ERCA: ENERGY-EFFICIENT ROUTING AND RE-CLUSTERING ALGORITHM FOR CCEF TO EXTEND NETWORK LIFETIME IN WSNS

Muhammad K. Shahzad[1], Jae Kwan Lee[1], and Tae Ho Cho[1,*]

1 College of Information and Communication Engineering, Sungkyunkwan University, Suwon 440-746, Republic of Korea

ABSTRACT

The pervasive application of wireless sensor networks (WNSs) is challenged by the scarce energy constraints of sensor nodes. En-route filtering schemes, especially commutative cipher based en-route filtering (CCEF) can saves energy with better filtering capacity. However, this approach suffer from fixed paths and inefficient underlying routing designed for ad-hoc networks. Moreover, with decrease in remaining sensor nodes, the probability of network partition increases. In this paper, we propose energy-efficient routing and re-clustering algorithm (ERCA) to address these limitations. In proposed scheme with reduction in the number of sensor nodes to certain thresh-hold the cluster size and transmission range dynamically maintain cluster node-density. Performance results show that our approach demonstrate filtering-power, better energy-efficiency, and an average gain over 285% in network lifetime.

KEYWORDS

Wireless sensor networks, energy-efficiency, network lifetime, re-clustering, filtering-power.

1. INTRODUCTION

Several en-route filtering schemes have been presented [3-6] which save energy by improved filtering of false report attacks in wireless sensor networks (WSNs). However, routing protocols used are not considered to save more energy. Commutative cipher based en-route filtering (CCEF) [1] can save up to 32% energy in case of large number of injected fabricated reports. However, CCEF suffers from the following problems; network lifetime is inefficient, fixed paths selection, and distance based routing originally designed for ad-hoc networks. Against different of attacks or fabricated traffic ratio (FTR) the security response is constant in CCEF. In this paper, we define FTR as number of attacks divided by total number of events and security response is number of verification nodes assigned in a path according to current FTR. The underlying routing in CCEF is greedy perimeter stateless routing (GPSR) [2] which is not suited for energy constraint WSNs. In past [7] it has been observed that unbalanced communication loads results in network partition or energy-hole problem which have drastic effects on network lifetime.

In pre-deterministic key distribution based CCEF (PKCCEF) [8] with energy-efficient routing, saves efficiency (16.05%) and prolongs network lifetime (81.01%). In this paper, energy-efficient routing

* Corresponding author
DOI: 10.5121/acii.2016.3102

and re-clustering algorithm (ERCA), significantly extends network lifetime (avg. 285%) while maintains filtering-power. The reason for improvement in energy-efficiency and network lifetime is due to dynamic re-clustering and sensor range as number of sensor nodes are reduced over time. Furthermore, attacks information is also obtained without causing energy consumption at sensor nodes. This FTR method will be explained in section 4.2 in detail. In this paper, to evaluate energy consumption, we will use first order radio model [17, 18]. The main contributions of this paper are:

- Improved energy-efficiency
- Significant network lifetime extension
- Improved security

2. COMMUTATIVE CIPHER BASED EN-ROUTE FILTERING (CCEF)

In this section, query-response model and verification example of CCEF is explained as shown in Figure 1.

In order to establish a session, the BS transmits a query message $[Q_{id}, CH_{id}, \{k_s\}_{Kn_{CH}}]$ to the CH that contains the Query ID (Q_{id}), CH ID (CH_{id}), and k_s key encrypted with the CH's k_{n}, i.e., $\{k_s\}_{Kn_{CH}}$ as shown in Figure 1(a). In order to establish a session, a plain text k_w key is dropped on each en-route node. Verification noes are randomly selected based on probabilistic method. In a sensor field events are randomly generated which the BS is interested in know certain event in an area in the field. In response the nodes receiving the event's information, select a CH, generate response.

An event report is endorsed by the event sensing nodes and forward it to the CH. Upon receiving the query, the CH uses k_n key to decrypt the k_s key to check validity of the query. The CH compress the MAC_s generated by above event sensing nodes by using a simple XOR operation. The response message is sent along with the MAC_s and the IDs of these nodes, as illustrated in Figure 1(b). In response, the CH sends a reply message $[Q_{id}, R, \{E_{id}, F_{id}, G_{id}\}, MAC_s, MAC_n]$, to establish a session. For the predetermined session duration, reports are generated by the event-receiving nodes in collaboration with the CH and are forwarded to the BS.

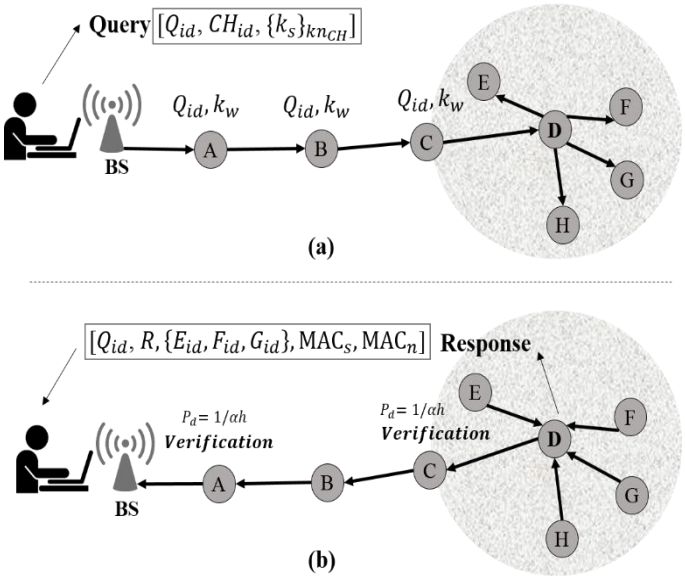

Figure 1. Query-reponse and route setup process in CCEF

For event reports verification, the sensor nodes with k_w keys first extract Q_{id} to determined that the query is valid, and if so, use k_w to verify the MAC_s without knowing k_s by using the property of commutative cipher. When the report in the response message reaches the BS, it generates the MAC_n and verifies it along with MAC_s. This will verify the CH and all of the report-endorsing neighbours if both tests are validated. If not, either the CH or one or more endorsing nodes is compromised.

3. PROPOSED SCHEME

In this section, system models and overview is presented.

3.1. System models

3.1.1. Network model

The N number of sensor nodes are randomly deployed within field F of area $A = F_h \times F_w$ with radius of R as illustrated in the Figure 2. This sensor field comprise of N number of sensor nodes represented by: $\{S_1, S_2, S_3, \dots, S_n\}$ respectively. The location of the BS is right mid edge of the sensor field. The clusters are represented by: $\{C_1, C_2, C_3, \dots, C_n\}$. At startup phase all the cluster are of equal size with $A = C_h \times C_w$. In each cluster equal number of nodes are randomly distributed, referred as node density or $\tilde{n}$. As the number of sensor nodes decreases with time due to energy depletion (i.e., remaining energy become zero and no more communication is possible), re-clustering and transmission range are adapted to maintain ñ. It will be further elaborated in section 3.2.3. Following are the assumptions related to this model:

- Network is composed of static homogenous nodes
- Communication links are symmetric
- Nodes can adjust transmission power as per distance

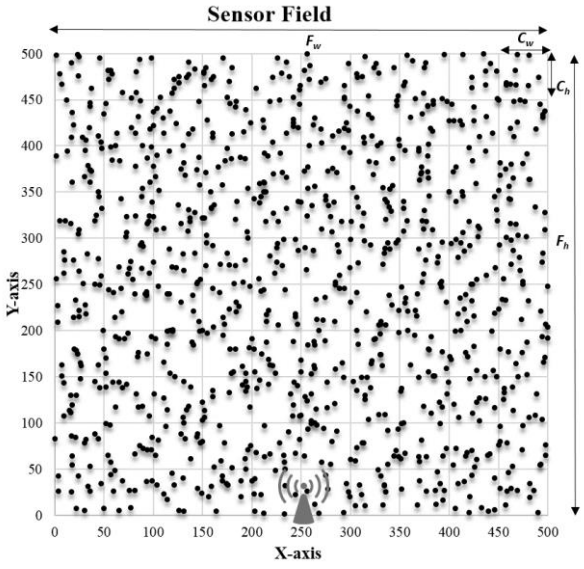

Figure 2. Sensor field

3.2.2. Energy consumption model

In this paper, we have used the first-order radio model [17] with a free space (d^2 power loss) channel model. A sensor node is composed of a radio communication components, data processing unit, micro sensor unit, antenna to transmit or receive data, amplifier, and power supply. In this paper for simplicity, we only consider the energy dissipation that is associated with the radio component and

electronics. A simple and commonly used first-order radio model block diagram is shown in Figure 3. The packet of m bits propagation at a distance d between the transmitter and receiver antennas, require the transmission energy of $E_{T_x}(k,d)$ as shown by Equation (1).

$$E_{T_x}(m,d) = E_{elec} \times m + E_{amp} \times m \times d^{\lambda} \quad (1)$$

E_{elec} is the energy used by the electronics of the circuit and $E_{elec} \times m$ is the energy used by the transmitter to sent m bits. Furthermore, E_{amp} is the energy required by the amplifier, and λ is the path loss constant. Similarly, $E_{R_x}(m)$ is the energy required to receive k-bits as shown in Equation (2).

$$E_{R_x}(km) = E_{elec} \times m \quad (2)$$

The energy used by transmitter amplifier for transmission is $E_{amp} = 100pJ/bit/m^2$. In addition the energy used by circuitry of transmitter and receiver is $50\ nJ/bit$.

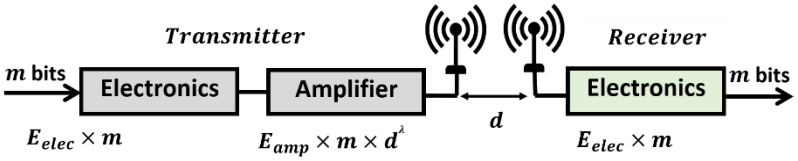

Figure 3. First order radio model for energy consumption

3.2.3. Clustering and re-clustering method

Over the time sensor nodes are depleted as the energy level reaches to zero. The probability of depletion of the sensor nodes is higher near the BS and on the paths. This reduces the number of event sensing nodes or report endorsing nodes which make it easier for the adversary to forge a report. This not only make easier to compromise security but also shortens the network lifetime. The depletion of nodes around sink and one established paths cause energy-holes which have adverse effect on network lifetime. This indicates that maintaining number of sensor nodes in a cluster can help security and extend network lifetime.

However, physical installation of sensor nodes may be both costly and hazardous task. A simple solution can be adjusting cluster size and transmission range to maintain cluster node density. Suppose ñ is the cluster node density at the network deployment or our desired number of nodes to be maintained in a cluster. In this paper as 10% of total number of nodes are depleted we apply cluster node density adaptive method to re-cluster the sensor network. The re-clustering formula used in this paper is illustrated with Equation (3).

$$C_{size_k} = \frac{\tilde{n}F_h^{\,2}}{N_{nk}} \quad (3)$$

As the total number of sensor nodes (N_{nk}) decreases, the cluster size at the k^{th}step is increased given ñ and the field higher and width. We assume same height and width of a cluster.

The number of CHs in a row (N_{CHs_r}) or column (N_{CHs_c}) of the sensor field is depicted by Equation (4).

$$N_{CHs_r} = N_{CHs_c} = \sqrt{N_{nk}/\tilde{n}} \quad (4)$$

The cluster, k height (C_{kh}) or width (C_{kw})in field F with height F_h and width $F_w$is defined by Equations (5) and (6).

$$C_{kh} = F_h/N_{CHs_r} \quad (5)$$
$$C_{kw} = F_w/N_{CHs_c} \quad (6)$$

Similarly, new range, R_k at the k^{th} step is given by Equation (7)

$$R_k = \frac{C_{kh}}{\partial} \quad (7)$$

Where $\partial = C_{ih}/R_i$ represent the system or the design parameter.

Initially all nodes are with same initial energy and there are no depleted nodes. Re-clustering algorithm keep track of the number of nodes depleted due to energy depletion. Our proposed method take care of the network topology conditions (i.e., range, cluster size etc.) and can adjust these parameters to maintain $\tilde{n}$. This does not only help extending network lifetime but also help maintaining security by taking care of minimum nodes in a given cluster.

3.3. System Overview

This section illustrates; setup initialization, key distribution, and forwarding node selection for the proposed method.

3.3.1. Network construction phase

A sensor field of area $(500 \times 500)\ \mathrm{m}^2$ with 1000 densely deployed sensor nodes is considered. In this phase sensor nodes are assumed secure during the network construction at boot-up process. It is also assumed that the BS cannot be compromised during this phase. The sensor nodes have a fixed initial energy of 1 Joules. At this phase, the randomly deployed nodes are granted unique IDs and k_n keys. Furthermore, each node knows it's location through some location mechanism to help it calculate its distance from the BS.

3.3.2. Key distribution phase

The k_w keys are distributed pre-deterministically for each session to a randomly selected percentage of sensor nodes on a path. The k_w is pre-deterministically disseminated before a session in the network, while k_s is transmitted securely to the CH in a query message. In contrast in CCEF, keys are distributed to all nodes on the path in the query message, whereas, the filtering nodes are assigned using probabilistic method $p = \frac{1}{\alpha h}$; where α is design parameter and h is distance or number of hopes. In ERCA, keys are only possessed by a predetermined percentage of nodes in the path and the same nodes are used as filtering nodes in response message. The percentage of nodes to be granted k_w keys are selected based on current FTR or attacks. Due to this reason, based on current FTR, we can dynamically determine a corresponding secure path. This method can dynamically select a suitable path depending upon the attack information. A session is changed after t time or after a node is depleted.

3.3.3. Route set-up phase

In the proposed method the route setup process is similar to CCEF with improved key distribution method and a forwarding node selection method.

The routing in proposed method is dynamic instead fixed path routing considering different parameters in addition of distance only as in CCEF. In order to make scheme to respond to different FTR, we consider presence of keys on nodes. If there are more attacks or higher FTR a path with more nodes having keys is preferred. This means with higher FTR ratio a path with more verification nodes (i.e., nodes with k_w keys) is selected and vice versa. The BS sends a query message to

establish a path through the CH in an area of interest. As events can take place randomly in different clusters, multiple sessions can be established at a given time between the BS and CHs.

3.3.4. Forwarding node selection method

Proposed method for selecting the next forwarding node among number of given candidate nodes to create a path is shown in Equation (8).

$$F_n = \arg_{max}\left\{k \times \left(1 - \frac{\beta}{2}\right) + (d + e) \times \frac{\alpha}{2}\right\} \qquad (8)$$

Where α and are is the system design parameter, d is the shortest distance of the closest neighbor to the sink, e is the residual energy, and k is the presence of k_w key on that node. All are variable and normalized by one and the node with the highest evaluation among candidate nodes is selected as forwarding node. By repeating this process a path is created between the set of the BS and the source CHs.

4. PERFORMANCE EVALUATION

4.1. Experimental Environment

A 1000-node sensor node are randomly distributed in field of area $500 \times 500\ m^2$ consisting of $k = 100$ clusters. In each cluster, a fixed number of nodes $\tilde{n} = 10$ are positioned at random locations. Each of the sensor nodes has an initial range of $50\ m$ which is used to determine the neighbours, candidate, and forwarding nodes. The BS is located at $(500, 250)$ m and aware of the node IDs, locations, and node keys (k_n) of all of the sensor nodes. The communication links are assumed to be bidirectional. Each node also assumes a unique ID and knows its k_n key. Table 1 illustrates the experimental parameters for the performance analysis. The values of E_{elec} and E_{amp} are chosen to achieve an acceptable ratio of E_b/N_0 [18]. The data packet or message size of 200 bits (referred as one time step) and a round is defined as four time steps of data received at the BS.

Table 1. Experiment parameters

Parameters	**CCEF**	**ERCA**
Sensors nodes	1000	-
Sensor field size	(500×500) m^2	-
BS location	$(250, 0)$ m	-
R_i	50 m	Variable
Cluster h/w	50 m	Variable
E_{elec} for Tx and Rx	50 nJ/bit	-
E_{amp}	100 pJ/bit/m2	-
Node energy	1 Joules	-
MAC verification	20 mJ	-
Data packet	32 bytes	-
Round	128 bytes	-
FTR	30%	-
Path loss constant (λ)	2	-

4.2. Attack information

In CCEF and ERCA the communication is query driven. In this model a query message is initiated by the BS to inquire about occurrence of an event in an area of interest. In response, a number of message reports of the event are transmitted during the session. Now, we explain how we can determine the number of attacks or FTR information without causing extra energy or message at the sensor nodes.

The number of event reports through designated CH are known to the BS. A legitimate report received at the BS will increment its counter by one to determine total number such reports. This need no extra message at the sensor nodes. For fabricated report there can be two cases or either report will be dropped en-route due verification is failed or at the BS. In first case, the BS after waiting for designated time window t will consider it dropped and increment the fabricated report counter by one. Similarly, verification failure at the BS will cause the fabricated report counter by one since it is also known.

Since, we can determine total number of legitimate and fabricated reports, by using equation (9), the current FTR ratio can be calculated for n events

$$FTR = \sum_{e=1}^{n} \frac{F_R}{F_R + L_R} \qquad (9)$$

4.3. Experimental results

The metrics used to evaluate network lifetime and energy-efficiency are; first node depleted (FND), half nodes depleted (HND), and total node depleted (TND). The depleted node is one which have used its total energy and cannot participate in communication. As mentioned earlier one round is four time steps 800 bits of data received at the BS. One time step is equal to the one packet size of 200 bits. A measure of better network lifetime performance is more number of rounds before node(s) depletion or maximum number of nodes depleted at the end of the simulation experiment. In case of energy-efficiency which scheme consume less average energy per round is more energy-efficient as per FND and HND metrics. The performance is evaluated at different network sizes (nodes) so some fluctuations are present in graphs.

4.3.1. Network Lifetime

In Figure 4 the network lifetime performance comparison of CCEF and EECA is shown using FND performance metric. The x-coordinate depicts network size in terms of number of sensor nodes and y-coordinate represents number of rounds. EECA shows a significant performance gain of an average 3.309 times or 330.90% over CCEF. For all network sizes (number of nodes) proposed scheme performance better than CCEF. The performance improvement of EECA over CCEF is 2.402 folds as shown in the Figure 5 for performance metric HND. The network lifetime performance of EECA is better than CCEF in most cases except at network size of 300 and 200 nodes. As shown in Table 2 the average performance gain is 2.856 times in two cases.

The Figure 6 illustrates performance comparison of CCEF and ERCA for %age of nodes depleted at the end of the simulation experiment for different network sizes. Except for the first case the ERCA performance is significantly better as compare the CCEF. The performance improvement is achieved due to more balance network energy consumption strategies which balance communication loads

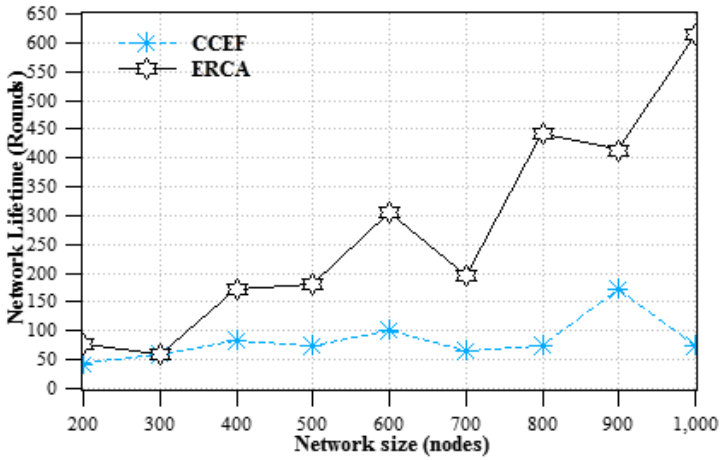

Figure 4. Network lifetime first node depleted (FND)

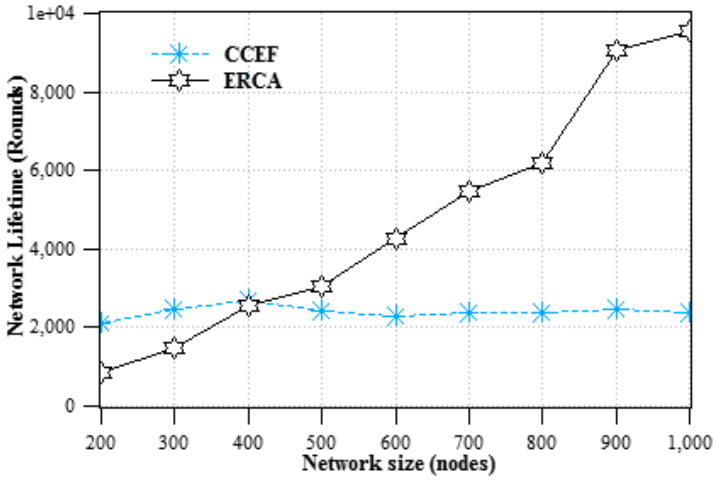

Figure 5. Network lifetime half nodes depleted (HND)

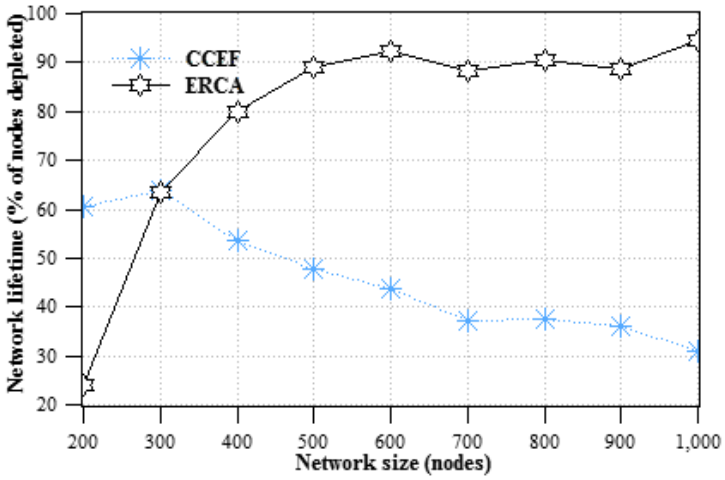

Figure 6. Network lifetime %nodes depleted (TND)

over large group of sensor nodes. Results have indicated that energy-efficient routing, dynamic path selection based on network conditions, and re-clustering help in solving energy-hole problem.

Table 2. Network lifetime gain of EECA over CCEF

metric	FND	HND	avg.
lifetime	3.309	2.402	2.856

4.3.2. Energy efficiency

In this section energy-efficiency performance of EECA and CCEF is discussed. Figure 7 shows that EECA have advantage over CCEF in energy-efficiency using FND metric. In all cases for different network sizes EECA performs better than CCEF in average energy-efficiency per round. The proposed scheme improved on average energy saving of 3.50% for different network sizes.

The case of performance improvement using HND metric is shown in the Fig. 8. In this case the average energy saving is 3.46%. The energy saving performance is summarizes in Table 3.

Table 3. Energy-efficiency gain of EECA over CCEF

metric	FND	HND	avg.
energy %	3.50	3.46	3.48

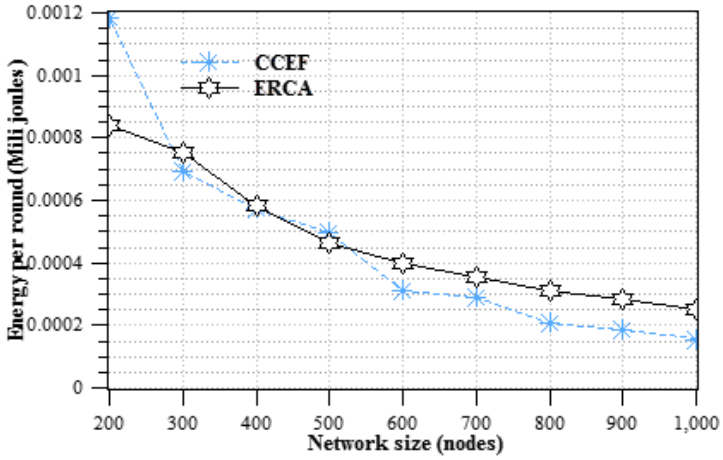

Figure 7. Energy-efficiency first node depleted (FND)

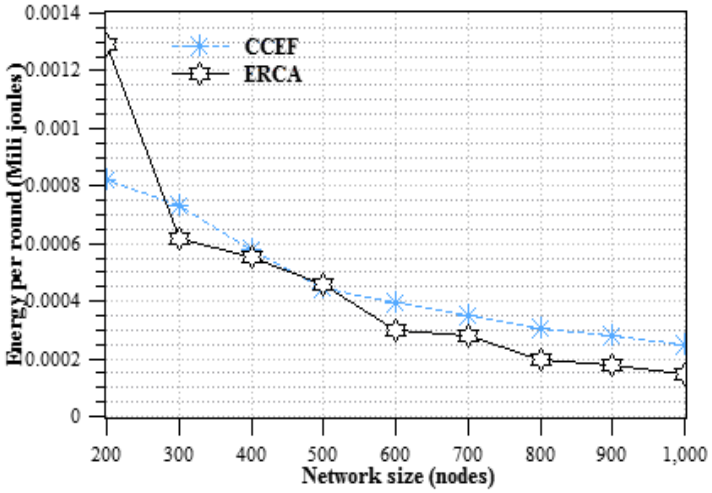

Figure 8. Energy-efficiency half nodes depleted (HND)

4.3.3. Security

In this section filtering-power of two compared schemes in highlighted. With pre-deterministic key re-distribution help achieving better performance as compare to the original scheme. The Figure 9 shows that EECA filtering-power in comparison with CCEF. Average filtering-power of for CCEF and ERCA are 71.31% and 75.93% respectively.

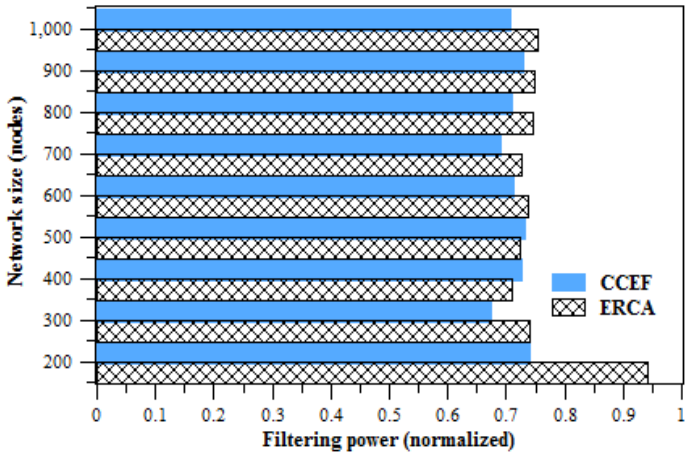

Figure 9. Filtering power of CCEF and EECA

5. RELATED WORK

In this section, research work related to our proposed scheme is explained. En-route filtering scheme such as CCEF [1] can save energy by early dropping of false report attacks. CCEF forms a secret association among the nodes and the BS for entire session where each node possesses its own witness. The en-route sensor nodes do not require to share a symmetric key, thereby offering stronger security protection than the existing symmetric key sharing schemes. Re-clustering is required, because; 1) when number of sensor nodes are less then t nodes the security is compromised and 2) network lifetime suffer from adverse effect. Security is compromised with less number of nodes in a cluster due to the need of less number compromised keys are needed to forge a report. It has adverse effects on network lifetime as with fewer nodes in a cluster limits the reachability.

The underlying routing protocol in CCEF is GPSR [3], which forwards packets based on a greedy approach in terms of the next-hop closer to the destination. GPSR does not consider residual energy level of the sensor nodes to determine the next hope. However, for energy constraint WSNs, it suffer from number of constraint; 1) consider distance only 2) fix path routing and 3) inefficient network lifetime.

Recently, several security schemes has been proposed in order to achieve energy-efficiency. One approach is to filter false reports en-route as early as possible. To cater this challenge several en-route filtering has been proposed. Statistical en-route filtering (SEF) [3] has first addressed the false report detection problems in WSNs by finding the number of compromised sensor nodes. It presents the general en-route filtering framework to serves as the source of subsequent en-route filtering security protocols. Dynamic en-route filtering (DEF) [4] uses the novel hill climbing method for key dissemination to filter false reports earlier, requires a key chain for authentication by each node in the chain.

The interleaved hop-by-hop authentication scheme (IHA) [5] can determine false data reports in case of no more than t nodes are compromised. It presents an upper bound to the number of hops a false report can travel before getting dropped in the presence of t colluding nodes. IHA is also based on GPSR routing as in CCEF and suffer from similar limitations. In a probabilistic voting-based filtering scheme (PVFS) [6], the number of message authentication controls (MACs) or votes is used to detect both fabricated reports with false votes and false votes on valid report attacks. The study [7] explores the uneven consumption of the energy in sink based networks. This problem results in energy holes having drastic effects on network lifetime.

In order to address, related limitations, several variants of above en-route filtering schemes has been propose to increase energy-efficiency and/or extend network lifetime. PKCCEF [8] improves CCEF which by using energy aware routing, improves network lifetime and saves energy. In research [9], a key index-based routing for filtering false event reports in the WSN is proposed. In this approach each node selects a path from the source to the destination based on the key index information of its neighbour nodes.

In work [10], a fuzzy-based path selection method (FPSM) is proposed which improves the detection of false reports in the WSN. In this approach each cluster selects paths by considering the detection capacity and the energy-efficiency. These schemes do not utilized re-clustering to further improve network lifetime. The paper [11] addresses the limitations of IHA, which is based on a single fixed path between the source and the sink. In order to address this problem, a multipath interleaved hop-by-hop authentication (MIHA) scheme is proposed. It creates multiple paths and select another available path if current path has re are t compromised nodes. Results demonstrate that it is more energy-efficient and can filter more attacks.

In work [12], it is observed that uneven distribution of the communication loads often results in energy hole problem. In order to counter this problem optimal and adjustable transmission ranges are dynamically assigned to improve the network lifetime. Performance evaluation shows the near optimal solution to prolong network lifetime both in uniform and non-uniform sensor nodes deployment. The effect of cluster size on energy consumption has been study by authors in an energy-efficient multi-hop hierarchical routing protocol (MHRP) for WSNs [13].

The authors in [14] studies the cluster size issue in a practitioner reference of the communication required for data collection. In [15], the authors present the optimal cluster size considering the network lifetime and energy-efficiency. These approaches demonstrates that optimal clustering sizes or re-clustering can extend the network lifetime.

In the adaptive decentralized re-clustering protocol (ADRP) [16], the CHs and the next CHs are determined by considering the residual energy level of each node and the average energy of each cluster. Results shows that improved network lifetime as compared to the other clustering protocols. However, these schemes does not support mobile sink. The paper [17] presents several radio transmission model. In order to calculate the energy dissipation in this paper, we first order radio model [18].

6. CONCLUSIONS AND FUTURE WORK

By distributing and balancing the communication loads over a larger group nodes EECA has been able cater with energy hole or network partition problem. Keys are pre-deterministically re-distributed on different paths to respond to different FTR ratios or attack frequency. This enable attack based dynamic path selection based routing. This helps in load balance over multiple paths alternatively which extend network lifetime.

We have saved energy by better detection of fabricated reports which limits number of hopes. In case of higher FTR, more verification nodes are assigned results in higher filtering of fabricated report. Whereas, when FTR is low, less number of verification nodes are selected resulting is less number of verifications for legitimate reports. Another main reason for significant network lifetime extension is re-clustering ability to reach nodes when node density in a cluster is reduced with depletion of sensor nodes. To maintain the node density proposed scheme adjust cluster size and transmission range. In future work we aim to achieve more energy-efficiency and improved filtering-power by selecting filtering nodes using fuzzy logic instead of pre-deterministic or probabilistic methods. The filtering capacity can further improved by using Generic Algorithm (GA) to optimized fuzzy membership functions.

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).

REFERENCES

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

[2]. B. Karp and H. T. Kung. GPSR: Greedy perimeter stateless routing for wireless networks. ACM MobiCom, 2000, pp. 243-254.

[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.

[4]. Zhen Yu, and Yong Guan. A dynamic en-route filtering scheme for data reporting in wireless sensor networks. IEEE/ACM Transactions on Networking, 2010, vol. 18(1), pp.150-163.

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

[6]. Feng Li and Jie Wu. A probabilistic voting-based filtering scheme in wireless sensor networks. Vancour, Canada, ACM IWCMC, 2006, pp. 27-32.

[7]. Liu, Tao. Avoiding energy holes to maximize network lifetime in gradient sinking sensor networks. Wireless Personal Communication. Springer Science + Business Media, LLC, 2012, pp. 581-600.

[8]. Muhammad K Shahzad and Tae Ho Cho, Extending the Network Lifetime by Pre-deterministic Key Distribution in CCEF. Wireless Sensor Networks. Wireless Networks, 2015, DOI 10.1007/s11276-015-0941-0.

[9]. S. Y. Moon and T. H. Cho. Key index-based routing for filtering false event reports in wireless sensor networks. IEEE Transaction on Communication. Tokyo. Japan, 2012, vol. E95-B (9), pp. 2807-2814.

[10]. Hae Young LEE and Tae Ho CHO. Fuzzy-based path selection method for improving the detection of false reports in sensor networks. IEICE Transaction on Information and System, 2009, pp. 1574-1576.

[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, 2010, vol. 33(10), pp. 1202-1209.

[12]. Chao Songa, Ming Liu, Jiannong Cao, Yuan Zheng, Haigang Gong, and Guihai Chen. Maximizing network lifetime based on transmission range adjustment in wireless sensor networks. Computer Communications, 2009, pp. 1316–1325.

[13]. 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, 2012, vol. 5(4), pp. 89-98.

[14]. 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, 2010, vol. 28, pp 49-63.

[15]. Amini N, Vahdatpour A, Xu W, Gerla M, and Sarrafzadeh M. Cluster size optimization in sensor networks with decentralized cluster-based protocols. Computer Communications, 2012, vol. 35, pp.207-220.

[16]. Fuad Bajaber, Irfan Awan. Adaptive decentralized re-clustering protocol for wireless sensor networks. Journal of Computer and System Sciences, 2011, vol. 77, pp. 282–292.

[17]. Swarup Kumar Mitra, Mrinal Kanti Naskar. Comparative study of radio models for data gathering in wireless sensor network. International Journal of Computer Applications, 2011, vol. 27(4), pp. 49-57.

[18]. Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Sensor Networks," Proceedings of the Hawaii International Conference on System Sciences, 2000, pp. 1-10, January 4-7

Authors

Muhammad Khuram Shahzad received a B.E.I.T degree from the University of Lahore and 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 and Communication Engineering at Sungkyunkwan University, South Korea. His research interests include wireless sensor networks and graph gheory.

Jae Kwan Lee received his B.S. degrees in computer information from BaekSeok Unive rsity, Korea, in February 2013. He completed his M.S. program from Sungkynkuwan University, Korea, in 2015. He is currently a PhD student in the College of Information and Communication Engineering at Sungkyunkwan University. His research interests include wireless sensor network security, intelligent system and modelling & simulation.

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