Node Density Based Security Level Determining to Prolong the Lifetime of WSN through Network Conditions

Jung-sub Ahn, Tae-ho Cho

Abstract*: A wireless sensor network (WSN) consists of sensor nodes with low cost and limited performance. The energy needed for node management is important because it is difficult to manage the deployed nodes. Several traditional security protocols prevent several known attacks in WSNs, such as s false report injection attack. However, the traditional protocols do not consider the false traffic ratio and geographical environment factors. Therefore, to extend the network lifetime, a new design is needed that maintains security and considers environmental factors. This paper introduces a method to increase the energy efficiency and increase the detection rate of false reports by adjusting the security strength of the report generated at the node according to the node density and geographical location. The proposed method has the advantage that it can be applied to various security protocols based on Message Authentication Code (MAC).

***Keywords*: Wireless Sensor Network, Security Protocol, Network Lifetime Extension, Node Density.**

I. INTRODUCTION

Nodes of sensor networks that performs various missions, such as animal detection and intrusion detection, are widely and densely configured in the field [1]. Sensor node density is differently arranged according to application [2]. A WSN consists of multiple sensor nodes that are low-resource, tiny-sized, and low-cost. In a dangerous environment application like a battlefield, maintenance of the deployed node in the sensor network is difficult, and network conditions are changeful, so network resources must be managed wisely according to the network environment. In this paper, we investigate an effective energy management method according to the density of deployed nodes and the network false traffic ratio. The proposed method applies a high level of security in dangerous areas so that bogus data can be quickly detected. Therefore, the proposed method increases the filtering performance compared to the existing method, reduces the overall network energy consumption, and prolongs the network lifetime. The sensor nodes are operating for a long time at fixed places [3-5]. Consequently, they are subject to attack. An attacker causes confusion in the network by injecting bogus data into the network using a compromised node [6]. To solve this problem, several security protocols, including a Statistical En route Filtering scheme (SEF), have been proposed to improve early detection and energy efficiency [7-9,15]. The traditional schemes perform node grouping to increase the energy efficiency of a node or improve routing to raise security, but they do not consider the network lifetime.

The node deployment strategy is done in a variety of ways [10]. In WSNs, a uniform random deployment strategy is used because this deployment method is easy as well as cost-effective. However, the nodes are distributed on a location that is not known with certainty. Various studies have been conducted as a resource management approach to solve the uneven distribution of energy [11-13]. Nodes transmit their report in a hop-by-hop basis to the Base Station (BS), the collection center for the reports. Therefore, it was observed that nodes closer to the BS consumed energy faster than other nodes [14]. If the energy of the nodes closer to the BS is exhausted, the generated report from other nodes cannot reach the BS. Therefore, to prevent unnecessary energy consumption, we filter out false reports early before they reach nodes closer to the BS. We propose a method to determine the efficient security level considering the node density and network conditions. The core idea of SEF [15] is to detect the generated false reports through collaborative verification between intermediate nodes. The intermediate nodes store a set of keys and statistically verify the reports through the Message Authentication Code (MAC) included in the report. It determines whether the same key index is included in the report when the intermediate node receives the report. If the node has the same key index, the node generates a MAC using the information included in the report. This is described in detail in Section 2. Therefore, the false report verification probability depends on the number of keys included in the report. However, if many keys are included in the report, the size of the report increases, so the size of the normal report also increases. Therefore, it is desirable to adjust the security strength appropriately according to the deployment location of the node. The rest of this paper is organized as follows. We introduce background and the existing scheme in Section 2. In Section 3 we discuss the proposed scheme in detail. Section 4 provides various experimental results including energy efficiency with the proposed scheme and the existing scheme. Finally, Section 5 summarizes our conclusions and future work.

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author
Jung-sub Ahn, Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea.
E-mail: sc4217@skku.edu
Tae-ho Cho*, Department of Computer Science and Engineering, Sungkyunkwan, University, Suwon, Republic of Korea. E-mail: thcho@skku.edu

1) Check that T{ i_j, MAC_{ij} } tuple sets exist in the report; drop the report otherwise.

2) Check the T key indices { i_j, $1 \le j \le T$ } belong to T instinct partitions; drop the report otherwise.

3) If it has one key $K \in \{ K_{ij}, 1 \le j \le T \}$, it computes $M = MAC(K, L_E||t||E)$ as in Equation 1 and see if the corresponding M_{ij} is the same as M. If so, it sends the packet to the next hop; otherwise the packet is dropped.

4) If it does not have any of the keys in { K_{ij}, $1 \le j \le T$ }, sends the packet to the next hop.

Fig. 1. The four operation phases of en-route filtering

II. BACKGROUNDS

This section describes the threats model and the SEF scheme that form the basis of the proposed scheme.

A. Statistical En-Route Filtering (SEF)

Fan Ye et al proposed the SEF scheme that has the characteristics of early detection of false data reports and low computation and communication overhead [15]. This scheme allows the verification of reports during transmission by including an additional encryption code with the event content. Therefore, that prevents unnecessary energy consumption of the intermediate nodes because the verification node drops the false reports before they reach the BS. In SEF, the following three steps are performed.

1) Each normal report stores multiple MACs generated by different nodes that detect the same event.
2) Intermediate nodes check whether reports include invalid MACs and filter out bogus reports.
3) The BS verifies the correctness of all MACs in a report and removes the remaining bogus reports using a key pool.

The BS has a global key pool that contains the keys of all the nodes. The global key pool with N keys {K_i, 0<= i <= N-1} is divided into *n* partitions {N_i, 0<=i<= *n*-1}. Each node is randomly distributed with random partitions and keys and is deployed in the field. When deployed nodes detect a stimulus, they communicate with neighboring nodes cooperatively and select the node with the strongest stimulus as the report generation node. Nodes that detected an event create a MAC based on the detected content and their own key. A MAC has node location information L_E, time information *t*, event content *E*, and a key-value K_i. Also, this node encrypts a MAC with a one-way function and transmits a MAC to the representative node. The representative node creates a report using the received MAC from nodes that detected the same event. Reports with more than one key index in the same partition are not transmitted. The number of MACs to be included in the report is determined according to the preset security level of the representative node. The verification node filters with a higher probability when more MACs are included in the report. However, this method increases the report size and cost of transmitting and receiving in proportion to the number of MACs. The generated report is forwarded to the BS through hop-by-hop communication according to a preset routing path. The intermediate nodes that received the report during forwarding verify the contents of the report as below.

Each node has a probability that the node stored the same key in the report. Therefore, it is possible to detect false reports by statistically verifying the reports.

Fig. 2. shows the report's intermediate verification process. MAC_n refers to the MAC belonging to the n^{th} partition. An attacker must have as many MACs as the threshold and distinct partition to generate a completely false report using a compromised node. We assumed that *n*-1 nodes of different partitions are damaged in a situation where the threshold is *n* in Fig. 2. The attacker falsifies MAC_2 because MAC_1 and MAC_3 know. Among the forwarding nodes, a node with the same key as MAC_2 verifies the forged MAC using its own key and drops the report. This mechanism can reduce the unnecessary energy consumption of the forwarding node by interpolating false reports. The node performs the verification process repeatedly until the false report is dropped or it reaches the BS. If the report reaches the BS, the BS verifies the entire MAC of the report using its global key pool.

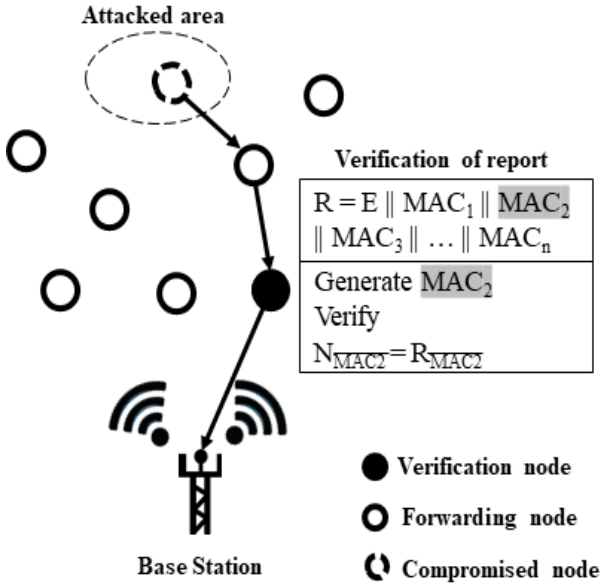

Fig. 2. En-route filtering phase in SEF

B. Threat Model

A false report injection attack causes node energy depletion and sends false information to the user [16]. WSN nodes are deployed in an open location. Therefore, an attacker can acquire and compromise nodes. The security level of nodes in the existing scheme described above is fixed. It is wise to set a relatively low security strength rather than a high filtering rate to extend the lifetime of the network in areas with low density.

III. PROPOSED SCHEME

This section explains the motivation and details of the proposed scheme.

A. Motivation

Nodes use a fixed routing path in the proposed scheme. The same path is used until the energy of a node is exhausted among the nodes in the network, and can no longer operate. Node performance, such as residual energy of the node and transmission range, was modeled based on the Mica2 Model [17]. This model is widely cited as a model of energy consumption. This model is based on the monitoring values of energy consumption that can be controlled by the actual WSN data communication components.

B. Detailed Proposed Scheme

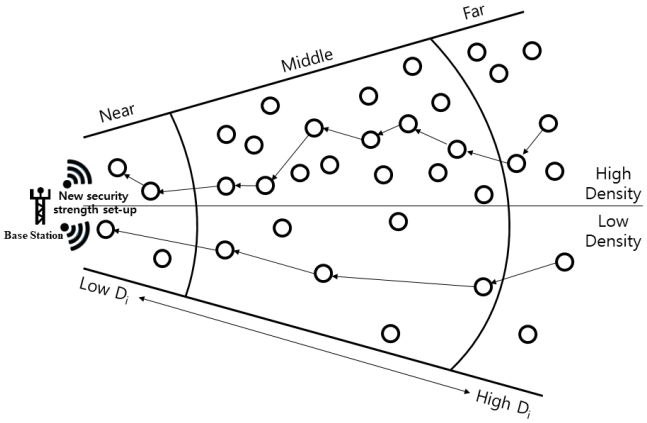

Fig. 3. An overview of the proposed scheme

Fig. 3. shows an overview of the proposed scheme. In a high-density environment, the report is transmitted to the BS through a high number of hops, and in a low-density environment, the report is transmitted through a low number of hops. Therefore, the probability of the report reaching the upstream node differs depending on the node density and the distance from the source location to the BS. Therefore, if the security strength is adjusted for each node density and distance, the number of transmissions/receptions of nodes around the BS can be lowered. This process can help to extend the network life. The BS, which is the report collection agency, has more energy than a deployed node. Voluntarily setting the security strength of nodes is not suitable because it requires a lot of computational cost. Hence, the proposed scheme is performed in the BS. Deployed nodes transmit their own node information to the BS in the routing setup phase. Through this, the BS can collect the hop number and location information of the nodes. The BS calculates equation (1) when the routing of nodes is completed.

$$D_i = \frac{N_{i\_hops}}{Net_{\max\ hop}} \quad (1)$$

Equation (1) represents the relative distance between the node and the BS in the network. The N_{i_hop} value of each node is calculated as the number of hops from where it is located to the BS. Net_{max_hop} is the maximum number of hops in the network obtained through the information collected in the routing configuration phase. The closer D_i is to 1, the farther it is from the BS, and the closer D_i is to 0, the closer it is to the BS. The BS performs equation (2) after calculating the D_i value of each node.

$$N_i\_Security\_Level = D_i + Net_{Dangerous\_Level} \quad (2)$$

$N_i\_Security\_level$ represents the security level of each node. $\text{Net}_{\text{Dangerous\_level}}$ is the percentage of false traffic measured by the BS. When the $N_i\_Security\_level$ value is closer to 1, the stronger the security strength requirements of the node. The resources of the nodes around the BS are depleted first depending on the nature of the WSN. In order to prevent these problems, the proposed scheme reduces the load on nodes close to the BS and increases the verification probability of nodes located far away. If the above steps have been successfully performed, the BS calculates equation (3). We divided $N_i\_Security\_level$ into 4 levels.

1. Minimum security threshold value
   ($0 < N_i\_Security\_level <= 0.25$)
2. Small security threshold value
   ($0.25 < N_i\_Security\_level <= 0.5$)
3. Large security threshold value
   ($0.5 < N_i\_Security\_level <= 0.75$)
4. Maximum security threshold value
   ($0.75 < N_i\_Security\_level <= 1$)

$$Flexible_{Strength} = \frac{BS_{partition} + BS_{keys}}{100} \quad (3)$$

A node can only generate a MAC with a unique key belonging to a distinct partition. An attacker should be able to create the security threshold value using the key of a separate partition as much as the security threshold value for false report generation. Therefore, the report verification probability of SEF varies depending on the number of keys and the number of partitions. If the partition size is large, it will be difficult for the attacker to construct a false report that cannot be detected. So, we apply the flexibility of security strength to the proposed method. The equation (4) for a node to construct a new security threshold is as follows.

$$N_{i\ Threshold} = N_{PT} \pm Flexible_{Strength} \times N_i\_Security\_Level \quad (4)$$

$N_{i\_Threshold}$ means a new security threshold to be applied to the node. The new security strength is increased or decreased by using the past threshold like N_{PT}, the security threshold value applied to the node. The network administrator can dynamically apply the security strength desired using $N_i\_Security\_Level$ because the security level required for each application is different in WSN. If the security level is "minimum" or "maximum", the strength is doubled. For example, If the N_{PT} as security strength applied to the N_i is 3, the security level is calculated as *Maximum*, and $Flexible_{Strength}$ is 2, the $N_{i\_Threshold}$ as new security strength of the node is calculated as 7.

IV. EXPERIMENT

We measured the network lifetime using the number of rounds until the node's energy level could not perform network communication. In this experiment, the existing method and the proposed method use the same routing method. Therefore, we have not considered the transmission/reception energy overhead for configuring the routing. Routing was configured with Direct Diffusion, the basic routing protocol of SEF [18].

Since the BS can calculate the network false traffic ratio through the received reports, we assumed that the BS can learn the attack level by collecting enough reports [19]. The experiment result is generated by performing the proposed scheme only once. We did not consider the execution cycle of the proposed scheme because it is beyond the focus of the paper.

Table- I: Energy consumption parameters [15]

Transmit	16.25μJ (per 1byte)
Receive	12.5μJ (per 1byte)
MAC Generation	15μJ
Verification	75μJ
Cipher	9μJ

We assume that 500 nodes in a 200 x 40 m^2 square region field are deployed for the experiment. And the BS is located at (200, 20). The initial energy is 2J for each node. The report size is 24 bytes and the size vary depending on the number of MACs. The ratio of false reports ranged from 0% to 100 FTR, and the size of the partition was limited to 10. In addition, A partition can store 20 keys and a node loaded 3 keys. The initial security strength was set to 5. 10 compromised nodes are placed at random locations. It was assumed that the event occurred at a random location. The energy consumption of the proposed scheme as shown in Table 1.

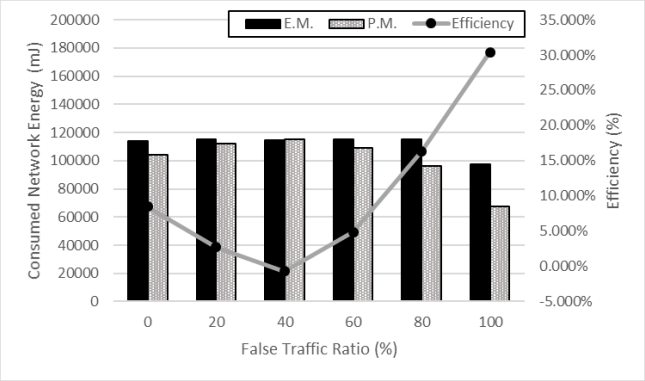

Fig. 4. Consumed network energy versus FTR

Fig. 4. shows the total amount of energy consumed in the network and the efficiency improvement rate according to the attack rate. The proposed method shows a better network lifetime than the existing method, as shown in Fig. 5. So, we are measured as the generation condition of the same number of the report. The reason for the difference in consumption energy is that the proposed method efficiently controls the security strength. However, when the FTR was 40%, the amount of filtering was less than that of the existing scheme, and it was found that the energy loss was 0.67%. Nevertheless, the proposed method saved 10.352% of the energy on average, compared to the existing method, and 30.365% of the energy when the FTR was 100%.

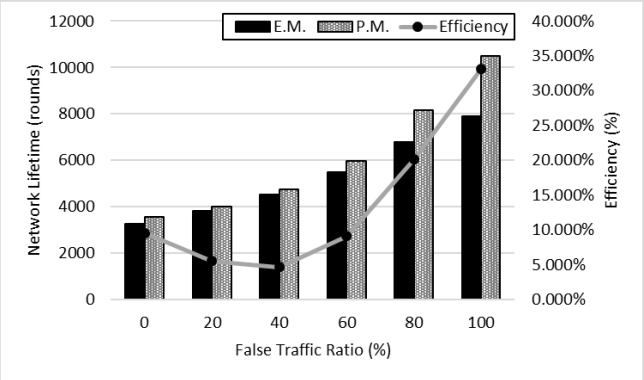

Fig. 5. Network lifetime for depletion of any one of sensor nodes

Fig. 5. shows the network lifetime using a number of rounds. The lifetime of the network was measured until the deployed node in the WSN was unable to perform the mission. As a result, it was confirmed that the maximum network lifetime increased by 33.164%. In addition, the proposed scheme resets the effective security strength for the situation, resulting in an average hop count reduction of up to 37.177%. These results mean that the proposed scheme has a better filtering probability than the existing scheme. The reason for the long life of the proposed scheme is that it sets an appropriate security strength value for the situation. Accordingly, it saves energy by lowering the reported transmitting/receiving count of a forwarding node with high node coverage and reducing the report size.

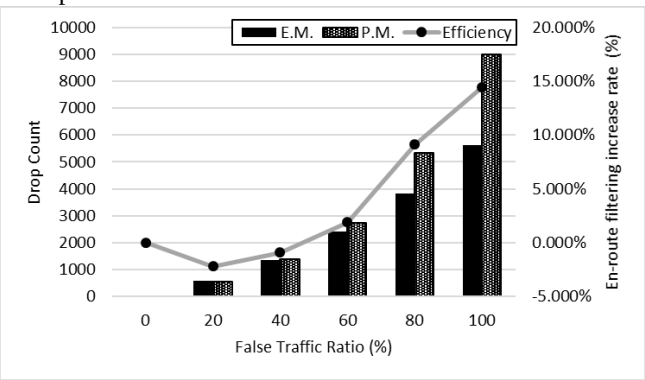

Fig. 6. Number of dropped false reports at the verification node versus FTR

Fig. 6. represents the number of dropped false reports on the verification nodes. On average, the proposed scheme showed a higher drop rate than the existing scheme. However, it can be seen that in the 20% and 40% FTR situation where the attack rate is relatively low, the drop rate has dropped because the security strength value is set lower than the existing scheme. However, false reports can be detected through MAC verification in the BS, and the purpose of the en route filtering is to extend the network lifetime. We proved that the proposed scheme is good, as shown in Fig.5. The proposed scheme increased the drop rate by up to 14.409% compared to the existing scheme in the case of the 100% FTR.

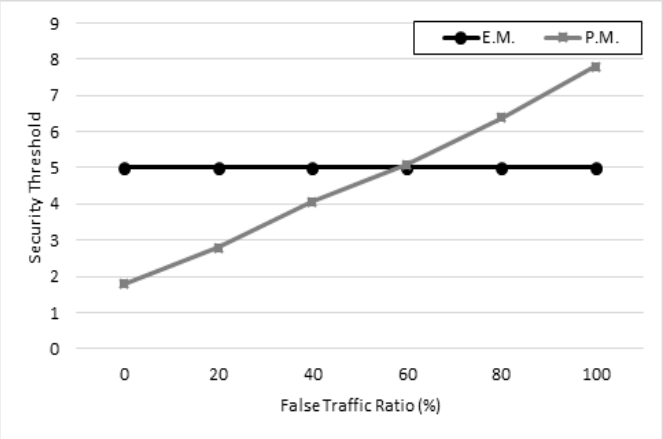

Fig. 7. Security threshold versus FTR

Fig. 7. shows the security threshold according to the FTR. The existing scheme is maintained at a static value. However, it can be seen that the proposed scheme sets the security threshold value control according to the attack rate. When the attack rate is 0%, a relatively low-security threshold value is set to reduce the size of the report and maintain the minimum security. In the case of an attack rate of 100%, the security threshold value is increased to improve the early filtering performance.

V. CONCLUSION AND FUTURE WORKS

The nodes around the report collection agency are exhausted of energy first depending on the nature of the WSN. This paper proposes a method to adjust the security strength considering node density to effectively solve this problem. The proposed method reduces the network total energy consumption while maintaining the minimum-security level by setting nodes to low-security strength in areas with low node density. In addition, this increases the filtering probability in the high-density area to reduce the amount of transmission and reception of nodes around the report collection institution and prevents unnecessary energy consumption. We demonstrate experimentally that the proposed method helps extend the network lifetime over that of the existing methods. However, this proposed scheme is applied to all regions, and it does not distinguish between danger zones and safety zones. In future research, we plan to improve the proposed scheme based on various attack situations in each cluster.

ACKNOWLEDGMENT

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. NRF-2018R1D1A1B07048961)

REFERENCES

1. Ali, Ahmad, et al. "A comprehensive survey on real-time applications of WSN." Future internet 9.4 (2017): 77.
2. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).
3. Salleh, Azhari, Kamaruddin Mamat, and Mohamad Yusof Darus. "Integration of wireless sensor network and Web of Things: Security perspective." 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC). IEEE, 2017.
4. Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey." Ad Hoc Networks 24 (2015): 264-287.
5. Kavitha, T., and D. Sridharan. "Security vulnerabilities in wireless sensor networks: A survey." Journal of information Assurance and Security 5.1 (2010): 31-44.
6. Lin, Jie, et al. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE Internet of Things Journal 4.5 (2017): 1125-1142.
7. Yu, Zhen, and Yong Guan. "A dynamic en-route scheme for filtering false data injection in wireless sensor networks." Proceedings of the 3rd international conference on Embedded networked sensor systems. 2005.
8. Liu, Zhixiong, et al. "A Cluster-Based False Data Filtering Scheme in Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 23 (2014).
9. Li, Feng, and Jie Wu. "A probabilistic voting-based filtering scheme in wireless sensor networks." Proceedings of the 2006 international conference on Wireless communications and mobile computing. 2006.
10. Zhang, Haitao, and Cuiping Liu. "A review on node deployment of wireless sensor network." International Journal of Computer Science Issues (IJCSI) 9.6 (2012): 378.
11. Xiangning, Fan, and Song Yulin. "Improvement on LEACH protocol of wireless sensor network." 2007 international conference on sensor technologies and applications (SENSORCOMM 2007). IEEE, 2007.
12. Jung Sub Ahn, & Tae Ho Cho. "Node Burden-Based Load-Balancing Management Method for Extended Network Lifetimes of WSNs" International Journal of Engineering and Advanced Technology (IJEAT), Vol. 9, No. 1, pp. 5602 - 5607, Oct. 2019.
13. Nam, Su Man, and Tae Ho Cho. "Context-aware architecture for probabilistic voting-based filtering scheme in sensor networks." IEEE Transactions on Mobile Computing 16.10 (2016): 2751-2763.
14. Yimin Yu, Chao Song, Ming Liu, and Haigang Gong. (2011). Energy-Efficient Algorithm for Sensor Networks with Non-Uniform Maximum Transmission Range. Sensors, vol. 11(6), pp. 6203-6213.
15. Ye, Fan, et al. "Statistical en-route filtering of injected false data in sensor networks." IEEE Journal on Selected Areas in Communications 23.4 (2005): 839-850.
16. Mo, Yilin, et al. "False data injection attacks against state estimation in wireless sensor networks." 49th IEEE Conference on Decision and Control (CDC). IEEE, 2010.
17. Ali, Nurul Amirah, Micheal Drieberg, and Patrick Sebastian. "Deployment of MICAz mote for wireless sensor network applications." 2011 IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE). IEEE, 2011.
18. Intanagonwiwat, Chalermek, Ramesh Govindan, and Deborah Estrin. "Directed diffusion: A scalable and robust communication paradigm for sensor networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.
19. Jung Sub Ahn, & Tae Ho Cho. "Node Burden-Based Load-Balancing Management Method for Extended Network Lifetimes of WSNs" International Journal of Engineering and Advanced Technology (IJEAT), Vol. 9, No. 1, pp. 5602 - 5607, Oct. 2019.

AUTHORS PROFILE

Jung Sub Ahn received his B.S. degree in computer information from Kyungil University, Korea, in February 2016. He is currently a doctoral student in the College of Information and Communication Engineering at Sungkyunkwan University, Korea. His research interests include wireless sensor network, network security, context aware architecture, and modelling & simulation.

Tae Ho Cho received his Ph.D. in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Computing at Sungkyunkwan University, Korea. His research interests include wireless sensor networks, intelligent systems, modeling and simulation, and enterprise resource planning.