LETTER

Fuzzy-Based Adaptive Countering Method against False Data Injection Attacks in Wireless Sensor Networks*

Hae Young LEE[†a)], *Member*

SUMMARY This letter presents a method to adaptively counter false data injection attacks (FDIAs) in wireless sensor networks, in which a fuzzy rule-based system detects FDIAs and chooses the most appropriate countermeasures. The method does not require en-route verification processes and manual parameter settings. The effectiveness of the method is shown with simulation results.

key words: *wireless sensor networks, network security, intrusion detection, false data injection attack, fuzzy logic*

1. Introduction

Wireless sensor networks (WSNs) are vulnerable to *false data injection attacks* (FDIAs) [1] in which malicious adversaries inject forged sensing reports into the networks with the goal of deceiving base stations (BSs) or draining limited energy resources of forwarding nodes (Fig. 1). To counter FDIAs, researchers have proposed security solutions [1]–[3] in which forged reports can be detected and discarded by forwarding nodes. However, especially under normal situations, these solutions are inefficient in terms of energy saving since they involve en-route verification processes [4].

This letter presents a fuzzy-based method to adaptively counter FDIAs in WSNs for object-tracking applications. A fuzzy rule-based system is exploited to determine FDIAs and to choose the most energy-efficient countermeasures at the same time. A countermeasure is activated only when it is chosen by the fuzzy system. Under normal situations, the method can conserve energy resources since the method does not require forwarding nodes to verify reports. Thanks to the adaptive selection of countermeasures, it can save extra energy resources also in the case of FDIAs. Moreover, the membership functions of its fuzzy system can be determined automatically [5], so that it does not need manual parameter settings. Simulation results show the effectiveness of the method.

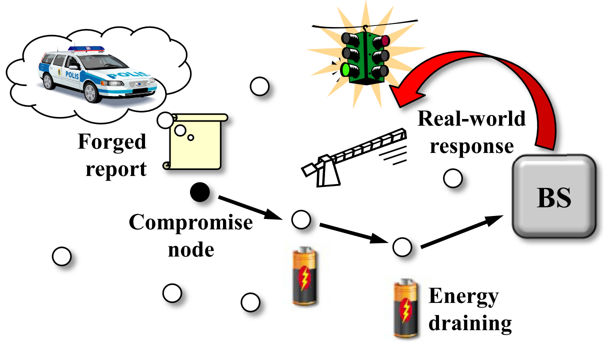

Fig. 1 False data injection attacks (FDIAs).

2. False Data Injection Attacks & Countermeasures

To minimize grave damage from FDIAs, researchers have proposed security solutions, such as the statistical en-route filtering (SEF) [1], the interleaved hop-by-hop authentication (IHA) [2], and the key index-based routing (KIR) [3]. These solutions require that every sensing report should include multiple message authentication codes (MACs) generated by different detecting nodes. While a report is being delivered to a BS, some forwarding nodes verify the legitimacy of the MACs attached in the report. If the verification fails, the report is dropped immediately. However, in terms of energy saving, they all are inefficient under normal situations since such en-route verification processes involve extra communication and computation overhead [4]. Therefore, centralized solutions, such as the adaptive countering scheme (ACS) [4] and the fuzzy-based FDIAs detection (FFD) [6], have been recently proposed to minimize the energy consumption due to the verification processes. They detect FDIAs through the analysis of reports collected at BSs, so that forwarding nodes need not to verify the legitimacy of MACs. However, each of them has still some flaws. ACS requires the users to determine multiple threshold parameters used for the detection of FDIAs. Although FFD can detect FDIAs without the determination of the parameters, it does not provide the ability to counter the detected FDIAs.

3. Fuzzy-Based Adaptive Countering Method

A large-scale high-density WSN for tracking of moving objects (e.g., vehicles) is considered. Each moving object appears/disappears on the border of the field and is continuously moving within the field. The object can be detected by multiple nodes at the same time. Every node has a unique

Manuscript received May 2, 2013.
Manuscript revised October 28, 2014.

[†] The author is with the Department of Information Security, Seoul Women's University, Seoul 139–774 Republic of Korea.

[*] This work was supported by a special research grant from Seoul Women's University (2015). This research was partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (NRF-2013R1A1A1006542).

a) E-mail: sofware@swu.ac.kr

DOI: 10.1587/transinf.2013EDL8110

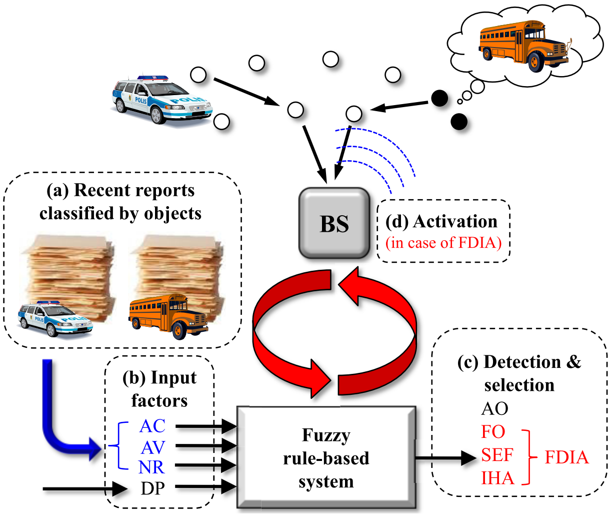

Fig. 2 Adaptive countering procedure.

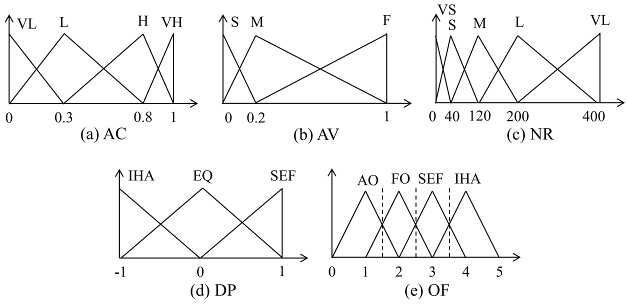

Fig. 3 Optimized fuzzy membership functions.

key shared only with the BS and some other keys for SEF [1] and IHA [2]. When a node has detected an object, it generates a sensing report for the object. A single MAC generated using its key is attached into the report. The report is then delivered to the BS through multiple hops. A malicious adversary can physically capture a few nodes and use them to launch FDIAs. However, the BS cannot be compromised.

The proposed method detects and counters FDIAs with the procedure shown in Fig. 2. It is loaded on the BS. (a) For each object of interest, the associated sensing reports are stored in a buffer at the BS for a certain period of time T. (b) Using four factors (three factors derived from the reports and a fixed one), a fuzzy rule-based system periodically determines whether the object is legitimate. (c) In case of an FDIA, the most energy-efficient countermeasure (either SEF or IHA) against the attack can be chosen by the fuzzy system simultaneously. (d) Finally, the chosen countermeasure is activated.

For each object, the fuzzy system uses the following four factors for the inference.

- The average correctness of the reports (AC): If all the reports for the object in the buffer are legitimate, ACR for the object is 1.0. This factor is used to determine FDIAs. If it is almost zero, we could consider that an FDIA has been launched without using compromised nodes (probably with the goal of depleting the energy resources). Also, the factor should be considered in the countermeasure selection since it largely determines the efficiency of the countermeasures in terms of energy conserving [7].
- The average velocity of the object (AV): The end-to-end distance between the final location of the object and the initial one of that for T is used to determine FDIAs. In general, the average velocity of each type of objects can be estimated. It is not easy to make non-existing objects moving using a few compromised nodes, so that objects moving very slowly could be a signature of FDIAs [4].
- The number of the reports (NR): NR is used to determine FDIAs. Generally, NR for each type of objects can be estimated based on T and AV. If too many reports have been collected for an object, they could be intentionally injected with the goal of depleting energy resources. Also, NR should be considered in the countermeasure; IHA would be more energy-efficient against a large number of forged reports, while SEF would be better in the opposite condition.
- The detection power of SEF relative to IHA (DP): The detection power of IHA is determined just by a security threshold value, whereas that of SEF is also affected by key distribution [7]. Thus, the relative power should be considered in the countermeasure selection.

Fuzzy systems can be used for approximate reasoning, so that they are particularly useful when there are imprecise data. In the proposed method, some of these parameters (especially AC) could be imprecise due to malfunctioning of nodes. Thus, approximate reasoning is needed to handle such fuzzy information.

The output of the fuzzy system (OF) can be:

- AO (actual object): The object is legitimate.
- FO (forged object): The object is forged by an FDIA. But the activation of a countermeasure is not recommended in terms of energy saving.
- SEF: The object is forged. SEF is recommended.
- IHA: The object is forged. IHA is recommended.

If the output of the fuzzy system is FO, SEF, or IHA, the method immediately notifies the users of the occurrence of the attack. If the output is SEF or IHA, it activates the chosen countermeasure against the attack simultaneously.

Figure 3 shows the fuzzy membership functions, which were optimized by the genetic algorithm-based optimization method (GAOM) [5] with the consideration of the characteristics of a given network. Note that the membership functions for OF are fixed (i.e., target-independent) and thus not determined by GAOM. The labels of the fuzzy variables are as follows:

- AC = {VL (very low), L, H, VH (very high)}
- AV = {S (slow), M (medium), F (fast)}
- NR = {VS (very small), S, M (medium), L, VL (very large)}
- DP = {IHA (the detection power of IHA is better than that

of SEF), EQ (equivalent), SEF}

The fuzzy system has (AC) 4 × (AV) 3 × (NR) 5 × (DP) 3 = 180 rules. Some of them are listed in Table 1. Rule 22, for example, can be read as, for an object, "if AC is VL and AV is M and NR is M and DP is IHA, then OF is AO."

These rules are derived from the features of the four input factors. For example, very high AC could be considered a signature of a real object (Rule 22). However, if AC is very high but AV is slow, the object would be forged by an FDIA using a few compromised nodes (Rule 45). Very low AC would indicate that an FDIA has been launched without node compromise (Rules 155 and 179). A very large NR could be also a signature of an FDIA on energy resources (Rules 107 and 137). If most reports for an object are incorrect (i.e., very low AC), SEF would be enough for the early detection of forged reports (Rule 155). But if not, the deterministic detection capability of IHA could be energy-efficient (Rules 107 and 110), unless the detection power of SEF is better than that of IHA (Rule 111). In case of an FDIA, IHA would be more energy-efficient against a very large NR since it can detect a forged report within a few hops (Rule 107 and 137). When NR is medium, SEF could save more energy resources (Rule 113). However, we would like not to activate a countermeasure for energy saving if NR is very small (Rules 45 and 179).

Table 1 Fuzzy if-then rules.

Rule	IF				THEN
	AC	AV	NR	DP	OF
22	VH	M	M	IHA	AO
45	VH	S	VS	SEF	FO
107	L	M	VL	EQ	IHA
110	L	M	L	EQ	IHA
111	L	M	L	SEF	SEF
113	L	M	M	EQ	SEF
137	VL	F	VL	EQ	IHA
155	VL	M	L	EQ	SEF
179	VL	S	VS	EQ	FO

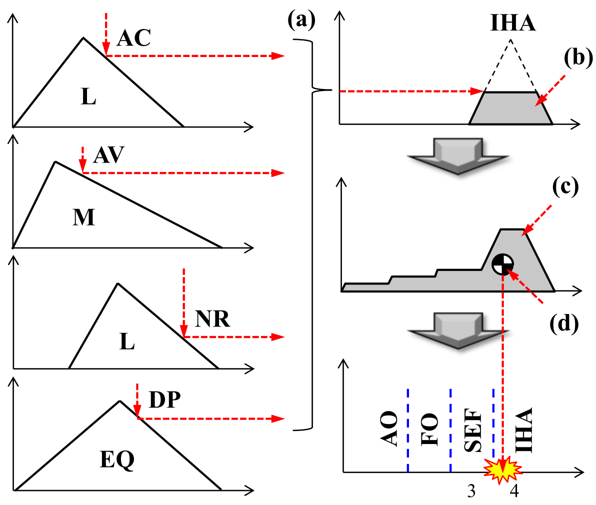

Fig. 4 Fuzzy inference procedure.

For an object, the inference procedure of the fuzzy system is as follows: First, for each rule, (a) the matching degree of the inputs is computed (the fuzzification of the inputs). Then, (b) the conclusion of the rule is generated by clipping the membership function corresponding to the then-part of the rule. Next, (c) the conclusions of all the rules (i.e., at most 180 conclusions) are combined into a single one. Finally, (d) the output of the fuzzy system is obtained by finding the center of gravity in the combined conclusion (i.e., through defuzzification). The final decision is made based on the output and the pre-defined threshold values shown as vertical dotted lines in Fig. 3 (e). In Fig. 4, the output of the fuzzy system is greater than 3.5. Thus, the system finally concludes that the object is forged and IHA is recommended.

Compared to ACS [4], the method can reduce space complexity as well as the detection errors. Moreover, it can be optimized by GAOM, so that the users need not to determine threshold parameters for the detection. Compared to FFD [6], the method can enhance the detection power slightly. Moreover, it can provide the ability to adaptively counter the detected FDIAs. Thus, in case FDIAs, extra energy resource saving can be achieved.

4. Simulation Results

To show the performance of the proposed method, the method has been compared with ACS and FFD through simulations. The size of a sensor field is 1,000 × 100m^2 and a BS is located at the end of the field. Every object appears/disappears on the border of the field and is continuously moving on the field. On average, an object can be detected by 15 nodes simultaneously. The fuzzy system of the method was optimized for the network using GAOM.

False positive error rate (FPER) and false negative error rate (FNER) in the detection of FDIAs were measured. Figure 5 shows FPER (circles) and FNER (rectangles) of ACS (empty ones), FFD (gray ones), and the method (filled ones) when T is between 40 and 200. As shown in the figure, FPER and FNER could be reduced as T increased since

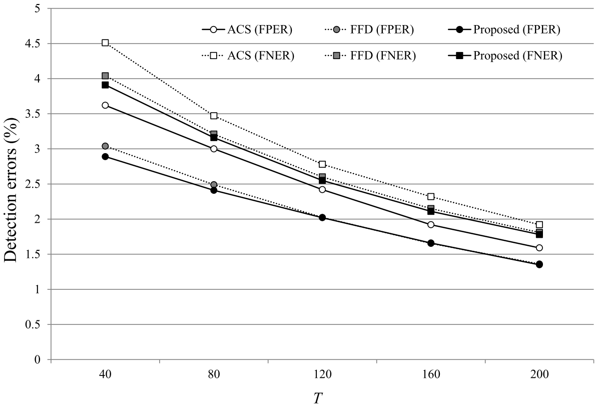

Fig. 5 Detection performance of the proposed method.

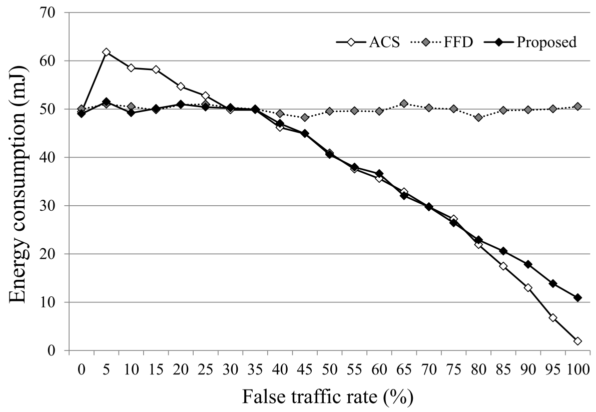

Fig. 6 Energy-efficiency of the proposed method.

they use data stored in the buffers for the detection. However, a large T would increase the detection time and space complexity. Compared to ACS, the method could reduce FPER and FNER thanks to the approximate reasoning provided by the fuzzy system. It would be particularly useful when T is small. Also, the method could reduce extra FPER and FNER than FFD due to the use of different factors.

Figure 6 shows the average energy consumption per report when the rate of false traffic (FTR) is between 0% and 100%. As shown in the figure, FFD (gray diamonds) did not provide any ability to counter the detected attacks. Both ACS (empty diamonds) and the proposed method (filled diamonds) could provide the adaptive countering ability against FDIAs. However, ACS activated countermeasures unnecessarily in case of very small FTR (i.e., very large AC), so that extra energy resources were consumed. In contrast, the proposed method did not activate a countermeasure in order to achieve further energy saving.

5. Conclusions

This paper presented a fuzzy-based method to adaptively counter FDIAs in WSNs. Based on four factors, a fuzzy system determines FDIAs as well as the most appropriate countermeasures. Compared to the existing solutions [6], [7], the method can reduce the detection error and space complexity. Also, manual parameter settings are not required since the fuzzy system can be automatically optimized.

Acknowledgments

The author would like to thank Tae Ho Cho and Hyung-Jong Kim for their valuable comments on the paper.

References

[1] F. Ye, H. Luo, and S. Lu, “Statistical en-route filtering of injected false data in sensor networks,” IEEE J. Sel. Areas Commun., vol.23, no.4, pp.839–850, April 2005.

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “Interleaved hop-by-hop authentication against false data injection attacks in sensor networks,” ACM Trans. Sensor Netw., vol.3, no.3, article no.14, Aug. 2007.

[3] S.Y. Moon and T.H. Cho, “Key index-based routing for filtering false event reports in wireless sensor networks,” IEICE Trans. Commun., vol.E95-B, no.9, pp.2807–2814, Sept. 2012.

[4] H.Y. Lee and T.H. Cho, “A scheme for adaptively countering application layer security attacks in wireless sensor networks,” IEICE Trans. Commun., vol.E93-B, no.7, pp.1881–1889, July 2010.

[5] H.Y. Lee and T.H. Cho, “Optimized fuzzy adaptive filtering for ubiquitous sensor networks,” IEICE Trans. Commun., vol.E94-B, no.6, pp.1648–1656, June 2011.

[6] H.Y. Lee, T.H. Cho, and H.-J. Kim, “Fuzzy-based detection of injected false data in wireless sensor networks,” Communications in Computer and Information Science, vol.76, pp.128–137, June 2010.

[7] H.Y. Lee and T.H. Cho, “Fuzzy adaptive selection of filtering schemes for energy saving in sensor networks,” IEICE Trans. Commun., vol.E90-B, no.12, pp.3346–3353, Dec. 2007.