MODIFIED CCEF FOR ENERGY-EFFICIENCY AND EXTENDED NETWORK LIFETIME IN WSNS

Muhammad K. Shahzad[1] and Tae Ho Cho[1, 2]

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

ABSTRACT

The widespread application of wireless sensor networks (WNSs) is obstructed by the severely limited energy constraints and security threat for sensor nodes. Since traditional routing and security schemes are not suited for these networks, a large part of research focusses on energy efficient routing protocols while extending the network lifetime. Uneven distribution of communication loads result in network partitioning. Traditional novel en-route filtering approaches, notably commutative cipher based en-route filtering (CCEF) saves energy by early filtering of false reports. However this approach main focus is security not network lifetime is limited by fixed paths and underlying routing not suitable for WSNs. In order to cater these problems we propose energy efficient routing and pre-deterministic key distribution with dynamic path selection in CCEF. Modified CCEF (MCCEF) aims at saving energy and extending network lifetime while maintaining filtering power as in CCEF. Experimental results demonstrate the validity of our approach with an average of three times network lifetime extension, 5.022% energy savings, and similar filtering power as the original scheme.

KEYWORDS

Wireless sensor networks, energy efficiency, network lifetime, filtering power.

1. INTRODUCTION

In en-route filtering schemes generally underlying routing protocols are not considered for further energy efficiency. Notably, a novel commutative cipher based en-route filtering (CCEF) [1] can save up to 32% energy in case of large number of injected fabricated reports. However limitations are; network lifetime is not main concern, based on fixed paths, and while in routing only distance is considered not energy level of a node. For different fabricated ratio (FTR) the security response is constant. FTR is number of attacks divided by total number of events. Security response is number of verification nodes assigned in a path as per current FTR. In order to save more energy CCEF does not improve underlying reedy perimeter stateless routing (GPSR) [2] which was originally design for ad hoc networks. The work [3] have demonstrated that unbalanced communication load results in network partition or energy-hole problem which have severe effects on network lifetime. In wireless sensor networks (WSNs) several en-route filtering

[2] Corresponding author

DOI:10.5121/iju.2015.6401

algorithms [4], [5], [6], and [7] saves energy by early filtering of attacks which do not consider energy-efficiency in routing.

Several improvement of CCEF [8], DEF [9], SEF [10], and IHA [11] have been proposed address some of the limitations. In pre-deterministic key distribution based CCEF (PKCCEF) [8] which showed up to 16.05% energy efficiency and 81.01% network lifetime extension. Our proposed modified CCEF (MCCEF) not only significantly extends network lifetime up to 300% but also maintain filtering power in addition to be more energy efficiency than original scheme. In research work [12], authors suggests that uneven distribution of the communication loads can results in energy-hole. In order to solve this problem they have suggested an adjustable transmission range can be assigned to optimize the network lifetime. In this paper in order to evaluate energy consumption, we will use first order radio model [13, 14]. In [15], authors have discussed different factors of RF power management in WSNs. The paper presents a micro-power spectrum analyser which enables low power operations throughout wireless integrated networks sensors (WINS).

MCCEF saves energy while significantly extending the network lifetime. Moreover our proposed scheme give similar filtering power as in the original scheme. Since creating path is more expansive then selecting from already created paths, MCCEF before creating a new path among a pair of nodes prefer to select from buffer if it already exists. FTR or attacks information is also obtained without causing additional messages or energy consumption at sensor nodes.

Our proposed scheme aims at distributing communication loads over larger group of nodes in the sensor to get more balanced energy distribution approach. This is achieved by energy efficient routing which consider different factors in addition to distance only in CCEF and pre-deterministically re-distribute keys. Based on current FTR ratio our algorithm can choose dynamically one of the paths which cater for security needs. Performance analysis demonstrate the validity of our approach which is more energy efficient and prolongs the network lifetime significantly while maintaining the filtering power as in the original approach.

The main contribution of this paper are:

- Energy efficient routing
- Extended network lifetime while
- Maintaining filtering power

2. RELATED WORK

In order to address the security of the WSN, the underlying routing protocol is generally ignored. In the security design, when the number of attacks exceeds a certain threshold, it is safe to assume that early detection would conserve energy that would have been wasted otherwise. However, further energy efficiency can be achieved if energy-efficient routing is considered.

CCEF [1] establishes a secret association among the nodes and the base station (BS) per session, and each node in the route possesses its own witness. The sensor nodes in the path do not need to share a symmetric key, thereby offering stronger security protection than the existing schemes.

Intermediate nodes have a witness key (k_w) and can verify a report without knowing the session key (k_s). Even though only a few nodes are used as the filtering nodes, k_w keys are distributed to all of the nodes. CCEF does only support static sink based networks and does not perform re-clustering after depletion of sensor nodes. When number of sensor nodes are less then t nodes the security as well as network lifetime suffer from adverse effect. The underlying routing for CCEF is GPSR [2] excessively use geography for greedy (distance) forwarding. This efficient geo routing method is scalable for large densely deployed networks. However, for energy constraints WSNs it suffer from number of constraint; 1) consider distance only not energy while forwarding messages 2) fix path routing and 3) low network lifetime. The study [3] 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 and extend the network lifetime dramatically. However this study is applicable for static sink based WSNs. In order to achieve energy efficiency and prolong network lifetime recently several approaches has been proposed. One approach to save energy is to filter false reports en-route as early as possible. To address this various novel en-route filtering has been proposed. Statistical en-route filtering (SEF) [4] 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. Dynamic en-route filtering (DEF) [5] uses the hill climbing approach for key dissemination in order to filter false reports earlier, where each node requires a key chain for authentication. The interleaved hop-by-hop authentication scheme (IHA) [6] 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 colluding nodes. As in CCEF, IHA also based on GPSR and suffer from similar limitations. In a probabilistic voting-based filtering scheme (PVFS) [7], the number of message authentication controls (MACs; referred to as votes in the paper) is used to prevent both fabricated reports with false votes and false votes on valid report attacks.

Recently several variations 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, significantly improves network lifetime and saves energy. The fuzzy-based path selection method (FPSM) [9] 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 [10], 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. However these schemes do not utilized re-clustering and assume static sink. 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. It proves to be more energy efficient and can filter more attacks than the original scheme.

Research work [16], suggests that uneven distribution of the communication loads often results in energy hole. In order to solve this problem optimal and adjustable transmission ranges are assigned to optimize the network lifetime. Results demonstrate the near optimal solution to extend network lifetime both in uniform and non-uniform deployment. The paper [13] presents

several radio transmission model. In order to calculate the energy consumption and comparison in this paper we first order radio model. In [14], authors use the first order radio model for their energy efficient communication protocol for wireless sensor networks. We use the same first order radio transmission model with same values for energy transmission and reception of a bit with an acceptable $\frac{E_b}{N_0}$ ratio.

3. PROPOSED SCHEME

In this section, motivation, system models, and system overview is presented in detail.

3.1. Motivation

Uneven energy consumption results in energy-holes around the Base Station (BS) in sink based networks. In order to solve this problem different approaches with an aim to distribute communication load over larger group of sensor networks has been adapted. The underlying routing in CCEF is GPSR which was originally proposed for ad hoc networks does not cater for energy limited sensor nodes requirements. In fix path routing a single path is used until it is broken by depletion of a node. MCCEF aims at dynamically selecting from different available paths based on a node's residual energy level, current attack ratio (FTR), and distance. Since different paths have different number of verification nodes based on number of keys in paths, our proposed scheme can respond based on FTR. MCCEF make use of these factors in design of energy efficiency approach while extending the network lifetime significantly and maintaining en-route filtering power as in CCEF.

3.2. System models

3.2.1.Network model

The sensor nodes are randomly deployed within square sensor field of area $A = F_h \times F_w$ within radius of R as shown in the Fig. 1. This sensor field comprise of N number of sensor nodes represented by: $\{S_1, S_2, S_3, \dots, S_n\}$ respectively. In this paper total number of sensor nodes $n = \{100, 200, \dots, 1000\}$. As shown in the Fig. The location of the BS is BS (500, 250) m. The clusters are represented by: $\{C_1, C_2, C_3, \dots, C_n\}$ where $n = 100$. All the cluster are of equal size with $A = C_h \times C_w$ where $h = w = 50m$. In each cluster equal number of nodes are randomly distributed in each cluster. Following are the assumptions associated with network model:

1. Network is composed of stationary homogenous nodes
2. Communication links are symmetric
3. Nodes can adjust transmission power as per relative distance

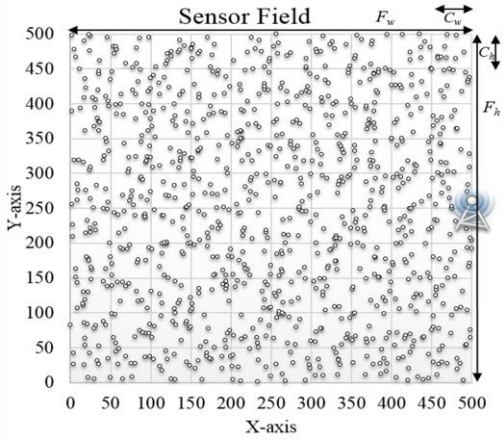

Figure 1. Sensor field

3.2.2.First order radio model for energy consumption

The first-order radio model [13, 14] is used with a free space (d^2power loss) channel model is used. A typical sensor circuitry consists of a data processing unit, radio communication components, a micro sensor unit, antenna, power supply, and amplifier. In our implementation of the energy dissipation model, we only consider the energy dissipation that is associated with the radio component. A simple and commonly used first-order radio model block diagram is shown in Fig. 2. In order to transmit a k-bits packet with a distance d between the transmitter and receiver, the transmission energy, $E_{T_x}(k,d)$, can be modeled by Equation (1).

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

Where E_{elec} is the energy used by the electronics of the circuit, and $E_{elec} \times k$ is the energy used

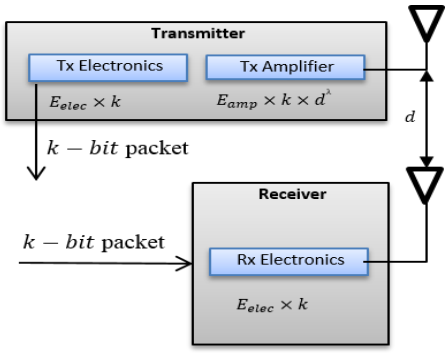

Figure 2: First order radio model

by the electronics of the transmitter to transmit k bits. Moreover, E_{amp} is the energy used by the amplifier, and λ is the path loss constant. Similarly, $E_{R_x}(k)$ is the energy needed to receive k-bits in Equation (2).

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

3.3. System Overview

3.3.1.Boot-up initialization

Sensor nodes are considered to be 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 it's location through a location mechanism.

3.3.2.Key distribution process

The witness keys (k_w) are distributed pre-deterministically for each session to a randomly selected percentage of sensor nodes. k_w is distributed before a session in the network, while k_s is sent securely to the BS in a query message. In CCEF, keys are distributed to all nodes on the path in the query message, while in the response message, the filtering nodes are determined probabilistically (p=1/αh). In our method, keys are only possessed by a predetermined percentage of nodes in the path and in the response message the same nodes are used as filtering nodes without using the probabilistic method. We can dynamically determine a path based on the attack information; therefore, depending upon the attack ratio, there can be different corresponding paths. A session is changed after t time units or after a node is depleted.

3.3.3.Route set-up process

Selecting a neighbor each time that is closest to the source node does not always result in energy-efficiency, as the path can be the shortest in terms of the number of hops or distance but may not be energy efficient. The distance and energy are inversely proportional, but both factors are crucial in determining the next hop. Therefore, it is desirable to consider both factors when making routing decisions to ensure an energy efficient route setup. The route setup process remains the same as in CCEF, except that the underlying routing considers a different key distribution method and a different next hop evaluation method. We assume that the BS knows the location of the events and sends a query message to establish a path. This path will be used for the duration of the session to report events located in that cluster. Since events --can take place randomly in any of the clusters, multiple sessions are established at a given time. The details of the route set-up phase are explained in Section 3.

3.3.4.Forwarding node selection

Our proposed method for selecting the next forwarding nodes to create a path is shown in Equation (3).

$$F_n = \mathrm{d}_i\left(\frac{1-\alpha}{2}\right) + r_e\left(\frac{1-\alpha}{2}\right) + \alpha \times [k] \quad (3)$$

Where α is the system design parameter, d_i is the shortest distance of the closest neighbor to the sink, r_e is the residual, remaining, or current energy level of a candidate sensor node and k is the presence of key on that node. Candidate nodes are set of sensors which are considered to find

forwarding nodes. All variables are normalized by one and the nodes with the highest evaluation using the above node selection method are selected as forwarding nodes. This process is repeated unless a path is created between the BS and the source CH.

4. PERFORMANCE EVALUATION

4.1. Experimental Environment

In this paper, we consider a 1000-node randomly distributed sensor network in area grid of $500 \times 500\ m$ with $k = 100$ clusters. In each cluster, a fixed number of nodes are located at random locations. Each of the sensor nodes has a range, $R_{i=}50\ m$ which is used to select the neighbors, candidate, and forwarding nodes. TheBS 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 considered to be bidirectional. 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. Table 1 shows the parameters for the experimental setup that was used for the performance analysis. The values of E_{elec} and E_{amp} are selected to achieve an acceptable $\frac{E_b}{N_0}$ [14]. The data packet or message size is 200 bits (or one time step) and a round is defined as four time steps or 800 bits of data received at the BS.

Table 1: Experimental parameters detail

Parameters	**Values**
Sensor	1000
Sensor field size	500 x 500 m^2
BS type	Static
BS location	(500, 250) m
$\boldsymbol{R_i}$	50 m
Cluster h/w	50 m
$\boldsymbol{E_{elec}}$	50 nJ/bit
$\boldsymbol{E_{amp}}$	100 pJ/bit/m^2
Node energy	1 Joules
Data packet	200 bits
Round	800 bits
FTR	30%
Path loss constant (λ)	2

4.2. Attack information

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

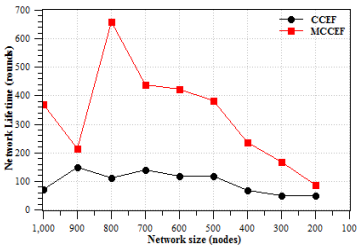

Figure 3: Network lifetime (FND)

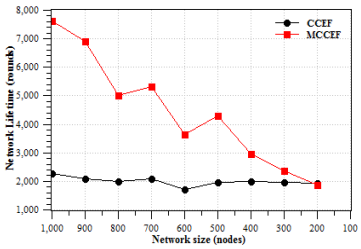

Figure 4: Network lifetime (HND)

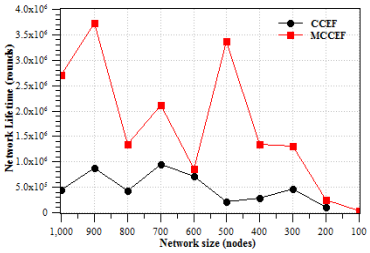

Figure 5: Network lifetime (LND)

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 FTR can be determined at any time. The FTR value along with a node energy level and distance from the BS is then exploited to determine number of keys to be distributed in each session per path basis. As mentioned before, this method does not need extra energy consumption at sensor nodes and calculations on the BS can be justified since it has sufficient power and computation capacity.

4.3. Experimental results

The performance evaluation metrics used to compare network lifetime and energy efficiency are; first node depleted (FND), half nodes depleted (HND), and last node depleted (LND). The depleted node is one which have exhausted its total energy and cannot participate in communication. A round is 800 bits of data received at the BS or four time steps. One time step is equal to the one packet size which is 200 bits. More the number of rounds a schemes can take before node(s) depletion the better the performance will be. Same parameters are used for energy efficiency to evaluate average energy consumer per round at each of the above performance indicators. Moreover filtering power and buffer performance at end of the each simulation experiment will be presented.

4.3.1. Network Lifetime

In Fig. 3 the network lifetime comparative performance of CCEF and MCCEF is shown for FND performance metric. The x-axis represents network size in terms of number of sensor nodes and y-axis indicates number of rounds. MCCEF shows a significant performance gain of 3.3964 times over CCEF. For all network sizes (number of nodes) proposed scheme performance better than CCEF. Figure 4 indicates network lifetime performance of compared schemes for HCO performance metric. This indicates performance of CCEF and MCCEF after half out of the nodes are depleted. MCCEF also outperform CCEF over this performance indicator by having 2.3964 folds network lifetime gain. In Fig. 5 compare the performance based on LND performance metric. In third case MCCEF again prolong the network lifetime by significant 3.4107 times over the original scheme.

The summary of network lifetime performance improvement of proposed scheme over CCEF is shown in the Table 2. As shown in the Table 2, average network lifetime gain of MCCEF over three different metrics is 3.0089 folder or over 300% as compare to CCEF. The performance gain is achieved with more balance network energy consumption strategies which distribute communication loads over large group of sensor nodes. Results have indicated that energy efficient routing, dynamic path selection based on network conditions, and pre-deterministic key re-distribution help solving energy-hole problem.

Table 2. Network lifetime gain of MCCEF and CCEF

Metric	**FND**	**HND**	**FND**	**Avg.**
Lifetime	3.3964	2.2196	3.4107	3.0089

4.3.2.Energy efficiency

In this section energy efficiency comparative analysis of MCCEF and CCEF is highlighted. In order to compare these schemes performance metrics of FCO, HCO, and FCO are used. The x-axis shows network size and y-axis indicates average energy consumption in mili joules per round. Figure 6 that MCCEF have advantage over CCEF in energy efficiency using FND. In most cases for different network sizes MCCEF outperforms CCEF in average efficiency energy per round. The average performance in energy saving over different network sizes is 7.80%. The case of performance improvement using HND metric is shown in the Fig. 7. In this case the average energy saving is better than previous case with 11.42% average energy saving. In the third case where LND comparison MCCEF has slightly energy inefficient with energy deficit of -1.76%. However on average in three cases our proposed method is 5.82% more energy efficient than CCEF scheme.

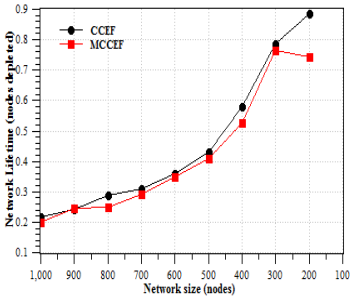

Figure 6: Energy efficiency

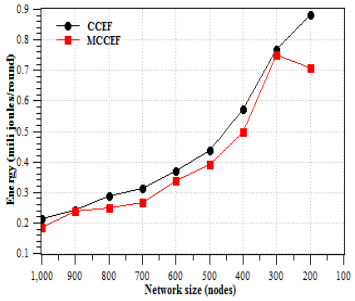

Figure 7: Energy efficiency

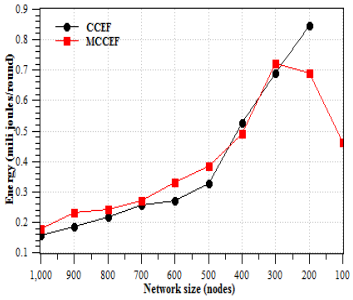

Figure 8: Energy efficiency D)

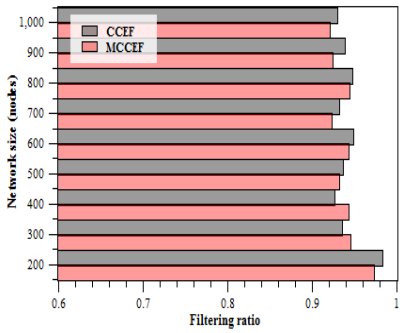

Figure 9: Filtering power of CCEF & MCCEF

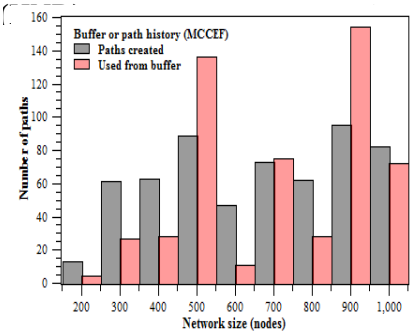

Figure 10: Buffer history in

Table 3 Energy efficiency gain of MCCEF and CCEF

Metric	FND	HND	FND	Avg
Energy	7.80%	11.42%	-1.76%	5.82%

Table 3 summarize the overall energy efficiency performance gain of MCCEF over CCEF with different performance metrics.

4.3.3.Security

In this section filtering power of two compared schemes in shown. In case of dynamic path selection it is hard to assign appropriate keys to verification nodes. Our main objective was to make CCEF energy efficient while extending the network life do not compromising security. With pre-deterministic key re-distribution help achieving similar performance as in original scheme. The Fig. 9 shows that MCCEF filtering power is similar to that of CCEF. Our performance little better at network sizes of 300 and 400 nodes while in other cases CCEF performance is slightly better. However since performance difference is very small we can claim that performance is almost similar in both schemes. This is still encouraging considering network lifetime and energy efficiency we have achieved.

4.3.4.Buffer history

Our proposed approach also make use of path buffer history. Creating a path is more expansive as compared to the selecting path from already created path in the buffer. Whenever a path is created between a pair of nodes it is saved and re-used when event source CH and the BS are same. This also saves some of the energy in MCCEF scheme. The Fig. 10 depicts the performance of MCCEF buffer history of paths created and used from buffer.

5. CONCLUSIONS AND FUTURE WORK

By distribute and balance the communication loads over a larger group nodes MCCEF has been able cater with energy hole or network partition problem. We have modified GPSR used in CCEF to apply it for sensor network condition and also save energy. Keys are pre-deterministically re-distributed on different path to respond to different FTR ratios or attack frequency. This enable dynamic path selection based routing. This helps in load balance over multiple paths alternatively which extend network lifetime.

Energy is saved by early detection of fabricated reports which limits them in travelling number of hopes. In case when FTR is low less number of verification nodes are selected resulting is less number of verifications for legitimate reports. Energy is also saved by using path buffer history in proposed scheme.

In future more energy efficiency and improved filtering power can be achieved with selecting filtering nodes using fuzzy logic instead of probabilistic method. Moreover further improvement in security can be achieved by using optimized fuzzy logic functions using genetic algorithm.

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. (2004). Commutative cipher based en-route filtering in wireless sensor networks. 60th Vehicular Technology Conference, vol. 2, pp. 1223-1227.

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

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

[4]. F. Ye, H. Luo, S. Lu, and L. Zhang. (2004). Statistical en-route filtering of injected false data in sensor networks. In IEEE Proceedings of INFOCOM 2004, pp. 839-850.

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

[6]. S. Zhu, S. Setia, S. Jajodia, and P. Ning. (2004). An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. Proceedings of EEE Symposium on Security and Privacy, pp. 259-271.
[7]. Feng Li and Jie Wu. (2006). A probabilistic voting-based filtering scheme in wireless sensor networks. Vancour, Canada, ACM IWCMC, pp. 27-32.
[8]. Muhammad K Shahzad and Tae Ho Cho, (2015). Extending the Network Lifetime by Pre-deterministic Key Distribution in CCEF in Wireless Sensor Networks. Wireless Networks, DOI 10.1007/s11276-015-0941-0.
[9]. Hae Young LEE and Tae Ho CHO. (2009). Fuzzy-based path selection method for improving the detection of false reports in sensor networks. IEICE Transaction on Information and System, pp. 1574-1576.
[10]. S. Y. Moon and T. H. Cho (2012). Key index-based routing for filtering false event reports in wireless sensor networks. IEEE Transaction on Communication. Tokyo. Japan, vol. E95-B(9), pp. 2807-2814.
[11]. P.T. Nghiem and T.H. Cho. (2010). A multi-path interleaved hop by hop en-route filtering scheme in wireless sensor networks. Computer Communications, vol. 33(10), pp. 1202-1209.
[12]. Chao Songa, Ming Liu , Jiannong Cao, Yuan Zheng, Haigang Gong, and Guihai Chen. (2009). Maximizing network lifetime based on transmission range adjustment in wireless sensor networks. Computer Communications. pp. 1316–1325.
[13]. Swarup Kumar Mitra, Mrinal Kanti Naskar. (2011). Comparative study of radio models for data gathering in wireless sensor network. International Journal of Computer Applications. vol. 27(4), pp. 49-57.
[14]. Mong Crossbow, 2011. http://www.xbow.com/.
[15]. BorMing Lee, Hui-Ming Hsieh, Wang, J. T., Kai-Long Hsiao, Note for LC Oscillator Power Management for Wireless Network Sensors Technique, Energy and Power Engineering Science, doi: 10.12966 / epes. 08. 01. 2014 , August 2014, v.1, p. 17-21

Authors

Khuram Shahzad Toor 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.

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.