Verification Probability Control Method in Sensor Networks

Soo Young Moon and Tae Ho Cho,

Sungkyunkwan University, Suwon 440-746, Republic of Korea

Summary
Wireless sensor networks (WSN) collect and report event information to users in many applications (e.g. monitoring, tracking). Due to the lack of infrastructure and management in the sensor field, WSN are vulnerable to many security attacks. In false report injections attacks, attackers inject false reports into the network through compromised nodes. The false reports cause false alarms at the base station (BS) and waste energy at forwarding nodes. In the statistical en-route filtering scheme (SEF), a countermeasure to the attacks, sensor nodes detect and drop false reports by endorsing and verifying event reports using shared keys. In SEF, each node verifies received reports based on fixed probability and do not consider sending nodes. For this reason, unnecessary energy consumption occurs. In this paper, we propose the verification probability control method in sensor networks. In the method, each node controls its verification probabilities for its neighbor nodes. The number of recent valid reports, hop counts from the BS and the last verification probability are used to determine the verification probability for a node. We confirm that our method decreases energy consumption of filtering schemes in sensor networks.

Key words:
Wireless sensor networks, security attacks, false reports, filtering.

1. Introduction

Wireless Sensor Networks (WSN) provide interaction between humans and environments by sensing physical events from sensor nodes and report them to users. WSN can be used in many applications such as monitoring and tracking [1-3]. A large number of sensor nodes and few base stations (BS) are organized in a WSN. Each sensor node has a processor, radio, and sensor modules. When an event occurs, the sensor nodes detect the event and report it to the BS. The WSN goal is to provide reliable event information in the sensor field to users. Fig. 1 simplifies the WSN organization. The arrows connecting nodes in the figure represents the routing path where event reports are forwarded to the BS.

Due to the lack of infrastructure and management, there are many possible security threats from attackers (e.g. overhearing message, manipulating user data, affecting routing path) [4, 5]. In false report injection attacks, the attackers compromise some portion of sensor nodes and inject false reports through the nodes into the networks. The false reports result in false alarms at BS and energy waste at forwarding nodes. Statistical En-route Filtering scheme (SEF) [6] is an existing countermeasure [6-10] to the attacks. In SEF, event sensing nodes generate event reports and endorse the report by appending message authentication codes (MACs) generated by using shared keys. Forwarding nodes perform en-route filtering operations, verifying the MACs. Each forwarding node verifies received reports with fixed probability and does not consider the report sending nodes. As a result, unnecessary energy consumption occurs.

In this paper, we propose the verification probability control method in sensor networks. In the proposed method, each node identifies its neighbor nodes and controls a verification probability for each of them. The number of recent valid reports from a neighbor node, hop counts from the BS and the previous verification probability for the node determine the next verification probability for the node. Consequently, the proposed method is able to decrease energy consumption of the filtering schemes.

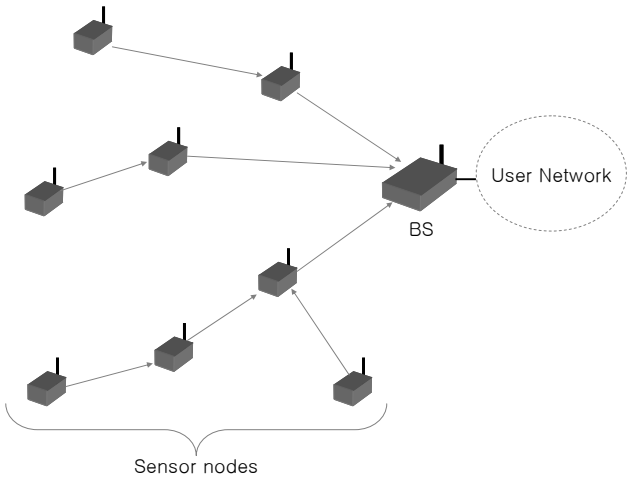

Fig. 1 Organization of WSN

The remaining sections are as follows. Section 2 reviews SEF. In section 3, we present the motivation and details of the proposed method. In section 4, simulation results show the effectiveness of the proposed method. Finally, section 5 concludes the paper and state future work.

Manuscript received August 5, 2008.
Manuscript revised August 20, 2008.

2. Background

In this section, we review SEF concepts and operations. We mainly focus on the en-route filtering phase.

2.1 Statistical En-Route Filtering (SEF)

In SEF, sensor nodes in the field and the BS share encryption keys to authenticate and verify event reports. BS stores all the keys and distributes them to sensor nodes. Keys are grouped into partitions and one sensor node possesses keys in the same partition. When an event occurs, sensing nodes elect one of the nodes as a center of stimulus (CoS) node. Then the other sensing nodes send message authentication codes (MAC) for the event to the CoS node. The CoS node collects the MACs and generates an event report. The security threshold value determines the number of MACs in the report. After that, it forwards the report to the next node. Each en-route node verifies the report by generating a MAC for the event information and comparing it with the corresponding MAC in the report. If the two MACs are different, it drops the report. If it does not have the keys to verify the MACs in the report, it just forwards the report to the next node. The BS is able to check the validity of all the MACs in the report, since it has all the keys to authenticate the report. Sensor nodes should be dense enough to ensure multiple sensing nodes to generate event reports [6]. Fig. 2 shows the SEF operations.

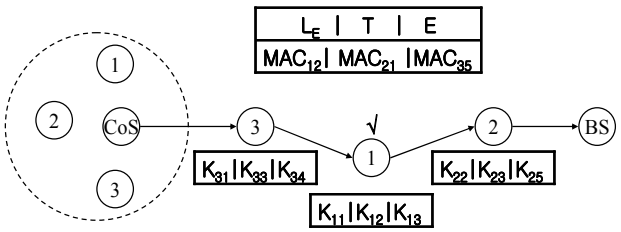

Fig. 2 En-route filtering in SEF

Each circle denotes a sensor node in the figure and the numbers in the circles are their partitions. K_{ij} is the j_{th} key in the i_{th} partition and MAC_{ij} is the MAC generated using the K_{ij}. The box top of the figure represents an event report. L_E and T is the location and time of the event and E is the event information. Three MACs are included in the report in the figure. At the second forwarding node which is associated with partition one, the event report is verified since the node possesses one of keys used to generate the MACs in the report. That is, K_{12}.

2.2 Verification probability

In SEF, a forwarding node is able to verify an event report only when it has one of keys used to create MACs in the report. The verification probability is defined by system parameters used in the system - the number of partitions (n), the number of keys in each partition (m), the number of keys in each node (k), security threshold value (T) and the number of compromised partitions (N_C). Eq.1 shows the relation between the verification probability and the system parameters.

$$p_1 = \frac{T - N_C}{n} \bullet \frac{k}{m} \quad (1)$$

The verification probability affects the efficiency of SEF significantly especially in terms of energy.

3. Proposed method

In this section, we introduce the motivation and detail our method.

3.1 Assumptions

The assumptions in our paper are as follows. There is no infrastructure and management in the sensor field. Sensor nodes have limited energy, computing power and memory. It also has short sensing and transmission range. BS is safe from security attacks and has sufficient resources. Every node is able to authenticate its ID when sending an event report and identify the sending node when receiving it. It also knows its hop counts from the BS to itself. Events occur at random locations in the sensor field. We target false report injection attacks where compromised nodes forge and transmit false reports until their energy depletes.

3.2 Motivation

In SEF, forwarding nodes verify event reports with fixed probability. Since energy consumption is not needed to verify valid reports, it is more efficient to control verification probability adaptively based on the network state. The verification probability is upper-bounded and the maximum is determined by the system parameters as described in 2.2. So it can be less than or equal to its initial value. When a forwarding node receives event reports from a reliable node, it verifies the reports with low probability, and vice versa.

3.3 Overview

In the proposed method, each sensor node has its own ID and identifies its neighbor nodes by their IDs. To verify event reports from different nodes with different probabilities, every node generates and maintains a node information table. The table includes the IDs of neighbor nodes, the recent valid reports from the nodes and the verification probabilities for the nodes. When forwarding nodes receive event reports from their neighbor nodes, they update their tables and control verification probabilities for neighbor nodes. A fuzzy rule-based system is used to derive verification probabilities for neighbor nodes.

3.4 System operation

The proposed SEF method involves two phases – network initialization phase and en-route filtering phase. In the network initialization phase, each sensor node finds its neighbor nodes and creates a node information table for the neighbor nodes. The table includes the ID, the number of recent valid reports (RVR), and the verification probability (VP) for each node. Key assignment, node deployment and ID assignment are all performed before the creation of the table. Fig. 3 represents each node's table to manage verification probabilities for its neighbor nodes.

ID	RVR	VP(%)
N1	0	30
N2	0	30
…	…	…

Fig. 3 Node Information Table

Each record in the table contains information of a neighbor node. N1 and N2 are IDs of neighbor nodes. Initially, RVR of every neighbor node is zero, since no event report has yet been received, and VPs for neighbor nodes are the same. In the en-route filtering phase, intermediate nodes receive event reports, verify the reports, and forward them to the next node, if the reports are found to be valid. Each node updates its node information table based on the result of verification. Three factors – RVR, the hop count from the BS to the current node and the last VP for a neighbor node – are used to determine the next VP for event reports from each node. Then it verifies the received reports based on the new probability. Fig. 4 shows the scenario where the VPs for neighbor nodes change.

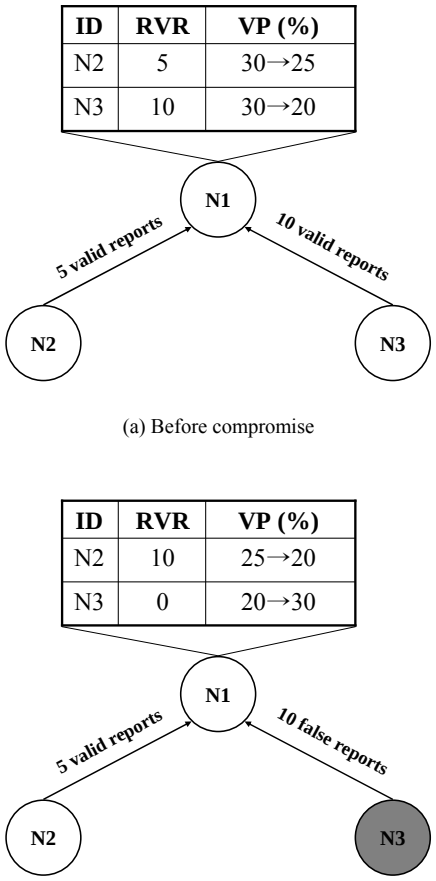

Fig. 4 Control of Verification Probability

N1 has two neighbor nodes, N1 and N2, in Fig. 4. At first, the RVR of both nodes are zero and their VPs are 30%. In Fig. 4(a), N2 sends five valid reports to the N1 and N3 sends ten valid reports to the N1. N1 verifies the reports with probability of 30%, and decreases the VPs of N2 and N3 by five and ten, respectively. Assume that N3 is compromised after the decrease. N2 still sends five valid reports to N1, but N3 sends ten false reports to N1. N1 verifies the reports and decreases VP for N2 by five, but increases VP for N3 by ten.

3.5 Fuzzy rule-based system

In our method, each node uses a fuzzy rule-based system [11] to derive verification probabilities from input factors. There are three fuzzy input variables – the number of

recent valid reports from a neighbor node (RVR), the hop count from the BS to the current node (HOP) and the last verification probability (LVP) - and one output variable, new verification probability (NVP). Fig. 5 shows the relationship of input and output variables for the fuzzy system.

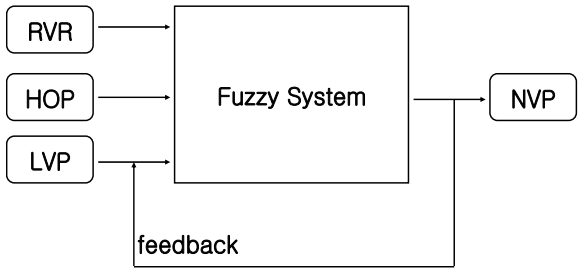

Fig. 5 Relationship of input and output variables

LVP is the feedback to the fuzzy system. Fig. 6 represents fuzzy membership functions for the input and output variables.

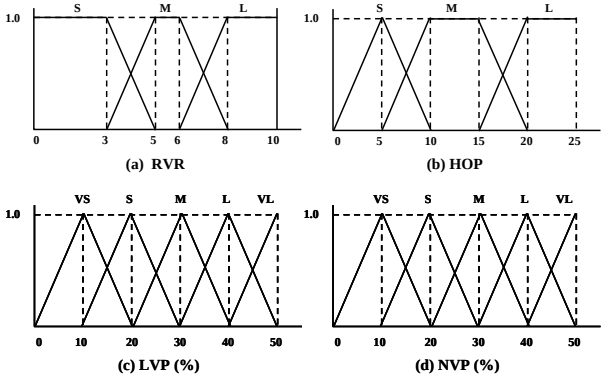

Fig. 6 Fuzzy membership functions

Table 1 shows some of the IF-THEN rules for the system.

Table 1. Fuzzy IF-THEN rules

Rule #	Inputs			Output
	RVR	FTR	LVP	NVP
1	S	S	S	L
14	S	L	VL	VL
28	M	L	L	M
30	L	S	VS	VS
44	L	L	VL	S

4. Simulation results

We simulated our method for false report injection attacks and compared its energy consumption with that of SEF. The assumptions in the simulation are as follows. The size of the sensor field is 50m × 200m and 600 sensor nodes exist in the field. 300 event reports including valid and false reports randomly occur throughout the field. The global key pool is divided to 10 partitions each of 10 keys. Energy consumption is 16.25μJ for transmission, 12.5μJ for receiving a byte and 75μJ for verification at one node [12, 13]. The Free Fuzzy Logic Library (FFLL) [14] was used to implement the fuzzy system. Fig. 7 represents the energy consumption of SEF and the proposed method.

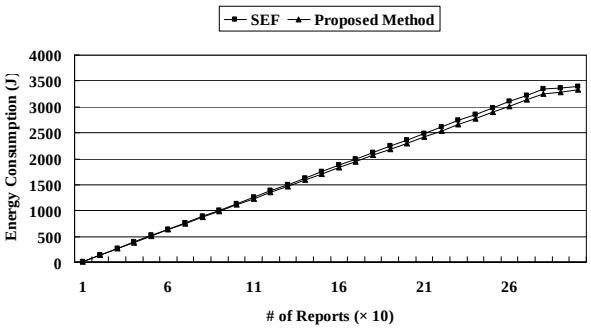

Fig. 7 Energy consumption

In the scenario used to perform the simulation, 90% (270) valid reports and 10% (30) false reports occur. The proposed method consumes less energy than SEF and the difference of energy consumption increases until the first false report (270^{th} report) occurs.

5. Conclusion

In this paper, we proposed the verification probability control method in sensor networks. Existing filtering schemes such as SEF do not consider sending nodes and verify event reports with fixed probability. Thus, energy consumption occurs unnecessarily. In our method, each sensor node identifies its neighbor nodes and controls verification probabilities for event reports from them independently. As a result, our method is more efficient than SEF in terms of energy consumption. Our method can be applied to other filtering schemes that can control the degree of verification. We plan to research more efficient way to control the verification probability of a node.

Acknowledgments

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2008-C1090-0801-0028)

References

[1] Xu, N. (2002). A Survey of Sensor Network Applications. Tech. Rep., University of Southern California.
[2] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002). A Survey on Sensor Networks. IEEE Communications Magazine, 40(8), 102-116.
[3] Al-Karaki , J.N. , Kamal , A.E. (2004). Routing techniques in wireless sensor networks: a survey. IEEE Wireless Communication Magazine, 11(6), 6-28.
[4] Djenouri, D., Khelladi , L., Badache, N. (2005). A Survey of Security Issues in Mobile Ad-Hoc and Sensor Networks. IEEE Communications Surveys & Tutorials, 7(4), 2-28.
[5] Karlof, C., Wagner, D. (2003). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, 1(2-3), 293-315.
[6] Ye, F., Luo, H., Lu, S., Zhang, L. (2005). Statistical En-route Filtering of Injected False Data in Sensor Networks. IEEE Journals on Selected Areas in Communications, 23(4), 839-850.
[7] Yang, H., Lu, S. (2004). Commutative Cipher Based En-route Filtering in Wireless Sensor Networks. Proc. of VTC, 1223-1227, IEEE.
[8] Zhu, S., Setia, S., Jajodia, S., Ning, P. (2004). An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks. Proc. S&P, 259-271.
[9] Yu, Z., Guan, Y. (2005). A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks. Proc. of SenSys, 294-295, ACM.
[10] Lee, H. Y., Cho, T. H. (2006). Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks. Lecture Notes in Computer Science, LNCS 4317, 116-127, Springer Verlag.
[11] Yen, John, Langari, Reza. (1999). Fuzzy Logic. Prentice Hall.
[12] Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., Pister, K. (2000). System Architecture Directions for Networked Sensors. Proc. of ACM ASPLOS IX, 93-104.
[13] Xbow sensor networks, http://www.xbow.com
[14] FFLL, http://ffll.sourceforge.net

Soo Young Moon received the B.S. degree in Electrical and Computer Engineering from Sungkyunkwan University in 2007. He is now a master's student in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include modeling and simulation, wireless sensor networks, network security, and artificial intelligence.

Tae Ho Cho received 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 School 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.