SELECTING VOTES FOR ENERGY EFFICIENCY IN PROBABILISTIC VOTING-BASED FILTERING IN WIRELESS SENSOR NETWORKS USING FUZZY LOGIC

Su Man Nam and Tae Ho Cho

College of Information and Communication Engineering, Sungkyunkwan University, Suwon, 440-746, Republic of Korea

ABSTRACT

Wireless sensor networks are easily compromised by an adversary, such as fabricated with false votes attacks and false votes on real reports attacks. These attacks generate false data to drain the energy resource of sensors and interrupt the inflow of a real report. PVFS was proposed to detect them by verifying votes in the real report. When a real event occurs, a cluster head collects all of the votes from its neighboring nodes and selects the votes up to a defined number of votes. In this paper, our proposed method decides the number of votes based on a fuzzy rule-based system to improve energy savings as compared to PVFS. We evaluated the effectiveness of the proposal as two attacks occur simultaneously in the sensor network. The experimental results show that our method saves energy resources and maintains the security level against these multiple attacks.

KEYWORDS

Wireless sensor network, Probabilistic voting-based filtering scheme, Fuzzy System

1. INTRODUCTION

Wireless sensor networks (WSNs) operate without the intervention of an administrator in a huge area [1]. These Sensor networks enable low-cost and low-power development in open environments [2]. However, the sensor network has restrictions on the resource utilization side, such as the energy of sensor nodes, computational capacity, and bandwidth [3]. In addition, network adversaries can easily compromise the sensor nodes [4-5].

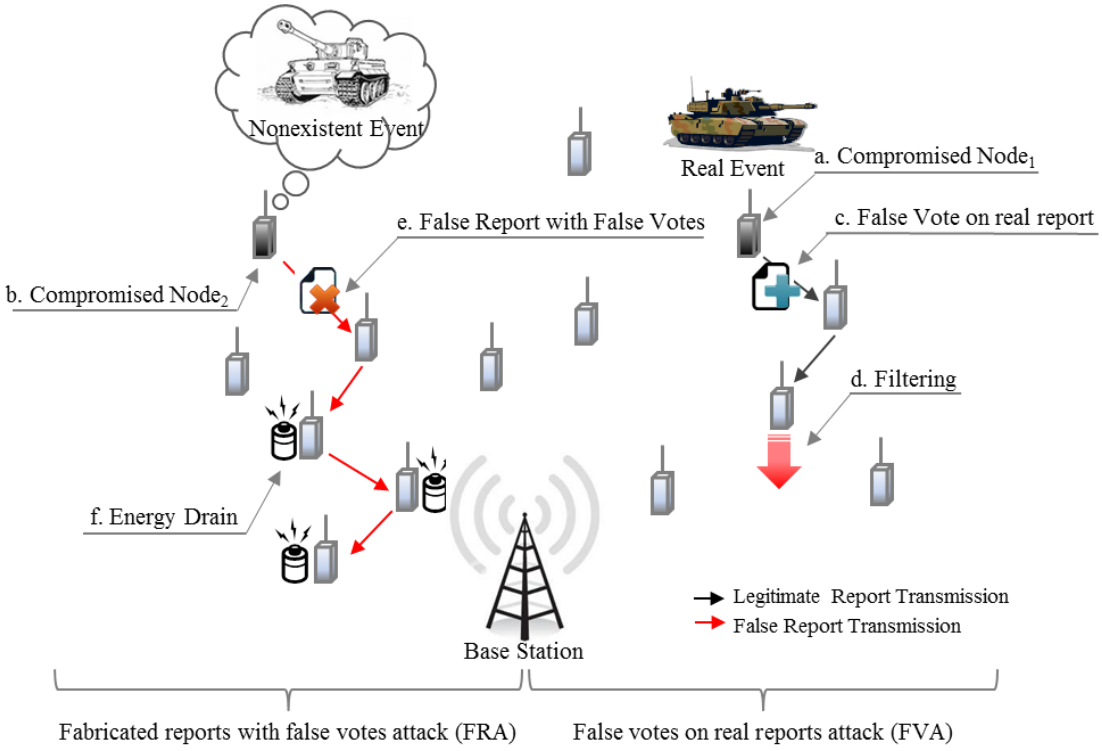

Figure 1.Multiple Attacks

Figure 1 shows a fabricated report with false votes attack (FRA) [6], and a false vote on real reports attack (FVA) [7], in the sensor network. Two compromised nodes inject the fabricated report and false votes, to destroy the sensor network. In an FRA, a compromised node generates a false report about a non-existent event, to drain the energy resource of intermediate nodes, and causes false alarms when the false report arrives in the base station. In an FVA, a compromised node injects a false vote in a legitimate report, to be intentionally dropped in an intermediate node, when a real event occurs. These attacks should be dropped, for reasons of information removal, and needless energy consumption.

A probabilistic voting-based filtering scheme (PVFS) [7] was proposed, to detect multiple attacks in intermediate nodes when FRA and FVA simultaneously occur in the sensor network. Before all of the sensors are deployed, factors, such as the required number of votes for a report, the threshold of verified true votes in the report, and the threshold of verified false votes in the report, are defined to operate the sensor network, and detect the multiple attacks. This method selects verification cluster-head nodes (CHs) with a probability to detect the attacks, before forwarding a report.

In this paper, we propose a method to effectively select a required number of votes for a legitimate report, based on a fuzzy rule-based system [8], before forwarding the report. Our proposed method decides the required number of votes through the energy level, hops from the report generation CH to the base station, and the forwarded report count. Therefore, the proposed method saves energy resources of each node, while maintaining security level against FRA and FVA, as compared to PVFS.

The remainder of this paper is arranged as follows: the background and motivation are described in Section 2, the proposed method is introduced in Section 3, the experimental results are discussed in Section 4, and the conclusions are made and future work is discussed in Section 5.

2. BACKGROUND

FRA and FVA are generated in the application layer of a sensor network, to consume unnecessary energy of sensor nodes, and to obstruct the delivery of a legitimate report. These attacks should be minimized, through early detection. We will discuss PVFS against FRA and FVIA in Section 2.1, and explain the motivation for our proposed method in Section 2.2.

2.1. PVFS

PVFS was proposed to achieve better resilience against compromised nodes, and offer protection for both FRA and FVA. PVFS executes five phases.

Before a sensor network is operated by using PVFS, every factor is defied such as the number of nodes, a global key pool in the base station, the required number of votes for a legitimate report (s), threshold of verified false votes to drop a report (T_f), etc. Before deploying sensor nodes, cluster-header node (CH) assigns keys from a partition of a global key pool and randomly distributes the keys to its normal nodes within a cluster. When a real event occurs within the cluster region, CH detects it and broadcasts its neighbors. After collecting all the votes of the neighboring nodes, the CH randomly selects the votes as s=5. The CH attaches the votes to a report noticed to the base station. The CH (d_0) selects intermediate CH (d_i) to be a verification CH with probability $P = d_i/d_0$. The report is verified in the verification CH while passing intermediate CHs to detect both FRA and FVA. We will discussion phases of the report generation, verification CH selection, and en-route filtering.

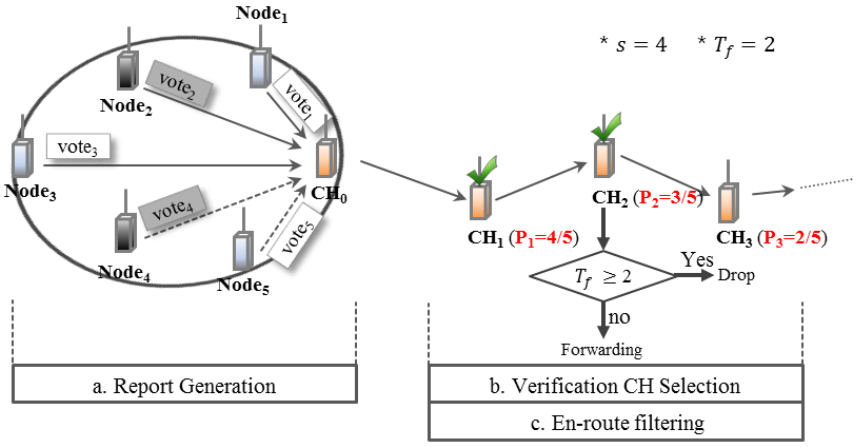

Figure 2.An example of PVFS.

Figure 3 shows the report generation, verification CH selection, and en-route filtering phases to detect both FRA and FVA. In Figure 3-a, a cluster has a CH and five neighbors, including two compromised nodes. When a real event occurs in the cluster, CH0 collects all the votes from all its neighboring nodes, and randomly selects the votes with i=1, 2, 3, 4, as s=4. The votes, including two false votes, are attached in a report, to be transmitted to the base station. Before forwarding the report, verification CHs are decided with probability, and CH1 and CH2 get keys K. When the report arrives in CH1, the false vote2 is detected through key 2. The report is then transmitted to the next intermediate CH, due to $T_f = 1$. The report is dropped in CH2 with recognizing FRA, because the false vote4 is detected through key 4 as $T_f = 2$. On the other hand, if CH0 selects the votes with i=1, 3, 4, 5, as s=4, one vote is included in a report. After choosing

verification CHs, the report arrives in CH1. When CH1 verifies the votes of the report, CH2 sends it to CH2, after confirming vote1 and vote5. When the report arrives in CH2, it detects a false vote in the report. CH2 then transmits it to CH3 without dropping it, because of recognizing FVA. Therefore, PVFS generates reports attaching votes as s, detecting both FRA and FVA, by using the threshold value (T_f) in the sensor network.

2.2. Motivation

In the sensor network, PVFS should be operated, to simultaneously detect multiple attacks, such as FRA and FVA. PVFS defines input parameters, such as the required number of votes for a legitimate report (s), before deploying the sensor nodes in the field. If an input parameter is unsuitable in the network, it causes a reduction of the network lifetime, due to unnecessary energy consumption. For example, if a high number of votes for attaching a legitimate report are defined, the report causes much energy consumption, while passing through intermediate CHs. On the other hand, if a low number of votes are defined, the probability of detecting false votes decreases in verification CHs. Thus, our proposed method considers the condition of the sensor network, and decides the number of votes for a legitimate report, based on fuzzy logic.

In this paper, we define the required number of votes for attaching a legitimate report in the sensor network, based on the fuzzy system, instead of the definition of the operator. In our proposed method, a CH runs a fuzzy rule-based system, to effectively decide the required number of votes before sending a report. Therefore, our proposal improves the energy resource of each node, through the required number of votes, based on the fuzzy system. In the next section, we will further discuss our proposed method.

3. PROPOSED METHOD

3.1. Assumptions

We assume the sensor nodes are fixed, after they are deployed. The sensor network is composes composed of a base station and a number of sensor nodes, e.g. the Berkeley MICAz motes [9], initial paths are established through directed diffusion [10], and minimum cost forwarding algorithms [11]. We choose the cluster-based model [1] to organize the sensor nodes. In a cluster, one node is elected to be a CH.

It is further assumed that every node forwards reports into the base station along their path. A compromised node generates false reports in a path. The generated false reports are forwarded from a compromised node toward the base station, before being filtered out.

3.2. Overview

Our method decides the verification CHs by using three input factors of an intermediate CH: a) the energy level, b) distance level, and c) number of detected false votes.

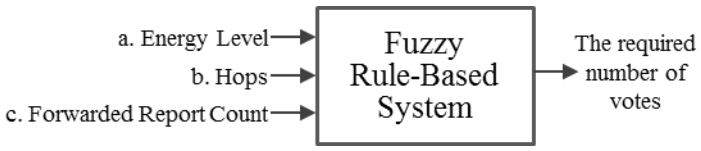

Figure 3.The core of the proposed method.

Figure 4 shows the phase of the report generation in a CH, by applying the three input factors, after collecting votes for its neighbors. Our proposed method considers that the required number of votes for attaching a legitimate report is decided through the energy level, hops, and forwarded report count. It is important to decide the number of votes in the report, because the energy consumption and the detection of false votes are affected in intermediate CHs. Thus, the proposed method effectively detects both FRA and FVA, by using the fuzzy rule-based system to choose the required number of votes.

3.3. Fuzzy Logic in the proposed method

This section discusses the factors that are used for fuzzy inference.

- Energy level: This factor indicates how much energy remains in each CH. The valuespecifiesthe energy level of each CH between 1 and 100. If the value is close to 100, the energy level of the CH is full.

- Hops: This factor indicates the hops count from the base station to a source CH. When the CH forwards a report, the factor influences the security level with energy consumption, through a high probability. For instance, if a CH in high hops forwards a report, the report passes through many intermediate CHs, with much energy consumption.The value specifies the hops of each CH from between 0 and 12. If this factor is small, the intermediate CH is close to the base station.

- Forwarded report count: This value indicates how many real events occur, for generating reports in the sensor network. A compromised node also forwards reports to inject false information into the base station. If a specific CH generates many reports, that CH is suspicious, because many false reports may be included. The value specifies the forwarded report count between 0 and 40. If the value exceeds 40, it keeps 40.

The input factors energy level (ENG), hops (HOP), andforwarded report count (FRC), to decide the required number of votes for attaching a report, by using the fuzzy rule-based system.

We tune membership functions as the best rule, with lots of experimentation. The input factors of the fuzzy variables are represented as:

- Energy Level (ENG) = {Insufficient (IN), Medium (MD), Sufficient (SF)}

- Hops (HOP) = {Very Short (VS), Short (SH), Medium (MD), Long (LN), Very Long (VL)}

- Forwarded report count (FRC) = {Low (LW), Middle (MD), High (HG)}

The output factors of the fuzzy variables are represented as:

- Number (NUM) = {Two (TW), Three (TR), Four (FR), Five(FV), Six (SX)}

3.4. Fuzzy Membership Functions and Rules

This section discusses fuzzy membership functions and rules.

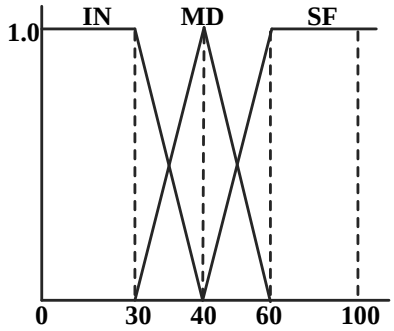

Figure 4.Input factor of energy level (ENG).

Figure 5 shows an input factor of energy level in a CH with three conditions: Insufficient (IN), Medium (MD), and Sufficient (SF).

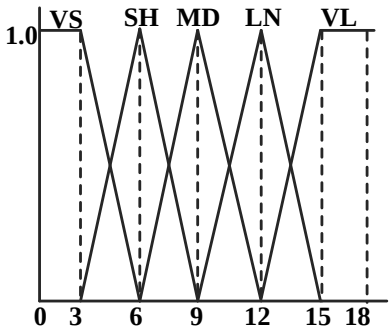

Figure 5.Input factor of hops (HOP).

Figure 6shows an input factor of hops in a CH with five conditions: Very Short (VS), Short (SH), Medium (MD), Long (LN), and Very Long (VL).

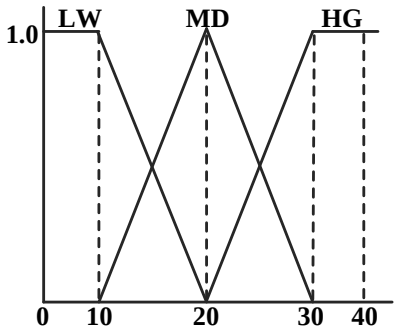

Figure 6.Input factor of the forwarded reportcount (FRC).

Figure 7shows an input factor of the forwarded report count in a CH with three conditions: Low (LW), Middle (MD), and High (HG).

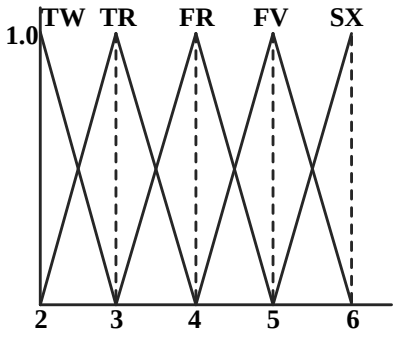

Figure 7.Output factor of the number (NUM).

Figure 8shows an output factor of the result for attaching votes to a report with five conditions: Two (TW), Three (TR), Four (FR), Five (FV), and Six (SX).

Table 1.Fuzzy if-then rules.

Rule No.	Input (if)			Output (then)
	ENG	HOP	FRC	NUM
1	SM	NR	SM	FV
15	SM	VF	LG	SX
23	MD	MD	MD	FR
31	LG	NR	SM	TW
45	LG	VF	LG	TH

Table 1 shows representative rules that frequently occur among the fuzzy if-then rules. For example, if ERL is SM, HOP is NR, and NFR is SM, then a CH attaches five (FV) votes in a report, such as Rule 1. If ERL is SM, HOP is VF, and NFR is SM, then a CH attaches six (SX) votes in a report, due to the strong security level, such as Rule 15. If ERL is MD, HOP is MD, and NFR is MD, then a report has four (FR) votes, such as Rule 23. If ERL is LG, HOP is NR, and NFR is SM, then a report has two (TW) votes, due to the energy saving. If ERL is LG, HOP is VF, and NFR is LG, then a CH generates three votes (TH) for forwarding a report. Therefore, our proposed method dynamically decides the required number of votes in a report, to use a strong security level, and energy saving, in the entire network.

4. EXPERIMENTAL RESULTS

We performed an experiment for comparison of our proposed method and PVFS. A sensor network has a base station and 500 total nodes in the simulation environment. The simulation environment is 1,000×1,000 m^2, which is composed of 50 clusters, and 10 nodes in a cluster. We arranged 20 compromised nodes in clusters of 11 hops. The compromised nodes inject FRA and FVA, to consume unnecessary energy, and false votes to drop legitimate reports, in verification CHs. The size of a report is 24 bytes, and the size of a vote is 1 byte. Each node uses 16.25 μJ to transmit per byte, 12.5 μJ to receive per byte, and 15 μJ to generate a vote per byte [15]. We randomly generate 300 events in clusters, and the ratio of false reports is 20% of the events. We randomly generate 250 events in clusters, and the ratio of false reports and false votes is 20% of the events.

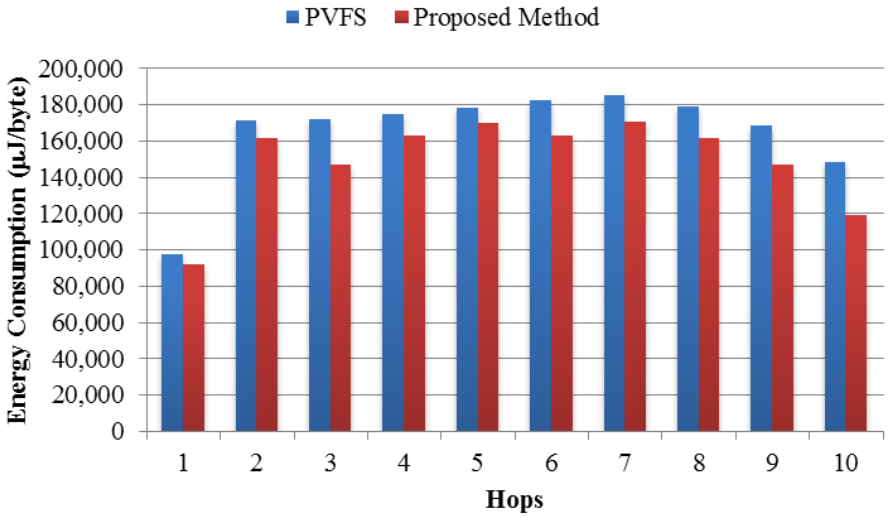

Figure 8.Energy consumption per hops.

Figure 9 shows the energy consumption of nodes per hops in the sensor network. FRA and FVA are randomly generated, by using compromised nodes in clusters of 11 hops. Two attacks forward false reports and votes with generating 20% toward the base station. PVFS consumes much more energy resources than the proposed method, due to the fixed number of votes in a report; while our proposal forwards a report with the selected number of votes in a CH, considering the condition of the network, based on the fuzzy rules. The proposal saves unnecessary energy resources, due to the decision of the vote number. In addition, when a particular CH injects many reports, the proposed method reasons FRA, and increases the number of votes for filtering them early. Therefore, our proposal reduces needless energy, through dynamically selecting the number of votes based on the fuzzy system, more than PVFS.

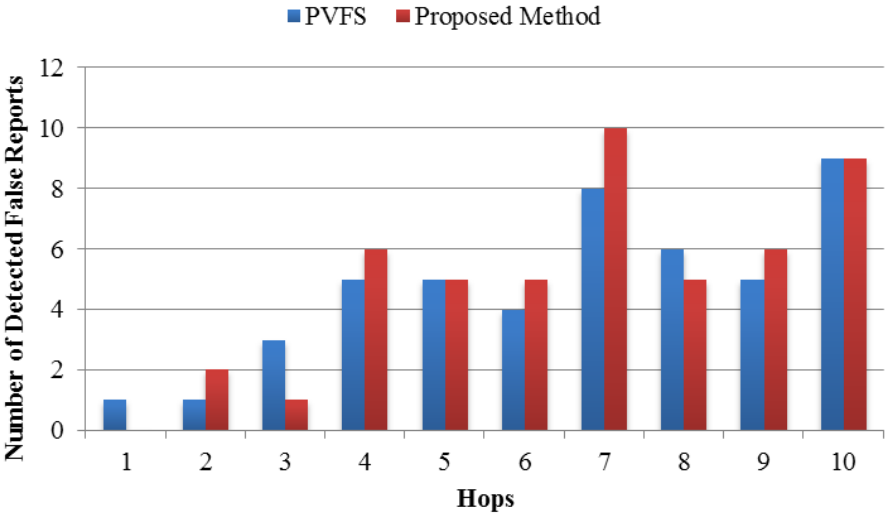

Figure 9. The number of filtered FRA her hops

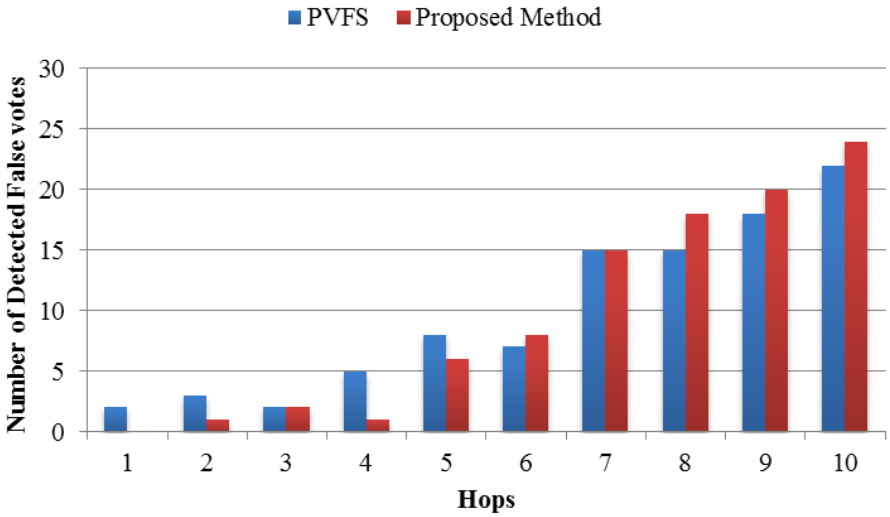

Figure 10.The number of filtered FVA her hops.

Figure 10 and Figure 11 show the number of filtered FRA and FVA per hops in the sensor network. They are generated and injected by compromised nodes of 11 hops. PVFS and the proposed method are almost similar to the number of detected votes in verification CHs. The proposed method maintains the security level of the two attacks, by using the fuzzy system, as compared to PVFS. Thus, our proposed method approximates the detection power of PFVS, with using the dynamic decision of the number.

5. CONCLUSIONS AND FUTURE WORKS

In a sensor network, FRA and FVA can be generated to drain energy resources of the sensor nodes, and block the inflow of a legitimate report [16]. PVFS was proposed to detect these attacks, by verifying votes of the report in verification CHs with a probability. The required number of votes for the report is defined, before deploying the sensors. In this paper, our proposed method decides the number of votes in the report, based on a fuzzy rule-based system. Our proposal improves energy savings of the sensor nodes, while maintaining the security level of two attacks. Therefore, our proposed method effectively saves energy resources, and maintains the detection power of false votes. In addition, in future work we will apply various attacks of the sensor network, to discuss further optimal solutions.

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. 2013R1A2A2A01013971).

REFERENCES

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

[2] Przydatek, D. Song and A. perrig, "SIA: Secure information aggregation in sensor networks," Proc. Of CCNC, Vol. 23. 2004, pp. 63-98.

[3] Kemal A. and Mohamed Y., "A survey on routing protocols for wireless sensor networks," Ad hoc Network. Vol. 3, May 2005, pp. 325–349.

[4] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: attacks and countermeasures Sensor Network Protocols and Applications," 2006 8th International Conference Advanced Communication Technology (2006), Vol. 1, 2006, pp. 314-318.

[5] Xiaojiang D., and Hsiao-Hwa C, "Security in Wireless Sensor Networks" IEEE Wireless Commununications, Vol. 15, Aug. 2008, pp. 60-66.

[6] Fan Ye; Luo,H., Songwu Lu and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on, Vol. 23, Apr. 2005, pp. 839-850.

[7] Li, Feng, Srinivasan, Avinash, Wu and Jie, "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks," International Journal of Security and Network, Vol. 3, No. 3, 2008, pp. 173-182.

[8] L. A. Zadeh, "Fuzzy Logic," 2011, http://en.wikipedia.org/wiki/Fuzzy_logic

[9] Crossbox Wireless Sensor Networks, http://www.xbox.com/

[10] C. Intanagonwiwat, R. Govindan, D. Estrin, Directed diffusion: A scalable and robust communication paradigm for sensor networks. In Proc. of MobiCOM '00, 2000, pp. 56-67.

[11] F. Ye, A. Chen, S. Lu, L. Zhang, A scalable solution to minimum cost forwarding in large sensor networks. Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on, 2001, pp. 304-309.

[12] Kemal A. and Mohamed Y., "A survey on routing protocols for wireless sensor networks," Ad hoc Network. Vol. 3, May 2005, pp. 325–349.

[13] Sencun Zhu, Setia, S., Jajodia, S. and PengNing, "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.,May 2004, pp.259-271.

[14] Xiaojiang D., and Hsiao-Hwa C, "Security in Wireless Sensor Networks" IEEE Wireless Commununications, Vol. 15, Aug. 2008, pp. 60-66.

[15] Fan Ye, Luo,H., Songwu Lu, and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on, Vol. 23, No. 4, 2005, pp. 839-850.

[16] H yun Woo Lee, Su Man Nam and Tae Ho Cho, "A Key Level Selection Within Hash Chains for the Efficient Energy Consumption in WSNs," International Journal of Ambient Systems and Applications (IJASA), Vol. 1, No. 3, Sep. 2013, pp. 1-14.

Authors

Su Man Nam received his B.S. degree in computer information from Hanseo university, Korea, in February 2009 and M.S degree in in Electrical and Computer Engineering from Sungkyunkwan University in 2013, respectively. He is currently a doctoral student in the College of Information and Communication Engineering at Sungkyunkwan University, Korea. His research interests include wireless sensor network, security in wireless sensor networks, and modelling & simulation.

Tae Ho Choreceived the Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and the B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests are in the areas of wireless sensor network, intelligent systems, modeling & simulation, and enterprise resource planning.