# Fuzzy-based Adaptive Multipath for En-route Filtering in Dynamic Wireless Sensor Network

Kyoung A Kim, Tae Ho Cho

***Abstract***: *Wireless sensor network is formed with limited energy resources, easily compromised by an adversary because of hostile environments. Adversary may use compromised nodes to inject false reports and launch DoS attacks, thus, sensor nodes are prone to failure and which makes the network topology configurations highly dynamic in real world applications. A variety of en-route filtering schemes have been proposed to drop and defeat these attacks by using their own cryptographic methods. Some of them ask for a fixed path between a base station and each cluster, so they are not feasible for dynamic network. Additionally, other proposals do not consider various environmental variables in a dynamic environment, so they only choose static paths. In contrast, we consider topology changes, communication costs, the maximum number of key dissemination hops, and the spread of nodes for providing optimum filtering capacity. This paper presents a fuzzy-based adaptive multipath selection method in dynamic environment of a wireless sensor network. Our proposed method can adjust the optimized number of multipaths during key dissemination. Experimental results show that relatively higher filtering capacity with lower energy consumption and suitable nodes for highly dynamic networks.*

***Keywords***: *Wireless Sensor Networks; Artificial Intelligence; En-Route Filtering; Secure Routing; Internet of Things (IoT)*

## I. INTRODUCTION

A wireless sensor network (WSN), as shown in Fig.1, is composed of a number of small sensor nodes that are densely deployed. These nodes process and sense data and communicate with each other, and the base station (BS) collects sensed reports and analysis from the sensor nodes. Sensor nodes have limited capabilities and communication resources and battery power [1]. WSNs require low cost, low power consumption, and good mobility to be suitable for dynamic environments. One powerful aspect of WSNs is their ability to be mobile and autonomous, they have no strings attached. Therefore, WSNs can be applied for target field imaging, distributed computing, detecting ambient intrusion, and monitoring of various dynamic environments. In real-world applications, WSNs are densely deployed by mobile entities that have frequent topology changes. Thus, the sensor network becomes vulnerable to failure when assessing successive events that demand high accuracy [2]. The structure of WSNs has become more dynamic. As a result, the demands on routing and security techniques for highly dynamic networks have significantly increased. There are a lot of routing paths that can be used to prevent false reports, depending on the network architecture and filtering schemes.

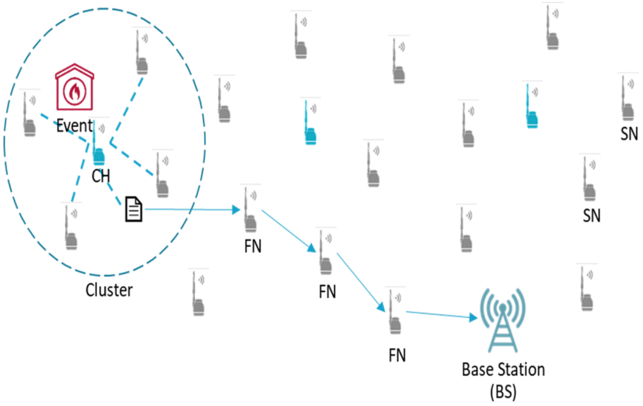


**Fig. 1.Wireless Sensor Network**

Attackers can compromise multiple sensor nodes using false report attacks [3] and DoS attacks by using selective forwarding, etc. Sensor nodes are affected by physical attacks, potentially compromising the sensor's cryptographic keys and waste limited energy. Various en-route filtering schemes such as dynamic en-route filtering (DEF), statistical en-route filtering (SEF), and bandwidth efficient cooperative authentication (BECAN) can solve these problems by filtering reports as they are forwarded towards the BS and by using the collaborative endorsement of reports [4].

In this paper, a fuzzy-based adaptive multi-path selection method is proposed for enhancing the filtering capacity and the efficiency of routing path. The proposed method can adjust the number of multipaths in key dissemination to obtain the optimum number and metric of routes. We analyze influential factors of topology changes for fuzzy logic [5] by considering network topology changes, communication costs, and the spread of events.

Our experiments show that, compared to existing schemes, our scheme achieves a higher filtering capacity with lower energy consumption, especially in a highly dynamic network environment. The rest of the paper is organized as follows: Section II presents related works and Section III presents problem statements.

Manuscript published on November 30, 2019.
* Correspondence Author

**Kyoung A. Kim***, Collage of Software Sungkyunkwan University / Product Planning Team Samsung Electronic Suwon, City, Republic of Korea. Email: ka1223@g.skku.edu / ka1223.kim@samsung.com

**Tae Ho Cho**, Collage of Software Sungkyunkwan University, Suwon, Republic of Korea. Email: thcho@skku.edu

The proposed method is described in Section IV. The experimental model and results are analyzed in Section V.

## II. RELATED WORK

### A. False Report Injection Attack

In WSNs, attackers generate false reports using the compromised node Fig. 2. They inject a false report into the WSN, and the false report causes a false alarm from the BS. This depletes limited energy resources from sensor nodes during the forwarding pass. It brings unnecessary energy losses, and ends up shortening the life time of the WSN.

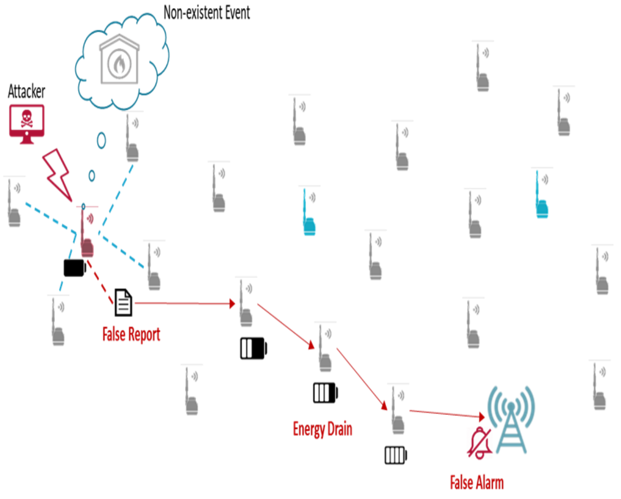


**Fig. 2.False report injection attack**

### B. En-route filtering Scheme

En-route filtering, as shown in Fig. 3, is used for detecting and filtering reports en-route from each sensor node to the BS to prevent against node compromised. Some nodes are randomly assigned key for verification. In en-route filtering, each report is attached with message authentication codes (MACs). Forwarding nodes check for the authenticity of these MACs and a false report is detected as early as possible. For example, if the same key is found, false report detection starts using a MAC at a forwarding node. This helps reduce the number of hops that false reports can travel and saves energy.

En-route filtering schemes have four main operation phases, as shown in Fig. 4: key pre-distribution, key dissemination, report forwarding and en-route filtering. In the key pre-distribution phase, before the sensor nodes are deployed to the field, each node is assigned some keys including authentication keys (Auth keys). In the key dissemination phase, nodes exchange Auth keys with neighbor nodes or forwarding nodes. In the report forwarding phase, a forwarding node receives the report from its upstream node and checks for the Auth keys. If no keys are found in the report, a forwarding node drops the report. In the en-route filtering phase for verification, a forwarding node discloses the Auth keys and verifies the report by using the keys.

If verification of keys is confirmed, then the report is forwarded to downstream nodes in the path. If verification of keys is not confirmed, the report is dropped.

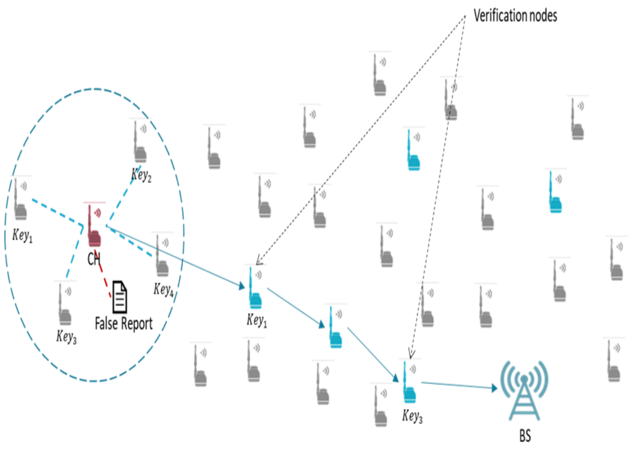


**Fig. 3.En-route filtering scheme**

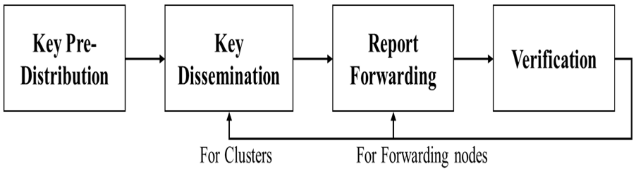


**Fig. 4.Four phases of en-route filtering**

### C. Dynamic En-route Filtering (DEF) Scheme

In DEF [6], which is a scheme proposed by Z. Yu and Y. Guan to defend against false report injection attacks, each sensor node is preloaded with a hash chain of Auth keys and secret keys (Fig. 5). These keys are used for authenticating reports, before nodes are deployed. After nodes are distributed in the field, they form clusters. Then, each cluster head (CH) collects keys from their member nodes and aggregates them into a report by attaching multiple MACs, which are generated using the authentication key stored in each node. For making the authentication key, a distinct seed key is preloaded on each node. The report is disseminated to the next node along the routing path toward the BS, as shown in Fig. 5. Each forwarding node verifies some of the MACs carried in the reports, whether it has any keys used to generate those MACs or not. These keys are used to determine if the event report is false or not. Each node has secret keys which are randomly selected from a global key pool. The n secret key is randomly selected from a y-key pool with a size of v, and l key is randomly selected from a z-key pool with size of w. All clusters have at least one other z key in the cluster. These secret keys are used to generate a sequence of Auth keys using a hash function thus each node maintains a hash chain of keys.

In the key dissemination phase, Auth keys of all the participating nodes are disseminated by the CH periodically to verify generated false reports from compromised nodes. This phase has multiple steps. First, each node generates an encrypted authentication message using one of its secret keys and sends to CH node.

Then, CH collects the authentication message from all nodes belonging to the cluster and aggregates them into message K(n). In (1), …, are the nodes of the cluster.

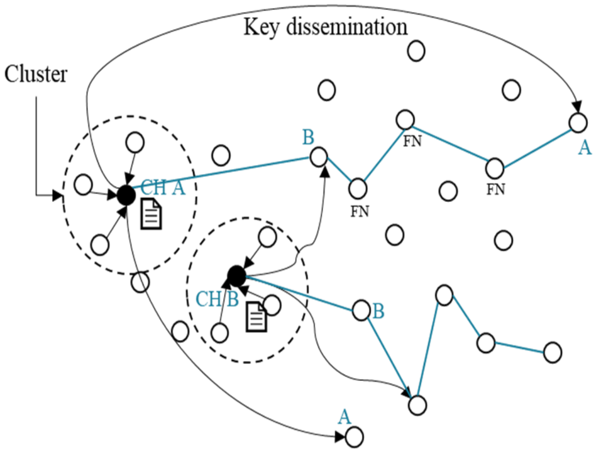


**Fig. 5.Key dissemination in the DEF, where CH selects q (q > 1) hyper-parameter in the DEF**

$$K(v) = \{Auth\ (v_1),\ldots,\ Auth\ (v_n)\} \qquad (1)$$

Next, CH selects q (q > 1) hyper-parameter downstream forwarding nodes from neighboring nodes and transfers K(n), as shown in Fig. 5.

Choosing q is important, because the report can be switched to another node when neighbor node is compromised. This makes the network filtering capacity higher and improves the efficiency.

When a forwarding node receives K(n), it performs the followings:

- It verifies that K(n) has at least t distinct z-key indexes. If not, K(n) is judged to be false and is discarded.
- If it has the same index as the secret key in K(n), the corresponding message is decrypted and the authentication key is stored in its own memory. If there is no index, K(n) is discarded.
- K(n) is transmitted to q neighbor nodes. Each node repeats the above operations until K(n) has been forwarded by the maximum number of hops along multipaths from neighbor nodes and transfers K(n).

Report forwarding is executed by each forwarding node in every round, and all nodes generate a MAC by using a new authentication key to authenticate the reports and send them to its CH. In the CH, the number of sensor nodes that participate in generating a report is pre-determined before deployment. The CH makes an aggregated report and forwards it to neighbor nodes toward the BS. The intermediate node sends an ok message when the report has been received correctly. The CH then exposes the authentication key of the sensor nodes and verifies the report. Finally, it informs the next hop node of the verified result. This process is repeated until the report arrives at the BS or is discarded.

For verification by the forwarding nodes, the intermediate node exposes its Auth keys. After receiving the Auth keys, the forwarding nodes verify the report, and inform the next hop node of the verified result. This process is repeated until the report arrives at the BS or is discarded.

## III. PROBLEM STATEMENT

In this section, we briefly provide the motivation of this paper by providing background description of en-route filtering schemes in dynamic WSNs. We also describe some improvements for this technique.

### A. Dynamic WSN environment Using En-route Filtering

When events occur continuously, the network topology becomes highly dynamic, which means nodes can join or leave the network. This means that key dissemination should be performed periodically, since some forwarding nodes can be aware of when the disseminated keys fail. At each key dissemination phase, networks have different percentages of sensor nodes in the OFF time, different communication costs regarding MLs, and different spreads of events. As a result, the dynamical nature of the WSN is different in each phase; therefore, WSNs need dynamic paths in every phase. However, most en-route filtering schemes use static paths in each phase without consideration of these mitigating factors, which can affect the dynamicity of the network. This is unsuited for use in a dynamic environment.

Hence, when using en-route filtering in dynamic WSNs, choosing q multipaths is very important for the filtering capacity. The value q is the appropriate path number of each filtering phase. Naturally, a larger q enables more nodes to receive the key for filtering reports. However, the memory-related resource constrains of filtering lead to limited storage space for keys of sensor nodes, which lowers the filtering capacity. Some filtering schemes also try to deal with this issue by selecting static multipaths. However, these schemes do not consider various environment variables, and the static paths are inefficient in real-world, dynamic WSNs. Since the report can be switched to another node by a dynamic network, selecting the paths is very important. Therefore, we considered various factors when choosing the appropriate q in each key dissemination phase.

### B. Routing and Security in Dynamic WSNs

Current routing protocols usually assume a stationary WSN, and advanced secure routing protocols need to be developed to satisfy dynamic WSNs [7]. Similarly, some en-route filtering schemes try to adopt multipath routing in the key dissemination phase to reduce the cost of updating keys and mitigate the impact of selective forwarding attacks; this is done by selecting q multiple downstream nodes. However, these techniques only consider a static factor, and they are still inefficient in dynamic networks. For a real network, we should pick various and flexible values of q for a dynamic network environment.

In terms of security, q downstream paths should be selected by considering the security factors. First, consider the number of keys for verification which are disseminated from the cluster in the path [8]. Furthermore, when redistributing keys, the communication and computational overhead should be less than initial authentication. However, most en-route filtering schemes and routing protocols do not consider these factors. Choosing adaptive routing paths is very crucial since they have a large effect on ability to detect false reports, especially in dynamic networks.

## IV. PROPOSED METHOD

In this section, we mention our assumptions for the proposed method in Section A, present an overview of the proposed method in Section B, explain the proposed method in detail in Section C, and discuss the fuzzy logic design in Section D.

### A. Assumptions

This paper makes the following assumptions. The sensor network is composed of multiple wireless sensor nodes and the network is divided into clusters. Each cluster consists of n member nodes. All nodes within the cluster have the same capacity and can be elected as a CH with the same ratio for balanced energy consumption. We used the LEACH head (Low Energy Adaptive Clustering Hierarchy) [9] algorithm to create the cluster and designate a CH. Because the LEACH head randomly selects a normal node as a CH and rotates this role constantly for uniform energy dissipation, it is suitable for our environment. For CH rotating, we set threshold values equal to 0.5, and a sensor node selects a random number, r (0~1). If r is less than 0.5, the node becomes a CH for the current round. The CHs broadcast a message in the network, and all non-CH nodes choose a cluster they want to join depending on the signal strength of the message.

Since sensor nodes are not tamper-resistant, they can be compromised by attackers and these nodes can cause false report injection attacks and DoS attacks. However, they cannot compromise the BS.

In addition, since the key pre-distribution phase is operated before dissemination, the BS has a global key pool, which contains the sets of keys distributed to each node. Any report can be verified by the BS. When a false report is delivered to the BS, the BS knows that the false report exists [10]. Reports do not disappear during transmission and the impact of link quality on report delivery is ignored. Since sensor nodes are prone to failure and need to switch their states between ON and OFF to maintain energy efficiency, the topologies of WSNs change frequently. Messages generated by the same cluster can be delivered along different paths to the BS using various routing protocols such as GPSR [11], or MCF [12]. Regarding changes in the network topology, the BS is aware of the node energy of the distribution request message path, source cluster ID, message length, maximum hop count, and node ON/OFF state. It is also knowledgeable of the estimated event spread level of the network. Furthermore, the BS has a mechanism to authenticate broadcast messages, and every node can verify the broadcast message. In the proposed method, referred to as cluster ID, the energy levels are stored in messages from the CH or forwarding nodes, as follows (2):

$$\text{CH} \,||\, \text{FN} <-> \text{BS: } \{\, Cluster_{id} \text{ , NS, EL}\} \qquad (2)$$

Here, FN is the forwarding node and, NS is the ON/OFF state of the nodes in the cluster, ER is the energy level of nodes, and $Cluster_{id}$ is the identity of the source CH. The notation || means "or", <-> means bidirectional communication, and {…} means messages.

### B. Overview

Most en-route filtering schemes use the same downstream paths in each key distribution phase without considering the network state or changing the number of paths. In the proposed method, the number and metric of multiple paths q is adaptively determined by considering the network state in each phase using a fuzzy rule-based system to improve the filtering capacity and energy efficiency, as shown in Fig. 6(a). To determine q, we define the percentage of nodes OFF time as the network churn rate (CR) [6], the number of nodes in each cluster as the Message Length (ML), and the maximum hop count during key dissemination as $H_{max}$ (HM) [6]. We also account for the node spread level (NSL) of the network.

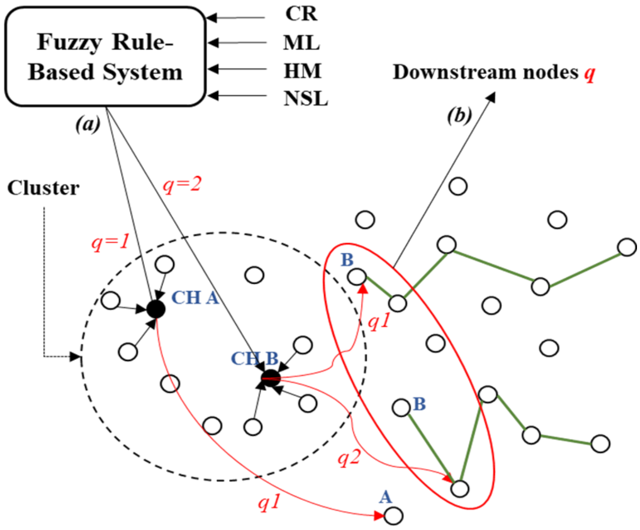


**Fig. 6.Overview of the proposed method**

The fuzzy system can evaluate q through these factors. As a result, our proposed method can determine a more suitable q. If the value of q is changed, the CHs determine different paths for key dissemination (Fig. 6(b)).

### C. Detailed Procedure

Each CH aggregates the authentication key of $v_1 – v_n$ nodes in the cluster into the message K(n) and then disseminates it to q neighbor nodes, as shown in Fig. 7(a).

One of the q nodes, i.e., the next node  decrypts Auth keys from K(n) and forwards this information to q downstream neighbors toward the BS as shown in Fig. 7(b). This is done until each K(n) has been disseminated  times or until it gets to the BS Fig. 7(c). During each key dissemination phase, the CHs receive a control message includes the CR, HM, NSL of the network, as well as the ML of the cluster. This stored information is used to estimate the topology change, filtering capacity and energy and memory efficiencies of the network.

Based on this information, each cluster can determine q multiple paths using fuzzy logic. Intuitively, a larger q means more nodes can receive the key information that is necessary for filtering false reports; this is more suitable for dynamic networks. However, the limited resources of the sensor can limit the number of stored Auth keys. As a result, the filtering capacity may be lowered.

Meanwhile, fuzzy logic is a form of many-valued logic that can handle the concept of a partial truth. Thus, we set key factors, (e.g., the CR and HM of the network, the ML of each cluster, and the NSL of the path) to optimize the value of q using fuzzy logic. These key factors are used for input parameters, as shown in Fig. 8(a). A CR = 0.4 indicates that 40% of the nodes in the network are OFF [6]. If the CR is greater than 0.6, topology changes occur too frequently, generating path breaks. Consequently, reports are dropped. In this case, the value of q does not decisively affect the filtering capacity, so q = 1 is suitable. In a fuzzy system, the CR is set to TD (Too Dynamic). On the other hand, when the CR is smaller than 0.6, the network partition is not a big problem. However, the frequency of key dissemination becomes a main issue for the filtering capacity, and q can be a key factor. More frequent topology changes require high q values. In a fuzzy system, the CR can be differentiated as D (Dynamic), N (Normal), and S (Static) when the CR is 0.

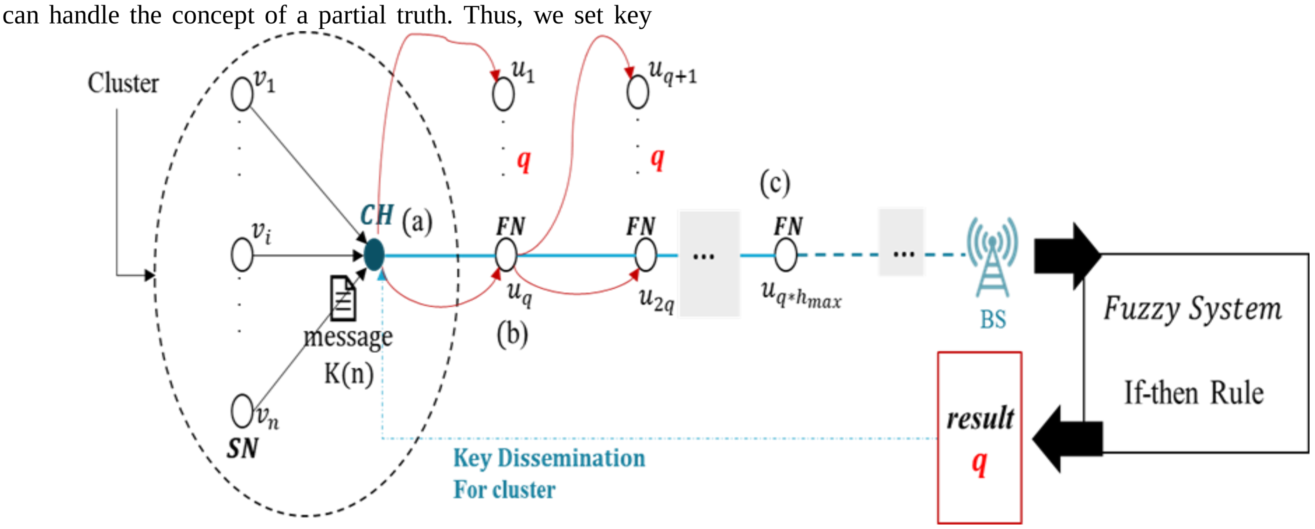


**Fig. 7.Detailed key dissemination procedure**

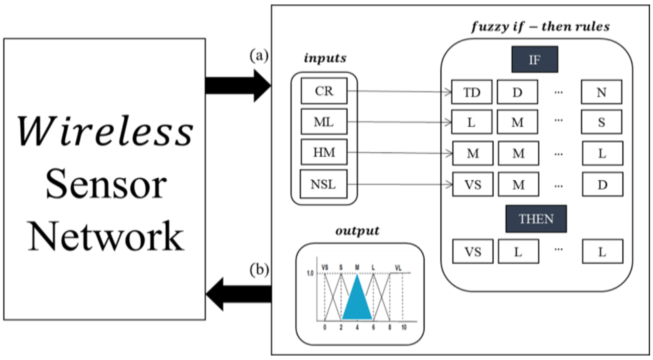


**Fig. 8.Detailed Fuzzy if-then rules in the proposed method**

The ML can calculate the number of nodes and the MACs in the cluster. The ML can be estimated by using (3):

$$ML = L_{Auth(vi)} \times NNC \qquad (3)$$

Here, NNC is the number of nodes in the cluster and $L_{Auth(vi)}$ is the Auth ML of each node. A large ML indicates that the message is long, i.e., there are many nodes in the cluster. This results in high overhead of the limited memory, and q cannot be larger than a small ML.

The large $h_{max}$ can make more nodes capable of filtering false reports. However, this only considers the hop count. By choosing q at the same time, the number of MHs and the path number are considered together. This makes managing the limited memory size more efficient.

The NSL is largely linked to the density of the network. If nodes are densely deployed (i.e., large NSL), many Auth keys and a large amount of energy are required; therefore, the q value and routing metric need to be evaluated for suitability. In this method, the NSL can be described as D (Dense) when there are over 5,000 nodes, M (Medium) when there are 1,000–5,000 nodes, S (Sparse) when there are 100–999 nodes, and VS (Very Sparse) when there are under 100 nodes.

The result of the fuzzy system is determined based on the defined fuzzy if-then rules (Fig. 8(b)). Depending on the output, q is selected. For every key dissemination phase, each CH chooses q multiple paths and the route metric adaptively.

## D. Fuzzy Logic Design

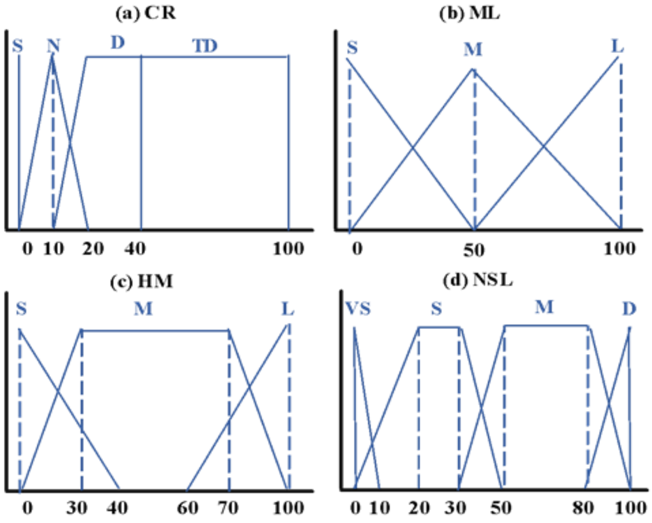


**Fig. 9. Input parameters of fuzzy membership functions**

Retrieval Number: D4545118419/2019©BEIESP
DOI:10.35940/ijrte.D4545.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Fuzzy logic has been applied to many fields and is especially useful for Artificial Intelligence (AI). Fuzzy logic can evaluate propositions with variable answers. It is employed to handle the concept of partial truth, where the truth value may range between completely true and false [13]. Thus, fuzzy logic can use degrees of truth as an equivocal mathematical model. With this feature, the sub-range of a continuous variable and non-numeric values can be used to facilitate the explanation of rules. Moreover, the output of a fuzzy system is a consensus of all inputs or rules, and it is easily implemented and robust. It can be argued that each phase can perform fuzzy computations. A fuzzy system is implemented only in the key dissemination phase, which does not the huge field. Hence, fuzzy logic is highly recommended when input values are not available or trustworthy, or when the number of inputs and the amount of storage space is small. To respond progressively and degrade gracefully in adaptive control systems, fuzzy logic is better than the AI methods such as deep-learning or random forest.

Fig. 9 (a), (b), (c), and (d) illustrate the membership functions of the fuzzy logic input parameters used. The labels of the fuzzy variables are represented as follows:

- CR = {S (Static), N (Normal), D (Dynamic), TD (Too Dynamic)}
- ML = {S (short), M (Medium), L (Long)}
- HM = {S (Small), M (Medium), L (Large)}
- NSL = {VS (Very Sparse), S (Sparse), M (Medium), D (Dense)}

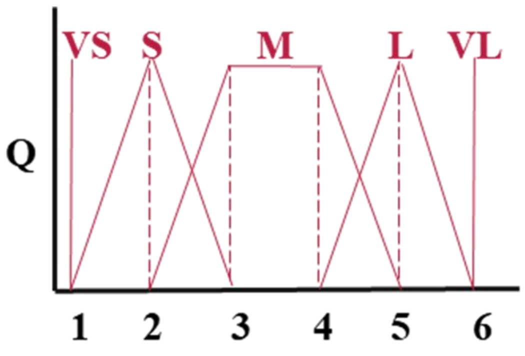


**Fig. 10. Output parameters of fuzzy membership functions**

The output parameter of the fuzzy logic Q is represented by the membership functions as shown in Fig. 10 and as follows:

- Q = {VS (Very Small), S (Small), M (Medium), L (Large), VL (Very Large)}

The rule base of the system is comprised of 144 = (4×3×3×4) rules. Some of the rules are shown in Table I. If the CR is N, ML is M, HM is M, and NSL is W (Rule 53), then the BS determines the q to be S. In other words, when keys are disseminated, the BS chooses the q value.

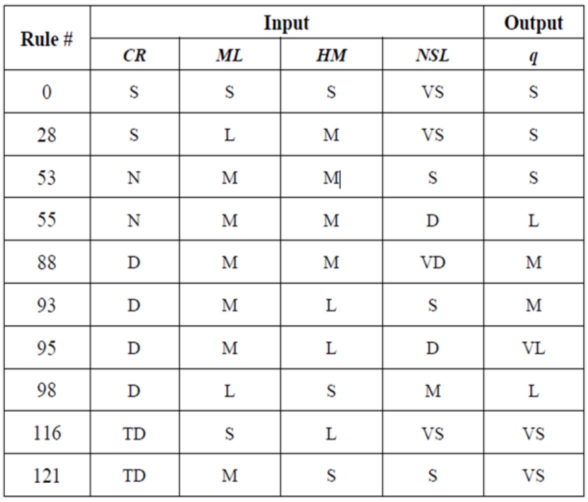
## V. EXPERIMENTAL RESULT

In this section, the efficiency of the proposed method is demonstrated through experimental results. Section A describes the experimental environment and Section B presents the experimental results.

### A. Experimental Environment

A virtual sensor network with a sensor filed size of 1,000 × 1,000 $m^2$ is used. In this sensor field, the number of nodes is randomly determined depending on the NSL. These nodes are divided into clusters. The number of clusters is 10% of the number of nodes, and each cluster contains a different number of nodes depending on the location of each node. Among these nodes, 10% of the nodes are CHs and 90% of the nodes are normal nodes (e.g., if there are 1,000 nodes, there are 100 clusters, 100 CHs, and 900 normal nodes). The BS is located at the top right (x, y = 1000, 1000) of the sensor field. Each node is randomly loaded with three secret keys in each key pool of size 20. Each node requires 16.25μJ to transmit a byte and 12.5μJ to receive a byte. Each MAC verification consumes 75μJ [14]. The size of the original report is 24 bytes, and the MAC is 1 byte. To simulate the dynamic topology, we use the CR and ON/OFF state of the nodes which are decided by a random distribution.

**Table-I: Fuzzy if-then rules**



| Rule # | Input | | | | Output |
|---|---|---|---|---|---|
| | *CR* | *ML* | *HM* | *NSL* | *q* |
| 0 | S | S | S | VS | S |
| 28 | S | L | M | VS | S |
| 53 | N | M | M | S | S |
| 55 | N | M | M | D | L |
| 88 | D | M | M | VD | M |
| 93 | D | M | L | S | M |
| 95 | D | M | L | D | VL |
| 98 | D | L | S | M | L |
| 116 | TD | S | L | VS | VS |
| 121 | TD | M | S | S | VS |

Among the various all en-route filtering schemes in a dynamic network, DEF has the best performance in terms of the filtering capacity: thus, we compared our scheme with DEF in this paper. Usually, in DEF, $h_{max}$ = 3 or 10, and q = 2. However, these factors are sometimes changed to see their effect. In our method, by contrast, $h_{max}$ is used for one of the fuzzy inputs, and q is the output of the fuzzy system. Compromised nodes can be normal nodes or CHs in the selected cluster. No packet loss occurs during node communication.

### B. Experimental Results

The original DEF scheme ( $h_{max}$ = 3 or 10, and q = 2) has been compared with the multipath selection method through the fuzzy rule-based system. The comparison items include the average number of hops traveled by a false report (to analyze the filtering capacity) and the amount of energy consumption (to analyze the energy efficiency). Every experiment shows the impact of hmax on the filtering capacity and the performance of the proposed method at the same time.

Naturally, a larger $h_{max}$ can increase the filtering capacity. However, increasing the value of $h_{max}$ by too much, especially when $h_{max} > 10$, does not offer much improvement, but it does increase the memory overhead. In contrast, adaptively selecting q considering $h_{max}$ leads to higher capacity. We conduct experiments in the dynamic network environment to measure the extent of topology changing. The degree of the network mobility is 10 times the CR, which indicates the extent of topology change. For instance, if the network mobility equals 6, this indicates that 60% of the nodes in the network are OFF. In this scenario, topology changes occur too frequently and path breaking occurs. We distinguish the following two cases [6]. First, when the network mobility is greater than 6, the deployed network is severely partitioned, and there are a lot of isolated nodes leading to path breaking. This means that when the mobility value is larger than 6, more and more false reports are filtered due to broken paths. In contrast, when the network mobility value is smaller than 6 (red box), the broken paths are not an issue, and the filtering capacity is mainly determined by the average number of hops.

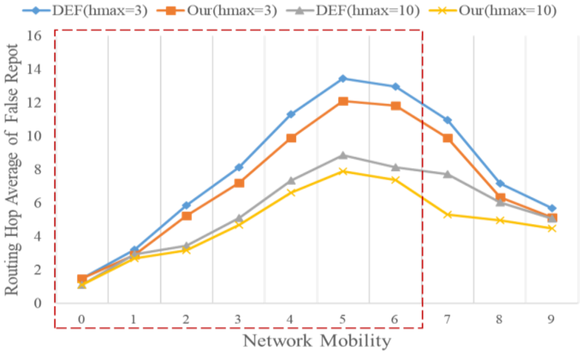


**Fig. 11. Average hop count of false report versus the network mobility (in a dynamic network)**

The smaller the number of hops, the higher the filtering capacity of a false report. Sensor nodes have limited energy and are prone to failure. Thus, they may also turn off the radio and CPU to save energy, which makes the topology of sensor networks highly dynamic. Fig. 11 depicts how the filtering capacity varies as a function of network mobility, where the filtering capacity is measured as the average number of hops traveled.

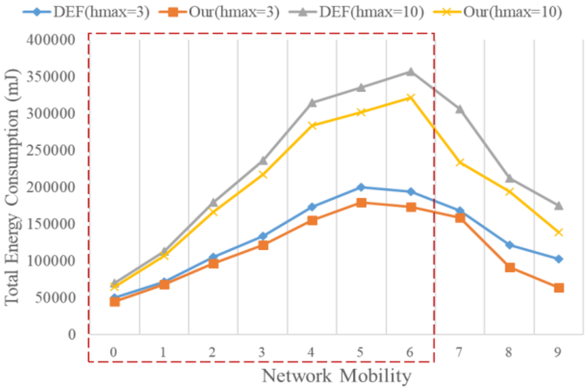


**Fig. 12. Energy consumption versus the network mobility (in a dynamic environments)**

Fig. 12 illustrates how the total energy consumption changes with the degree of network mobility (in a dynamic network). In the proposed method, q paths are adaptively selected by fuzzy logic. The total energy consumption is calculated by combining the energy used by key dissemination and false reports. In both schemes, when the value of $h_{max}$ is greater, more energy is consumed due to the number of key disseminations. By adaptively selecting q multiple paths, the proposed scheme can generally save energy. However, when the network mobility degree is 5, the proposed method requires q more downstream paths to disseminate keys, and it needs to spend more energy along the key distribution. Intuitively, the higher filtering capacity makes this reasonable.

**Table-II: Average network mobility values of DEF and the proposed method**

| | Routing Hop of F/R | Energy Consumption |
|---|---|---|
| DEF | 6.81 | 181,137 |
| Proposed Method | 8.03 | 159,415 |
| **Improve** | **9.31%** | **10.59%** |

Table. II. Shows that when $h_{max}$ = 3 or 10, DEF sets q = 2. Alternatively, the proposed method sets q depending on the results of fuzzy logic. The proposed method improves the number of routing hops by an average of 9.31%. Additionally, the proposed method demonstrates 10.59% energy savings compared to the original DEF.

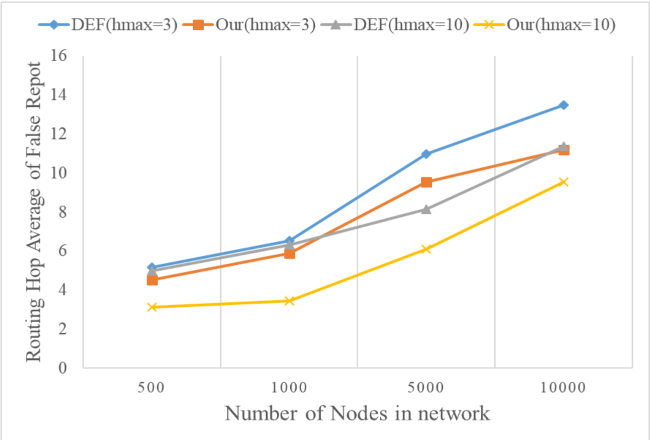


**Fig. 13. Average hop count of false report versus the number of nodes**

Fig. 13 and Fig. 14 show the effects of the number of nodes in the network. As the number of nodes in the network increases, the network becomes more dynamic and more energy is required. In the proposed method, q paths are adaptively selected by considering the network environments; this leads to higher filtering capacity and less energy consumption than the original DEF. The experiment shows that there is 9.31% routing hop improvement on average and an average energy saving of 10.59%.

When there are a lot of nodes in the network, the proposed method selects a higher q to distribute keys when filtering false reports; however, when keys are re-distributed, our method checks the states of nodes in the network and adaptively re-selects q paths, which makes it more suitable for dynamic networks.

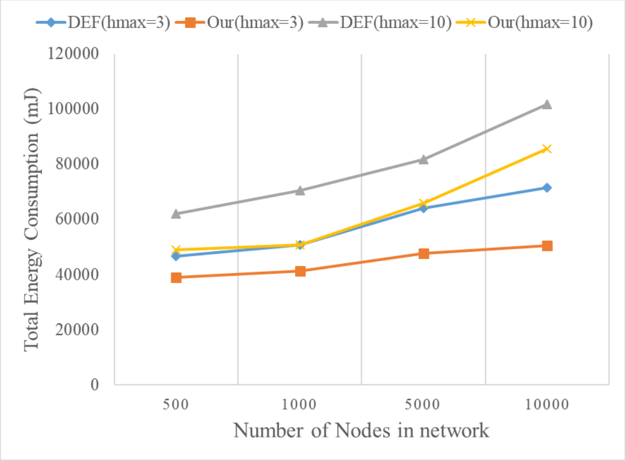
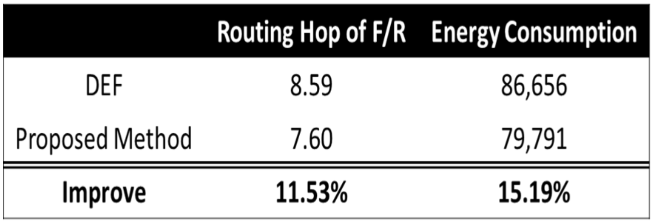


**Fig. 14. Total energy consumption versus the number of nodes in the network**

**Table-III: Average number of nodes in the network for DEF and Proposed method**



| | Routing Hop of F/R | Energy Consumption |
|---|---|---|
| DEF | 8.59 | 86,656 |
| Proposed Method | 7.60 | 79,791 |
| **Improve** | **11.53%** | **15.19%** |

Table. III. Shows that when $h_{max}$ = 3 or 10, DEF sets q = 2. Alternatively, proposed method sets q depending on the results of fuzzy logic. The proposed method improves routing hop by an average of 11.53%. It also reduces the energy consumption by the average of 15.19% compared to the original DEF.

## VI. CONCLUSION AND FUTURE WORKS

WSNs are supplied with limited energy resources, being deployed in open environments. More than that, demands on routing and security techniques for highly dynamic networks have been significantly on the rise in the real world. Therefore, both routing and security protocols should consider the energy consumption behavior of the dynamic network as well as capacity of protocol. Surprisingly, very few studies deal with considering the en-route filtering scheme efficiency for energy and filtering capacity for security at the same time. In this paper, we propose an enhanced en-route filtering scheme for energy savings and detection performance improvement in dynamic networks. Through the proposed method, q multiple paths are selected adaptively using fuzzy logic. By optimizing the number and the metric of multipath, our scheme obtains higher security capacity and energy efficiency in dynamic networks. In accordance with the degree of the topology change, q is adjusted, thus reducing the unnecessary memory waste and energy consumption. Moreover, optimum value of q that considers limited memory size enables more nodes to receive the key information necessary for filtering, so it is more suited for dynamic networks.

In the future, we will compare attack metrics in dynamic network and study when nodes switch awakes or sleep states for energy efficiency in dynamic network. Moreover, we will study how to obtain highly efficient routing metrics of each cluster of q multiple paths considering the network environment and implement changes more specific to applications.

## 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. S. Zhu, S. Setia, S. Jajodia, and P. Ning. “An Interleaved Hop-by-hop Authentication scheme for filtering of injected false data in sensor networks”. *Proc. of the IEEE Symposium on Security and Privacy*, May 2004.
2. H. S. Han and T.S. Shon. “Sensor authentication in dynamic wireless sensor network environments”. *IJRFIDSC*, vol. 1, 2012, pp. 36-44
3. H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, “Toward resilient security in wireless sensor networks”. *Proc. of ACM MobiCom*, 2005, pp. 34-45.
4. A. kumar and A. R. pais. “En-route filtering techniques in wireless sensor networks: a survey”. *Wireless Personal Communications*, vol. 96, 2017, pp. 697-739.
5. J. Yen and R. Langari, Fuzzy Logic: Intelligence, Control, and Information, *Prentice-Hall*, Inc., 1998.
6. Z. Yu and Y. Guan. “A Dynamic En-route Filtering scheme for reporting in wireless sensor networks”. *IEEE/ACM Transl. on Networking*. vol. 18, 2010, pp.150-163.
7. J. SEN. “A survey on wireless sensor network security”. *IJCNIS*, Vol. 1, 2009, pp. 5578
8. H. Y. Lee and T. H. Cho. “Fuzzy-based path selection method for improving the detection of false reports in sensor networks”. *IEICE Transactions on Information and Systems* vol. 92, 2009, pp.1574-1576.
9. W. Heinzelman, A. Chandrakasan and H. Balakrishnan. “Energy-Efficient Communication Protocol for Wireless Microsensor Networks”. *Proc. 33rd Hawaii Int’l. Conf. Sys. Sci.*, Jan. 2000.
10. H. Yang and S. Lu. “Commutative cipher based en-route filtering in wireless sensor networks”. *Proc. of VTC*, 2003, pp.1223-1227.
11. B. Karp and H. T. Kung. “GPSR: Greedy perimeter stateless routing for wireless networks”. *Proc. of ACM MobiCom*, 2000, pp. 243-254.
12. F. Ye, A. Chen, S. Lu, and L. Zhang. “A scalable solution to Minimum Cost Forwarding in large sensor networks”. *Proc. ICCCN*, 2001.
13. V. Novák, I. Perfilieva, and J. Močkoř, “Mathematical principles of fuzzy logic Dodrecht: Kluwer Academic”. 1999. ISBN 0-7923-8595-0
14. F. Ye, H. Luo, S. Lu, and L. Zhang. “Statistical en-route detection and filtering of injected false data in sensor networks". *Proc. of IEEE INFOCOM*, 2004, vol. 4, pp. 2446-2457.

## AUTHORS PROFILE

**Kyoung A Kim** received the B.S. degree in Computer Science and International relationship from the University of Seoul, Republic of Korea, in 2011. She is currently pursuing a M.S. degree in Semiconductor and Display Engineering at Sungkwyunkwan University, Suwon, Korea. Since 2010, she has been working in the Memory division of Samsung Electronics. Her research interests are in the areas of artificial intelligence, and enterprise resource planning.

**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 system, modeling & simulation, and enterprise resource planning.