IEICE TRANS. INF. & SYST., VOL.E92–D, NO.8 AUGUST 2009

LETTER

Fuzzy-Based Path Selection Method for Improving the Detection of False Reports in Sensor Networks

Hae Young LEE[†] ***and*** **Tae Ho CHO**[†a)]**,** ***Members***

SUMMARY This paper presents a fuzzy-based path selection method for improving the security level, in which each cluster chooses paths based on the detection power of false data and energy efficiency.

key words: *ubiquitous sensor networks, security attacks, secure routing, false data injection attacks, fuzzy logic*

1. Introduction

In many applications, ubiquitous sensor networks (USNs) are deployed in open environments. Consequently, they are vulnerable to false data injection attacks [1] in which an adversary injects false sensing reports into the network, through compromised nodes, with the goal of deceiving the base station (BS) or draining the limited energy resource of the network's nodes. The dynamic en-route filtering scheme (DEF) [2] can filter out such false reports en-route, before they consume a significant amount of energy. In DEF, each node's cryptographic keys, which are used to verify sensing reports, are disseminated to some of their neighboring nodes, before setting up routing paths. Thus, the detection power of false reports is largely determined by the selection of routing paths.

In most routing protocols (e.g., the minimum cost forwarding; MCF [3]), routing paths are chosen by considering only energy efficiency factors, such as distance and energy level. However, under some security attacks, such paths may waste more energy resource than the unchosen ones. For example, some of the chosen paths cannot filter any single false report out during the forwarding process, so that a significant amount of energy would be exhausted. Therefore, routing paths should be chosen with the consideration of both the security level and energy efficiency.

In this paper, a fuzzy-based path selection method (FPSM) is proposed for improving the false data detection power of routing paths in the DEF-based USNs. Each control message to set up routing paths includes the key possession information of the forwarding nodes so that the detection power of the paths can be subsequently measured. Therefore, routing paths can be chosen with the consideration of the security level and energy efficiency. A fuzzy rule-based system is exploited to evaluate the fitness of paths due to uncertainty in the reasoning process.

Manuscript received March 27, 2009.
Manuscript revised April 16, 2009.

[†]The authors are with School of Information and Communication Engineering, Sungkyunkwan University, Suwon 440–740, Republic of Korea.
a) E-mail: taecho@ece.skku.ac.kr (Corresponding author.)

DOI: 10.1587/transinf.E92.D.1574

2. Dynamic En-Route Filtering Scheme (DEF)

In DEF, each sensor node is preloaded with a single cryptographic key, which is used to endorse and to verify sensing reports, before it is deployed. After node deployment, the nodes form a number of clusters, and each of them randomly *disseminates* its keys to some of its neighboring nodes within h_{max} hops, as shown in Fig. 1. When an event occurs in a cluster after the key dissemination, the cluster nodes collaboratively generate a sensing report and endorse the report by attaching the multiple message authentication codes (MACs) generated using their keys. As the report is forwarded toward the BS through multiple hops, each forwarding node verifies some of the MACs carried in the report, if it has any of the keys used to generate those MACs.

In DEF, the choices of the routing paths are very important since they largely determine the detection power of false reports. For example, in Fig. 1, the upper path has more detection power than the lower path since the forwarding nodes on the upper path have one more key for verification disseminated from the cluster, compared to the nodes along the lower path. Thus, in terms of security, the cluster should choose the upper path if the network exploits a single-path routing protocol. However, in most routing protocols, routing paths are chosen without the consideration of such security factors.

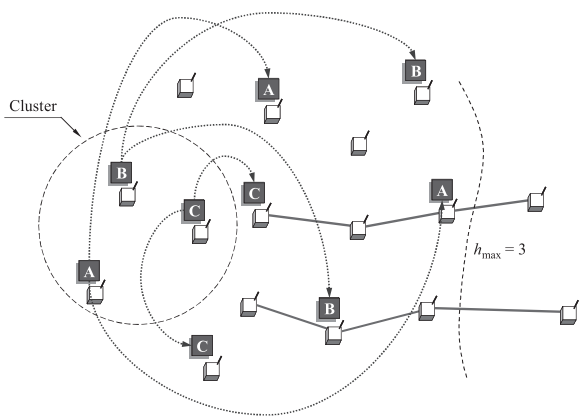

Fig. 1 Key dissemination in DEF.

3. Fuzzy-Based Path Selection Method (FPSM)

After the key dissemination phase of DEF, the routing paths are established by flooding a control message, which the BS broadcasts. This fashion is commonly used in most routing protocols at the initial establishment of the paths [3], [4]. A control message generally includes the sender ID, the number of hops from the BS, and the energy level of the forwarding nodes. In the FPSM, a queue (a sliding array) of key IDs is additionally attached to each control message and this is used to record the key possession information of the forwarding nodes. The size of the queue is a design parameter, which is determined by the network designer.

When a node receives a control message, it stores the sender ID, the distance (the hop count), the energy level, and the key possession information attached in the message. The stored information is used to measure the detection power and energy efficiency of the incoming paths. If the received message is the first instance of the control message, the node inserts the IDs of the keys used for the report verification (called *verification keys*) into the head of the queue, and removes the tail of the queue in the message. The node increases the hop count in the message, and then forwards the updated control message.

Figure 2 shows how a queue can be updated as a control message propagates. For simplicity, it is assumed that each node can have only a single verification key. When node (a) receives a control message, it stores the information attached in the message. If the received message is the first instance of the message, the node inserts the ID of the verification key, 'A', into the head of the queue in the message, and removes the tail of the queue, 'F.' Then, it increases the hop count of the message and forwards the updated message. Node (b) stores the information when it receives the message from node (a). If the message is the first instance, the node updates the information of the message and then forwards the message. The cluster in the figure may receive the two instances of the message. The detection power of the paths can be measured using the stored queues. In terms of security level, the cluster should choose the upper path since the queue (c) from the upper path contains one more verification key than the queue (d) from the lower path.

After the flooding of a control message, for each cluster, one of the cluster nodes evaluates the fitness (f) of incoming paths, using a fuzzy rule-based system, as shown in Fig. 3. To evaluate the fitness of a path, the detection power (DP) of the path, the distance (DI) from the BS, and the energy level (EL) of the path are used. DP = 1.0 indicates that the nodes along the path posses all the verification keys of the cluster. The path with the highest fitness value is chosen for the data routing. In multi-path routing, multiple paths can be chosen based on the fitness evaluation results.

The FPSM exploits a fuzzy-rule based system in order to evaluate the fitness of the incoming paths since there is uncertainty in the reasoning process. It can be argued that each node can perform such fuzzy computations and so the fuzzy system would be implemented on a small node, using hard-coding which can reduce the size of the codes. The membership functions of the fuzzy system are illustrated in Fig. 4. The input membership functions for EL and DI have been optimized by a genetic algorithm-based membership function optimizer, which was first presented in [5]. Each chromosome in a population represents a trial set of the input membership functions and is evaluated through a simulation run, as shown in Fig. 5. These chromosomes are evolved by applying genetic operators, until a termination condition has been reached. The rule base of the system comprises of 18(= $3 \times 3 \times 2$) rules. Some of the rules are shown in Table 1.

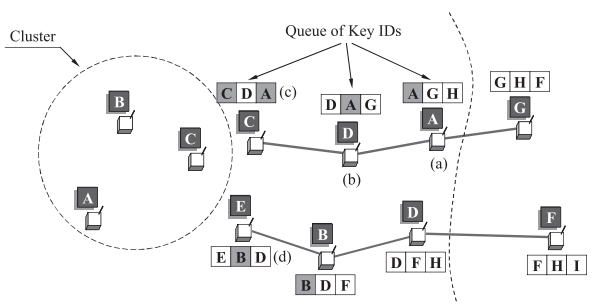

Fig. 2 Updating of a queue of key IDs.

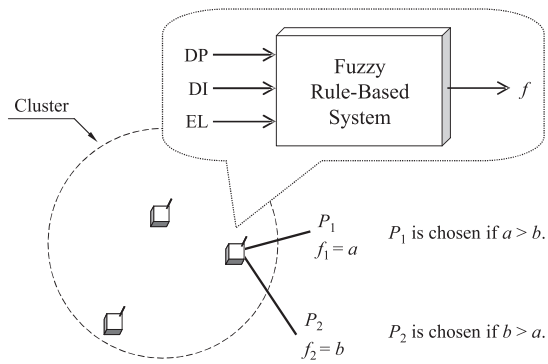

Fig. 3 Fitness evaluation of incoming paths.

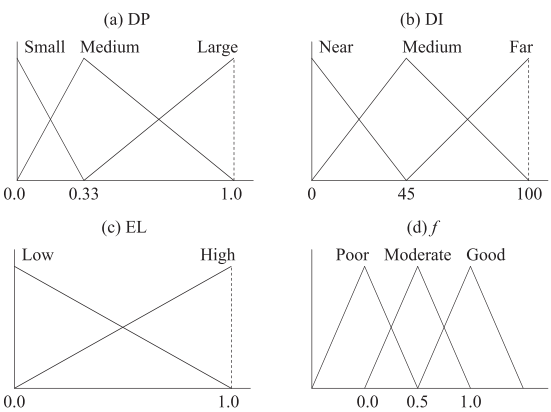

Fig. 4 Fuzzy membership functions.

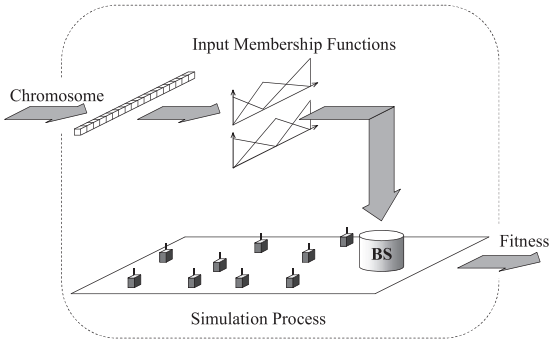

Fig. 5 GA-based membership function optimization.

Table 1 Fuzzy if-then rules.

Rule No.	Input			Output
	DP	DI	EL	f
01	Small	Near	Low	Poor
02	Medium	Near	Low	Moderate
03	Large	Near	Low	Good
04	Small	Medium	Low	Poor
05	Medium	Medium	Low	Poor

4. Simulation Results

Simulations have been used to verify the FPSM solution that has been presented in the paper. A field size of $200 \times 20\,\mathrm{m}^2$ is used, where 340 nodes are uniformly distributed. Each node takes $16.25\,\mu$J/$12.5\,\mu$J to transmit/receive a byte, and each MAC generation consumes $15\,\mu$J. The sizes of an original report and of a MAC are 24 and 1 bytes, respectively. We argue that such MAC size would be enough appropriate since each report includes multiple MACs (6 MACs in this simulation). $h_{max} = 5$, the size of a key ID is 2 bytes, and the size of a queue is 10 bytes. The results of the simulation are summarized in Table 2. During the setup phase, which consists of the key dissemination and routing path establishment, the FPSM consumes more energy resource than MCF [3], since the FPSM requires the additional information in each control message. However, the FPSM can conserve more energy resource than MCF after the setup phase, especially against false traffic, since the FPSM can detect false reports earlier than MCF. The energy-efficiency of the FPSM would increase as time elapses.

Table 2 Simulation results.

Indexes	MCF	FPSM (%)
Setup cost (J)	783.9	795.7 (101.5)
Energy consumption / legitimate report (mJ)	25.36	25.36 (100.0)
Energy consumption / false report (mJ)	11.90	9.75 (81.9)
Detected false reports (%)	72.8	78.3 (107.6)
Hop count that a false report traveled (hops)	4.10	3.39 (82.7)

5. Conclusion

In this paper, FPSM has been proposed, in which the routing paths of a cluster are chosen by a fuzzy rule-based system, with consideration of the security level and energy efficiency. A queue is used to measure the detection power of incoming paths. The effectiveness of the FPSM was confirmed by simulation results. The results show the FPSM can improve the false data detection capability of DEF, compared to MCF. The FPSM is basically designed for DEF but can also be applied to other non-deterministic filtering schemes, such as the statistical en-route filtering scheme [1].

Acknowledgements

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

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] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," Proc. INFOCOM, pp.1–12, April 2006.
[3] F. Ye, A. Chen, S. Lu, and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks," Proc. ICCCN, pp.304–309, Oct. 2001.
[4] J.N. Al-Karaki and A.E. Kamal, "Routing techniques in wireless sensor networks: A survey," IEEE Wirel. Commun., vol.11, no.6, pp.6–28, Dec. 2004.
[5] J. Kim, Y. Moon, and B.P. Zeigler, "Designing fuzzy net controllers using GA optimization," Proc. CACSD, pp.83–88, March 1994.