A Region Segmentation Based Path Selection Method for WSNs

Hyuk Park, Soo Young Moon, Tae Ho Cho,

School of Information and Communication Engineering, Sungkyunkwan University, Suwon 440-774, Korea

Summary
Routing paths are important for the network security in wireless sensor networks (WSNs). Most en-route filtering schemes predetermine routing paths using various path selection methods to protect against security threats before network operation. However, the topology of a sensor network may frequently change. Path reselection is needed to guarantee data collection when this occurs. Nevertheless, global path selection is inefficient due to the large number of message transmissions. Therefore, it is necessary to reduce the number of global path selection operations if possible. In this paper, we propose the region segmentation and regional path selection method to enable regional path selection using several distinguishing nodes. We also highlight the advantages of regional path selection method and show the effectiveness of the proposed method via simulation.

Key words:
Wireless Sensor Network, regional path selection method, Statistical En-route Filtering, false report injection attack.

1. Introduction

Recent advancements in micro-electro-mechanical system (MEMS) technology, digital electronics and wireless communication have made the development of low-cost, low-power and multifunctional small size sensor nodes possible [1]. A sensor node has sensing, computing and wireless communication modules. A sensor node also senses the changes in the surrounding environment and reports the sensing results to base stations (BSs) using these modules [1, 2].

A sensor network is made up of one or more BSs and multiple sensor nodes. Generally, wireless sensor networks (WSNs) are practical in open and unattended environments without infrastructure. Hence, numerous studies on where and how to apply them in various fields abound [3]. Conversely, the fact that WSNs operate in open and unattended environments means that they are exposed to various security threats [3-5]. Hence, there are many studies on conceivable attacks, countermeasures and how to more efficiently use constraints in which a sensor node has limited energy resources and processing power.

False report injection attack is an attack type in the application layer [6], in which a malicious adversary first takes one or more sensor nodes over from a large-scale sensor network, and then generates and injects bogus sensing reports into the network, exploiting the key information acquired from compromised modes. Once the reports are forwarded to the BS, such an attack causes false alarms and unnecessary depletion of the limited energy resources [7]. If such an attack occurs without detection, several nodes can no longer work due to the exhaustion of their finite amount of energy. Therefore, the operating time of the network is shortened [6, 7].

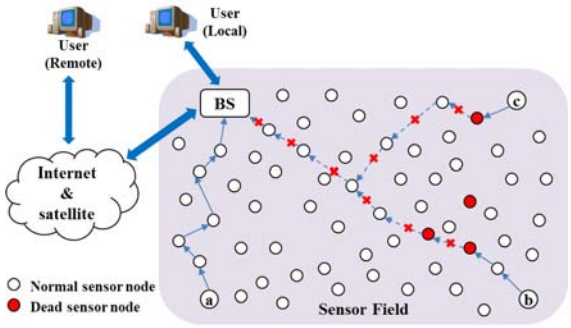

Fig. 1 Forwarding paths to report sensing data in WSN

One countermeasure is the statistical en-route filtering (SEF) [7] scheme [7-12] against injection of false data. Proposed by Ye et al., the main goal of SEF is to detect bogus sensing reports early, with low computation and low communication overhead. In the en-route filtering phase, each forwarding node verifies event reports utilizing its key information. Thus, the kinds of nodes belonging to a routing path have a decisive effect on the detection power of false data injection. Therefore, selecting routing paths is a crucial issue in en-route filtering based WSN.

Generally, the first establishment of routing path begins immediately after sensor nodes are deployed in a target field. However, the topology of a sensor network can frequently change [1]. Therefore, routing path reselection is needed repeatedly after the initial establishment. Even though there are no topology changes, for the network management, the path reselection is executed with consideration of the energy level of sensor nodes and network security. Fig. 1 shows the structure of a WSN and event report routing paths. In Fig. 1, the event report generated by node A is usually forwarded to the BS; however, the event report generated by node B and C

Manuscript received February 5, 2011
Manuscript revised February 20, 2011

are not delivered to the BS, since there are several dead sensor nodes in the paths. Even if partial flaws occur in a network, global path reselection is executed to solve them.

In this paper, we propose the region segmentation and regional path selection method to allow regional path selection using several distinguishing nodes (DNs). These DNs are dispersed in a sensor network and utilized to divide the network into sub-regions hierarchically. In addition, they perform roles that determine and manage routing paths in their regions, unlike normal sensor nodes. Using our proposed method, we can minimize the number of needless global path selections, thus the energy consumption of routing path reselection can be reduced.

The remainder of the paper is organized as follows. We briefly explain the operating process of SEF and one of the existing path selection methods in Section 2. Section 3 presents our new proposed method. Section 4 evaluates the method through simulation. Finally, Section 5 discusses future work and concludes the paper.

2. BACKGROUND

2.1 Statistical En-route Filtering (SEF)

Sensor nodes fulfill the generation of sensing reports and the en-route verification collaboratively in SEF. SEF has a characteristic in that the false report detection power of each node is decided probabilistically. The operating process of SEF can be separated into three processes: a) key assignment; b) report generation; c) en-route filtering and BS verification. Fig. 2-(a) shows a global key pool and key assignment process. The entire key information of a network is in the global key pool managed by the BS. The global key pool exists as a kind of set that is composed of numerous keys divided into several non-overlapping partitions. Each node receives a small number of keys from a randomly chosen partition before deployment to a target area. In the report generation process, first, the center-of-stimulus (COS) node is selected from among nodes sensing the same event. Then, the elected COS node collects message authentication codes (MACs) sent by the sensed nodes. Subsequently, the COS node classifies the collected MACs by partitions and reorganizes them. Finally, the COS node attaches the MACs to the sensing report. Fig. 2-(b) shows the report generation process in which nodes, sensing the same event, generate a sensing report cooperatively. After the report generation process, the sensing report is delivered to the BS via multiple hops. In this process, each forwarding node can verify the correctness of the MACs if the keys each forwarding node has are the same as one of the keys used to generate the MACs in a sensing report. As soon as a sensing report arrives at the BS, it is verified again using the entire key information of the global key pool by the BS. Fig. 2-(c) shows the process of en-route filtering and BS verification in terms of an event report.

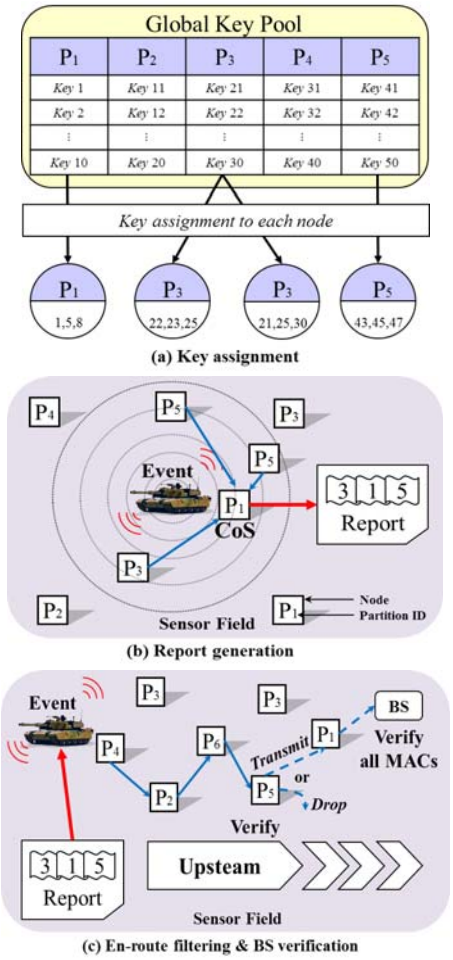

Fig. 2 SEF operation process

2.2 Existing Path Selection Method

This existing path selection method [13] is proposed to improve the detection power of false reports in SEF-based WSN. In the method, the BS floods a control message first to establish routing paths in a target field. Every node in the network receives one or more control messages, and each node determines the next forwarding node using the proposed evaluation functions based on the information stored in each control message. The two evaluation functions are as follows:

$$Q(p) = D(p) + \omega[P(p) + \sigma\{Cn\}] \quad (1)$$

$$R(p) = O(p) \cdot \frac{1}{s-1} \quad (2)$$

All information to calculate the evaluation functions, Q(p) and R(p), can be obtained from the control message, where p is a path, D(p) is the distance of p in the hop count, ω is a security parameter whose value is adjusted between 0 and 1 by the network administrator, P(p) is the number of unset columns in the check count, σ{Cn} is the standard deviation value of the elements in the check count low, O(p) is the number of overlaps among the partition IDs in the queue of partition ID, and s is the size of the queue of partition ID. Using equations (1) and (2), it is possible to grasp which nodes are in the incoming path. Smaller values for Q(p) and R(p) mean that the path has various keys in different partitions. Therefore, the one with the minimum value is selected as the optimal path among the incoming paths. Note that the smaller the values of the two evaluation functions, the better the path.

3. Proposed Method

In this section, we present the region segmentation based path selection method. First, the basic assumptions and motivation of our proposed method are provided. Then, the proposed method is described divided into three phases.

3.1 Assumptions

The basic assumptions of this paper are as follows. The network is composed of a large number of small sensor nodes and several DNs. Sensor nodes have limited energy, memory and computing power, whereas the BS and DNs do not. The path establishment phase is safe from the security threats. The BS or DNs flood a control message to establish the routing paths and the determined routing paths last, until the BS or DNs request path reselection. A control message is flooded only downstream. The network uses a single path routing protocol to send event reports, hence every sensing report is delivered to the BS only using the routing path determined by each node.

3.2 Goal and Motivation

The frequent repetition of global path selection causes the depletion of limited energy resources in networks. Thus, the goal of our proposed method reduces the number of frequent repetitions, and the global path selection is carried out when necessary. To achieve the goal, we divide the network into several sub-regions using DNs, so that the regional path selection is available by the sub-region after the initial establishment of routing paths. The initial establishment is executed hierarchically and sequentially by the sub-area, so it is possible that energy consumption drops and is limited in certain sub-regions when the routing path reselection process occurs.

3.3 Region Segmentation Based Path Selection Method

We explain the proposed method, focusing on the initial establishment phase. Key assignment is the same as for SEF in network initialization. The aforementioned evaluation functions in Section 2.2 are used for the incoming path assessment performed by each node.

3.3.1 Hierarchical WSN structure

Several DNs are deployed and fixed in the network to provide the region segmentation. In addition, the distance of BS-DN or DN-DN is regular. Fig. 3-(a) shows one possible WSN model to separate the network into several sub-areas. Moreover, the WSN model can have a hierarchical structure, as in Fig. 3-(b). The hierarchical WSN structure is completed through n steps for the division of the network into sub-regions. The target area, belonging to the first step, is divided into three sub-regions, BS-DN1, BS-DN2 and BS-DN3. Every sensor node in these sub-regions belongs to more than one sub-region. From the second step to n-1 step, the division process is carried out repetitively, as the first step between super DNs (was sub-DN at the previous step) and sub-DNs (will be super-DN in the next step). In the final n step, super DNs have no sub-DNs, so the last target area is segmented only by the last super-DNs. Note that every node deployed in the sensor field belongs to one or more sub-regions.

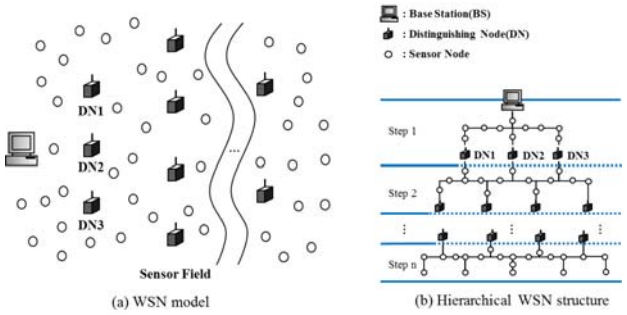

Fig. 3 Region segmentation

3.3.2 Region Establishment

The BS and each DN broadcast an advertisement message first to let sensor nodes know where they belong for region establishment. Every node uses the received signal strength indication (RSSI) that is a measurement of the power present in a received radio signal to accurately check the affiliated regions. The threshold value of the RSSI is needed when each node decides whether to regard

the region that sends an advertisement message as its region; hence, the network administrator needs to set up the threshold value before the network operates. At least, the total range formed by the threshold value covers the whole network without any isolated nodes. As aforementioned, each node knows where to belong by receiving advertisement messages from certain regions. However, even if a node receives an advertisement message from a certain region but the signal power is less than the threshold, the region is not regarded as its region. Fig. 4 shows the advertisement message broadcasting process.

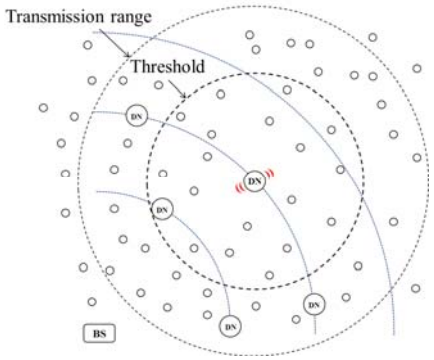

Fig. 4 Advertisement message broadcasting

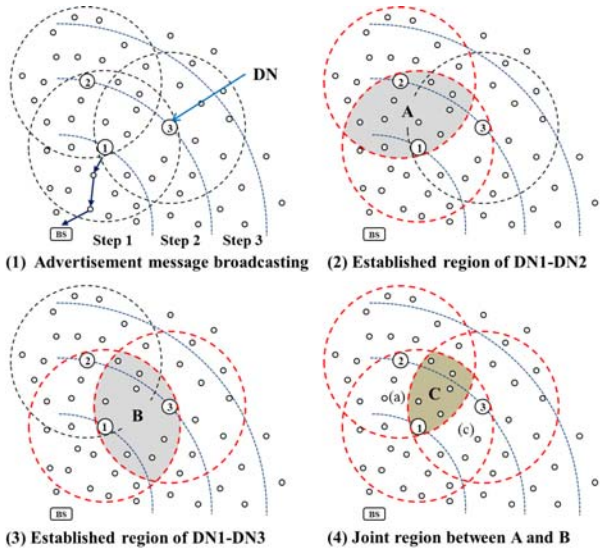

Fig. 5 Region establishment by RSSI

Fig. 5 shows the region establishment process among the three neighboring DNs in more detail. In Fig. 5-(1), the routing path between BS-DN1 is already determined through the region establishment process and the regional path selection process that is detailed in the next section. In addition, it is shown that the DN1, DN2, and DN3 are broadcasting an advertisement message. After broadcasting, the nodes that receive the messages, decide whether to join the region by comparing the received signal power and the threshold value of the RSSI. That is, if a node receives the messages from a super-DN and a sub-DN with satisfied signal power within the threshold value, then the node regards the region (super DN- sub DN) as its region. Fig. 5-(2) and (3) show the established regions of DN1-DN2 and DN1-DN3, respectively. The nodes located in region A (Fig. 5-(2)) belong to the region of DN1- DN2; in region B (Fig. 5-(3)), belong to the region of DN1-DN3; and in the region C (Fig. 5-(4)), belong to both region A and B.

3.3.3 Regional Path Selection

The BS floods a control message after the region establishment process is completed, and then every node assesses all its incoming paths based on each received control message to determine the routing path. Furthermore, this process is executed hierarchically and sequentially from the BS to the leaf nodes that are at the boundary of the network. The control message can be presented, as shown in Fig. 6. The control message can store the sender ID and the hop count as a control message is used by most routing protocols, and in addition, the super- and sub-DNs IDs, the lowest energy level (LEL), and the two additional arrays are in the control message. It is possible to know, from the arrays in the received message, what kind of nodes are in the incoming path approximately [13]. The super- and sub-DNs IDs in a region are stored in a control message, so when each forwarding node receives a control message, the received node can make sure for which region's path selection this message pertains. In the LEL, the energy level of the node that has the least energy in the forwarding nodes is stored.

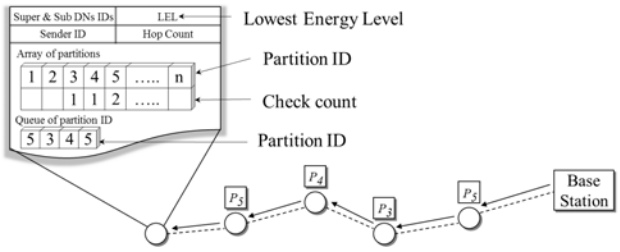

Fig. 6 Control message

When a node receives two or more different control message, the incoming paths are evaluated based on the acquired information from each control message. First, the node checks the LEL to see if the value is exceeds the minimum energy level. Before the network operates, the administrator determines the minimum energy level,

considering the period of regular path reselection. This is done to guarantee the lifetime of selected paths at least up to the next period, unless the network topology changes. After the LEL check, the incoming paths are assessed, using the evaluation functions, Q(p) and P(p), mentioned in Section 2-2. The initial establishment process is completed using the proposed method. Finally, path reselection is possible selectively the region.

4. Simulation

Simulation studies show the effectiveness of the proposed method compared to existing global path selection methods [13]. The simulation environment conditions are as follows: The size of sensor field is 575 x 575m^2, consisting of one BS, 7 DNs, and 500 to 2,500 sensor nodes. In addition, the sensor field is separated into 13 sub-regions, each of similar density. The global key pool has 10 partitions. As each partition has 100 keys, the total number of keys is 1,000. Each sensor node loads 5 keys in a certain partition and the threshold value is 5. The size of advertisement message is 1 byte the size of control message is 15 bytes. Each node takes 16.25μJ/12.5μJ to transmit/receive a byte [7, 14-15]. The BS and DNs have sufficient energy resource.

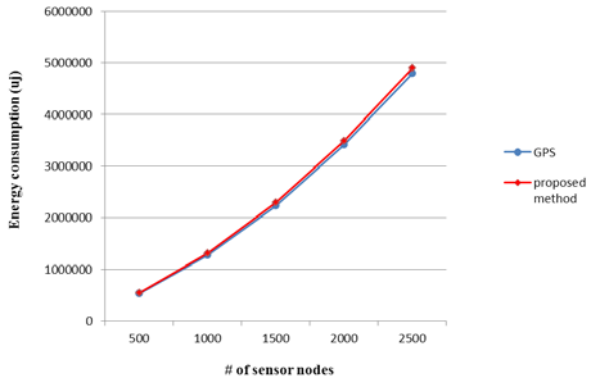

Fig. 7 Energy consumption of initial global path selection

Fig. 7 shows comparing an existing global path selection (GPS) and our proposed method in energy consumption of initial global path selection. As show in the figure, the proposed method spends more energy than GPS in drips and drips when the number of sensor nodes increase in sensor field.

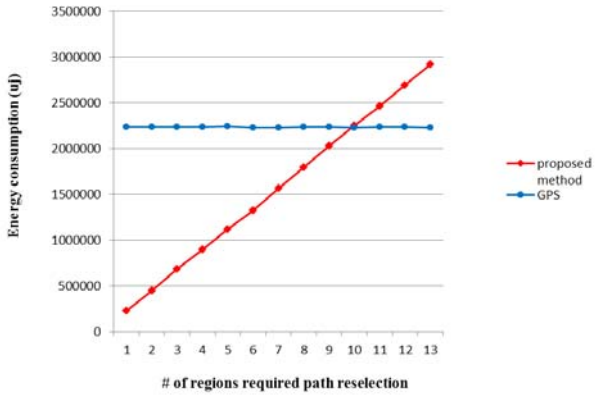

Fig. 8 Energy consumption of path reselection

Fig. 8 shows comparing GPS and the proposed method in energy consumption of path reselection when the BS requires path reselection to one or more regions. In this, the proposed method uses less energy than GPS when the required regions are fewer. Note that the proposed method is not always better than GPS.

5. Conclusion

Although global path selection is necessary, it is inefficient due to the large number of message transmissions. Hence, we proposed a region segmentation based path selection method for WSNs to reduce the number of global path selections. The WSN model using DNs and the hierarchical structure of the model are presented for the proposed method. Then, RSSI separates the network is into several sub-regions. This segmentation enables routing path selection by sub-region. Furthermore, simulations show that the proposed method can limit the amount of global path selection and reduce the energy consumption of the path reselection. Our plan for the next step is to maintain a balance between network security and energy efficiency by setting up different security power by sub-region, considering each region's environment. This will be also evaluated via simulations.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2010-0011188).

References

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. 2002. A Survey on Sensor Networks: A Survey. IEEE Communications Magazine, 40(8), 102-144.

[2] Al-Karaki, J. N. and Kamal, A. E. 2004. Routing Techniques in Wireless Sensor Networks: A Survey. IEEE Wireless Communication Magazine, 11(6), 6-28.

[3] Karlof, C. and 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.

[4] Przydatek, B., Song, D., and Perrig, A. 2003. SIA: Secure Information Aggregation in Sensor Network. In Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, 255-265

[5] Djenouri, D., Khelladi, L., and Badache, N. 2005. A Survey of Security Issues in Mobile Ad-Hoc and Sensor Networks. IEEE Communications Surveys & Tutorials, 7(4), 2-28.

[6] Zhang, W. and Cao, G. 2005. Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach. In Proceedings of 24th IEEE Annual Joint Conference on the Computer and Communications Societies, 503-514.

[7] Ye, F., Luo, H., Lu, S., and 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.

[8] Yu, Z., Guan, Y. 2010. A Dynamic En-route Scheme for Data Reporting in Wireless Sensor Networks. IEEE/ACM Transactions on Networking, 18(1), 150-163

[9] Yang, H. and Lu, S. 2004. Commutative Cipher Based En-route Filtering in Wireless Sensor Networks. In Proceedings of Vehicular Technology Conference 2004-Fall Symposium on Wireless Technologies for Global Security, 1223-1227, IEEE.

[10] Zhu, S., Setia, S., Jajodia, S., and Ning, P. 2004. An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks. In Proceedings of S&P, 259-271.

[11] Lee, H. Y. and 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.

[12] Li, F. and Wu, J. 2006. A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks. In Proceedings of International Conference on Wireless Communications and Mobile Computing, 27-32.

[13] Park, H., Sun, C. H., and Cho, T. H. 2010. A Secure Path Determination Method for Statistical En-route Filtering Based Wireless Sensor Network. In Proceedings of 3rd International Conference on Advanced Computer Theory and Engineering, V2-603-607

[14] Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., Pister, K. 2000. System Architecture Directions for Networked Sensors. In Proceedings of ACM ASPLOS IX, 93-104.

[15] Xbow sensor networks, http://www.xbow.com

Hyuk Park received his B.S. degree in E-commerce from Semyung University in 2010. He is now a master's student in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include wireless sensor networks, modeling and simulation and security in wireless sensor networks.

Soo Young Moon received his M.S. and B.S. degrees in Electrical and Computer Engineering from Sungkyunkwan University in 2009 and 2007, respectitively. He is currently a graduate 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.