JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 30 No. 10, pp. 121-134, October 2025
https://doi.org/10.9708/jksci.2025.30.10.121

Extending Network Lifetime with Dynamic Path-based IHA Routing in WSN

Sooyoung Moon*

*Researcher, Convergence and Open Sharing System Immersive Media, Pai Chai University, Daejeon, Korea

[Abstract]

Some studies have investigated the relationship between routing methods and application layer security methods in wireless sensor networks (WSNs). However, routing is strongly related to the security of filtering methods in order to detect false reports. In addition to that, it is also related to the energy consumption of nodes and the network lifetime. The interleaved hop-by-hop authentication scheme (IHA) guarantees that every false report is detected and dropped if the number of compromised nodes is less than *t*. Nevertheless, IHA sensor nodes exploit the same routing path from a cluster head (CH) to the base station (BS) until a node on the routing path fails or its energy is depleted. Therefore, imbalance of the nodes' energy consumption occurs and network lifetime is reduced. We propose a new filtering scheme where each node on the routing path can adaptively select the next hop node based on fuzzy logic with a consideration for energy consumption, the distance to the BS, and the key information of its neighbor nodes. Our proposed method can provide the same level of security as IHA and can increase network lifetime when compared to IHA.

▸ **Key words**: Message authentication, Routing protocols, Wireless sensor networks

[요 약]

본 연구는 무선 센서 네트워크(WSN)에서 거짓 보고서 탐지를 위한 필터링 방법의 보안성과 라우팅 간의 관계를 다룬다. 기존의 interleaved hop-by-hop 인증 방식(IHA)은 t개 미만의 노드가 침해될 경우 모든 거짓 보고서를 탐지하고 차단할 수 있으나, 클러스터 헤드에서 기지국까지 동일한 라우팅 경로를 사용하여 노드의 에너지 소비 불균형과 네트워크 수명 단축 문제가 발생한다. 본 논문에서는 라우팅 경로상의 각 노드가 에너지 소비량, 기지국까지의 거리, 이웃 노드의 키 정보를 고려하여 퍼지 논리 기반으로 다음 홉 노드를 적응적으로 선택하는 새로운 필터링 방식을 제안한다. 제안된 방법은 IHA와 동일한 수준의 보안성을 제공하면서도 네트워크 수명을 증가시킬 수 있다.

▸ **주제어**: 무선 센서 네트워크, 메시지 인증, 라우팅 프로토콜, 위조 보고서 필터링, 퍼지 로직, 에너지 효율성, 네트워크 수명

• First Author: Sooyoung Moon, Corresponding Author: Sooyoung Moon
*Sooyoung Moon (symoon@pcu.ac.kr), Convergence and Open Sharing System Immersive Media, Pai Chai University
• Received: 2025. 10. 02, Revised: 2025. 10. 13, Accepted: 2025. 10. 21.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

Wireless sensor networks (WSNs) collect contextual information (such as light, temperature, and images) from the surrounding environment, process the information, and provide it to users to implement intelligent systems [1-4]. A large number of micro sensor nodes and at least one base station (BS) organize a WSN. Those sensor nodes forward the contextual information to the BS through a multi-hop routing protocol. WSNs can be applied in many areas, such as disaster prevention, lab safety management, and for military applications [5].

Sensor nodes are provided with limited resources, such as energy, memory, and computation capability, and they communicate with each other via wireless communications [6]. In addition to that, WSNs typically operate without infrastructure or human operators. Therefore, there are various threats of WSNs [7, 8]. One of them is that of false report injection where attackers forge nonexistent event reports and inject the false reports through compromised nodes. The injected false reports deplete the limited energy of the sensor nodes and deceive the BS. There have been many studies on security methods to detect false reports [9-17]. The interleaved hop-by-hop authentication scheme (IHA) [10] guarantees that every false report is detected and dropped if the number of compromised nodes is less than or equal to t, where t is a system parameter. However, in IHA, a routing path from a cluster head (CH) to the BS does not change until one of the nodes on the path fails or its energy is depleted. Therefore, imbalance of energy consumption occurs and network lifetime is decreased.

For the above reason, we propose a new filtering method in which each node can adaptively select the next hop forwarding node based on the energy consumption, distance to the BS, and key information of its neighbor nodes. It determines the next hop node based on a fuzzy rule-based system. Additionally, a message authentication code (MAC) that would be included in an event report is dynamically created and forwarded to the current node on the routing path. We confirm through experiments that our proposed method can increase network lifetime when compared to IHA with the same level of security. The contributions of the paper are as follows:

1) a fuzzy rule-based mechanism for determination of the next node to achieve balanced energy consumption of the sensor nodes,

2) a modified association phase that allows multiple upper and lower association nodes for each node,

3) a modified report endorsement and en-route filtering phase based on dynamic MAC generation, and

4) a new concept, *cutoff ratio*, to evaluate the network lifetime.

II. Background

1. Interleaved hop-by-hop authentication scheme (IHA)

IHA [10] is a filtering scheme that detects and removes false reports injected through compromised nodes. It guarantees detection of false reports under the condition that there are no more than t compromised nodes, where t is a system parameter that determines the security level of IHA. Sensor nodes in IHA build association relationships and share pairwise keys with each other for endorsement and verification of event reports.

It is assumed that sensor nodes in a network field organize clusters and that there are at least (t+1) nodes in each cluster. There are five phases of IHA operation. We assign a unique ID to each node and store key material in it in the node initialization and deployment phases. Every node is able to establish pairwise keys with other nodes from the key material.

A routing path from each CH to the BS is

constructed during the association phase. Each node on the routing path discovers its upper and lower associated nodes that are (t+1) hops away. Once a node discovers the IDs of its upper and lower association nodes, it derives the pairwise key shared with the association nodes from their IDs based on an ID-based scheme such as Blundo scheme [18].

There are two steps in the association phase: *BS HELLO* and cluster *ACK*. In *BS HELLO*, each node discovers its upper association nodes when BS initiates a *HELLO* message and broadcasts to its neighbor nodes. The *HELLO* message is repetitively propagated to entire network. During the step, each node discovers the *ID* of its upper association node that is (t+1) hops closer to the BS and stores the upper association node *ID* in its memory. In *CLUSTER ACK*, each *CH* constructs an *ACK* message and sends it in the direction of the *BS*. Each *ACK* message includes the cluster *ID* and the (t+1) lower node IDs. Each receiving node of the ACK message discovers the ID of its lower association node that is (t+1) hops closer to the *CH* and stores the lower association node ID in its memory. Figure 1 shows the association relationship of nodes when t=3.

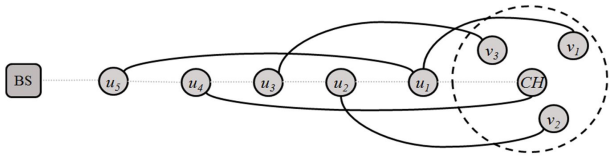


Fig. 1. Association of nodes in IHA (t=3)

There are t+1=4 nodes in the cluster (the right dotted-lined circle in the figure). The cluster nodes (*CH*, v_1, v_2, v_3) and the intermediate nodes (u_1~u_5) are associated with each other. Each node on the routing path is connected to the upper associated nodes that are 4 hops closer to the BS and to the lower associated node that are 4 hops closer to the CH. A node within 3 hops from the CH is associated with one of the cluster nodes. For example, u_3 has a lower association node, v_3. A node within 4 hops of the BS has no upper association node.

During the report endorsement phase, (t+1) nodes, including CH, collaborate to generate event reports. Specifically, each of the (t+1) nodes generates two MACs, an individual MAC and a pairwise MAC, by using its own authentication key shared with BS and its pairwise key shared with its upper association node, respectively. Then it sends an endorsement message that includes the two MACs to the CH. The CH collects (t+1) individual MACs and (t+1) pairwise MACs, and constructs a final event report. The individual MACs are compressed by using an XOR operation whereas the pairwise MACs are included in a plaintext format.

During the en-route filtering phase, each node on the routing path receives an event report. The receiving node verifies the pairwise MAC in the report generated by its lower associated node by using the pairwise key. If the verification succeeds, it removes the verified MAC and inserts its own pairwise MAC generated by using the pairwise key shared with its upper association node. Otherwise, if the verification fails, it drops the event report. Figure 2 shows false report detection in IHA.

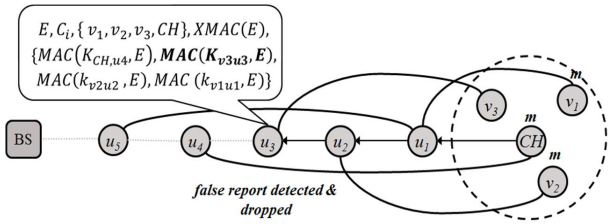


Fig. 2. False report detection.

In the above figure, CH, v_1 and v_2 represent compromised nodes with 'm' marks above them. The attacker collects keys from the compromised nodes and generates a false report with one false MAC [$MAC(K_{v3u3}, E)$] that can be computed by using the shared key K_{v3u3}. Since v_3 is not compromised, K_{v3u3} is not disclosed to the attacker. Therefore, u_3 verifies $MAC(K_{v3u3}, E)$ and detects the false report.

In the base station verification phase, the BS verifies the compressed individual MAC and detects the remaining false reports.

2. Geographical and energy aware routing (GEAR)

Geographical and energy-aware routing (GEAR) [19] is a routing protocol that considers the distance to the destination and the energy consumption of the neighbor nodes of each node when choosing the next node on the forwarding path. The objective of GEAR is to achieve balanced energy consumption among the nodes and to improve the overall energy efficiency, leading to an increase in network lifetime. Each node in GEAR selects the next node on the message forwarding path based on the learned cost as shown in the following equation:

$$h(N, R) = h(N_{\min}, R) + C(N, N_{\min}) \quad (1)$$

In equation (1), $h(N, R)$ is the learned cost from the node N to the destination R of the message. It is determined as the sum of the least learned cost $h(N_{min}, R)$ of its neighbors and the link cost $C(N, N_{min})$. The following equation shows the derivation of the estimated cost from the node N to R, which is the default value for $h(N, R)$:

$$c(N, R) = \alpha_G \cdot d(N, R) + (1 - \alpha_G) \cdot e(N) \quad (2)$$

In equation (2), αG and $(1-\alpha_G)$ are weight values for the factors representing the distance from the node N to the destination R and the energy consumption of the node N, respectively. GEAR can deliver 25-35% more packets in a uniform traffic environment than can greedy perimeter stateless routing (GPSR) [20], which is a geographic routing protocol that considers only distance to the destination.

III. Proposed Method

1. Network model

The sensor field is divided into a geographic grid and each cell in the grid corresponds to a cluster. A CH is responsible for data aggregation, event report generation, and inter-cluster communication, whereas remaining nodes in the cluster sense events and generate MACs for endorsing the events. $(t+1)$ sensor nodes are deployed in each cell and the location of each node in the cell is determined randomly based on a uniform distribution where t is a design parameter that is determined prior to the deployment of sensor nodes. The resources of the sensor nodes, such as energy, computation speed, and memory, are limited [6].

Sensor nodes exploit bidirectional wireless links to communicate with each other. Since the transmission range of each node is limited, multi-hop routing protocols [19-22] are exploited to deliver event reports from a source CH to the BS.

Any two nodes can construct a pairwise key that is shared only by them from their IDs. For example, Blundo [18] can be used to construct a pairwise key. Sensor nodes endorse and verify event reports by using the pairwise key, and events occur throughout the sensor field.

2. Threat Model

This study addresses the false report injection attack, which is one of the most critical security threats in wireless sensor networks [10, 18]. In this attack scenario, we consider the following threat model:

Adversary Capabilities:

- The adversary can compromise up to t sensor nodes in the network, where t is a predetermined security parameter
- Compromised nodes can collaborate to forge false event reports
- The adversary can extract all cryptographic keys stored in the compromised nodes
- Compromised nodes can inject fabricated reports claiming non-existent events
- The adversary cannot compromise the base station (BS), which is assumed to be a trusted entity

Attack Objectives:

The primary objectives of false report injection attacks are:

- Energy depletion: False reports are forwarded through multiple hops, consuming the limited energy resources of intermediate nodes
- BS deception: False reports reaching the BS trigger unnecessary responses and operations
- Network disruption: Continuous injection of false reports can lead to premature network failure

Security Goal:

Our security goal, consistent with IHA [10], is to detect and filter out all false reports before they reach the BS, provided that the number of compromised nodes does not exceed t. Specifically:

- If (t+1) message authentication codes (MACs) are verified within (t+1) hops from the cluster head, all false reports generated by up to t compromised nodes will be detected and dropped en-route
- This ensures that no false report can reach the BS as long as the adversary's capability remains within the threshold t.

3. Motivation

In IHA, routing paths from CHs to the BS are constructed prior to event report forwarding. Then, event reports originated in a cluster are forwarded through the same path from the CH to the BS until some nodes on the path fail or their energy is depleted. Therefore, an imbalance of energy consumption among the nodes may occur and network lifetime may decrease. If a sensor node on a routing path is able to select the next hop node based on its energy consumption, its distance to the BS, and the number of pairwise keys of its neighbor nodes, then we can balance the energy consumption of the nodes and increase the network lifetime.

4. Operation

The operational process of the proposed method involves five phases: 1) node initialization and deployment, 2) association, 3) report endorsement, 4) en-route filtering and 5) BS verification.

In the node initialization and deployment phase, we assign a unique ID and key materials to each node before the node deployment. Key materials may include an initial network key and a symmetric bivariate polynomial of degree k, based on key management schemes [18]. Then, we randomly deploy sensor nodes in the sensor field, and we assume that (t+1) nodes are deployed in each cell in the grid. For example, if t=3, four nodes are deployed in each cell. Sensor nodes deployed in each grid organize a cluster and elect a CH among them.

In the association phase, sensor nodes discover the IDs of their upper and lower association nodes. First, BS initializes a *HELLO* message that includes its own ID and a sequence number of the message, and then it broadcasts the *HELLO* message to its neighbor nodes. The CHs in clusters adjacent to the BS receive the *HELLO* message and assign the ID of the BS as their parent. Then each of them attaches its ID to the message and forwards the message to its neighbor nodes.

When a CH receives a *HELLO* message from neighbor CHs, it accepts the message only when the number of its "candidate parent nodes" is less than *nc*, where *nc* is a system parameter that determines the maximum number of candidate parent nodes. A CH is able to forward event reports only to one of its candidate parent nodes during the en-route filtering phase. If a CH accepts a *HELLO* message, it inserts the ID of the sender into its candidate parent node list and increments the number of its candidate parent nodes by one. Then it stores the IDs of the nodes 2-hops, 3-hops, …, (t+1)-hops closer to the BS in its upper node lists. Specifically, the nodes that are (t+1)-hops closer to the BS become the upper association nodes of the receiver. Additionally, the CH assigns the upper nodes' IDs as the upper association

nodes of the remaining cluster nodes. Specifically, the IDs of each of the nodes that are i-hops ($1 \leq i \leq t$) closer to the BS are assigned as the upper association nodes of the i-th node (except CH) in the cluster. The CH then generates a new *HELLO* message that includes its ID and the IDs of the nodes that are 1-hop, 2-hops, ⋯, t-hops closer to the BS and broadcasts the *HELLO* message to its neighbor nodes. When the *HELLO* message is propagated to the entire network, every node constructs its upper association node list.

After all the nodes construct their upper association nodes list, each CH generates an *ACK* message that includes the IDs of the t+1 nodes (including itself) in the cluster and forwards the *ACK* message to its candidate parent nodes. When a CH receives an *ACK* message, it deletes the IDs of the nodes that are (t+1)-hops farther from the BS and stores the IDs in its lower association nodes list. Then it attaches its ID to the *ACK* message and forwards the message to its candidate parent nodes. When *ACK* messages from all the CHs are delivered to the BS through the forwarding nodes, every node constructs its lower association node list. At the end of the phase, every node derives the pairwise keys shared with its upper and lower association nodes, based on ID-based pairwise key establishment schemes [18, 23]. Figure 3 shows a *HELLO* message broadcast in the association phase when nc = 3.

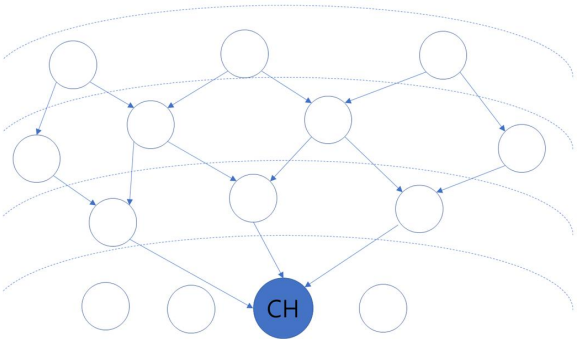


Fig. 3. *BS HELLO* step in association phase (nc=3)

Each node receives at most three *HELLO* messages and forwards a *HELLO* message after the processing described above. Figure 4 represents the *ACK* message forwarding from a CH in the association phase when nc=3.

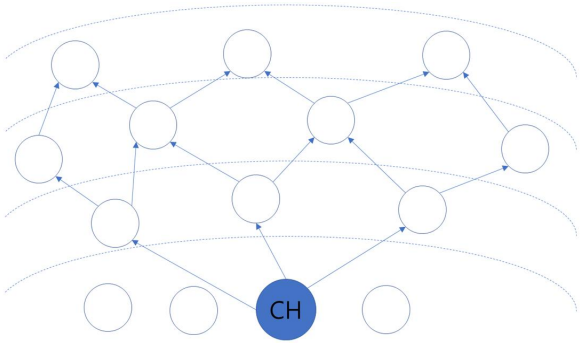


Fig. 4. *Cluster ACK* step in association phase (nc = 3)

The CH generates an *ACK* message and sends the *ACK* message to its candidate parent nodes. A node receiving the *ACK* message processes the *ACK* message as described above, and then forwards the *ACK* message to its candidate parent nodes.

In the report endorsement phase, an event(s) occurs in a cluster and the CH and remaining nodes in that cluster collaborate to generate an event report, and the CH forwards the event report to a selected next hop node. Each node in the cluster generates an individual MAC by using its authentication key shared only with the BS, and it sends the *endorsement* message that includes the individual MAC to the CH. The CH collects (t+1) individual MACs from cluster nodes (including itself) and compresses the individual MACs into a single MAC. Then the CH determines the next hop forwarding node based on fuzzy if-then rules, as shown in Figure 5.

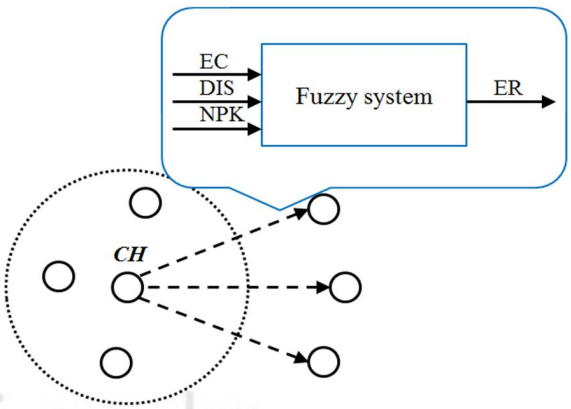


Fig. 5. Fuzzy rule-based determination of the next hop node

Each node exploits three input parameters to evaluate the fitness of candidate parent nodes: energy consumption, distance to the BS, and the number of pairwise keys of each candidate parent node.

We prefer a candidate parent node that has consumed less energy, thereby achieving balanced energy consumption of nodes. We can include the information of energy consumption of a node in periodic beacon messages [24].

If other conditions are equal, we choose a candidate node that is closer to the BS than another to reduce hop counts for the event report and corresponding communication overhead (i.e., energy consumption for forwarding the event report). The number of pairwise keys is related to the number of possible paths to the BS that are constrained to include the candidate parent node. The more nodes a node is associated with, the higher the number of pairwise keys stored in the node is. Therefore, if we choose a candidate parent node with a large number of pairwise keys, we can balance the energy consumption of the nodes since there are many possible paths to the BS that include the candidate parent node. We can include the distance to the BS and the number of pairwise keys in a *HELLO* message. Figure 6 represents the fuzzy membership functions for the input and output variables for the fuzzy system.

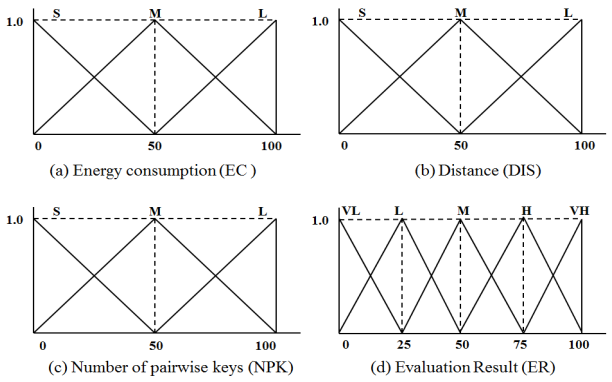


Fig. 6. Fuzzy membership functions for the input and output variables.

The values of the input and output variables are normalized into the range between 0 and 100. Each of the three input variables is associated with three fuzzy sets, while the output variable that represents the evaluation result is associated with five fuzzy sets. The linguistic variables and corresponding linguistic terms for input/output variables for the fuzzy system are as follows:

- EC (Energy Consumption) = { S (Small), M (Medium), L (Large) }
- DIS (Distance) = { S (Small), M (Medium), L (Large) }
- NPK (Number of Pairwise Keys) = { S (Small), M (Medium), L (Large) }
- ER (Evaluation Result) = { VL (Very Low), L (Low), M (Medium), H (High), Very High (VH) }

Table 1. Sample fuzzy if-then rules

Rule no.	Fuzzy rule
2	IF **EC** is **Small**, **DIS** is **Small**, and **NPK** is **High**, THEN **ER** is **Very High**
11	IF **EC** is **Medium**, **DIS** is **Small**, and **NPK** is **High**, THEN **ER** is **High**
12	IF **EC** is **Medium**, **DIS** is **Medium**, and **NPK** is **Small**, THEN **ER** is **Low**
14	IF **EC** is **Medium**, **DIS** is **Medium**, and **NPK** is **High**, THEN **ER** is **Medium**
22	IF **EC** is **High**, **DIS** is **Medium**, and **NPK** is **Medium**, THEN **ER** is **Low**
24	IF **EC** is **High**, **DIS** is **High**, and **NPK** is **Small**, THEN **ER** is **VeryLow**

According to Rule 2, if the energy consumption of a candidate parent node and its distance to the BS are both ***Small*** and the number of pairwise keys is ***High***, the evaluation result is ***Very High*** since the candidate parent is considered most suitable to be selected as the next hop forwarding node.

If either the energy consumption or the distance to the BS is ***Small***, and the other is ***Medium***, and the number of pairwise keys is ***High***, then the evaluation result is ***High*** (Rule 11).

If both the energy consumption and the distance to the BS are ***Medium***, the evaluation result becomes ***Low*** or ***Medium*** depending on the number of pairwise keys of the candidate parent node (Rules 12 and 14).

If the energy consumption is ***High***, the distance to the BS is ***Medium***, and the number of pairwise keys is ***Medium***, then the evaluation result is ***Low*** (Rule 22).

If both the energy consumption and the distance to the BS are ***High***, and the number of pairwise keys is ***Small***, the evaluation result becomes ***VeryLow*** since the candidate parent node is considered most unsuitable to be selected as the next hop forwarding node (Rule 24).

The CH sends a *MAC_REQUEST* message that includes the ID of the next node to the cluster node that is a lower association node to the next hop node. The cluster node that receives the *MAC_REQUEST* message generates a pairwise MAC by using the pairwise key shared with the next hop node. Then the cluster node sends a *MAC_RESPONSE* message that includes the pairwise MAC to the CH. The CH receives the *MAC_RESPONSE* message and constructs a final event report as follows:

$$R : E, C_i, v_1, v_2, v_3, CH, XMAC(E), MAC(K_{v_1,u_1}, E) \quad (3)$$

The above equation shows the example of the event report format when t = 3.

The node that received the event report from the source CH operates during the en-route filtering phaseby verifying the pairwise MAC in the received event report by using the pairwise keys shared with the lower association node that generated the pairwise MAC. If the verification succeeds, the node determines its next hop forwarding node among its candidate parent nodes based on the proposed fuzzy system. Then the node sends a *MAC_REQUEST* message that includes the ID of the next hop forwarding node to the lower association node of the next hop forwarding node. The lower association node of the next hop forwarding node receives the *MAC_REQUEST* message, extracts the node ID, and generates a pairwise MAC by using the pairwise key shared with the next hop forwarding node. Then the lower association node sends back a *MAC_RESPONSE* message that includes the pairwise MAC to the current node. The current node receives the *MAC_RESPONSE* message, replaces the old MAC in the event report with the received MAC, and forwards the event report to the selected next hop forwarding node. If the verification fails, the event report is dropped. The same process is repeated until the event report reaches to the BS or is dropped by an intermediate node due to false report detection. Figure 7 illustrates a dynamic MAC generation-based event report forwarding of the proposed method. The numbers in each arrow represent the sequence of the message exchange.

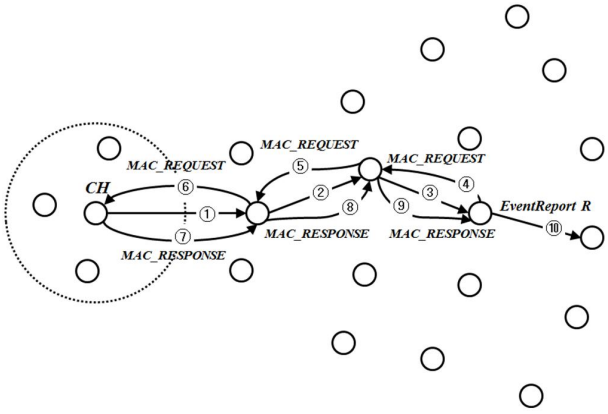


Fig. 7. Dynamic MAC generation and event report forwarding

The BS knows all the nodes' authentication keys. Therefore, in the BS verification phase, it can generate individual MACs of the endorsing nodes for the received event E and can compute *XMAC(E)*. If the compressed MAC in the received event report is different from the computed MAC, the BS detects a false report and drops it.

IV. Performance Analysis

1. Security Analysis

An attacker tries to forward false reports that are injected through compromised nodes in as many hops as possible. In the proposed method, each node shares a pairwise key with each of its multiple upper and lower association nodes. In the

en-route filtering phase, each forwarding node verifies the pairwise MAC created by its lower association node. Figure 8 shows the verification of the pairwise MACs by the forwarding nodes.

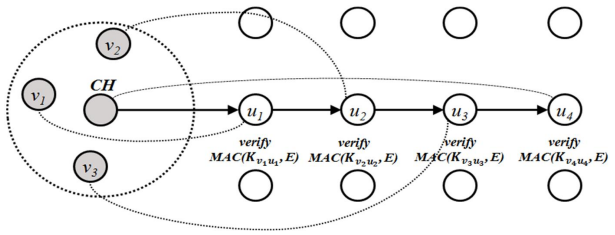


Fig. 8. Verification of pairwise MACs

In the above figure, v_1~v_3 represent cluster nodes except for the CH, and u_1~u_4 represent the forwarding nodes on the routing path. Each of the forwarding nodes is selected by the previous node on the routing path and can be changed for different event reports. Every forwarding node verifies a MAC generated by its lower association node.

There are (t+1) MACs in an event report and each of the MACs is verified within (t+1) hops. Therefore, if the number of compromised nodes is no more than t, every false report is detected and dropped. In addition, if a node knows authentic IDs of its upper and lower association nodes, the false report is detected and dropped after it is forwarded by at most t non-compromised nodes [10]. As a result, the proposed method provides the same level of security as IHA.

2. Cost Analysis

2.1 Communication overhead

The communication overhead of the proposed method is caused by four types of messages: *HELLO*, *ACK*, *MAC_REQUEST*, and *MAC_RESPONSE* messages. The communication overhead incurred by the *HELLO* and *ACK* messages is related to the number of upper association nodes and the number of lower association nodes, respectively. Theoretically, each node can have at most nc^{t+1} upper association nodes. However, the actual number of upper association nodes is usually far less than the theoretical limit since a node can be a candidate parent node for multiple nodes at the same time. Figure 9 illustrates an example of one-hop and two-hop upper nodes of a node.

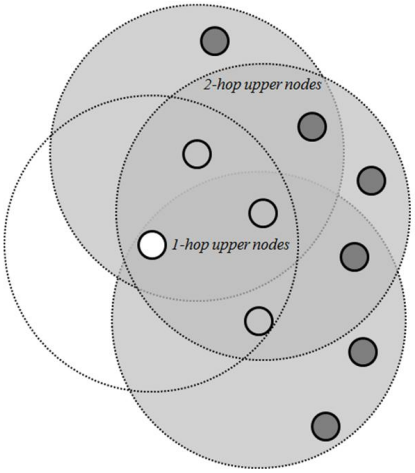


Fig. 9. Example: one hop and two hop upper nodes of a node (nc=3)

Figure 9 shows an example of one-hop and two-hop upper nodes of a node when nc=3. That is, each node can have at most three candidate parent nodes. Two-hop upper nodes of the node (white circle in the figure) exist in the shaded area in the figure. If we assume that two-hop upper nodes of a node cannot exist within the transmission range of the node, the area is further reduced. If the distance between two adjacent one-hop upper nodes (i.e. candidate parent nodes) is the same as the transmission range r of each node, we can calculate the upper bound of the shaded area as follows:

$$A_S = 3\pi r^2 - 2(2\pi r^2 \cdot \frac{2\pi}{3} \cdot \frac{1}{2\pi} - r^2 \sin\frac{\pi}{3}) \approx 2.2\pi r^2 \quad (4)$$

In the above equation, AS represents the upper bound of the shaded area in Figure 9, and r is the transmission range of each node.

Let us define the node density as the number of nodes within a node's transmission range. If we assume that the node density is the same as nc, which is the maximum number of candidate parent nodes of each node, the number of nodes in the shaded area is Similarly, we can calculate the

number of three-hop upper nodes of the node as Table 2 shows the average number of upper nodes of a node, when nc=3, and hop distance under the assumptions described above.

Table 2. The number of upper nodes of a node (upper bound).

hop distance	number of upper nodes
1	N_1 = nc = 3
2	N_2 = 6.6
3	N_3 = 13.1
4	N_4 = 24.7

We can generalize the number of upper nodes as follows:

$$\begin{cases} N_1 = nc \\ nc(0.6 \cdot N_{i-1} + 0.4)(2 \le i \le t+1) \end{cases} \quad (5)$$

The number of upper association nodes of each node is . For example, if t=3 and nc=3, then UN = 24.7, and if the ID size is 2 bytes, the communication overhead becomes 50 bytes.

The sum of the number of upper association nodes for nodes in one cluster is . Since only a CH can become an upper association node of another node, we can derive the average number of lower association nodes of a CH as follows:

$$DN = \sum_{t+1}^{i=1} N_i \quad (6)$$

For example, if t=3 and nc = 3, DN = 47.4, and the corresponding communication overhead becomes 95 bytes if the ID size is 2 bytes.

The communication overhead incurred by *HELLO* and *ACK* is larger than a typical message size (ex. 36 bytes) in WSN [24]. However, they are exploited only in the node initialization and deployment phase that is executed once in each round and that is usually composed of thousands of events. Therefore, the communication overhead incurred by the two types of messages is smaller than the energy consumption for forwarding and processing event reports in each round.

A *MAC_REQUEST* message includes the ID of the next hop forwarding node selected by the current node. Since each node can have at most nc candidate parent nodes, the size of the ID can be reduced as follows:

$$REDUCEDIDSIZE = \log_2 nc \text{ (bits)} \quad (7)$$

For example, if nc=3, the reduced ID size becomes 2 bits. A *MAC_REQUEST* message is sent from the current node to the node that is t-hop closer to the CH since the event report is forwarded by one-hop. Therefore, the corresponding communication overhead is as follows:

$$t \cdot log_2 nc \text{ (bits)} \quad (8)$$

For example, if nc=3 and t=3, the communication overhead becomes 6 bits/message.

A *MAC_RESPONSE* message includes a pairwise MAC generated by a lower association node of the next hop forwarding node. A *MAC_ RESPONSE* message is sent from the lower association node of the next hop forwarding node to the current node that is t-hops closer to the BS whenever the event report is forwarded by one-hop. Therefore, communication overhead is the same as the pairwise MAC size multiplied by t. However, the number of pairwise MACs in each event report in the proposed method is less than IHA by t. Therefore, the communication overhead incurred by *MAC_RESPONSE* messages is offset by the reduced size of event reports in the proposed method.

2.2 Computation overhead

In the proposed method, each node on the forwarding path of event reports performs two MAC operations to verify and endorse the event report, respectively, in the same manner as IHA. In addition to that, it performs a fuzzy rule-based inference to determine the next hop forwarding

node. Lee and Cho explained that a sensor node can perform such fuzzy computation based on a fuzzy system implemented by using hard-coding [15]. Therefore, the computation overhead of the proposed method is reasonable.

2.3 Storage overhead

Each node stores in its memory the IDs of its upper and lower association nodes. Therefore, the memory overhead is as follows:

$$(UN + DN) \cdot IDSIZE \quad \text{(bytes)} \qquad (9)$$

For example, if t=3, nc=3, and ID_SIZE = 2 (bits), the memory overhead becomes 146 bytes. Since a typical sensor node is equipped with 4 KB RAM and 512 KB flash memory, the memory overhead is affordable.

V. Experimental Results

We evaluated the performance of IHA and of our method through experiments in an environment as follows. The total number of senor nodes is 3,600, they are deployed in a 900 900 m^2 sensor field, and the sensor field is composed of 900 clusters each of which has a size of 30 30 m^2.

The value of the system parameter t is t=3. Therefore, four (i.e. t+1) nodes including a CH are deployed in each cluster based on a uniform random distribution. In addition to that, each node is associated to the nodes with a four-hop distance. The transmission range r of each node is 75 m. Each node can have at most three (nc) candidate parent nodes that can be selected as a next hop node for forwarding event reports.

We follow the energy model presented by Ye et al [9]. Therefore, we assume that sensor nodes consume 16.25/12.5 μJ for transmitting/receiving a byte and consume 15 μJ for a single hash or MAC computation. Every sensor node is assumed to have 1 Joule as its initial energy.

The false traffic ratio (FTR) is defined as the number of false event reports over the total number of event reports. In our experiments, we exploited various FTR values such as 0, 30 and 50%.

We proposed the concept of *cutoff ratio* to evaluate the network lifetime of IHA and the proposed method. Cutoff ratio is defined as the number of events that could not be reported to the BS due to energy depletion of nodes divided by total number of occurred events. For example, if the cutoff ratio is 50%, that means half of the total events could not be reported to the BS due to the energy depletion of the source CH or of other forwarding nodes.

As the number of occurred events increases, the number of depleted nodes increases, and, therefore, the cutoff ratio also increases. We observed variations in the number of occurred events with increasing cutoff ratio values to compare the network lifetime of the two methods. Figure 10 shows the number of occurred events as the cutoff ratio increases when FTR = 30%.

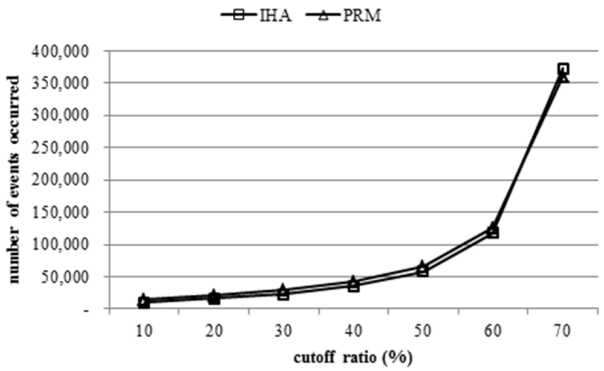


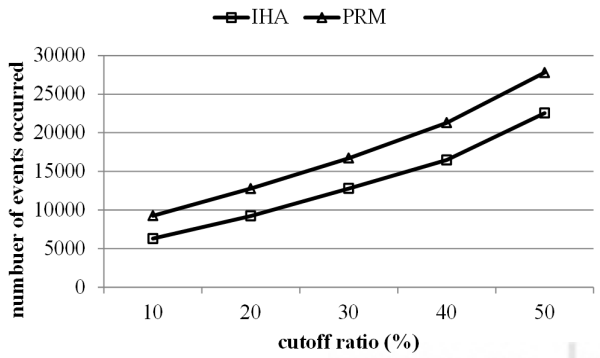
Fig. 10. Number of occurred events versus cutoff ratio. (FTR = 30%, termination condition: cutoff ratio = 70%)

The result shows that the number of occurred events of IHA and the proposed method increase as the cutoff ratio increases. The reason is that the number of depleted nodes and the cutoff ratio increase as the number of occurred events increases. Additionally, the growth rate of the number of occurred events gradually increases as the cutoff ratio increases. In other words, the growth rate of the cutoff ratio decreases as the number of occurred events increases. This is

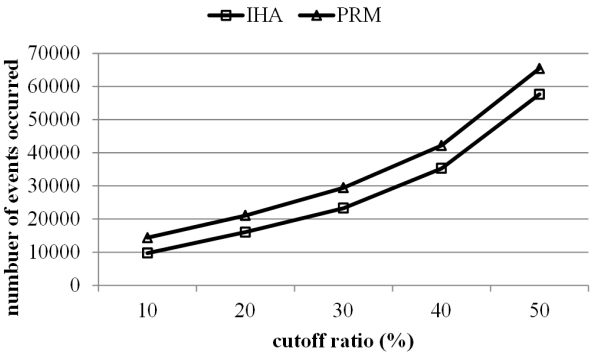
because the growth rate of the number of depleted nodes decreases as the number of occurred events increases, since the average number of hop counts for an event report decreases as the number of depleted nodes increases.

When the *cutoff ratio* is less than 60%, the number of occurred events of the proposed method is larger than IHA since the proposed method could dynamically select the next hop node among candidate parent nodes, while IHA could not. However, when the cutoff ratio is larger than 70%, the proposed method has a lower number of occurred events than IHA does. The reason for this follows below.

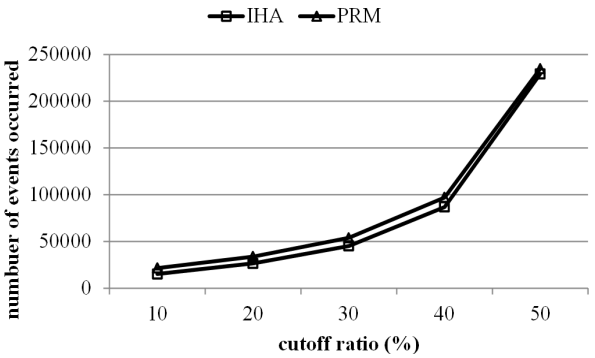
After the first *cutoff* (that is, the situation where an event report cannot be forwarded to the BS due to energy depletion of the source CH or other forwarding nodes) occurs in the network, most (about 90%) events are not delivered to the BS because of the energy depletion of the nodes. Each node in the proposed method still tries to forward event reports to a candidate parent node that is not yet depleted, whereas each node in IHA does not forward event reports if its only parent node has been depleted. Therefore, after the first cutoff occurs, event reports in the proposed method pass a larger number of hops than in IHA. As a result, the proposed method consumes more energy for forwarding event reports, especially when a cutoff occurs, and has a lower number of occurred events when the cutoff ratio is larger than 70%. Figure 11 shows the number of occurred events when FTR is 0, 30, and 50%.



(a) number of occurred events versus cutoff ratio (FTR = 0%)



(b) number of occurred events versus cutoff ratio (FTR = 30%)



(c) number of occurred events versus cutoff ratio (FTR = 50%)

Fig. 11. Number of occurred events versus cutoff ratio (termination condition: cutoff ratio = 50%)

The overall number of occurred events in the proposed method is larger than IHA since each node in the proposed method selects a candidate parent node that is not yet depleted and forwards event reports to the candidate parent node, whereas a node in IHA cannot forward event reports when its only one parent node is depleted.

The performance difference between the proposed method and IHA decreases as the cutoff ratio increases since when a cutoff occurs, the proposed method has higher communication overhead than IHA as we explained in Figure 9.

The performance differences between the proposed methods and IHA decrease as FTR increases. The reason is that a false report passes fewer numbers of hops on average than a valid event report, and therefore there are fewer numbers of possible paths that can be constructed for the event report, reducing the load balancing effect due to the next node selection mechanism of the proposed method.

When FTR = 0, the number of occurred events of the proposed method is 147%, 138%, 131%, 129%, and 123% of IHA when the cutoff ratio is 10, 20, 30, 40, and 50%, respectively. In another case, when FTR = 50%, the number of occurred events of the proposed method is 142%, 127%, 119%, 112%, and 102% of IHA when the cutoff ratio is 10, 20, 30, 40, and 50%.

VI. Conclusion

WSNs are prone to various threats due to the resource limitation of sensor nodes, wireless communication, and the lack of infrastructure. In false report injection, attackers inject false reports through compromised nodes that lead to energy depletion of sensor nodes and deception of the BS. IHA is one of the existing filtering schemes that detects false reports, and it guarantees that every false report is detected and dropped if the number of compromised nodes is less than or equal to *t*. However, IHA exploits the same path from a CH to the BS until one of the sensor nodes on the routing path fails or its energy is depleted. Therefore, imbalance of energy consumption of nodes occurs and network lifetime decreases.

We proposed a new filtering method in which each node on a routing path can select the next hop forwarding node based on the fuzzy rule-based system with consideration of energy consumption, the distance to the BS, and pairwise key information of its candidate parent nodes.

We confirmed through performance analysis and experiments that our proposed method can provide the same security level as IHA and can increase the network lifetime when compared to IHA. In addition to that, we proposed a new measure, *cutoff ratio*, to evaluate the network lifetime of WSNs.

We will study, based on the current results, a new key pre-distribution and rekeying method with consideration of the proposed filtering method. Then we will integrate the proposed methods into the unified security protocol for WSNs.

REFERENCES

[1] J. A. Stankovic, "When sensor and actuator networks cover the world," ETRI Journal, vol.30, no.5, pp.627-633.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," Communications magazine, IEEE, vol.40, no.8, pp.102-114.

[3] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," Wireless Communications, IEEE, vol.11, no.6, pp.6-28.

[4] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards," Comput.Commun., vol.30, no.7, pp.1655-1695.

[5] N. Xu, "A survey of sensor network applications," Tech. Rep., University of Southern California.

[6] M. Datasheet, "Crossbow technology inc," San Jose, California.

[7] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc networks," IEEE communications surveys, vol.7, no.4.

[8] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad hoc networks, vol.1, no.2, pp.293-315.

[9] F. Ye, H. Luo, and S. Lu, "Statistical en-route filtering of injected false data in sensor networks," IEEE J. Sel. Area Comm., vol.23, no.4, pp.839-850.

[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks," ACM Trans.Sen.Netw., vol.3, no.3, aug.

[11] Z. Yu and Y. Guan, "A dynamic en-route filtering scheme for data reporting in wireless sensor networks," IEEE/ACM Transactions on Networking (ToN), vol.18, no.1, pp.150-163.

[12] H. Lee and T. Cho, "Key inheritance-based false data filtering scheme in wireless sensor networks," Lecture notes in computer science, vol.4317, pp.116-127.

[13] T. P. Nghiem and T. H. Cho, "A fuzzy-based interleaved multi-hop authentication scheme in wireless sensor networks," Journal of Parallel and Distributed Computing, vol.69, no.5, pp.441-450.

[14] H. Y. Lee and T. H. Cho, "Fuzzy adaptive selection of filtering schemes for energy saving in sensor networks," IEICE Trans.Commun., vol.90, no.12, pp.3346-3353.

[15] H. Y. Lee and T. H. Cho, "Fuzzy-based path selection method for improving the detection of false reports in sensor networks," IEICE Trans.Inf.Syst., vol.92, no.8, pp.1574-1576.

[16] S. Y. Moon and T. H. Cho, "Key index-based routing for filtering false event reports in wireless sensor networks," IEICE Trans.Commun., vol.95, no.9, pp.2807-2814.

[17] J. M. Kim, Y. S. Han, H. Y. Lee, and T. H. Cho, "Path renewal

method in filtering based wireless sensor networks," Sensors, vol.11, no.2, pp.1396-1404.

[18] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences,"Advances in cryptology—CRYPTO'92, pp.471-486.

[19] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks,", vol.UCLA/CSD-TR-01-0023.

[20] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks,"Proceedings of the 6th annual international conference on Mobile computing and networking, pp.243-254.

[21] F. Ye, A. Chen, S. Lu, and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks,"Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on, pp.304-309.

[22] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," Networking, IEEE/ACM Transactions on, vol.11, no.1, pp.2-16.

[23] S. Zhu, S. Setia, and S. Jajodia, "LEAP : Efficient security mechanisms for large-scale distributed sensor networks," ACM Transactions on Sensor Networks (TOSN), vol.2, no.4, pp.500-528.

[24] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, and E. Brewer, "Tinyos: An operating system for sensor networks," in Ambient intelligence, pp.115-148.

Authors

Sooyoung Moon received the B.S., M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Korea, in 2007, 2009 and 2015, respectively.