AN ENHANCED DETECTION AND ENERGY-EFFICIENT EN-ROUTE FILTERING SCHEME IN WIRELESS SENSOR NETWORKS

Muhammad K. Shahzad[1] and Tae Ho Cho[1]

[1]School of Information and Communication Engineering,
Sungkyunkwan University Suwon 440-746, Republic of Korea

ABSTRACT

Wireless sensor networks (WSNs), due to their small size, low cost, and untethered communication over a short-range, have great potential for applications and services. Due to hostile environments and an unattended nature, they are prone to many types of attacks by adversaries. False data injection attacks compromise data accuracy at the sink node and cause undesirable energy depletion at the sink and intermediate nodes. In order to detect and counter false data attacks, a number of en-route filtering schemes have been proposed. However, they lack a strong false report detection capacity or cannot support network dynamics well. Commutative cipher-based en-route filtering (CCEF) is based on fixed paths, and a fixed detection probability, and does not consider the residual energy of a node. In an enhanced detection-capacity and energy-efficient en-route filtering (EDEF) scheme, we use a fuzzy logic system which considers the residual energy, false traffic ratio (FTR), and number of message authentication codes (MACs) in a report to evaluate the fitness of a node to be a verification node. This helps to balance network energy usage and reduce the number of hops a false report may travel. The simulation results demonstrate the validity of our scheme with increased energy-efficiency (4.55 to 13.92%) and detection power (99.95%) against false report attacks in WSNs.

KEYWORDS

Wireless sensor networks, energy-efficiency, detection-capacity, en-route filtering &fuzzy logic

1. INTRODUCTION

Advances in wireless communication have offered low cost, low energy, small size, and multi-purpose sensor nodes over short range communications. Given extremely limited resources, uncertain network conditions, and a hazardous environment, network resources should be managed wisely to cater to wireless sensor network (WSN) needs. Increasing false report detection-capacity and energy-efficiency is an important challenge. In this paper we investigate a fuzzy-based approach to increase the detection power and to save more energy in comparison with variants of commutative cipher-based en-route filtering (CCEF) [1] scheme.

In a WSN, sensor nodes are randomly distributed and are left unattended for long periods of time. An attacker can compromise these nodes, steal information, or waste scarce network resources. Such attacks are prevented or minimized by implementing security measures that save energy through early or better detection and the prevention of such attacks. A typical false report injection attack in sensor network is shown in Figure 1. As the reports from a compromised sensor node traverse the path from the false event location to the sink-node or base station (BS), energy along the path is drained. Ultimately, a false alarm is triggered for a non-existent event at a user's device.

DOI : 10.5121/ieij.2015.3302

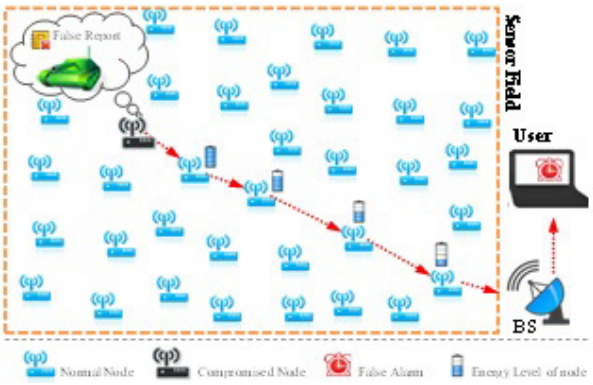


Figure 1. A typical Attack Scenario in Wireless Sensor Network

Research has sought to increase the security of WSNs using en-route filtering schemes and their modifications [1-12], underlying routing protocols [13-17], and energy-efficient clustering and resource management [18-22]. Recently, it has been observed that the sensor nodes closer to the sink and on critical paths tend to deplete their energy at a faster rate than the other nodes [23].This results in energy-holes or uneven energy-distribution around the sink which results in a reduced network lifetime. This indicates that while making routing decisions or selecting filtering nodes, the residual energy of a node should also be considered. An interleaved hop-by-hop authentication (IHA) scheme [4] and CCEF rely on fixed paths routing such asgreedy perimeter stateless routing (GPSR)[14]; they create a path and use it for the life of the communication route between the source and theBS. Another limitation of CCEF is that it does not consider energy when making routing decisions or selecting a filtering node.

In this paper, we propose an enhanced detection-capacity and energy-efficient en-route filtering (EDEF) scheme. We use a fuzzy logic system which takes the residual energy level ($ENERGY$), false traffic ratio (FTR), and number of message authentication codes ($MACs$) in a report and determined the fitness ($FITNESS$) of an en-route node to be a verification node. Fuzzy logic deals with uncertainty or errors in engineering by adding some degree of certainty in the answering of logical questions. Normal logic relies on a series of true or false statements; however, for many situations, the input is similar to ‘maybe’ or ‘not sure’, rather than a certain 0 or 1. Fuzzy logic is simple, practical, and a strong candidate for applications which require minimum onboard computation and fast implementation. The fuzzy system may not be optimal but it can be acceptable for sensor networks due to lowers size and cost. If the fitness value of an evaluated node is greater than threshold T_h, the fuzzy fitness value of a sensor node, this node can be selected as a filtering node.

The main features of EDEF are as follows: 1) design and implementation of a new detection power technique, 2) fuzzy logic is used to carefully select verification nodes, and 3) detection probability depends on variation in the number of attacks, which is fixed in CCEF. The simulation results demonstrate the validity of our scheme with increased energy-efficiency due to better detection-capacity against false report attacks in WSNs.

EDEF has the following advantages:

- Improvement in energy-efficiency
- Increased detection-capacity
- Ability to adapt to network conditions

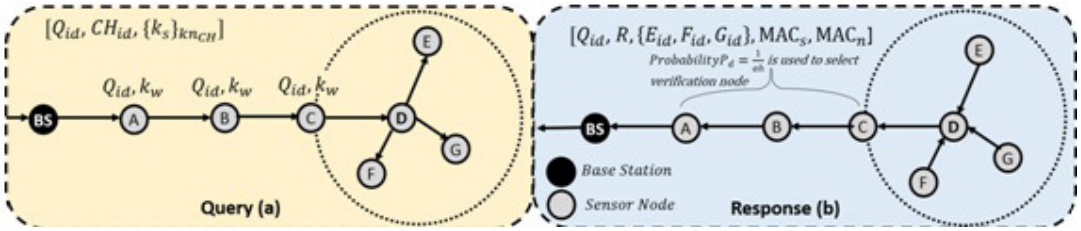


Figure 2. Query and response procedure in CCEF

With an increased FTR, a greater number of filtering nodes are assigned; hence, more verifications take place. Energy is therefore saved by dropping false reports earlier. For a low FTR, fewer filtering nodes are assigned so a small number of verifications take place. Energy can also besaved since true or legitimate reports may to go through a smaller number of verifications. However, our scheme rely on the better and early filtering with more verifications, it means more energy is saved in fabricated report whereas less on legitimate reports which has to go through more verifications.

1.1Background

In this section, we present working of CCEF in detail.

1.1.1. Query and Response

The simple query and response procedure of CCEF is shown in Figure 2. The query message consisting of Query ID (Q_{id}), a cluster head (CH) ID (CH_{id}), and a session key (k_s) encrypted with a CH node key (k_n) i.e., $\{k_s\}_{kn_{CH}}$, is forwarded to the source CH.TheQ_{id} and$k_w$keys are dropped on every node in the path as shown in Figure 2(a). The verification node(s) on reverse path are selected based on probability $P_d = 1/\alpha h$, where α is design parameter and h is number of hops. The response consists of Q_{id}, a report (R), the $IDs$of $E, F,$ and G, a session MAC (MAC_s) and a node MAC (MAC_n).The MAC_n is generated by a simple XOR operation using the selected t nodes, and the $MAC_s$is generated by the k_s key.

A report is endorsed by the neighbors (*i.e. an event sensing node sends event information along with* MAC_n*- it verifies that event report is from legitimate neighbor*)which receive the event's information and is forwarded to theCH, as shown in Figure 2(b). When the query reaches D, the k_n key is used to decrypt the k_s key to verify if the query was sent by the originalBS. The CH compresses the $MACs$ of event sensing nodes to generate its MAC_n using an exclusive OR (XOR) operation. The XOR operation is used because of its simplicity to obtained single compressed MAC_n of CH node. In case of one or more event sensing nodes will send report with wrong MAC_n, theBS will know one or more event sensing nodes or $CH$is compromised because same MAC_n of CH node could not be regenerate. It prepares and sends response message along with the MAC_s and the IDs of the endorsing nodes. Using a detection probabilistic method intermediate nodes A and C are selected as verification nodes. After the CHreplies, a session is established. Following this procedure, a path is created to the event location. A session expires after t time units or after a node is depleted (*i.e. sensor node residual energy reaches to zero and cannot communicate*).

1.1.2. Verification and MAC Generation

When the report in the response message reaches the BS, it generates theMAC_n of the CH using the $MACs$ of nodes with IDs in the report and verifies it along with the MAC_s. This validates the CH and all of the report-endorsing neighbors if both conditions are verified. If not, either the CH or one or more of the endorsing nodes are compromised as mentioned earlier. CCEF is based on

an expansive public key infrastructure [10]. It is a non-symmetric key-based filtering scheme in which intermediate nodes can verify the authenticity of the session without having an authentication key. Instead of authentication keys, $k_w$keys are used to verify the legitimacy of a session. Before communication, a secure session is established between the source of the event and the BS.

2. EXPERIMENTAL ENVIRONMENT

In this section, we explain the experimental environment assumptions and how we obtain the attacks information or FTRwithout incurring extra messages on sensor nodes.

2.1. Assumptions

An adversary can compromise a sensor node; however, the BS cannot be compromised and has sufficient amount of energy and processing power. Moreover, a CH is also assumed to be secure for the duration of a session. The cooperation between multiple nodes is outside the scope of this paper. Sensor field sensor nodes and the BS in the sensor fields are assumed to be static. Unique IDs and k_n keys are preloaded in the sensor nodes. The BS knows the IDs and k_n keys of all nodes. In our implementation of the energy dissipation model, we only consider the energy dissipation that is associated with the radio component. Moreover, we assume that underlying platform for our experimental environment is Mica2 sensor motes [25].

2.2. Experimental model

In this paper, we consider an evenly distributed 5000-node sensor network in grid area of (250×250) $m^2$with a cluster size of (10×10) m^2. In each cluster, an equal number of nodes are randomly positioned. TheBS is aware of the nodeIDs, locations, and k_n keys of all of the sensor nodes. The experiments are performed in a custom built simulator in Microsoft Visual Studio using the C++ programming language. Each sensor node has a fixed energy (e.g., 1 joule) and a limited sensing range. We perform experiments with different FTRs, and as the FTR increases, compromised nodes may also increase.

The energy required to transmit (T_x) and receive (R_x)a bit is 4.28 µJ and 2.36 µJ respectively [24] for Mica2 platform. An event message is 320 bits long and the energy needed to transmit and receive it is 1.37 mJ 0.755 mJ. The energy used in commutative cipher-based computation is 9 mJ [25]. Table 1 shows the parameters for the experimental setup that was used for performance analysis. The communication links are considered to be bidirectional in the sense that if a node A can send a message to$B$, then$B$ is also capable of sending a message back to$A$. When nodes are deployed, the boot-up process is initialized with a localization-awareness component. Each node also assumes a unique $ID$and knows its k_n key.

Parameter	Value
Field area	$(250 \times 250)\ m^2$
Cluster area	$(10 \times 10)\ m^2$
Sensor nodes	5000
Sensor range	25 m
T_x	4.28 mJ[25]
R_x	2.36 mJ[25]
Communicative cipher	9 mJ[26]
Data packet size	320 bits
Node energy	1 J

Table 1. Network environment setup parameters

The energy required to transmit (T_x) and receive (R_x)a bit is 4.28 µJ and 2.36 µJ respectively [24] for Mica2 platform. An event message is 320 bits long and the energy needed to transmit and receive it is 1.37 mJ 0.755 mJ. The energy used in commutative cipher-based computation is 9 mJ [25]. Table 1 shows the parameters for the experimental setup that was used for performance analysis. The communication links are considered to be bidirectional in the sense that if a node A can send a message to$B$, then$B$ is also capable of sending a message back to$A$. When nodes are deployed, the boot-up process is initialized with a localization-awareness component. Each node also assumes a unique $ID$and knows its k_n key.

2.3. Attack information or FTR

The communication in our method is query-driven in which a query message is initiated by the BS to inquire about an event in an area. For one query-response session, the BS knows the expected number of event reports from the source CH. A legitimate report received at the CH will increment the respective counter by one to determine total number such reports. For this case no extra messages or energy consumption is required at the sensor nodes. Fabricated or false reports can be dropped either en-route or at the BS. In first case a fabricated report is dropped en-route, the BS will know report is dropped after a time window is elapsed. In second case, if a fabricated report is reached at the BS, it will be dropped after final verification. In both cases of legitimate and fabricated reports, the BS will know the total number both types of reports by their respective counters. Therefore, by using this information the value of the attack information or simple FTR can be determined at any time by using following formula:

$$FTR = \sum_{e=1}^{n} \frac{Fabricated\ reports\ (injected\ false\ report\ attacks)}{Total\ reports\ (fabricated\ and\ legitimate)} \quad (1)$$

Where e is the number of events from 1 to n.The counters and computations on the BS can be justified since it has sufficient power and computation capacity.

3. PROPOSED SCHEME

In this section we elaborate on the workings of EDEF in detail including boot-up, session and key-distribution, en-route filtering and verification processes at the BS.

3.1. Boot-up initialization

Sensor nodes are considered secure for the initialization during the boot-up process, and it is also assumed that the BScannot be compromised. The sensor nodes have a fixed amount of energy. At this phase, the randomly deployed nodes are granted unique IDs and k_n. Furthermore, each node can know its location through a location mechanism.

3.2. Session set-up and key-distribution

In the proposed method, the BS sends a Q_m message to the CH (*i.e., node D*) that contains the Q_{id}, CH_{id}. In order to establish a session, a plain text k_w key is pre-deterministically disseminated to the portion of the nodes that have a large enough fitness value (*i.e., explained in section 3.3.1*) in as determined by the fuzzy system. However, if k_w keys are distributed pre-deterministically before a session is established, different paths with different numbers of k_w keys may exist, allowing for the identification of a desired path corresponding to the FTR. This helps with dynamically supporting different FTRs in contrast to CCEF where the probability of detection is fixed independent of FTR.

In response, R_m when forwarding a report to the BS, only the nodes selected for k_w keys are used as verification nodes. The rest of the session setup process is similar to CCEF, as explained in background Section 1.1. A session expires after t time units or after a node is depleted.

3.3. Verification

3.3.1. Fitness Value determination

The verification nodes are assigned based on fuzzy rule based evaluation. The fuzzy system output value is called the fitness value used to assign a node as verification role. If the fitness value is greater than threshold (T_h) node can be verification node. The fitness value is determined by using If-Then roles. Some of the rules are presented in Table 2.

Table 2. Selected Fuzzy If-Then Rules

Rule#	$MACs$	$ENERGY$	FTR	$FITNESS$
0	VL	S	VL	U
5	VL	M	L	U
11	VL	L	VH	U
17	E	M	L	N
23	E	L	VH	F

Keys: These abbreviations are defined in section 3.4 where fuzzy logic system used in proposed method is explained with detail.

3.3.2. Membership functions

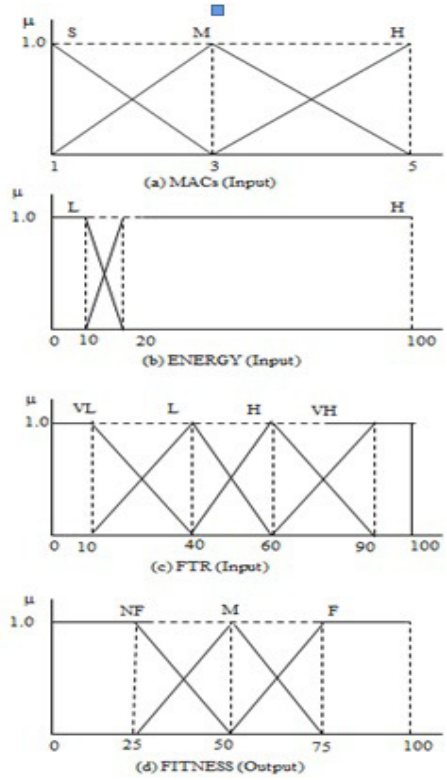
The three input and one output factors of the fuzzy system are called fuzzy membership functions. The three input membership functions are; $MACs$,$ENERGY$,andFTR. The output membership function is$FITNESS$. The role of various membership functions and their impact on performance is illustrated in the Table 3. The number of fuzzy sets of a membership function are selected based security and energy is saving criteria.

Table 3. Selected Fuzzy If-Then Rules

Membership function	Fuzzy sets	Role	Impact on performance
$MACs$	3	Reflect # of nodes attach MACs to report	More MACs more communication overhead
$ENERGY$	2	To prefer higher energy nodes for verifications	Balance energy usage over the larger group of sensor nodes.
FTR	4	Assign verification nodes according to current attacks	Saves more energy at higher FTR by performing more verifications
$FITNESS$	3	Determine verification nodes with T_h	Determine # of verifications nodes depending on T_h

3.3.3. Use of fuzzy logic system

In recent years, the number and diversity of applications of fuzzy logic have been increased significantly from house hold items to industrial process controls. It is methodology which deal with words instead of number to represent human intuition. Dealing with words instead of numbers accommodates the uncertainty of the real world and lower the cost of the solution by exploiting the tolerance for imprecision. In this paper we exploits the tolerance of imprecision, uncertainty, and partial truth (i.e., opposite to T/F or 1/0) in order to achieve tractability, robustness, and low cost of solution.Although mathematical methods are simple, however, finding correct formula in many cases is complex task. In such cases as in this case we have to use fuzzy logic to get an acceptable performance with simple IF-Then roles. As results will demonstrate the use of fuzzy logic we not only achieve better detection-capacity also save energy. Sensor nodes with a fitness value higher than 20% can have verification status by assigning k_w keys and Q_{id} .



3.4. Fuzzy-based fitness evaluation

As mentioned before in order to drive the fitness value of an intermediate node our fuzzy system considers three inputs: a) MACs, b) ENERGY, c) FTR, and returns d) FITNESS. Moreover, the number of fuzzy sets assignment to a membership function is based on its importance to security and energy-efficiency. The number of fuzzy sets determine the level of granularityor degree of a membership function. Moreover, the range of the fuzzy sets is set equal as per standard or based on their importance. Fuzzy membership functions and their associated fuzzy sets are highlighted in Figure3.

- MACs represent the number of MACs attached to the report. The higher the number, the more the communication overhead is associated, and vice versa. This fuzzy membership function has three fuzzy sets, namely small (S), medium (M), and high (H).

- ENERGY represents the residual energy level of a node between 0 to 100%. It has two fuzzy sets, namely low (L) and high (H). The nodes with energy higher than 20% can participate in routing, event information forwarding, and candidates to be verification nodes. The nodes with energy between 10 - 20% cannot be verification node but can still participate in routing and event information forwarding. The nodes with less than 10% can participate in information forwarding only and nodes with energy 0% are depleted nodes.

- FTR has four fuzzy sets; these are very small (VS), small (S), high (H), and very high (VH). This has more fuzzy membership sets due to its relative importance for security to counter different ratios of attacks.

- FITNESS has fuzzy outputs of not fit (NF), medium (M), and fit (F). If the fitness value is higher than threshold$T_h$or 25%, a node is fit to be selected as a verification node. We used hit and trial to find an acceptable level ofT_h.

For the three input factors there are two, three and four fuzzy sets, so there are 24 combinations or rules to be considered for driving the fitness value for the inputs. When the fuzzy rules are matched to one the three fuzzy outputs a sensor node can be assigned one of the NF, M, or F status. The total number of fuzzy sets is reasonable for acceptable solution, which is neither very trivial nor complex for the practicality of a fuzzy system on a sensor node.

4. RESULTS AND DISCUSSION

In both CCEF and proposed schemes, all of the keys, number of keys, types of messages and message lengths are identical. Most of the computations for selecting verification nodes are being done on the BS so there is no extra overhead. Energy savings occurs by reducing the number of hops false reports travel in the sensor network and dynamically adapting to the attack ratio in the fuzzy-based EDEF scheme. We can increase the probability or power for better detection with feasible initial key distribution as proposed in the fuzzy-based fitness method presented in the previous section. The reason for the increase in detection power is that more matching keys are found in a given path as compared to the probabilistic method in the original scheme. In this section, we present the energy-efficiency and detection-capacity of the EDEF scheme in comparison with CCEFvariants (i.e., with different P_d). Similar performance improvement may be expected in the IHA scheme [4], which is also based on a fixed path and detection power.

4.1. Energy-efficiency

In this section, the energy-efficiency is compared with different detection probabilities. In CCEF, the detection probability is independent of the FTR and has a fixed value. In order to compare it with the EDEF scheme, we set $\alpha = \{0.25, 0.50, 0.75, 1.00\}$ with detection capacity $P_d = 1/\alpha h = \{4/h, 2/h, 4/3h, 1/h\}$, where h depends on the number of hops between the source and the BS. If $e_{\frac{1}{\alpha h}}$ is the energy consumed by fix probability based CCEF when $P_d = \frac{1}{\alpha h}$ and e_{EDEF} is the energy consumed by the fuzzy-based EDEF scheme, then the average energy-efficiency is defined by

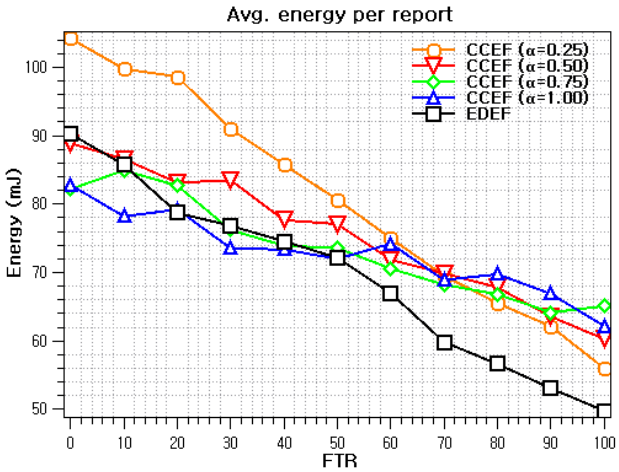


Figure 4: Avg. energy per report in CCEF and EDEF

$$E_e = \left(\left| e_{\frac{1}{\alpha h}} - e_{EDEF} \right| / \left(\frac{e_{\frac{1}{\alpha h}} + e_{EDEF}}{2} \right) \right) - (2)$$

For the values in the set of P_d, the detection power is in descending order with the first value corresponding to $\alpha = 0.25$, which represents the highest detection probability. In the Figure 4 the proposed scheme energy-efficiency over four variants of CCEF is given by $E_e = \{13.91,\ 7.908,\ 5.420,\ 4.553\}\%$. It can be observed with the higher the detection-capacity, the greater is the energy saving. This is also shown in Figure 4 that as the FTR increases the energy consumption the different schemes decreases.

However, this is not the case in Figures 5 and 6 which are the special case of Figure 4. Figure 4 is decomposed into two figures representing only fabricated reports and legitimate report cases. The so called FTR label on x-axis is symbolic to indicate that energy consumption is calculated at given FTRs as have been done in parent Figure 4 but this time only energy consumption for fabricated and legitimate reports have been calculated separately. These two figures show roughly constant energy consumption along x-axis. The jittery curves are because of the fact that number of verifications nodes on a path cannot be equally assigned according to the FTR. For example; in a path of 8 hop counts with FTR as 30% how many nodes should be assigned as verification nodes (to get detection-capacity of P_d=30%)? At best we can select 2 nodes representing 25% of the nodes and 3 nodes with 37.5% of the nodes.

As shown by example we cannot get exact 30% nodes which is required to represent smooth behavior, therefore performance is jittery. The purpose of having separate cases is to help understanding that actual (or significant) energy saving is made by dropping fabricated reports (Figure 5) whereas comparable energy saving in case of energy saving by legitimate reports (Figure 6). Fabricate reports case uses much less (almost half) energy as compare to the legitimate reports which have to go through more verifications.

As shown in Figure 5, EDEF in case of fabricated reports consumed significantly less average per report energy as compared to all four variants of CCEF. This is due to the fact that fabricated reports are dropped earlier as a result corresponding energy consumption is reduced.

However, as shown in Figure 6, the case of legitimate reports, our scheme does not outperform all variants of CCEF. This is because our scheme bank on better detection-capacity which saves energy by restricting fabricated report travelling less number of hops. The better detection-capacity indirectly results in move verifications. This means on average legitimate reports have to go through increased number of verifications and thus more energy. Therefore our scheme does

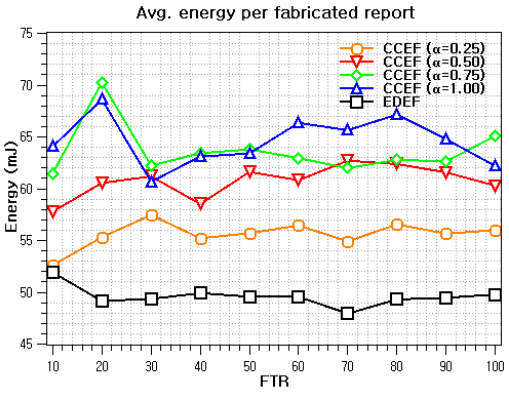


Figure 5: Avg. energy per fabricated report

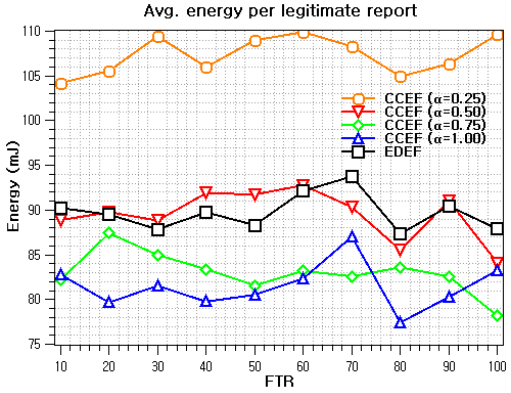


Figure 6: Avg. Energy per legitmate report

not outperform all variants of CCEF.For variants of CCEF the intensity verifications is related to value of α. In case of CCEF with $\alpha = 0.25$, since $P_d$is highest resulting in most number of verification. Thus energy consumptions for legitimate reports in that case is highest of all other variants and proposed scheme. For rest of the cases with increase in α the value of $P_d$decreases and thus verifications and corresponding energy consumption is reduced.

Moreover, CCEF comparatively consumes less energy when $P_d$is low (CCEF: $\alpha = \{0.75, 1.00\}$) as shown in Figure 6, but the detection-capacity is compromised as we will observe in the detection-capacity section 4.2 in Figure 7.

4.2. Detection Capacity

The detection-capacity is directly proportional to the detection probability. However, a high detection probability causes greater energy consumption due to increased verification for true reports and vice versa. Our EDEF scheme based on fuzzy logic has a detection capacity of 99.95%. For different P_d values, CCEF in four scenarios resulted in the following detection capacities: $C_{CCEF} = \{98.3,\ 87.53,\ 75.88,\ 64.25\}$ %.

If $c_{\frac{1}{\alpha h}}$is the detection capacity of CCEF with $P_d = \frac{1}{\alpha h}$ and $c_{EDEF}$is the detection capacity of the EDEF scheme, then the average detection-capacity (i.e., percentage difference) improvement over CCEF is defined by

$$C_{di} = \left(\left| c_{\frac{1}{\alpha h}} - C_{EDEF} \right| / \left(\frac{c_{\frac{1}{\alpha h}} + c_{EDEF}}{2} \right) \right) - (3)$$

Hence, detection-capacity improvement $C_{di}$of the EDEF scheme in four scenarios against CCEF is given by $C_{di} = \{1.66, 12.44, 24.08, 35.72\}\%$. The performance analysis of the EDEF scheme against CCEF with different detection probabilities is shown in Figure7.It can be observed by close analysis of Figure 4 and 7, by increase the P_d the filtering capacity can be increase however the energy consumption will also increase. For illustration see case of CCEF with $P_d = 0.25\%$detection is closer to EDEF in Figure 7 but corresponding energy consumption in Figure 4 for the same case is highest as compare to other three cases of CCEF and EFEF.

4.3. ReportsDrop per Hop

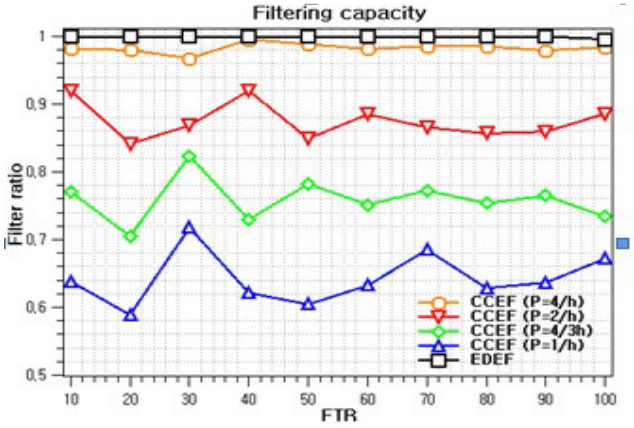


Figure 7: Detection capacity comparison

In this section, we illustrated that energy-efficiency and false report detection improvement is based on the better detection per hop. Three cases of false number of report drops per hops for different values of P_d and FTR are shown. In case of $P_d = \frac{4}{h}$ and FTR=50%, the respective number of reports dropped in CCEF and EDEF per hop are shown in the Figure 8. Since both schemes detection is based on distance more reports are dropped on starting hops. However, EDEF in addition to distance also consider FTR and energy of a node based on fuzzy based system, it has more detection-capacity. This is due to the fact that on average most number of reports dropped in proposed scheme is higher and more reports are dropped at earlier hops. Therefore our scheme detection-capacity is make use of both better and early detection. Similar trend is highlighted in two other cases in Figure 9 and 10.

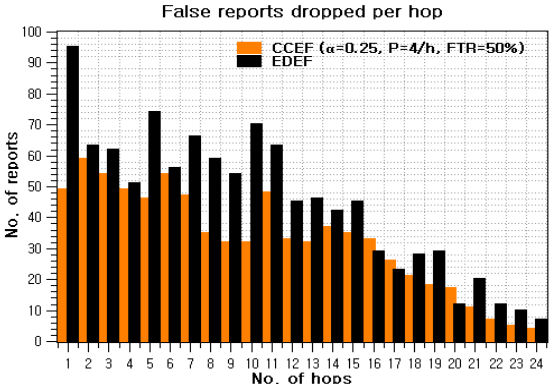


Figure 8: False reports dropped per hop (FTR=50%)

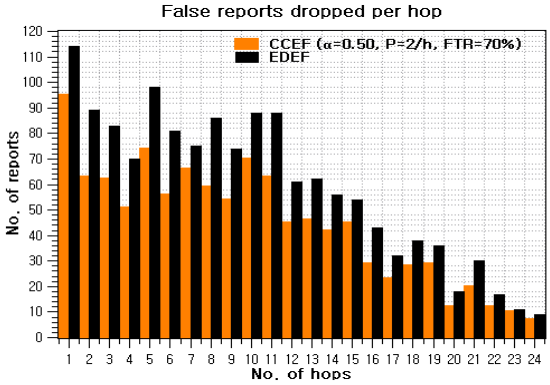


Figure9: False reports dropped per hop (FTR=70%)

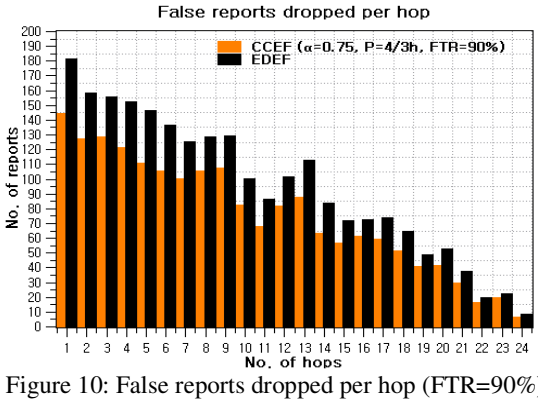


Figure 10: False reports dropped per hop (FTR=90%)

5. RELATED WORK

In the last decade, a great deal of research has been done on security, energy efficiency, and network lifetime. The work in CCEF [1] is most closely related to our proposed work, which is explained in background Section 1.1. Dynamic en-route filtering (DEF) [2] uses the hill climbing approach for key dissemination in order to filter false reports earlier, where each node requires a key chain for authentication. Statistical en-route filtering (SEF) [3] first addressed the false report detection problems by determining the number of compromised sensor nodes. It introduces the general en-route filtering framework, which serves as the basis of subsequent en-route filtering-based security protocols.

The IHA scheme [4] can detect false data reports when no more than t nodes are compromised. It provides an upper bound to the number of hops a false report can traverse before it is dropped in the presence of t clouding nodes. The authors of [5] analyze different security schemes, showing that en-route filtering is an efficient way to deal with false data injection attacks in WSNs.In a probabilistic voting-based filtering scheme (PVFS) [6], the number of votes (i.e., MACs) is used to prevent both fabricated reports with false votes and false votes in valid report attacks. The fuzzy-based path selection method (FPSM) [7] improves the detection of false reports in the WSN, in which each cluster chooses paths by considering the detection power of the false data and the energy efficiency. In [8], a key index-based routing for filtering false event reports in the WSN is presented. Each node selects a path from the event source to the destination based on the key index of its neighbor nodes.In [9], the authors propose an active en-route filtering scheme which supports dynamic network conditions. Hill climbing is used to increase the filtering capacity of the proposed scheme resulting in energy savings and less memory being needed.

The paper in [10] reviews a number of en-route filtering schemes in WSNs and analyzes their performance considering filtering efficiency. The work in [11] addresses the limitations of IHA, which works on a single fixed path between the source and the destination. The authors propose a multipath interleaved hop-by-hop authentication (MIHA) scheme that creates multiple paths and switches to another path if there are t compromised nodes in the current path. The authors in [12], propose an en-route filtering scheme based on SEF to counter false reports and wormhole attacks. The results validate the improved performance with increased detection power and up to 20% energy savings. An evaluation of the en-route filtering schemes in WSNs [13] addresses both false report filtering and denial of service (DoS) attacks in WSNs. Multipath routing is used to distribute the keys to forwarding nodes in order to reduce the cost of updating the keys and to accommodate frequent topology changes.

In [14] a greedy perimeter stateless routing for wireless sensor networks has been presented. This simple routing method make use of geographical information based on distance. In an energy-efficient multi-hop hierarchical routing protocol (MHRP) for WSNs [15], the authors studied the effect of cluster size on energy consumption. The protocol uses residual energy for routing decisions along with clustering to prolong the network lifetime. The low-energy adaptive clustering hierarchy (LEACH) [16] uses a random rotation of local CHs to evenly distribute the energy load among the sensors in the WSNs. It uses data fusion to achieve an eight-fold reduction in energy usage in comparison with traditional routing protocols. The work in [17] presents a detailed survey on routing techniques in WSNs.

The work in [18] discusses the cluster size issue from a practitioner's perspective in terms of the communication needed for data collection. In [19], the authors present the optimal cluster size considering the network lifetime and energy-efficiency. With the adaptive decentralized re-clustering protocol (ADRP) [20], the CHs and the next CHs are chosen considering the residual energy of each node and the average energy of each cluster. The work in [21] presents dynamic

decentralized resource allocation in changing conditions with the aim to maximize the contribution of each node to the network. The authors present the self-organizing resource allocation (SORA) approach for optimal resource allocation in WSNs.

In [22], the problem of resource control is addressed. Increasing the resources without considering the type of congestion, traffic pattern, and network topology can make the situation worse. The topology-aware resources adaptation (TARA) strategy presents a topology-aware resource adaption that addresses the congestion problem. The study in [23] investigates the uneven consumption of the energy in gradient sinking networks. This leads to the presence of energy holes resulting in a significant reduction in the sensor network lifetime. The results demonstrate that the stated strategy can reduce energy consumption, cater to energy holes, and extend the network lifetime dramatically. In this work the underlying platform is considered as Mica2 based on energy consumption values from [24, 25].

6. CONCLUSIONS AND FUTURE WORK

We have demonstrated the improved energy efficiency and detection capacity of the EDEF scheme in comparison with CCEF with different detection probability settings in four scenarios. A fuzzy-based system enabled our scheme to have an increased detection capacity and inputs of fuzzy membership functions catering to the FTR and ENERGY for determining the fitness of a node to be a verification node resulted in energy efficiency. We saved energy by supporting dynamic changes in the FTR and ENERGY of a sensor, which can vary with time. Our scheme in all four scenarios performed better than CCEF in security (i.e., increased detection capacity, better or early detection per hop) and energy savings (i.e., increased energy efficiency). In CCEF with a higher P_d, the detection capacity increases, however, the energy overhead increases as well. This can be observed by comparing the curves in Figs. 4 and 7. In the future, we plan to propose a new en-route filtering scheme based on A* tree hierarchy management, re-clustering using genetic algorithm (GA), and optimized fuzzy membership functions. This is expected to give improved detection power and extended network lifetime.

ACKNOWLEDGEMENTS

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2013R1A2A2A01013971).

CONFLICTS OF INTEREST

The authors have no conflicts of interest to declare regarding the publication of this paper.

REFERENCES

[1] Hao Yang and Songwu Lu, “Commutative cipher based en-route filtering in wireless sensor networks,” 60th Vehicular Technology Conference, vol. 2, pp. 1223-1227, 2004.

[2] Zhen Yu, and Yong Guan, “A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks,” IEEE/ACM Transactions on Networking, vol. 18, no. 1, pp.150-163, February 2010.

[3] F. Ye, H.Luo, S. Lu, and L.Zhang, “Statistical En-route Filtering of Injected False Data in Sensor Networks,” In IEEE Proceedings of INFOCOM 2004, pp. 839-850, 2004.

[4] 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,” in Proceedings of EEE Symposium on Security and Privacy, pp. 259-271, 2004.

[5] Shahina K, A. P. Filtering Schemes for Injected False Data in Wsn. IOSR Journal of Computer Engineering (IOSR-JCE), vol. 13, issue 6, pp. 29-31, 2013.
[6] Feng Li and Jie Wu, "A probabilistic voting-based filtering scheme in wireless sensor networks," Vancour, Canada, ACM IWCMC, pp. 27-32, 2006.
[7] Hae Young LEE and Tae Ho CHO, "Fuzzy-based path selection method for improving the detection of false reports in sensor networks," in IEICE Trans. INF. & Syst., pp. 1574-1576, vol. E92-D, no. 8, August 2009.
[8] S. Y. Moon and T. H. Cho, "Key Index-Based Routing for Filtering false event reports in wireless sensor networks," in IEEE Trans. on Commun., Tokyo. Japan, vol. E95-B, No. 9, pp. 2807-2814, September 2012.
[9] Jithender Reddy Gopu, T.P.Shekar, D.Sagar, "An Active En-route Filtering Scheme for Information Reporting in Wireless Sensor Networks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, Issue 4, pp. 349-356, April 2012.
[10] S.V.AnnlinJebaDr.B. Paramasivan, "An Evaluation of the En-route Filtering schemes on Wireless Sensor Networks," Internatioanl Journal of Computer Engineering & Technology (IJCET), vol. 3, Issue 2, pp. 62-73, July- September 2012.
[11] P.T. Nghiem and T.H. Cho, "A Multi-path Interleaved Hop by Hop En-route Filtering Scheme in Wireless Sensor Networks," Computer Communications, Elsevier, vol. 33, issue 10, pp. 1202-1209, Jun. 2010.
[12] H.M. Choi and S.M. Nam and T.H. Cho, "A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks," Wireless Sensor Network, vol. 5, no. 3, pp. 33-40, Mar. 2013.
[13] Jaydip Sen, "A Survey on Wireless Sensor Network Security," In International Journal of Communication Networks and Information Security (IJCNIS), vol. 1, no. 2, pp. 55-78, August 2009.
[14] B. Karp and H. T. Kung., "GPSR: Greedy perimeter stateless routing for wireless networks," in ACM MobiCom, pp. 243-254, 2000.
[15] Jin Wang, Xiaoqin Yang, Yuhui Zheng, Jianwei Zhang and Jeong-Uk Kim, "An Energy-Efficient Multi-hop Hierarchical Routing Protocol for Wireless Sensor Networks," International Journal of Future Generation Communication and Networking, vol. 5, no. 4, pp. 89-98, December, 2012.
[16] Wendi RabinerHeinzelman, AnanthaChandrakasan, and Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Sensor Networks," Proceedings of the Hawaii International Conference on System Sciences, pp. 1-10, January 4-7, 2000.
[17] Jamal N. Al-Karaki, Ahmed E. Kamal, "Routing Techniques in Wireless Sendor Network: A surway," IEEE Wireless Communications, pp. 6-27, December 2004.
[18] Anna Forster, Alexander Forster and Amy L. Murphy, "Optimal cluster sizes for wireless sensor networks: An experimental analysis," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 28, pp 49-63, 2010.
[19] Amini N, Vahdatpour A, Xu W, Gerla M, and Sarrafzadeh M. "Cluster Size Optimization in Sensor Networks with Decentralized Cluster-Based Protocols." Computer Communications, vol. 35, pp.207-220, 2012.
[20] FuadBajaber, Irfan Awan, "Adaptive decentralized re-clustering protocol for wireless sensor networks," Journal of Computer and System Sciences, vol. 77, pp. 282–292, 2011.
[21] Geoffrey Mainland, David C. Parkes, and Matt Welsh. "Decentralized, Adaptive Resource Allocation for Sensor Networks." Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation. Berkeley, USA: NSDI'05, pp. 315-328, 2005.
[22] Jaewon Kang, Yanyong Zhang, and BadriNath. "TARA: Topology-Aware Resource Adaptation to Alleviate Congestion in Sensor Networks." IEEE Transaction on Parallel and Distributed Systems, IEEE Computer Society, vol. 18, no. 7, 919-931, 2007.
[23] Liu, Tao. "Avoiding Energy Holes to Maximize Network Lifetime in Gradient Sinking Sensor Networks." Wireless Personal Communication. Springer Science+Business Media, LLC, pp. 581-600, 2012.
[24] María Gabriela Calle Torres, "Measuring Energy Consumption in Wireless Sensor Networks using GSP (Thesis)," IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1-5, 2006.
[25] Crossbow, 2011, http://www.xbow.com/

Authors

Khuram Shahzad Toor received a B.E.I.Tdegree from the University of Lahoreand an M.S. degree in Information Technology from the National University of Science and Technology, Isalamabad, Pakistan in 2004 and 2007, respectively.He is now a Ph.D.scholar in the College of Information andCommunicationEngineering at Sungkyunkwan University, South Korea. Hisresearch interests include wirelesssensor networks and graph gheory.

Tae Ho Cho (Corresponding author)received a Ph.D. degree in Electrical andComputer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical Engineering fromSungkyunkwan University, Korea and the University ofAlabama, USA, respectively. He is currently a Professor in the College of Information and Communication Engineering at SungkyunkwanUniversity, Korea. His research interests include wireless sensor networks, intelligent systems, modeling and simulation, and enterprise resource planning.