I.J. Information Technology and Computer Science, **2017, 4, 1-8**
Published Online April 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2017.04.01

A Fuzzy Rule-based Key Re-Distribution Decision Scheme of Dynamic Filtering for Energy Saving in Wireless Sensor Networks

Dongjin Park[1]
College of Software, Sungkyunkwan University, Suwon, 16419, Republic of Korea
E-mail: jin1307e@skku.edu

***Taeho Cho**[2]
College of Software, Sungkyunkwan University, Suwon, 16419, Republic of Korea
E-mail: thcho@skku.edu

***Abstract*—**A wireless sensor network's sensor nodes have scarce resources, are exposed to the open environment, and use wireless communication. These features make the network vulnerable to physical capture and security attacks, therefore adversaries attempt various attacks such as false report injection attacks. A false report injection attack generates a false alarm by forwarding a false report to the base station. It confuses a user and lowers the reliability of the system. In addition, it leads to depletion of the node energy in the process of delivering a false report. A dynamic en-route filtering scheme performs detection in the data transfer process, but it incurs unnecessary energy loss in a continuous attack situation. In this paper, in order to solve this problem, a scheme is proposed for determining whether or not to redistribute keys at execution. The proposed scheme saves energy by detecting false reports at an earlier hop than the existing scheme by using fuzzy logic and the feature of a loaded secret key of each node in the key pre-distribution phase. Furthermore, it improves the detection performance with an appropriate re-distribution of the key. Experimental results show up to 52.33% energy savings and an improved detection performance of up to 18.57% compared to the existing scheme.

***Index Terms*—**Wireless sensor network, False report injection attack, Dynamic en-route filtering scheme, Fuzzy logic system.

I. Introduction

Wireless sensor networks (WSNs) have been actively used in various applications that require real-time monitoring, such as enemy detection/identifying movement paths on a battlefield, pollution measurement, building security and fire monitoring [1-5]. In these applications, because accurate measurements are required along with safe collection and transmission, security is an essential detail. WSNs consist of numerous small sensor nodes for detecting an event, and a base station (BS) for collecting the detected event data and sending it to a user. The sensor node of a low-cost product has resource constraints such as processing power, memory capacity, and energy, and it also communicates wirelessly in an open environment [6]. Therefore the node is easily exposed to various attacks such as environmental damage as well as physical capture or false report injection attacks from malicious attackers [7]. A false report injection attack causes a false alarm at the BS by randomly generating false reports by an attacker and it creates confusion for a user. Therefore, a false report must be detected as early as possible, and many schemes have been proposed for this purpose [8-11].

A dynamic en-route filtering (DEF) scheme was proposed by Yu and Guan [12]. This scheme can detect a false report in the transfer process using the authentication key and secret keys. DEF has three operation phases: key pre-distribution, key dissemination and report forwarding. In DEF, however, when a network is exposed to a continuous attack from adversaries, there is unnecessary energy loss. DEF has no suitable measures for this problem. Although it executes the key dissemination phase again due to the key being considered stolen [13], it still does not solve the problem that occurred before because the method does not consider the current attack situation. Accordingly, a proper key re-distribution scheme is needed, and it should be considered whether the scheme is running because the scheme also consumes additional energy.

In this paper, in order to reduce unnecessary energy consumption during a constant attack situation, we propose a decision scheme of the key re-distribution that detects a false report at the next node of a cluster in which an attack occurs (source) and considers the network situation information. The proposed scheme calculates a count when it detects a false report, and if the count number is more than a threshold then it delivers the information required for the key re-distribution to the BS. The BS uses the received information from a verified node as input values for fuzzy logic [14] and determines whether to execute the key re-distribution via the resultant value of the fuzzy logic. If the result is a flag for execution, the BS re-distributes authentication keys in

Copyright © 2017 MECS

order to detect a false report at an earlier hop node than the existing scheme, thus energy loss is reduced. Experimental results show that compared to the existing scheme, our scheme achieves energy savings of up to 52.33% and improves the detection performance by up to 18.57%.

The rest of this paper is organized as follows. We introduce related work in Section II and then present the problem statement of the existing scheme in Section III. In Section IV, the proposed scheme is provided and the performance evaluation is discussed in Section V. Finally, we summarize our conclusions and future work in Section VI.

II. Related Work

In this section, we describe the false report injection attack in Section A and introduce the existing DEF scheme in Section B.

A. False report injection attack

A false report injection attack is an attack that injects a false report into the network for the purpose of deceiving the BS and depleting the limited network energy. Fig. 1 shows an overview of the false report injection attacks through compromised nodes by an attacker in a WSN. The attacker obtains control by seizing several nodes distributed on the field and then creates and injects the false report (no real event) using the compromised nodes. The false report is delivered to the BS without being detected on the intermediate node along the normal routing path. The BS receiving the false report confirms the contents of the report and generates false alarms. This causes a disruption for appropriate measures responding to the report content, which results in a financial and time losses. In addition, the normal nodes on the forwarding path incur unnecessary energy losses via delivering the attacker's malicious false reports made through the compromised node. Due to the continual attack, the lifetime of the entire network is eventually reduced.

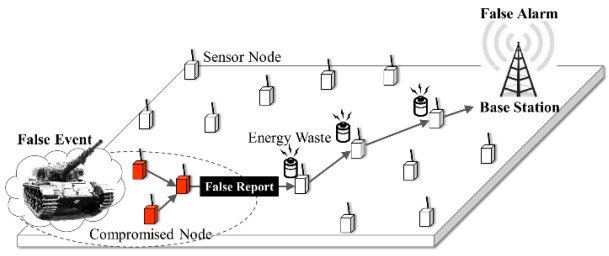

Fig.1. False report injection attack in WSN.

B. Dynamic en-route filtering

DEF is a scheme proposed by Yu and Guan to defend the false report injection attacks in cluster-based WSNs. A WSN-based cluster divides the distributed nodes into clusters and each cluster elects a cluster head (CH) as a representative node. The member nodes of the cluster send the event information to the cluster head.

In this scheme, each node is preloaded with an authentication key and secret keys at the BS and then each node is distributed on the field. After that, each CH collects the authentication keys from their member nodes and aggregates them into a message. This message is passed on to the next node along the routing path. The forwarding node that received the message additionally loads the authentication key in the memory from the message. This authentication key is used to determine if the event report is false or not. DEF has three operation phases, as shown in Fig. 2.

Fig.2. Three operation phases of DEF.

The key pre-distribution phase is executed only once at the BS when the sensor node is initially deployed to the field. Each node loads the other different seed keys and creates an authentication key using the common hash function from the seed key, and then configures the hash chain. At this time, if the node has sufficient memory, the node has all authentication keys generated. Otherwise, the authentication key is generated whenever needed. In addition, a node has $l+1$ secret keys. l keys are called the y-key and they are randomly chosen from a y-key pool of size v. The last key is called the z-key and it is randomly chosen from a z-key pool of size w. The z key is distinguishable from other nodes.

The key dissemination phase has a four-step procedure. First, each node in the cluster encrypts the current authentication key using one of the secret keys. The authentication key message structure of the node is shown in Equation (1).

$$\begin{aligned} Auth(v_i) = \{ & v_i,\ j_i,\ id\left(y_1^{v_i}\right),\ \left\{id\left(y_1^{v_i}\right),\ k_{j_i}^{v_i}\right\}_{y_1^{v_i}},\ \\ & \ldots, id\left(y_l^{v_i}\right),\ \left\{id\left(y_l^{v_i}\right),\ k_{j_i}^{v_i}\right\}_{y_l^{v_i}},\ \\ & id(z^{v_i}),\ \left\{id(z^{v_i}),\ k_{j_i}^{v_i}\right\}_{z^{v_i}} \} \end{aligned} \quad (1)$$

In (1), j_i is the index of the current authentication key, and $j_i = 1$ denotes the first dissemination. Additionally, $id\left(y_1^{v_i}\right)$ is the index of $y_1^{v_i}$ in the y-key pool and $\{*\}_{y_1^{v_i}}$ is encrypted using the key $y_1^{v_i}$. Then, the CH collects the authentication message from all nodes in the cluster that they belong to and aggregates them into message $K(n)$. $K(n)$ is shown in Equation (2). In (2), $v_1, \ldots, v_n$ are nodes in the cluster.

$$K(n) = \{\, Auth(v_1), \ldots, Auth(v_n)\} \quad (2)$$

Next, the CH selects q $(q > 1)$ forwarding nodes from neighbor nodes and forwards them to $K(n)$. The reason for selecting q is so that $K(n)$ can be delivered to another node without key re-dissemination of $K(n)$ when the next node is compromised. When a forwarding node receives

$K(n)$, the node performs the following steps.

1) It checks whether $K(n)$ has at least t distinct z-key indexes. If not, $K(n)$ is determined to be false and is dropped.
2) It checks the secret key indexes of $K(n)$. If it has the same key index, it decrypts the message and stores the authentication key in its own memory.
3) It drops $K(n)$ if $K(n)$ has already been forwarded by h_{max}. Each node repeats the above operation until $K(n)$ has been forwarded by h_{max} or $K(n)$ has reached the BS.

In the report forwarding phase, the sensor node detects an event, generates a message authentication code (MAC) about the event information using a new authentication key, and forwards the MAC to its CH. In the CH, the number of sensor nodes that participate in generating a report is pre-determined before deployment and the CH forwards the report to q neighbor nodes. When the next node sends an ok message that the report has been received correctly, the CH exposes the authentication key of the sensor nodes and verifies the report, and then informs the next hop node of the verified result. This operation is repeated until the report arrives at the BS or the report is detected as being false.

III. Problem Statement

This section describes background on the DEF and introduces improvements. DEF is an effective scheme for defending false report injection attacks in a dynamic environment but has several problems in terms of energy efficiency.

- DEF quickly detects a false report using keys distributed randomly. However, when DEF is exposed to a continuous attack situation, it causes unnecessary energy consumption from forwarding the non-existing report until the false report is detected.
- In DEF, the key dissemination phase for distributing the entire key again may be performed arbitrarily to reduce the energy loss due to continuous attacks; however, it is very important to determine when the phase executes because it consumes a lot of energy. Furthermore, even if the condition of the entire key distribution phase execution is matched (topology change) and the phase is actually executed, there may still be a loss of energy. The reason for this is that the phase is a scheme that it does not figure out and does not consider the attack situation.

To improve these problems, we propose the following improvements.

- In order to understand that there is a constant attack on the current network, the forwarding node counts the number of detected false reports corresponding to each source CH. If the count value exceeds the threshold value, the forwarding node requests the key re-distribution for the BS. After the key re-distribution, if a false report is generated using the same false key, unnecessary energy consumption is minimized by detecting this at the next-hop node.
- Because the entire key re-distribution consumes a lot of energy, it is executed locally by considering the state of the network. The proposed scheme considers three factors: the false traffic ratio (FTR) of the network, the remaining energy of the node, and the distance between the detection node and the source CH. When receiving the key re-distribution request message from the forwarding node, the BS determines a key re-distribution using fuzzy logic.

In this paper, we propose an energy-efficient key re-distribution scheme that considers the state of the network for early detection of false reports when exposed to constant attacks. Through this scheme, we expect to minimize unnecessary energy consumption associated with the existing scheme.

IV. Proposed Scheme

In this section, we present an overview of the proposed scheme in Section A, mention assumptions for the proposed scheme in Section B and explain the proposed scheme in detail in Section C.

A. Overview

DEF has the property that there is no change in the secret key loaded in the key pre-distribution phase. Using this property, the proposed scheme modified the report forwarding phase of DEF and added the key re-distribution phase. Fig. 3 shows the operation procedure of this proposed scheme. When the false report count value is less than the threshold, proposed scheme operates in the same manner as DEF at the report forwarding phase. When the forwarding node that received the report determines the presence or absence of the false report at the report forwarding phase, Fig. 3(a) shows that if the report is detected as false, then the forwarding node identifies a source CH and increases the false report count value. Following this, the behavior is the same as the existing DEF. Fig. 3(b) sends the key re-distribution request message to the BS when the count value is more than the threshold value at the report forwarding phase. The proposed key re-distribution phase operates at the BS and the BS determines whether to execute the key re-distribution by using the FTR of the network, the energy, and distance as inputs for fuzzy logic. Following this, the behavior is the same as DEF in the key dissemination phase.

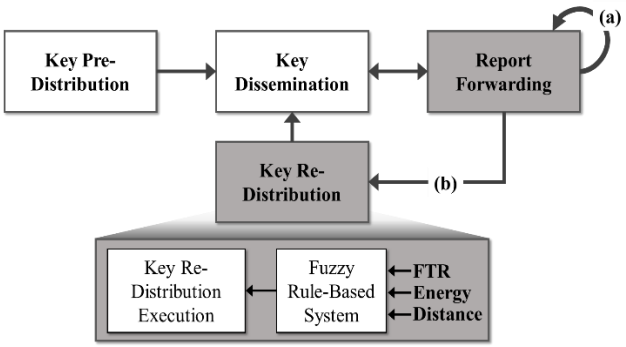

Fig.3. Operation phase of the proposed scheme.

B. Assumptions

This paper has the following assumptions. Since the key pre-distribution phase is operated before dissemination in the field, the BS knows the key information of all the nodes. Since the BS has all of the keys through the global pool key, when a false report is delivered to the BS, the BS can know that the false report exists. The BS knows the node energy on the re-distribution request message path. There is no change in the network topology. The forwarding node has the space to store the number of false reports detected. When the node stores the authentication key from $K(n)$ in memory, it also stores the decrypted secret key. The structure of the key re-distribution request message sent to the BS from the forwarding node is defined as follows:

$$FN \rightarrow BS : CH_{ID} \parallel KI_A \parallel KI_{S,}$$

where FN is the forwarding node and CH_{ID} is the identity of the source CH that generated the false report. KI_A refers to the index of the authentication key detecting a false report and KI_S is the index of the secret key used for storing the authentication key. The notation ‖ means consecutive concatenation.

C. Detailed procedure

This section describes an operation of the proposed scheme in detail. Fig. 4 show the entire execution process of the proposed scheme. Compromised nodes $v_1 \sim v_x$ in the cluster and CH generate a false report and then send it to q neighbor nodes (Fig. 4[a]). The next forwarding node u_j, which received the report, verifies the report. It cannot detect the false report and sends the report to the next q neighbor nodes (Fig. 4[b]). u_{j+k} of the forwarding node on the path detects the false report and drops it. At this time, u_{j+k} knows the source CH through the received report and stores the false report detection count value corresponding to the source CH (Fig. 4[c]). If the attack occurs continuously and the count value of a certain CH exceeds the threshold, the forwarding node encrypts the message of the key re-distribution request and sends it to the BS. Because the BS that received the message knows all the keys, it decrypts this message and stores the CH_{ID}, KI_A and KI_S (Fig. 4[d]). The BS that received the key re-distribution request uses the information of the network for a fuzzy logic system. The fuzzy logic system is based on three factors: FTR, remaining energy level (REL), and distance from the source CH to the verification forwarding node (HPC; Fig. 4[e]). The result of the fuzzy system is determined through defined fuzzy if-then rules (Fig. 4[f]). Depending on the result, the BS runs or holds the key re-distribution (Fig. 4[g]). If the key re-distribution is determined, the BS finds the source cluster through the CH_{ID} value and then checks whether there is a node with the same authentication key as the KI_A key in the source cluster. If there is a node with the same key among the member nodes, the BS considers the node to be suspicious and notifies the source CH and then takes appropriate measures (Fig. 4[h]). These measures are out of the scope of this paper. If the BS cannot find the node that has the same authentication key in the source cluster by updating the authentication key of the compromised node, it confirms a node with the same secret key, KI_S, and aggregates the authentication keys of the nodes. The aggregated authentication key message is encrypted and is transmitted to the next hop forwarding node, u_j, of the source CH. This is because there are authentication keys that are stolen from the attacker among the collected authentication keys. The u_j that received the message decrypts the message and stores the authentication keys in memory (Fig. 4[i]). If attackers try to inject a false report using the same stolen key again, the false report is detected quickly at the next node, u_j (Fig. 4[j]).

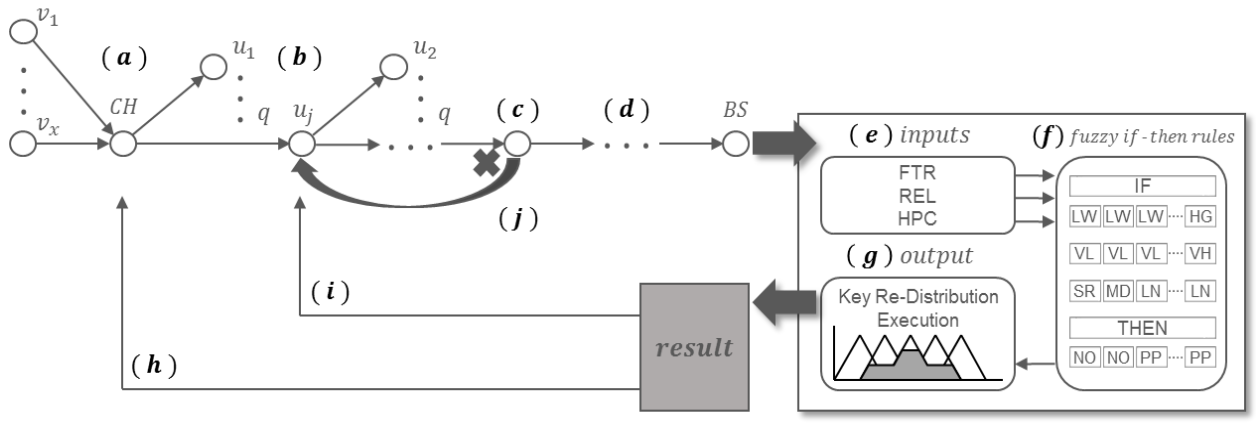

Fig.4. Detailed execution phases of the proposed scheme.

D. Fuzzy logic system

Fuzzy logic provides approximate reasoning to describe the behavior of a system. The fuzzy logic has advantages as follows:

- Execution of approximate reasoning using fuzzy sets rather than fixed and exact values
- Easy implementation and robustness
- Ability to approximate to any non-linear mapping
- Operation of a small amount of storage space such as microcomputers, sensors, and so on.

There are existing AI (artificial intelligence) algorithms such as genetic algorithm, neural networks, etc. However, they have a demand for exact values and complexity of computation in small sensors. We use the fuzzy logic in the proposed scheme due to its features and advantages.

Fuzzy membership functions are defined as shown in Fig. 5. The following are fuzzy variable labels:

- FTR = { LW (low), MD (middle), HG (high) }
- REL = { VL (very low), LW (low), MD (middle), HG (high), VH (very high) }
- HPC = { SR (short), MD (middle), LN (long) }

The output value is determined by these three elements. The label of the output variable is as follows:

- RST = { NA (no action), EP (execute the proposed scheme) }

In the fuzzy if-then rules, using the three factors and labels, we defined 45 rules based on the experiment. Table 1 shows a portion of these fuzzy rules.

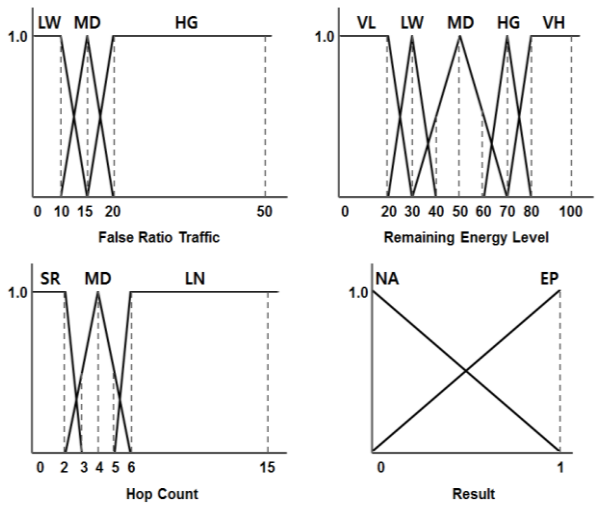

Fig.5. Detailed execution phases of the proposed scheme.

If the FTR is MD, REL is VL, and HPC is MD (Rule 16), then the BS determines the RST to be NA to consider the lifetime of the network. If HPC is LN and the other conditions are the same (Rule 17), then the RST is determined to be EP. In other words, the BS executes the key re-distribution. The reason for this is that the consumption energy that it takes to forward to the verification node from the source node is larger than the energy needed to execute the key re-distribution.

Table 1. Fuzzy if-then rules.

Rule No.	IF			THEN
	FTR	REL	HPC	RST
0	LW	VL	SR	NA
1	LW	VL	MD	NA
2	LW	VL	LN	EP
		.		
		.		
		.		
5	LW	LW	LN	EP
6	LW	MD	SR	NA
7	LW	MD	MD	EP
		.		
		.		
		.		
16	MD	VL	MD	NA
17	MD	VL	LN	EP
18	MD	LW	SR	NA
		.		
		.		
		.		
24	MD	HG	SR	NA
25	MD	HG	MD	EP
26	MD	HG	LN	EP
		.		
		.		
		.		
35	HG	LW	LN	EP
36	HG	MD	SR	NA
37	HG	MD	MD	EP
		.		
		.		
		.		
44	HG	VH	LN	EP

V. Performance Evaluation

In this section, we evaluate the performance of the proposed scheme. Section A describes the experimental environment and Section B presents the experimental results.

A. Experimental environment

The experimental environment is configured as follows: 1,000 nodes are randomly disseminated at sensor fields, which are $1{,}000 \times 1{,}000\ m^2$ in size. Among these nodes, 900 nodes are normal nodes and 100 nodes are CHs. The BS is positioned in the top right (x, y = 1000, 1000) of the sensor field. Each node is randomly loaded with $l = 2$ y-keys and one z-key in each key pool of size 20. The energy required to transmit one byte is 16.25 μJ and the energy required to receive one byte is 12.5 μJ. The energy required to verify a MAC is 75 μJ [15]. The size of a report is 24 bytes and a MAC is one byte. Each node has

an energy resource of $1J$. The false report injection attacks occur depending on the FTR of the five clusters selected. Target nodes that can be compromised are normal nodes and CHs in the selected cluster. No packet loss occurs in the communication the node and 1,000 events are randomly run at the selected five clusters.

B. Experimental results

The experiment was performed to compare the proposed scheme with DEF. The comparison items include the amount of energy consumption, the false report detection performance and the average number of routing hop counts of the false report. Experiments with the proposed scheme are conducted using a proper threshold (α), which is referenced when transmitting the message to the BS at a forwarding node. Through simulation, we select two thresholds (α = 25, 15).

Fig. 6 shows the number of times key re-distribution is performed according to the FTR. When the α value is 15, it can be seen that the number of key re-distribution is larger than when the α value is 25.

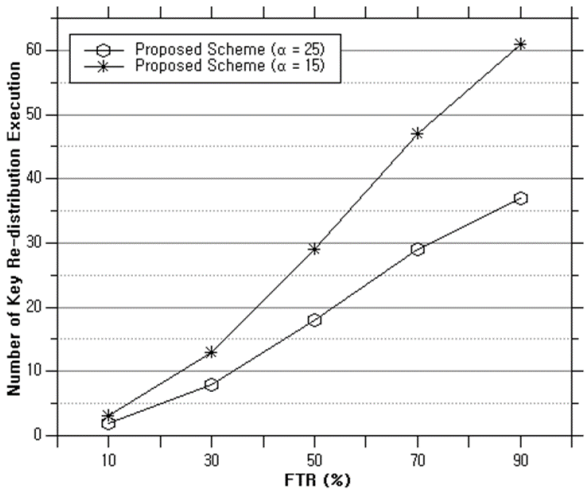

Fig.6. Number of key re-distribution execution versus the FTR

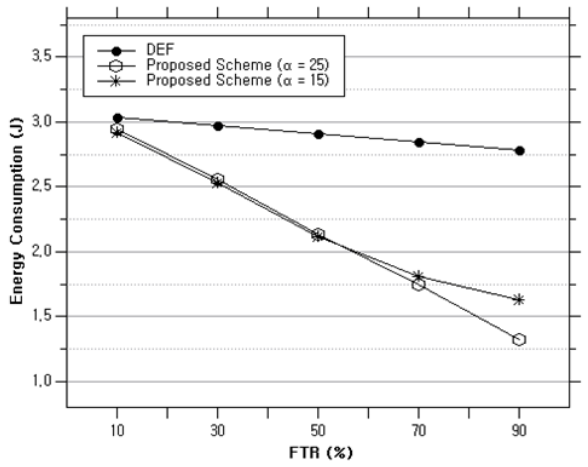

Fig.7. Energy consumption versus the FTR.

Fig. 7 shows the total energy consumption of the network according to the FTR. In both schemes, the number of false reports that were detected previously at the BS increased according to the FTR, and therefore the total energy consumption is reduced. The energy difference between the two schemes is due to the reduced number of hop counts of false reports through the proposed key re-distribution phase. Thus, the unnecessary energy loss is reduced. As the FTR increases, we see that the difference in the energy consumption of both schemes increases. The reason for this is that the number of false reports that are detected at the early hop is much more than the existing scheme.

Fig. 8 shows the number of false reports detected. Both schemes have greater than 80% performance. The proposed scheme seems to have a slight improvement in the performance. The reason for this is as follows. When a false report is not detected on the intermediary forwarding node and reaches the BS, the BS counts the false report according to the source CH. If the count value exceeds the threshold, the BS executes the key re-distribution in the next node of the source cluster, similar to a forwarding node. The detection power is improved because the false report that was forwarded until the BS is dropped at the next node of the source CH.

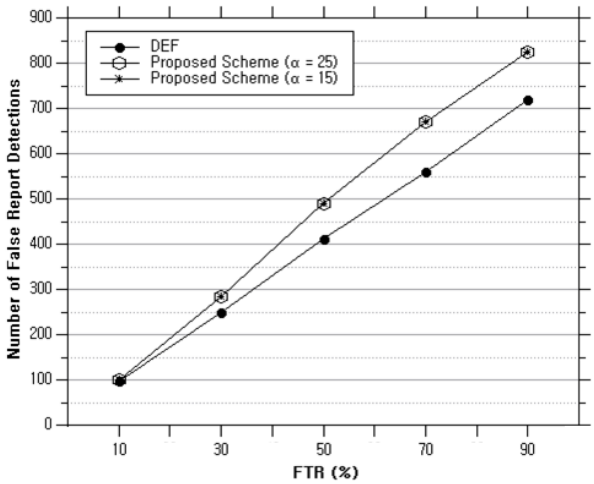

Fig.8. Number of dropped false reports versus the FTR

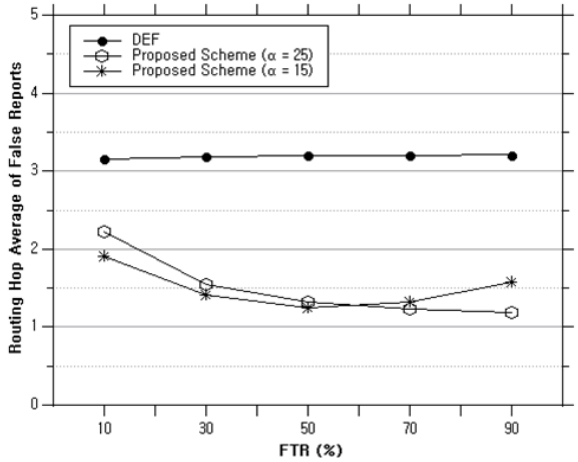

Fig.9. Average hop count of false report versus the FTR.

Fig. 9 shows the average travel hop of a false report. The difference between the two schemes is due to the

earlier detection of the hop compared to the DEF, and the detection of a false report that was not detected in the existing scheme at the next node of the source CH. The average hop count of a false report of DEF, however, is constant because DEF randomly distributes the key; the proposed key re-distribution is executed by the fuzzy logic that was applied to the network information. Therefore, the average hop counts of the proposed schemes differ.

Table 2 provides a summary of the experimental results.

Table 2. Experimental results.

FTR (%)	Energy efficiency (%)		Filtering performance (%)	
	α = 15	α =25	α = 15	α = 25
10	3.88	2.89	3.03	3.03
30	14.76	13.84	13.72	13.72
50	27.08	26.43	15.92	15.92
70	36.33	38.73	16.54	17.89
90	41.30	52.33	12.74	18.57

VI. Conclusions and Future Work

WSNs are placed in an open field and have limited sensor node resources. Therefore, it is essential that a security protocol considers the energy consumption behavior of the network when it is applied to WSNs. In this paper, we propose an enhancement of the DEF scheme for energy savings and detection performance improvement. In our scheme, the BS receiving the re-distribution request message from the detecting node determines whether or not to redistribute the keys by using fuzzy logic. Our scheme obtains the following advantages.

- Energy efficiency: The forwarding node detects the false report and requests the key re-distribution. Through this, the BS executes a key re-distribution to the next node of the source cluster. In an attack situation with the same stolen authentication key, the false report is immediately dropped at the next forwarding node. Thus, it reduces the unnecessary energy consumption. The key re-distribution is sensitive to energy use, so it is determined by the fuzzy logic at the BS and the threshold in the forwarding node. The flag of the fuzzy logic execution results considers the network situation, so more energy is saved.
- Security improvement: The BS counts false reports sent to the BS that are not detected at the intermediate nodes. When the count value exceeds the threshold, the BS decides to execute the key re-distribution through fuzzy logic. Because the distributed key detects false reports that are not detected in the existing scheme, the detection performance is improved.

In the future, we will study how to obtain high efficiency of the proposed scheme in diverse attacks and security protocols. We will also study the selection of an appropriate value of the threshold (α) condition to pass the forwarding node's key re-distribution request message to the BS.

Acknowledgment

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-2013R1A2A2A01013971).

References

[1] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," 2006.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, pp. 393-422, 2002.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102-114, 2002.

[4] K. Romer and F. Mattern, "The design space of wireless sensor networks," IEEE Wireless Communications, vol. 11, pp. 54-61, 2004.

[5] J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, pp. 2292-2330, 2008.

[6] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," IEEE Trans. Ind. Electron., vol. 56, pp. 4258-4265, 2009.

[7] S. Zhu, S. Setia, S. Jajodia and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, 2004, pp. 259-271.

[8] Y. Huang, H. Li, K. A. Campbell and Z. Han, "Defending false data injection attack on smart grid network using adaptive cusum test," in Information Sciences and Systems (CISS), 2011 45th Annual Conference on, 2011, pp. 1-6.

[9] S. Jeba and B. Paramasivan, "False data injection attack and its countermeasures in wireless sensor networks," European Journal of Scientific Research, vol. 82, pp. 248-257, 2012.

[10] Y. Mo, E. Garone, A. Casavola and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in 49th IEEE Conference on Decision and Control (CDC), 2010, pp. 5967-5972.

[11] S. A. Jeba and B. Paramasivan, "Energy efficient multipath data transfer scheme to mitigate false data injection attack in wireless sensor networks," Comput. Electr. Eng., vol. 39, pp. 1867-1879, 2013.

[12] Z. Yu and Y. Guan, "A dynamic en-route filtering scheme for data reporting in wireless sensor networks," IEEE/ACM Transactions on Networking (ToN), vol. 18, pp. 150-163, 2010.

[13] C.I. Sun and T.H. Cho, "A Key Redistribution Method for Enhancing Energy Efficiency in Dynamic Filtering based Sensor Networks," The Korea Society for Simulation, vol. 19, No. 1, pp. 125-131, 2010.

[14] J. Yen and R. Langari, Fuzzy Logic: Intelligence, Control,

Copyright © 2017 MECS

and Information. Prentice-Hall, Inc., 1998.
[15] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on, vol. 23, pp. 839-850, 2005.

Authors' Profiles

Dongjin Park received his B.S degree in Computer Engineering from Sungkyunkwan University, Korea, in 2009. He is currently a master student in the College of Software at Sungkyunkwan University, Korea. His research interests include wireless sensor network, network security, and modelling and simulation.

Taeho 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 Software at Sungkyunkwan University, Korea. His research interests include wireless sensor networks, intelligent systems, modeling and simulation, and enterprise resource planning.

How to cite this paper: Dongjin Park, Taeho Cho,"A Fuzzy Rule-based Key Re-Distribution Decision Scheme of Dynamic Filtering for Energy Saving in Wireless Sensor Networks", International Journal of Information Technology and Computer Science(IJITCS), Vol.9, No.4, pp.1-8, 2017. DOI: 10.5815/ijitcs.2017.04.01