Interleaved Hop-by-Hop Authentication using fuzzy logic to defend against of False Report Injection by Replaying an attack

Jong Hyun Kim[†] **and Tae Ho Cho**[††],

School of Information and Communication Engineering, Sungkyunkwan University

Summary

The wireless sensor node, being a micro electronic device, can only be equipped with a limited power source (< 0.5 Ahm 1.2 V). In some application scenarios (which is like military area), replenishment of power resources might be impossible. Sensor node lifetime, therefore, shows a strong dependence on battery lifetime. An adversary may compromise some sensor nodes and use them to inject false sensing reports. False report can lead to not only false alarms but also false depletion of limited energy resource in battery powered networks. The interleaved hop-by-hop authentication scheme detects and filters such false reports through interleaved authentication. However an Adversary can make energy spent in nodes as false report injection of replaying attack relaying attack. The aim of adversary is to drain the limited energy in sensor nodes not to send false report to the Base Station. In this paper, we propose a countermeasure from this attack in using fuzzy logic in IHA scheme.

Sensor network, IHA, Fuzzy logic

1. Introduction

The recent advances in micro-electro-mechanical systems technology, wireless communication and digital electronics have enabled the development of low-cost, low-power and multi-functional sensor nodes [1]. A wireless sensor network (WSN) is composed of small nodes with sensing, data processing and wireless communicating capabilities [2]. Sensor networks have emerged as an tool that monitors the enemy's tracking in a battlefield environment [3].In most applications, such as military surveillance, the sensor nodes are deployed in open, large-scale or even hostile environments. Therefore they are unattended and so are subject to the threat of being captured and security being compromised [4]. In addition, the battery power of sensor nodes is limited and irreplaceable [2]. Hence, security and energy efficiency are the most challenging aspects when designing Wireless Sensor Networks (WSNs).

In many applications, the sensor nodes are deployed in open environments, and so they are vulnerable to physical attacks, which potentially compromise the node's cryptographic keys [6]. False sensing reports can be injected through compromised nodes that can lead to not only false alarms, but also to the depletion of the limited energy resources in battery powered networks (Fig. 1) [7].

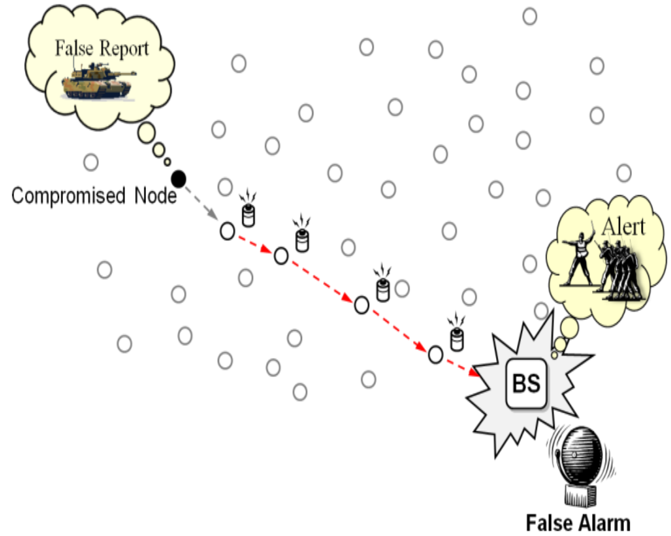


Figure 1. False report can be injected through compromised node, which can lead to not only false alarm but also the depletion of limited energy resource.

To minimize damage that drains the limited energy resources, false reports have to be dropped en-route as early as possible, and the ones that elude being dropped should be further rejected at the base station [4]. Recently, many en-route filtering schemes have been proposed [4], [7-9] and researched [10, 11] for defending against a false report injection attack [4], [7-9].

The interleaved hop-by-hop authentication (IHA) scheme detects false reports and it has the false reports filtered by every en-route node and finally filtered by the base station [11]. However, in the sensor network, all nodes on the path must spend energy receiving, authenticating and transmitting a false report when it is forwarded to the BS [2]. An adversary can cause energy to be spent in nodes as a false report injects a replaying (FRIR) attack.

In this paper, we propose a countermeasure against a FRIR attack by using fuzzy logic in the IHA scheme.

The rest of the paper is organized as follows. In section 2, we describe the background of the IHA. Section 3 illustrates Motivation. In Section 4, we describe the our proposed scheme using fuzzy logic through the result of simulation. Finally, we conclude the study in Section 5.

Manuscript received July 5, 2009
Manuscript revised July 20, 2009

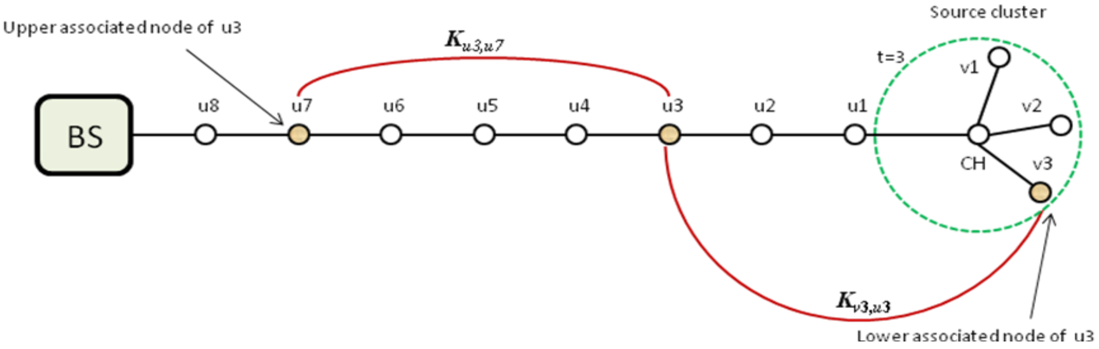


Figure 2. Lower and upper associated nodes in IHA

2. Background

In this section, we briefly illustrate the Interleaved Hop-By-Hop authentication (IHA) scheme [9]

2.1. The Interleaved Hop-By-Hop authentication (IHA) scheme

We illustrate the main characteristics of the IHA scheme. The IHA scheme involves the following five phases. :

2.1.1. Node Initialization and Deployment

The key server loads a unique integer ID and individual key Ku, which are shared with the base station for every node u. After deployment, each node establishes a one-hop pairwise key with each of its neighbors that are discovered by each node. The IHA scheme is to establish one-hop pairwise key with using LEAP [12].

2.1.2. Association Discovery

In this phase, the node discovers the IDs of its associated nodes. These are the upper and lower association nodes that are less than t + 1 hops away from the cluster head and each cluster has t + 1 sensor nodes. Fig. 2 show an example where t = 3. Node u3 selects u7 which is four hops away. The u7 is u3's upper associated node. In addition, since the distance from CH2 to the source cluster head CH0 is two (less than t+1=4), it chooses CN2, a cluster node in the source cluster, as its lower associated node. When a node fails to detect its neighbor, the association discovery phase may be initiated by the BS or by a node.

2.1.3. Report Endorsement

When a sensor node detects an event of interest, these two types of individual MACs and pairwise MACs are computed. The individual MAC uses its individual key that is shared with the BS, while the pairwise MAC uses its association key that is shared with its upper associated node. The cluster head collects both individual and pairwise MACs from all of its cluster nodes; it compresses the individual ones and attaches all of them to the report as an ordered list.

The report R that node u1 forwards to node u2 is as follows (R is also authenticated with K_{u1u2}).

$$
\begin{aligned}
R:\ & E, C, \{v1,v2,v3,CH\}, XMAC(E),\\
& \{MAC(K_{u1u5},E), MAC(K_{CHu4},E)\},\\
& \{MAC(K_{v3u3},E), MAC(K_{v2u2},E).
\end{aligned}
$$

2.1.4. En-route Filtering

The generated report which is detected an event in interest is forwarded to the BS through all en-route nodes. The report received by any en-route node verifies the authenticity with the following steps.

i. Calculating a pairwise MAC with using shared a pairwise key of lower associated nodes.
ii. Comparing the first pairwise MAC with the newly generated MAC attached to the report.
iii. Generating another MAC with using upper associated node and the shared key, then attaching it after authenticating it.

The report is sent to the BS in this way if these two MACs match. Otherwise the report is dropped as shown Fig 3.

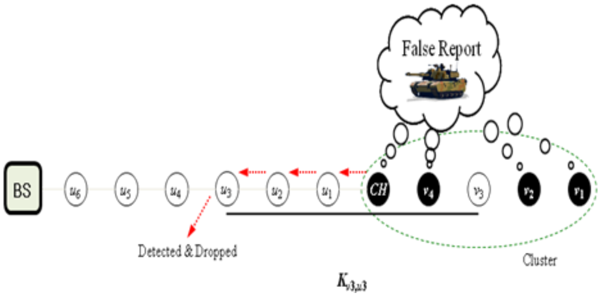


Figure 3. The false report is detected & dropped in IHA scheme

2.1. Base station verification

As the last verification of the transmitted report is performed, the BS serves the final step to detect false report. Under the authentication key of the nodes based on its ID, the BS can compute authentication key easily. And, if the report is authenticated and the BS knows the location of all the cluster nodes, then it can locate these reporting nodes and then react to the event. In another words, the BS will drop the report if the verification fails.

3. Motivation

Some drawbacks still exist even though the Interleaved Hop-by-Hop Authentication (IHA) scheme is very efficient in filtering false reports.

When the generated report is forwarded to the BS, all the en-route nodes must spend energy on receiving, transmitting, and authenticating [2]. An adversary can cause energy to be spent in nodes by using characteristics of the sensor network as the false report injects replaying (FRIR) attack. The aim of the adversary is to drain the limited energy in sensor nodes not to send false report to BS shown as fig 4.

In this paper, we propose a countermeasure against FRIR attacks by using fuzzy logic in the IHA scheme.

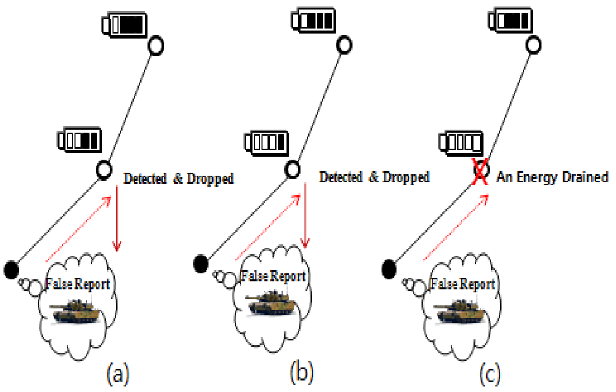


Figure 4. The energy drain from a FRIR attack

4. Proposed scheme

4.1 Assumption

We assume that a sensor network is composed of a large number of small sensor nodes. The nodes within the cluster can elect one cluster head from amongst them. To balance energy consumption, all the nodes of the same cluster may take turns playing the role of a cluster head. As nodes are not equipped with tamper-resistant hardware, they can be compromised by adversaries and the can inject false reports. However, the base station (BS) cannot be compromised. We also assume the BS can determine the estimated distance from the BS to each cluster, the rate of reports rejected by the BS, and the energy consumption. We further assume that the BS has a mechanism to authenticate broadcast messages (e.g., based on the μTESLA [13]), and every node can verify the broadcast messages.

4.2 Overview

In IHA, with using the associated pairwise of MACs, it filters the false reports. When we are faced with the FRIR attacks, we can reduce the energy consumption by using fuzzy logic without authentication. However, we can change the nodes into the sleep mode when they receive false reports from the compromised nodes because all the en-route nodes must spend energy just on receiving. Fig. 5. shows the use fuzzy logic in IHA.

.

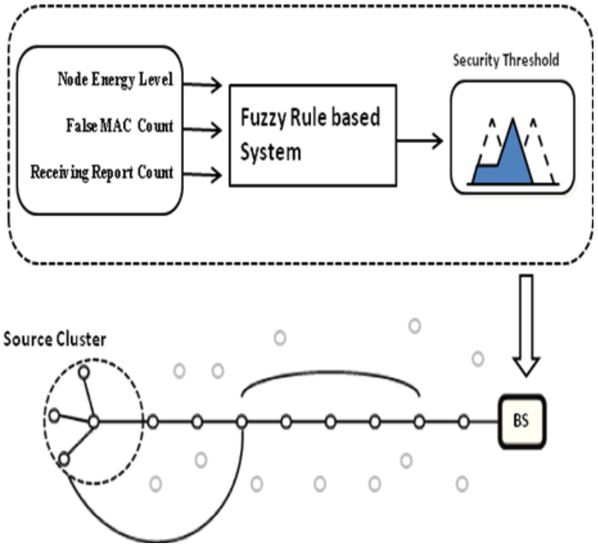
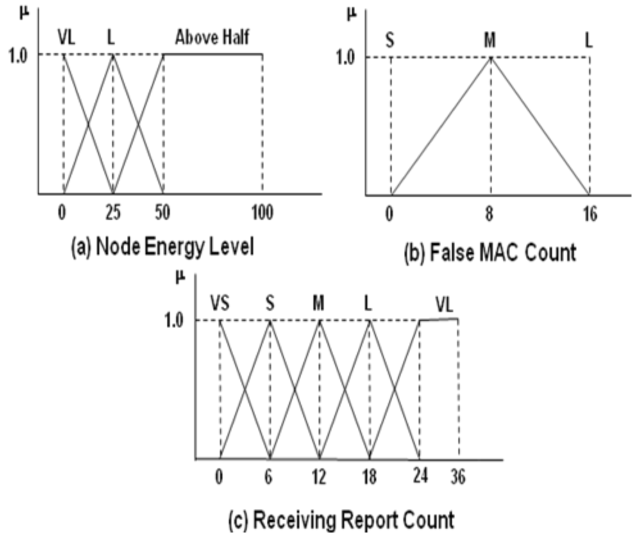


Figure 5. An IHA using the Fuzzy logic system

4.3. Fuzzy Logic Design

Fig. 5 illustrates the membership functions of three input parameters: (a) Node Energy Level (NED), (b) False MAC Count (FMC), (c) Receiving Report Count (RRC). The labels of the fuzzy variables are represented as follows:

- NED = { Very Low, Low, Above Half }
- FMC = { Small, Medium, Large }
- RRC = { Very Small, Small, Medium, Large, Very n Large }



(a) Node Energy Level

(b) False MAC Count

(c) Receiving Report Count

Figure 6. The membership functions of input

The Node Energy Level (NEL) is the most important factor because the battery is limited and it cannot be recharged. If the NEL is small, then the fuzzy logic can discard most of the false reports or the legitimate reports when it receives a number of reports.

The False MAC Count is the number of failed authentications when the two MACs do not be match.

The Receiving Report Count is the number of receiving reports.

The output parameter of the fuzzy logic is the Security Threshold = { None Mode, Drop Mode, Sleep Mode }, and this is represented by the membership function, as shown in Fig. 7 (a).

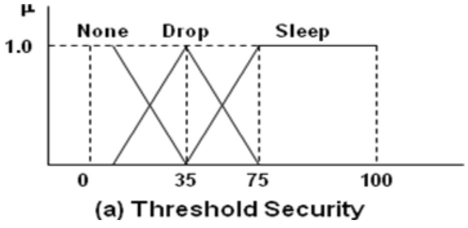


Figure 7. Membership function of output

Table 1. shows a the fuzzy-If/Then rule. In rule 25, although the FMC is in a sleeping security mode and the RRC is in a medium security mode,, the nodes don't change to the Drop mode or the Sleep mode because the NEL has enough battery power.

In rule 14, because the NEL has about 25% ~ 50% energy, the FRC is Medium and RRC is Bad, so the node discards any report.

In rule 3 because the NEL, FMC and RRC are very bad, the node doesn't receive any reports.

.

Table 1. Fuzzy rules.

Rule no.	if			Then
	Node Energy Level	False MAC count	Receiving Report Count	Security Threshold
0	VL	G	G	Sleep
1	VL	G	M	Sleep
2	VL	G	B	Sleep
3	VL	M	G	drop
4	VL	M	M	drop
5	VL	M	B	sleep
6	VL	B	G	Sleep
7	VL	B	M	Sleep
8	VL	B	B	Drop
9	L	G	G	Sleep
10	L	G	M	Drop
11	L	G	B	Drop
12	L	M	G	Drop
13	L	M	M	Drop
14	L	M	B	Drop□
15	L	B	G	None
16	L	B	M	Drop
17	L	B	B	Drop
18	AH	G	G	None
19	AH	G	M	None
20	AH	G	B	Drop
21	AH	M	G	None
22	AH	M	M	None
23	AH	M	B	None
24	AH	B	G	None
25	AH	B	M	None
26	AH	B	B	Drop

5. Simulation result

We compared the original IHA and IHA with using fuzzy logic. In the simulation background, we use a virtual sensor network that has 500 randomly distributed clusters; each cluster consists of 10 nodes.

Each node consumes 16.25/12.5 µJ to transmit/receive, respectively, a byte and each MAC consumes 15 µJ for verification [4]. The size of the original report is 24 bytes, and the MAC is 1 byte [14].

.

Fig. 8 shows the result of simulation with the original IHA and IHA with using the fuzzy logic from a FRIR attack. Fig. 8. (a), (b), and (c) shows the energy spent according to the number of FRIRs in a different NEL. We can see continuous energy being spent for authenticating and receiving in spite of filtering false reports. As result, the nodes can cause paralysis of the network as a result of the lack of energy. However, in the case of using fuzzy logic as shown in Fig. 8., the nodes drop the report by rejecting more authentications when the false reports are authenticated over 7 times under the rate of 25% energy. However, even receiving the report when false reports are replayed spends significant energy. Hence, nodes change into a sleep mode after receiving the reports over 18 times. theIn Fig. 8. each of (a), (b), and (c) shows the simulation result of the original IHA and IHA with using fuzzy logic XXXXfollowing to the rest of node energy.

.

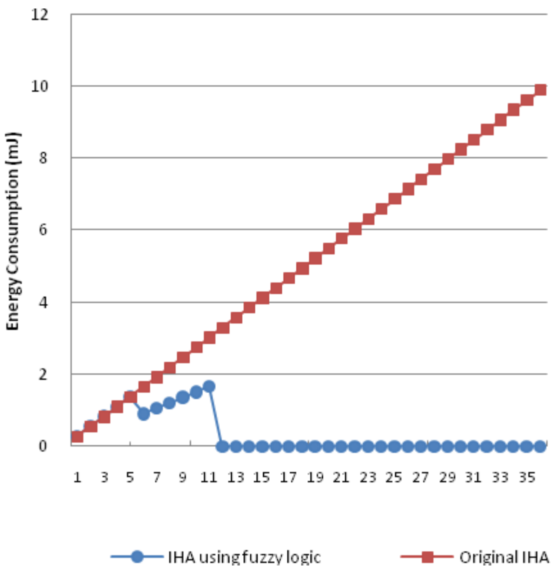


Figure 8. (a) NEL less than 25%

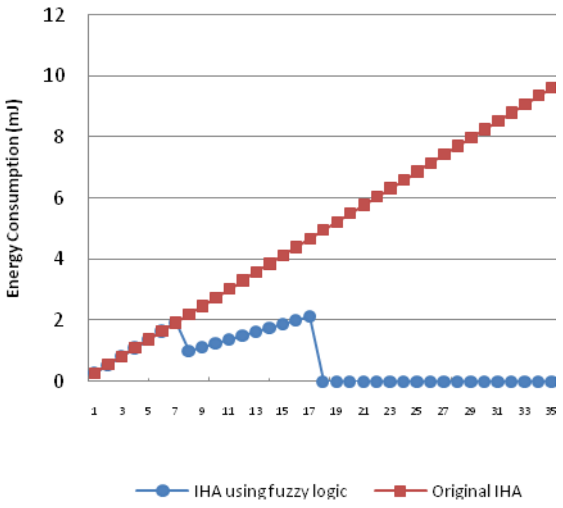


Figure 8 (b) NEL from 25% to 50%

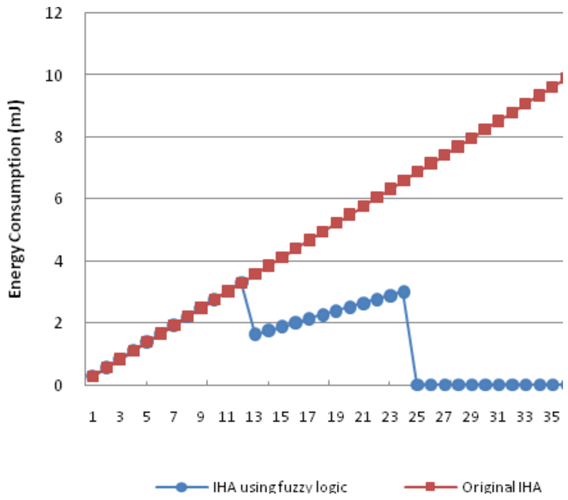


Figure 8. (c) NEL more than 50%

6. Conclusion

In this paper, we proposed a scheme using fuzzy logic in the IHA to defend against injecting false report by a replay attack. The effectiveness of the proposed method was shown by the simulation result..

Acknowledgments

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-313-D00827).

References

[1] Wang, G., Zhang, W., Cao, G., Porta, T.L.: On Supporting Distributed Collaboration in Sensor Networks. In Proc. of MILCOM (2003) 752-757

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirici, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[3] Qiangfeng jiang and Manivannan, D.: Routing Protocols in Sensor Networks. Consumer Communications and Networking Conference (2004) 93-98

[4] H.Yang, S. Lu, Commutative Cipher Based En-route Filtering in Wireless Sensor Network, in : Vehicular Technology Conf. vol. 2, 2004, pp. 1223-1227

[5] Wang, D., Xu, L., Peng, J., Robila, S. : Subdividing hexagon-clustered wireless sensor networks for power-efficiency : Proceedings - 2009 WRI International Conference on Communications and Mobile Computing, CMC 2009 2, art. no. 4797165, pp. 454-458

[6] Przydatek, B., Song, D., Perrig, A.: SIA: Secure Information Aggregation in Sensor Networks. In Proc. of SenSys (2003) 255-265

[7] Ye, F., Luo, H., Lu, S.: Statistical En-Route Filtering of Injected False Data in Sensor Networks. IEEE J. Sel. Area Comm. 23(4) (2005) 839-850

[8] Yu, Z. Guan, Y. (2005), "A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks", Proc. of SenSys, pp. 294-295, ACM.

[9] S. Zhu, S. Setia, S. Jajodia, P. Ning, An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks, security and privacy, 2004. in: Proceedings. 2004 IEEE Symposium, 2004 pp. 259–271.

[10] H.Y. Lee and T.H. Cho, Key inheritance-based false data filtering scheme in wireless sensor networks, Lecture Notes in Computer Science, LNCS vol. 4317, Springer Verlag (2006), pp. 116–127.

[11] Thao P. Nghiema, and Tae Ho Cho, "A fuzzy-based interleaved multi-hop authentication scheme in wireless sensor networks", J. Parallel Distib. Comput. vol.69, pp.441-450. May. 2009.

[12] S. Zhu, S. Setia, S. Jajodia, LEAP: Efficient security mechanisms for large-scale distributed sensor networks, in: Proc. of the 10th ACM Conf. on Computer and Communication Security, 2003.

[13] Perrig A, Szewczyk R, Tygar J D, Wen V, Culler D E. SPINS: Security Protocols for Sensor Networks. *Wirel. Netw.*, 2002, 8(5): 521-534

[14] Baeg, S.B., Cho, T.H.: Transmission Relay Method for Balanced Energy Depletion in Wireless Sensor Network using Fuzzy Logic. Lect. Notes Artif. Int. 3614 (2005) 998-1007

Jong Hyun Kim received his B.S. degree in Computer Science from Dan-Kook University, Republic of Korea, in February 2009. He is currently a graduate student in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include wireless sensor networks, intelligent systems, and security.

Tae Ho Cho received his 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 system, modeling & simulation, and enterprise resource planning.