Adaptive Key Diffusion Restriction Method for Dynamic Filtering in Sensor Networks Based on Fuzzy Logic

Man Ho Han, Sang Jin Lee, Tae Ho Cho
School of Information and Communication Engineering
Sungkyunkwan University
300 Cheoncheon-dong, Jangan-gu
Suwon 440-746, Korea
{mhhan, sjlee, taecho}@ece.skku.ac.kr

Abstract: - Wireless sensor networks are vulnerable to false data injection attacks, because they are disseminated in hostile environments. Adversaries can inject false report into the network using compromised nodes, with the goal of deceiving the base station and draining the energy resource of forwarding node. The dynamic en-route filtering scheme (DEF) can detect and drop false data for the forwarding process. In this scheme the select of threshold value that restricts the key diffusion is important since it represents a trade-off between detection power and overhead. A large threshold value increases probability that detect false reports, but it consumes too much energy in the key diffusion phase. In this paper, we proposed adaptive key diffusion restriction method with fuzzy-based framework for DEF. A fuzzy-based system controls the adaptive threshold value of DEF through practical factors. The proposed method can provide energy saving and sufficient resilience against false data injection attacks and show simulation.

Key-Words: - wireless sensor network, false data inject attack, fuzzy-based system, dynamic en-route filtering scheme

1 Introduction

Recently wireless communications and electronics have enabled the development of small, low-cost, low-energy, multifunctional sensor nodes. Sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of a large number of sensor networks [1]. Wireless sensor network consist of a large number of sensor nodes that have limited processing power, small storage space, narrow bandwidth and limited energy, and a few base stations that collect the sensor readings. Sensor nodes are usually scattered in unattended area and can communicate either among each node or directly to an external base station [2].

Sensor nodes are vulnerable to physical attacks, potentially compromising the node’s cryptographic keys since they are deployed in open environments with many applications [3]. Forged sensing reports can be injected through compromised nodes, which can not lead only false alarms but also the depletion of limited energy resource in battery powered networks (Fig. 1) [4].

To minimize damage, forged reports should be dropped en-route as early as possible, and few eluded ones should be further rejected at the base station (BS) [5]. False data injection attacks may cause energy and false alarms in sensor network.

Various security solutions [4-8] and adaptive methods [9-12] have been proposed to detect and drop false reports before the data consume a significant amount of energy. One of the these solutions is the dynamic en-route filtering scheme (DEF) proposed by Yu and Guan [6]. In this sheme, the select of a threshold value, that restricts the key diffusion is important since it represents a trade-off between detection power and overhead. A large threshold value increases probability that detect false reports, but it consumes too much energy in the key diffusion phase.

In this paper, we proposed adaptive key diffusion restriction method with fuzzy-based framework for DEF. A fuzzy-based system controls the adaptive threshold value of DEF through practical factors.

The remainder of the paper is organized as follows: Section 2 briefly describes DEF. Section 3 describes the...
proposed method in detail. Section 4 reports the simulation results. Finally, the conclusion is discussed in Section 5.

2 Dynamic En-Route Filtering (DEF)

Yu and proposed DEF[6] that is able to detect and drop false data en-route. Compared to existing filtering schemes, DEF is able to better deal with dynamic topologies of sensor networks and exceeds them in term of energy efficiency, especially for large sensor networks. (i.e., a network consists of a large number of clusters).

DEF consists of three phases: the pre-deployment phase, post-deployment phase, filtering phase. In the pre-deployment phase, each sensor node is preloaded with a seed authentication keys and \((l + 1)\) secret keys which is randomly picked form a global key pool. This phase is performance just one time. In the post-deployment phase, every cluster node encrypted its authentication key using its \((l + 1)\) secret key, then sends the encrypted its authentication key to its cluster head (CH) (Fig. 3(a)). Each cluster head disseminates the authentication keys, collected from its cluster node, to forwarding nodes (Fig 3(b)). When a forwarding node accepts the authentication keys, it decrypts the keys using its own \((l+1)\) secret key, if its secret key happens to be the same as the secret key used to encrypt one of the keys. In the filtering phase, forwarding nodes detect and drop false data (Fig 3(c)). After the dissemination of the keys, a cluster head is able to send the data of several events by aggregating message authentication codes (MACs) generated by its cluster nodes using their authentication keys. Each data ought to contain distinct MACs of those cluster nodes.

Suppose that an adversary has compromised a cluster head as shown in Fig. 3(c). It can inject false data through the cluster head. The false data may be forwarded by G1 and G2, since it has compromised N6, and G2 does not have an authentication key shared with a cluster node. However, the data may be detected and dropped by node G3, since it may not have N3.

3 Key Diffusion Restriction Method

In this section, we decribe the proposed Method in detail.

3.1 Assumptions

We consider that a sensor networks is composed of a large number of small sensor nodes. We assume that sensor nodes form a number of clusters after deployment. We also assume that BS can know or estimate the average network energy level and distance from the BS to the cluster. The BS also knows a number of authentication keys in each cluster, in addition, it has mechanism to authenticate broadcast message, and every sensor node is able to verify the broadcast messages. We futher assume that BS can not compromised.

3.2 Overview

Fig. 4 depicts the proposed method. Our proposed method is based on the DEF. BS periodically determines adaptive threshold using fuzzy-based system to determine an efficient adaptive threshold when the network configuration is changed or needed to changed.
An efficient adaptive threshold is able to be achieved through sufficient detection ability, whilst conserving energy consumption. The rate of false reports rejected by BS (FRR), distance from BS to that cluster (DS), and value of the key diffusion restriction (KDR) are used to determined adaptive threshold. Adaptive threshold is changed by KDL and KDL is periodically changed. The BS broadcasts determined adaptive threshold to the corresponding cluster.

![Fig. 4 Overview of proposed Method](image)

### 3.3 Input parameters

We consider three input parameters: value of the key diffusion restriction (KDR), rate of false reports rejected by BS (FRR), and distance from BS to that cluster (DS). The value of the key diffusion restriction (KDR) is considered that it can estimate the adaptive threshold and compare previous adaptive threshold.

The rate of false reports rejected by BS (FRR) is considered. Small FRR indicates that a large number of false reports have been dropped before arriving at the BS. The filtering scheme provides sufficient detection capability, even if an adversary is attack the network.

The distance from BS to that cluster (DS) should be considered that it conserve the network energy and enable efficient key diffusion. Sensor nodes near the BS consume less energy than other nodes in forwarding reporting reports to the BS and used as a path that leads to the BS. Thus, we have to adjust adaptive threshold to conserve energy and reduce the overhead of diffusion messages.

### 3.4 Fuzzy Logic Design

Fig 5 illustrates the membership functions of three input parameters: (a) FRR, (b) DS, and (c) KDR. The labels of the fuzzy variables are represented as follows:

- FRR = { F (Fine), N (Normal), B (Bad) }
- DS = { N (Near), AR (Around), AW (Away) }
- KDR = { D (Decrease), H (Hold), I1 (Increase by one), I2 (Increase by two), TO (Turn Off) }

The output parameter of fuzzy-based system is $P_{KDR} = \{ D \ (Decrease), \ H \ (Hold), \ I1 \ (Increase \ by \ one), \ I2 \ (Increase \ by \ two), \ TO \ (Turn \ Off) \}$, which is represented by the membership function as shown in Fig. 5 (d)

Selected fuzzy if-then rules are shown in the Table 1. If ERR is B, DS is AW, KDR is I2, then we should turn off $P_{KDL}$ (Rule 09).

![Table 1: Fuzzy if-then rules](image)

### 4 Simulation Results

We compare the proposed method and DEF using simulation to show the effectiveness of the proposed method. Each cluster consists of 10 sensor nodes. Each node consumes 16.25, 12.5μJ to transmit/receive a byte and each MAC generation consumes 15μJ [4]. The size of the original data is 24 bytes and the size of a MAC is 1 byte.
We compare to the original DEF ($h_{\text{max}} = 2, 5$), and proposed method. The initial value of $h_{\text{max}}$ in proposed method is two, but it is adaptive change by fuzzy-base system. The original DEF (ODEF) has static value of $h_{\text{max}}$.

Fig. 6 shows the Average energy consumption between ODEF and Proposed method. The proposed method is more efficient in energy consumption, than ODEF ($h_{\text{max}} = 5$).

Fig. 7 shows the rate of filtered reports caused by false reports. As shown in figure, the proposed method is more efficient in filtering out false reports, than ODEF ($h_{\text{max}} = 2$). The proposed method can conserve more energy than ODEF ($h_{\text{max}} = 5$). Fig. 8 show the average number of hops that a filtered report traveled. As shown in figure, the proposed method can detect false reports earlier than ODEF ($h_{\text{max}} = 2$). The proposed method can conserve more energy than ODEF ($h_{\text{max}} = 5$).

In conclusion, we compare ODEF that is more efficient in some aspect than proposed method. On the other hand, proposed method is more efficient in filtering out false reports than ODEF.

5 Conclusion

In this paper, we proposed an Adaptive Key Diffusion Restriction Method for DEF. In the proposed method, Adaptived threshold is adaptively determined by a fuzzy-based system with the consideratin of FRR, DS, and KDR. The proposed method can conserve energy and provide sufficient. Simulation results show that the proposed method is able to filtering out false reports, while it provides sufficient resilience.

6 Acknowledgments

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

References:


Fig. 6 Average energy consumption

Fig. 7 The filtered reports ratio

Fig. 8 Average traveled hops of forged reported


