The base station knows all the information including the key and location information of the nodes. It is assumed that the step of establishing routing is not attacked. The routing path is set using directed diffusion and GPSR [17-18]. All generated reports are forwarded to the BS according to the routing path. We assume that a false report occurs randomly among the compromised nodes.

3.3. Proposed Scheme

This section describes details of the proposed scheme. In Section 3.3.1, the detailed operation procedure of the proposed method will be described. In Section 3.3.2, the fuzzy logic applied to the proposed system will be introduced.

3.3.1. Detailed Procedure

An adversary can arbitrarily generate a MAC using the security information of the node. After compromising the node, the CH node generates a false report using false MAC and forwards the report to the upstream node. The intermediate node verifies reports using the MAC. If a false report is detected, a node can extract to know the report source identification. Also, the verification node encrypts the verification report including information on the compromised source node with its own key and transmits it to the BS. The BS receiving the report can decode the verification report using the global key pool. Also, the BS requests the cluster environment information using the data-centric routing information of the compromised node and operates the fuzzy logic system based on this information.

The fuzzy function input uses the False Traffic Ratio (FTR), Density (Number of Members), and residual energy of the node. The fuzzy system determines whether to block the compromised node based on these three factors. Fuzzy logic systems use If-Then rules. If the fuzzy system output result is positive, the BS creates a node blocking report using the routing table and global key pool surrounding the nodes. The report transmitted from the BS to the compromised node is as follows.

$$R: (R\| E(CH_x(NODE_{ID}))| \ldots |E(CH_y(NODE_{ID})))$$

CH_x indicates the key of the closest node starting from the BS, and CH_y indicates the key of the cluster head node with the compromised node. The nodes on the routing path to the destination decode the report with their keys when receiving the report and store the ID of the node to be added to the blacklist. Afterward, the report is transmitted downstream.

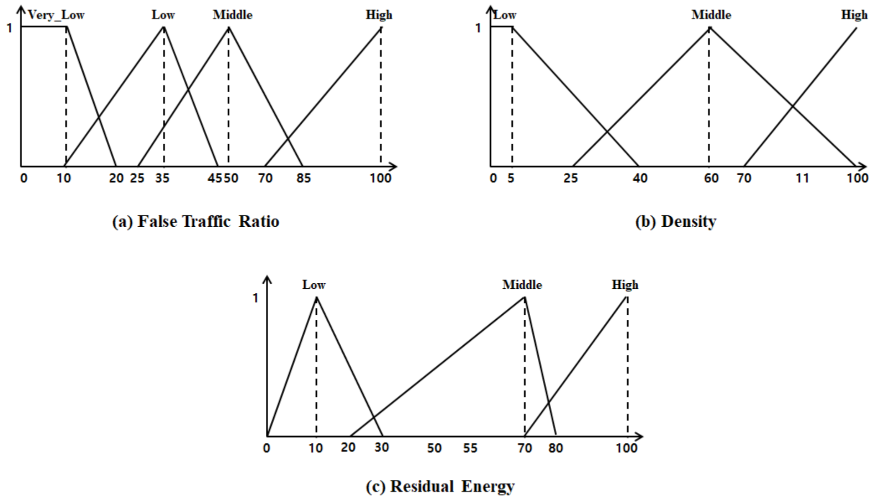
Upon reaching the destination CH, the CH adds the source ID to the blacklist and ignores the MAC that is transmitted later. As a result, even if an adversary continually injects a false report, it is filtered within the cluster to which it belongs.

3.3.2. Fuzzy Logic

Fuzzy logic is a logic concept that expresses itself multi-dimensionally when the state is unclear [19]. Fuzzy logic is a rule-based method that expresses imprecision by generating specific rules. Fuzzy logic is flexible enough to allow for inaccurate information. In addition, any complex nonlinear system can be modeled.

- False Traffic Ratio (FTR) = { Very_Low (VL), Low (L) , Mid (M), High (H) }
- Density (DE) = { Low (L) , Mid (M), High (H) }
- Residual Energy (RE) = { Low (L) , Mid (M), High (H) }
- Additional Key Distribution (AKD) = { ON, OFF }

3.3.3. Fuzzy Membership Function



(a) False Traffic Ratio

(b) Density

(c) Residual Energy

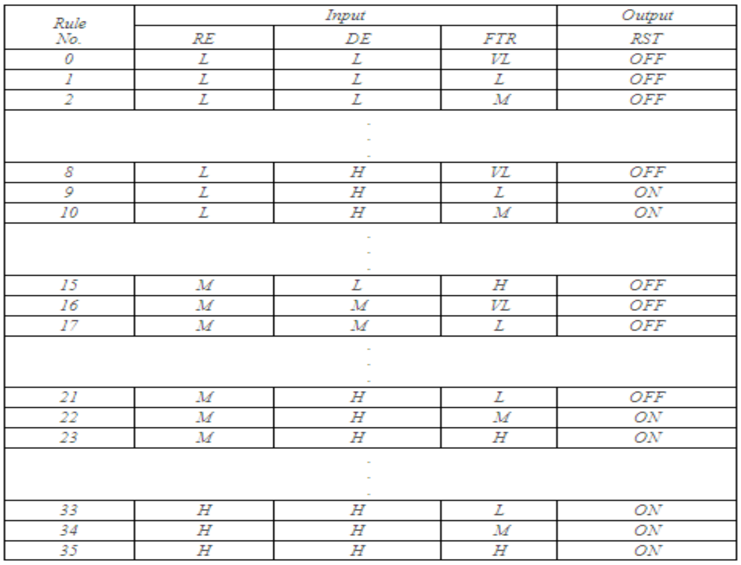
Figure 6. Fuzzy Membership Function

(a) False Traffic Ratio: The false traffic ratio represents the corrupt ratio reports in a WSN. It is calculated using normal reports and the false report capture ratio.

(b) Density: Density is calculated by the number of member nodes that belong to a cluster. The BS determines the density through the tree configuration phase after all the nodes have been distributed. Density is required to compare against the security threshold and determine the key distribution.

(c) Residual Energy: The residual energy refers to the remaining energy of the node. The BS can request residual energy information from the node with a query-driven method. Residual energy is represented as a percentage and is used to extend the life of the node.

Table 1. Fuzzy if-then rules for additional key distribution



Rule No.	*Input*			*Output*
	RE	*DE*	*FTR*	*RST*
0	*L*	*L*	*VL*	*OFF*
1	*L*	*L*	*L*	*OFF*
2	*L*	*L*	*M*	*OFF*
		⋮		
8	*L*	*H*	*VL*	*OFF*
9	*L*	*H*	*L*	*ON*
10	*L*	*H*	*M*	*ON*
		⋮		
15	*M*	*L*	*H*	*OFF*
16	*M*	*M*	*VL*	*OFF*
17	*M*	*M*	*L*	*OFF*
		⋮		
21	*M*	*H*	*L*	*OFF*
22	*M*	*H*	*M*	*ON*
23	*M*	*H*	*H*	*ON*
		⋮		
33	*H*	*H*	*L*	*ON*
34	*H*	*H*	*M*	*ON*
35	*H*	*H*	*H*	*ON*

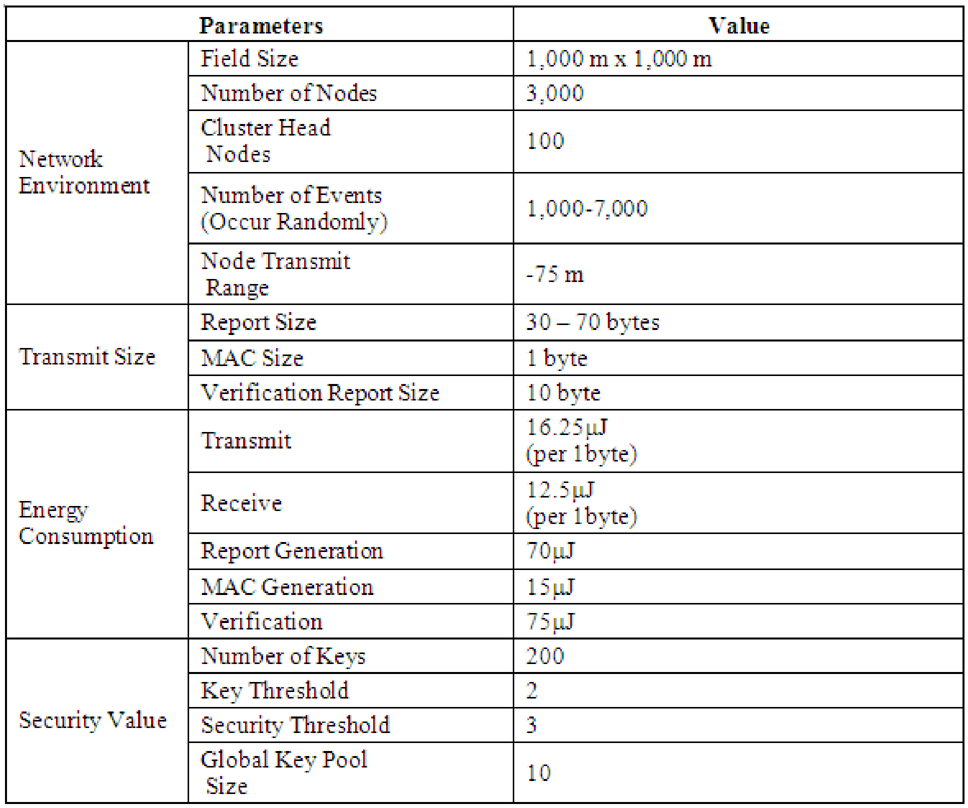
Table 1 represents part of the established 36 if-then rules for key distribution decisions. The fuzzy system uses the Mamdani-type inference method and the center-of-gravity method for defuzzification [20-21]. The proposed fuzzy system does not cause additional key distribution about the compromised nodes if the density is low even though the remaining energy is low or the FTR is high. If the density is below the CFFS security threshold value, there is a critical problem because the cluster is inactivated. Therefore, we constructed rules for maintaining the cluster communication so that nodes are not blocked until the DE input reaches M value. Also, when the remaining energy is low, the attacker can quickly deactivate the cluster with repetitive attacks. In this case, the node is blocked depending on the FTR regardless of the density.

4. PERFORMANCE EVALUATION

In this section, we introduce the experiment parameter and evaluate the energy performance of the existing method of CFFS and the proposed scheme.

4.1. Experimental Environment

Table 2. Experiment parameters



Parameters		Value
Network Environment	Field Size	1,000 m x 1,000 m
	Number of Nodes	3,000
	Cluster Head Nodes	100
	Number of Events (Occur Randomly)	1,000-7,000
	Node Transmit Range	-75 m
Transmit Size	Report Size	30 – 70 bytes
	MAC Size	1 byte
	Verification Report Size	10 byte
Energy Consumption	Transmit	16.25μJ (per 1byte)
	Receive	12.5μJ (per 1byte)
	Report Generation	70μJ
	MAC Generation	15μJ
	Verification	75μJ
Security Value	Number of Keys	200
	Key Threshold	2
	Security Threshold	3
	Global Key Pool Size	10

The experiment parameters constructed the node parameters based on the Mica2 node [22]. Our experiment network field size is 1000 x 1000 m^2. A total of 3000 nodes are arranged randomly and 100 of them are composed of CH nodes. The number of partitions is 10 and the key is 200. The energy required to transmit is 16.25 μJ per one byte and the energy required to receive is 12.5 μJ per one byte. The energy required to verify a MAC is 75 μJ [23]. In addition, report size is 30-70 bytes and a MAC size is one byte. Events occur at random locations and false report injection attacks occur at nodes that are randomly corrupted according to FTR. Packet loss does not occur during communication in the experiment. The total number of events is 1,000-7,000.

4.2. Experiment Result

We analyzed energy consumption according to the attack ratio, the number of reports and the report size of the network. The BS does not consider computed power dissipation for the fuzzy system because the resource is not finite, unlike the node. The residual energy of the input value of the fuzzy node is set at random because we implemented a virtual network situation.

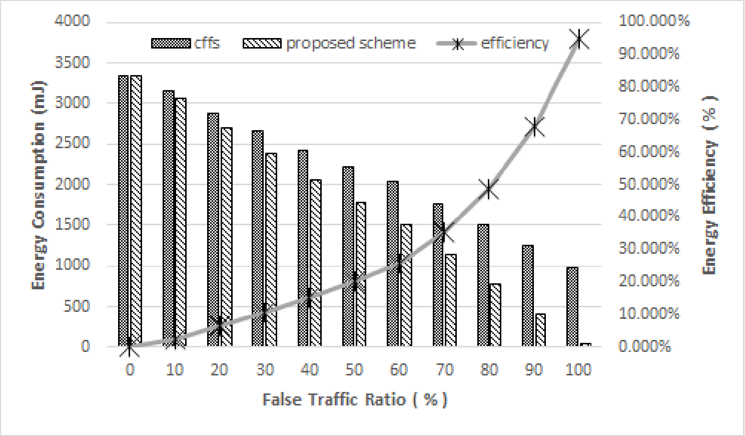


Figure 7. Energy consumption versus the FTR and energy efficiency improvement ratio

Figure 7 shows the energy consumption of the network versus FTR when 1000 events occur. The energy efficiency increases up to 95.01% as the attack ratio increases. When the attack ratio increases, the false report is filtered one hop from the compromised node through blacklist verification. Our proposed method shows an energy improvement rate of 29.771% on CFFS.

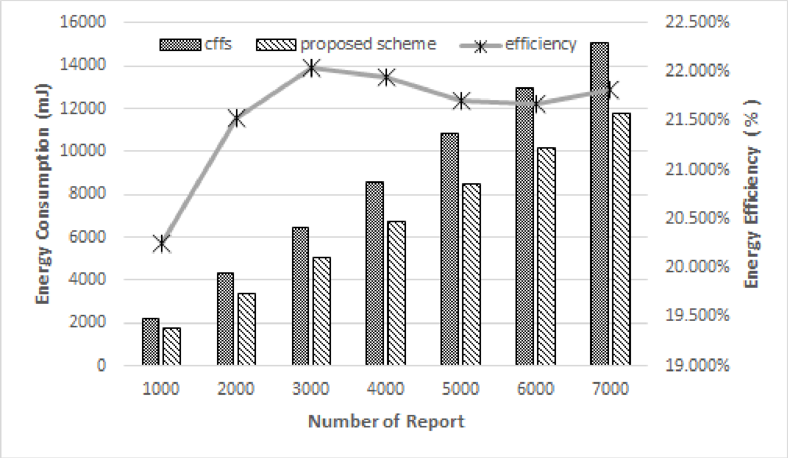


Figure 8. Energy consumption versus the number of reports and energy efficiency improvement ratio

Figure 8 shows the analysis of the energy consumption according to the number of reports. From the above results, we can confirm that the proposed scheme has an average energy improvement of 21.567% when the attack rate is 50% more than CFFS.

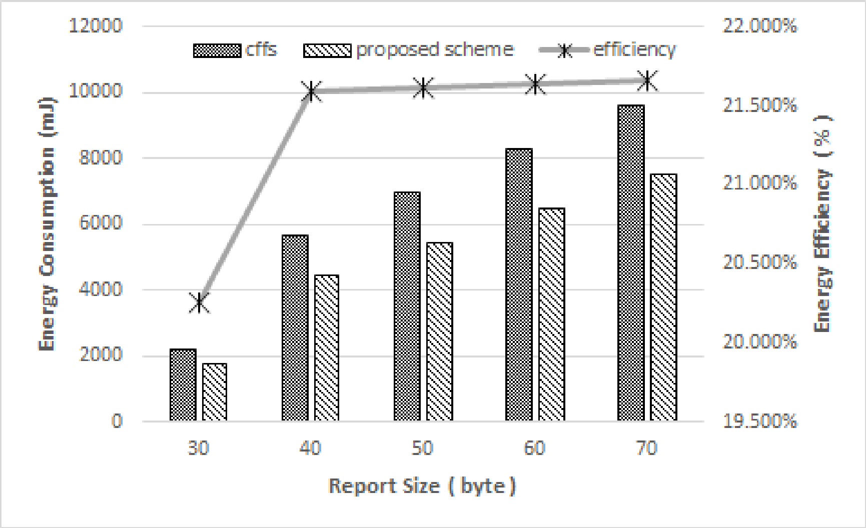


Figure 9. Energy consumption versus the report size and energy efficiency improvement ratio

Figure 9 shows the energy consumption versus the report size. This experiment includes a total of 2000 event reports with an average energy efficiency improved by 21.352% compared with CFFS.

In a CFFS with a tree structure, upstream nodes have more load factors than downstream nodes. The proposed scheme can reduce the load factor of BS neighbors significantly by providing fast filtering. As a result, the proposed scheme can prove that the network lifetime is prolonged by distributing the additional key distribution via the fuzzy rules.

5. CONCLUSIONS

Sensor nodes are vulnerable to attack by an adversary because they are deployed in an open environment. An adversary can use a compromised node to perform a false report injection attack. To prevent this problem, the CFFS scheme is proposed in a WSN security protocol. However, the CFFS scheme does not consider repetitive attacks that involve false report filtering. We proposed a method of determining additional key distributions using fuzzy logic to improve the energy efficiency in CFFS. The environmental information for the WSN is input to determine if the key is redistributed in the fuzzy logic system. We also demonstrated the effectiveness of the proposed method through experimental results. Future work will be carried out to reduce the transmission and reception energy by performing fuzzy logic in the cluster unit of the CFFS.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2015R1D1A1A01059484)

REFERENCES

[1] Akyildiz, Ian F., et al. "A survey on sensor networks." IEEE communications magazine 40.8 (2002): 102-114.

[2] Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

[3] Akkaya, Kemal, and Mohamed Younis. "A survey on routing protocols for wireless sensor networks." Ad hoc networks 3.3 (2005): 325-349.

[4] Levis, Philip, et al. "TinyOS: An operating system for sensor networks." Ambient intelligence. Springer, Berlin, Heidelberg, 2005. 115-148.

[5] Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." Computer networks 38.4 (2002): 393-422.

[6] Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." IEEE wireless communications 11.6 (2004): 6-28.

[7] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on. IEEE, 2003.

[8] Kavitha, T., and D. Sridharan. "Security vulnerabilities in wireless sensor networks: A survey." Journal of information Assurance and Security 5.1 (2010): 31-44.

[9] Mohammadi, Shahriar, and Hossein Jadidoleslamy. "A comparison of physical attacks on wireless sensor networks." International Journal of Peer to Peer Networks 2.2 (2011): 24-42.

[10] Ahn, Jung-Sub, and Tae-Ho Cho. "PREVENTION METHOD OF FALSE REPORT GENERATION IN CLUSTER HEADS FOR DYNAMIC EN-ROUTE FILTERING OF WIRELESS SENSOR NETWORKS."

[11] Kumar, Alok, and Alwyn Roshan Pais. "En-route filtering techniques in wireless sensor networks: a survey." Wireless Personal Communications 96.1 (2017): 697-739.

[12] Ye, Fan, et al. "Statistical en-route filtering of injected false data in sensor networks." IEEE Journal on Selected Areas in Communications 23.4 (2005): 839-850.

[13] Yu, Zhen, and Yong Guan. "A dynamic en-route scheme for filtering false data injection in wireless sensor networks." Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM, 2005.

[14] Li, Feng, and Jie Wu. "A probabilistic voting-based filtering scheme in wireless sensor networks." Proceedings of the 2006 international conference on Wireless communications and mobile computing. ACM, 2006.

[15] Zhu, Sencun, et al. "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks." Security and privacy, 2004. Proceedings. 2004 IEEE symposium on. IEEE, 2004.

[16] Liu, Zhixiong, et al. "A Cluster-Based False Data Filtering Scheme in Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 23 (2014).

[17] Intanagonwiwat, Chalermek, Ramesh Govindan, and Deborah Estrin. "Directed diffusion: A scalable and robust communication paradigm for sensor networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.

[18] Karp, Brad, and Hsiang-Tsung Kung. "GPSR: Greedy perimeter stateless routing for wireless networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.

[19] Yen, John, and Reza Langari. Fuzzy logic: intelligence, control, and information. Vol. 1. Upper Saddle River, NJ: Prentice Hall, 1999.

[20] Babuška, Robert. Fuzzy systems, modeling and identification. Technical Report, 1997.

[21] Mamdani, Ebrahim H. "Application of fuzzy algorithms for control of simple dynamic plant." Proceedings of the institution of electrical engineers. Vol. 121. No. 12. IET, 1974.

[22] https://www.eol.ucar.edu/isf/facilities/isa/internal/CrossBow/DataSheets/mica2.pdf

[23] Nam, Su Man, and Tae Ho Cho. "Context-aware architecture for probabilistic voting-based filtering scheme in sensor networks." IEEE Transactions on Mobile Computing 16.10 (2017): 2751-2763.

Authors

Jung Sub Ahn received the B.S. degree in computer engineering from Kyunil University in 2016 and now doing Ph.D. degree in Department of Electrical and Computer Engineering from Sungkyunkwan University. His research interests include wireless sensor network security, modelling & simulation, IoT security

Tea Ho Cho received a Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical and Computer Engineering from Sungkyunkwan University, Repulic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Software at Sungkyunkwan University, Korea.