Balancing Energy Consumption Over the Network to Extend the Network Lifetime in Wireless Sensor Networks

Muhammad K. Shahzad, Jae Kwan Lee, and Tae Ho Cho[*]
{khuram; windljk; thcho}@skku.edu
[*]Corresponding aurthor

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

***Abstract*— Wireless sensor networks (WSNs) are composed of non-rechargeable energy limited large number of densely deployed sensor nodes. Achieving energy-efficiency and extending network lifetime without compromising security of WSNs is a critical challenge. Traditional novel en-route filtering approach; i.e., commutative cipher based en-route filtering (CCEF) can provide stronger security against compromised nodes than symmetric key sharing based designs. However, underlying routing is not energy-efficient and not designed to prolong network lifetime. In order to overcome these limitations an energy-efficient dynamic routing and pre-deterministic key distribution are presented. Our proposed modified method in experiments demonstrate energy-efficiency and network lifetime improvement over CCEF while not compromising on security.**

Keywords-Wireless sensor networks; network lifetime; filtering-power; energy-efficiency.

I. Introduction

The advances in microelectromechanical systems (MEMS) [1] have been instrumental in realization of numerous new devices and applications. MEMS have introduced 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. However for their widespread deployment, researchers need to address variety of challenges. These challenges includes; energy efficient routing, network lifetime, and security which should be addressed at design level. In this paper, we investigate commutative cipher based en-route filtering (CCEF)[2] to extend the network lifetime with energy-efficient dynamic path based routing and pre-deterministic key distribution. CCEF is limited by fix path selection which has drastic effects on network lifetime. With better filtering capacity, false reports are dropped earlier, resulting in energy saving and thus further increasing network lifetime.

The core idea of CCEF is that it drops a fabricated report that does not participate in symmetric key sharing among sensor nodes. Intermediate nodes have a witness key ($\mathrm{k_w}$) and can verify a report without knowing the session key (k_s). Even though only a few nodes are used as filtering nodes, k_w key copies are distributed to all intermediate nodes on a path. Only a selected number of nodes participate in report verification, so it is desirable to store the keys on most suited verification nodes with respect to security and lifetime. This is determined by selecting nodes with most residual energy and presence of keys. Furthermore, 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 the identification of a desired path corresponding to the false traffic ratio (FTR). The procedure to obtain the FTR or attack information without extra messages or corresponding energy consumption will be explained in section 4.1.2. The underlying routing protocol in CCEF is greedy perimeter stateless routing (GPSR) [3], which forwards packets based on a greedy approach in terms of the next-hop closer to the destination. It does not consider the residual energy of the nodes taking part in the routing decisions.

In a wireless sensor network (WSN), the sensor nodes are randomly distributed and are left unattended for long periods of time. An adversary can compromise these nodes, steal information, or waste scarce network resources. Such attacks can be countered by implementing security measures that save energy through early detection and prevention of such attacks.

Recently, several security protocols have been proposed [2, 4-7] that enhance the energy-efficiency by detecting and filtering false report attacks earlier. In addition to having distinct limitations, these schemes do not consider further enhancing the network lifetime and/or energy-efficiency by improving the underlying routing. Some methods address the limitations of the existing security protocols [8-11]. The authors [12] demonstrate that unbalanced communication may result in network partitions cause by energy-holes. In the past, it has been observed that the sensor nodes closer to the sink tend to deplete their energy at a faster rate than the other nodes [13], resulting in energy holes or uneven energy distribution around the sink. Since, no further communication is possible at the sink, a significant amount of energy is wasted, resulting in a reduced network lifetime.

In this paper in order to perform energy dissipation analysis, the first order radio model [14], has been used. The authors [15] presents a comprehensive survey on en-routing filtering schemes in WSNs. There has been need to make existing en-route filtering scheme more energy-efficiency by making underlying routing schemes safe energy. This approach will not only help in saving energy but also more secure with better filtering capacity. For experimental evaluation, the underlying platform Crossbow Mica2 [16] is considered and energy consumption values from [17]. The sensor nodes are synchronized using an energy-efficient time synchronization protocol (ETSP) on WSNs [19].

In this paper, we achieve energy-efficiency by early filtering false reports and extend network lifetime by shifting communication overload to larger group of sensor nodes. Our proposed method adapts the network conditions (i.e., residual-energy, attacks etc.) to extend network lifetime. Performance analysis indicate that our approach has the following contributions:

- Improves detection-capacity
- Increases energy-efficiency
- Significantly increases in network lifetime

II. Background

In this section, we will illustrate working example of CCEF query-response and verification process and modifications in proposed method. The underlying routing protocol GPSR and its limitations will also be elaborated.

A. Query-response process

The example of query-response procedure of CCEF is illustrated in Figure 1. 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 or D node. The copies of Q_{id} and k_w keys are dropped on every node in the path as shown in Fig. 1(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.

The query response message is illustrated in the Figure 1(b). 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 the CH . 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 original BS. 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, the BS 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 CH replies, 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).

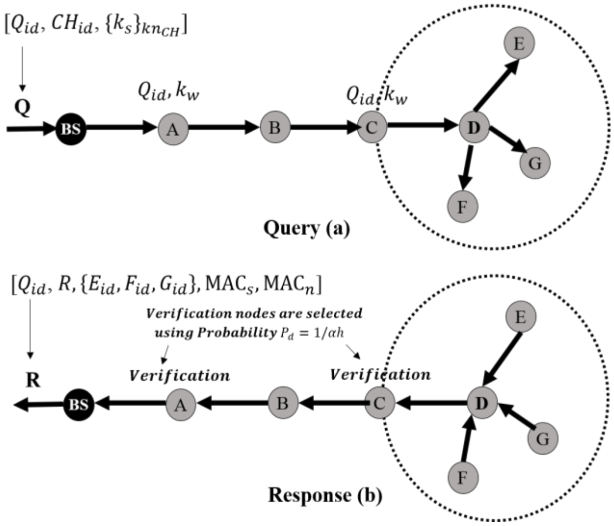
$[Q_{id}, CH_{id}, \{k_s\}_{kn_{CH}}]$
Q
Q_{id}, k_w
Q_{id}, k_w
BS
A
B
C
D
E
F
G
Query (a)
$[Q_{id}, R, \{E_{id}, F_{id}, G_{id}\}, \text{MAC}_s, \text{MAC}_n]$
Verification nodes are selected using Probability $P_d = 1/\alpha h$
R
Verification
Verification
BS
A
B
C
D
E
F
G
Response (b)

Figure 1. Query and response procedure in CCEF

B. Verification process

After the report in the response message reaches the BS, it generates the MAC_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.

C. Greedy perimeter stateless routing

For query-response routing in CCEF underlying routing is performed using GPSR [3], and its suitability for the sensor network context is not discussed further. GPSR make excessive use of geography to achieve scalability under increasing numbers of nodes and mobility. The protocol makes greedy forwarding decisions based on the router's immediate neighbors and uses local topology information to address frequent topological changes.

Hierarchy and caching are used to determine scalability. In the greedy forwarding, a packet is forwarded to a node from N_i neighbors that are closer to the destination(D), and this process is carried on to reach D . For a situation in which greedy forwarding does not work, the right hand rule is used to route around the perimeter in a counter-clockwise direction. The process forwards packets based on the greedy approach in terms of the closer next-hop to D and does not consider the residual energy of the nodes taking part in the routing decisions. This is critical in wireless sensor networks, which have stringent energy, storage, and processing requirements, which is not the case for the ad-hoc wireless networks for which GPSR was originally designed.

III. Experimental Environment

In this section, we explain the experimental environment assumptions and how we obtain the attacks information or FTR without incurring extra messages on sensor nodes.

A. 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 [17]. 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.

B. Experimental model

We consider randomly deployed 1000-node sensor network in grid area of $(500 \times 500)\ \mathrm{m}^2$. In each cluster, an equal number of nodes are randomly positioned. The BS is aware of the node IDs, 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 initial energy (e.g., 1 joule) and a limited sensing range of $50\mathrm{m}$. We perform experiments with false traffic ratio (FTR) of 30%.

The energy required by electrical circuit to transmit one bit is 50nJ and power used by amplifier is 100pJ to transmit one bit for the Mica2 platform [17]. The energy required for MAC verification is 20mJ. Table I shows the parameters for the experimental setup that was used for performance analysis.

TABLE I. Experimental parameters detail

Parameters	***values***
Sensors nodes	1000
Sensor field size	$(500 \times 500)\ \mathrm{m}^2$
BS location	$(250, 0)$ m
R_i	50 m
Cluster h/w	50 m
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

C. 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 (1), the current FTR ratio can be calculated for n events

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

IV. Proposed Method

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

A. Boot-up phase

The BS is assumed cannot be compromised and sensor nodes are considered to be secure during the initialization setup phase. All the send nodes have equal initial amount of energy. Randomly deployed nodes are assigned unique Sensor nodes are considered secure for the initialization during the boot-up process, and it is also assumed that the BS cannot be compromised. The sensor nodes have a fixed amount of energy. Every node can know its location through a location mechanism. At this phase, the randomly deployed nodes are granted unique IDs and k_n.

B. Session set-up and key-distribution

The BS sends a Q_m message to the CH (i.e., node D) that contains the Q_{id} and CH_{id}. In order to establish a session, a plain text k_w key is pre-deterministically distributed to a portion of the nodes that have a large enough fitness value.

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. A session expires after t time units or after a node is depleted.

C. Route setup process

In CCEF route setup process uses GPSR for routing which is based on pure distance based routing. The rest of the route set-up process used in CCEF is explained in the background sub-sections 2.1 and 2.3. The energy-efficient route setup process used in proposed by selecting next forwarding node is given by the Equation (2).

$$F_n = \alpha \times (d_i + e_i) + k_w \times \beta;\ where\ (1 < \alpha, \beta < 0) - (2)$$

The BS determines the subset of neighbor nodes from the neighbor set within the antenna range Ri closer to the itself as compared to the CH. In order to calculate the next forwarding node from the neighbor subset, the distance d_i, energy e_i, and presence of k_w are considered. This process is repeated to establish path from the BS to destination D.

V. Results and Discussion

In this section, the performance analysis of energy-efficiency, network lifetime, and detection capacity is experimental evaluated. The energy-efficiency and network lifetime value are measured using performance matric of first cut off (FCO) and half cut off (HCO). The FCO is defined as the number of rounding taken until the first sensor node in the network is depleted. A sensor node is depleted when initial energy resource reaches zero after number of communications. Similarly, the HCO is defined as the number of rounds taken for the half and last of the sensor node(s) in the network is depleted. The nine cases of different network sizes or number of nodes {i.e., 200, 300,…, 1000} with fixed sensor field are considered.

A. Energy-efficiency

The Figure 2 illustrates the energy-efficiency performance analysis using FCO. There is mix performance, however, oveall our proposed method performance on average is better than the original scheme. The average energy saving over the nine network sizes shows an energy saving of 3.17%.

In case of HCO performance matric used for energy-efficiency analysis the average energy saving is 4.78%. The performance comparison using HCO performance metric is shown in the Figure 3. The small improvement in energy–efficiency is due to the better detection-capacity of proposed algorithm.

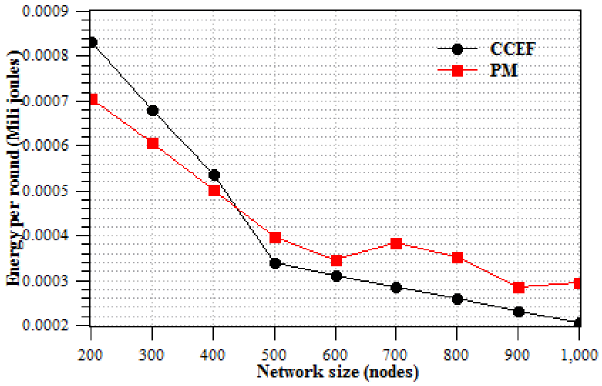

Figure 2: Energy-efficiency per round using FCO

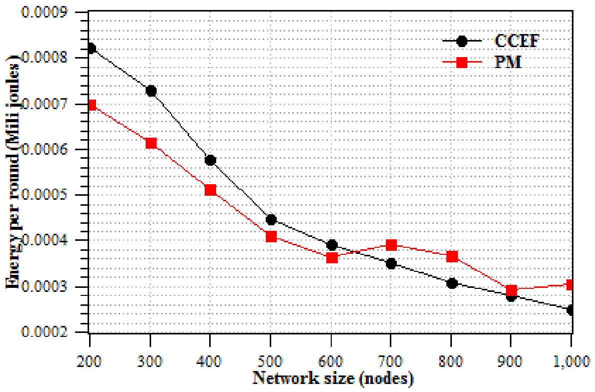

Figure 3: Energy-efficiency per round using HCO

B. Network Lifetime

The Figure 4 and Figure 5 depicts the network lifetime results using FCO and HCO performance analysis metrics. A significant network lifetime extension of 3.564 times (or 356.4%) is observed using FCO with our proposed method as compared to original scheme as highlighted in the Figure 4. The HCO performance parameter also shows an improvement of 1.921 folds over the CCEF. This result analysis is illustrated in the Figure 5.

There are some fluctuations in number of rounds values along the x-coordinate are observed as we are using difference network, however, they fall within certain range. The gain in network lifetime is because of distribution of communication loads over the larger group of sensor nodes in the sensor

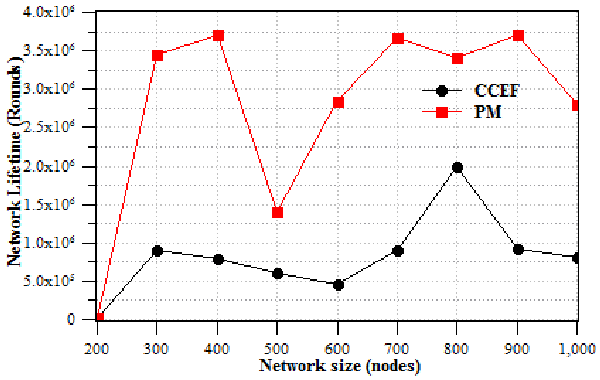

Figure 4. Network lifetime using FCO

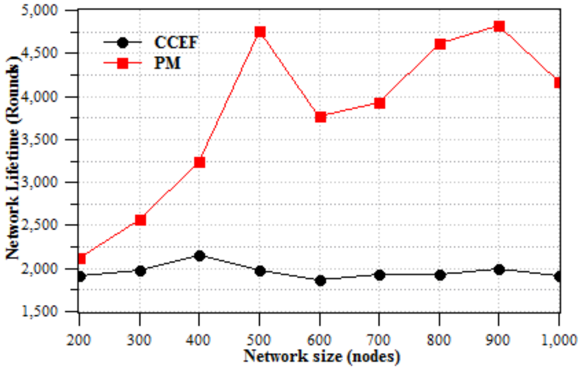

Figure 5 Network lifetime using HCO

network. This due to dynamic path selection routing based on energy level, possession of key, and distance as against distance only in GPSR routing in CCEF.

C. Detection capacity

The proposed method demonstrate better detection capacity as compare to CCEF. This is because of pre-deterministic key distribution which consider possession of keys for the selection of verification keys as against probabilistic key distribution method in the original scheme. Our proposed method performance comparison with CCEF is illustrated in Figure 6. The average detection capacity of CCEF in nine cases was 81.95% as compare to 86.43% in the proposed method.

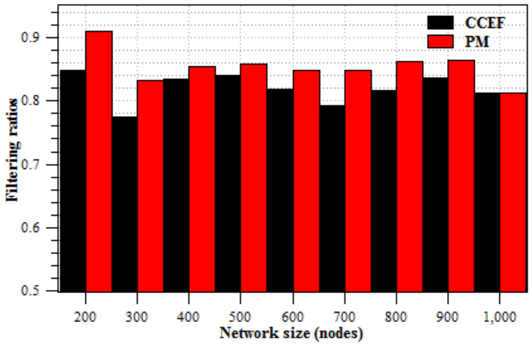

Figure 6: Detection-capacity performance

VI. Related Work

The novel CCEF [2] scheme can save energy by early dropping of false event messages. This probabilistic en-route filtering scheme cannot adapt to the changing FTR and is based on fixed path routing. These characteristics may lead to adverse effects energy and network lifetime. Our proposed method cater these limitations for energy efficiency and extended network lifetime. 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. It does not consider the residual energy of the nodes taking part in the routing decisions.

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 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 clouding nodes. In a probabilistic voting-based filtering scheme (PVFS) [7], 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) [8] 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 [9], 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 [10], 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 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 this paper in order to perform energy dissipation analysis, the first order radio model [14], has been used. The authors [15] presents a comprehensive survey on en-routing filtering schemes in WSNs. The underlying platform Crossbow Mica2 [16] is considered and energy consumption values from [17].

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.

VII. Conclusions and Future Work

The proposed method prolonged the network lifetime significantly due to more even distribution of communication overloads due to dynamic path selection method or routing. It also saved some energy due to the better detection capacity by dropping fabricated reports earlier.

In future, we plan to performance experiments on real sensor network test-bed using 802.15.4 error traces [18].

ACKNOWLEDGMENT

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] Deepak Uttamchandani. (2013). Handbook of Mems for Wireless and Mobile Applications. Woodhead Publishing.

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

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

[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] 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.

[9] 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.

[10] J.M. Kim, Y.S. Han, H.Y. Lee and T.H. Cho. (2011). Path renewal method in filtering based wireless sensor networks. Sensors. vol. 11, pp. 1396-1404.

[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] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan (2000). Energy-efficient communication protocol for wireless sensor networks. Proceedings of the Hawaii International Conference on System Sciences, pp. 1-10.

[13] 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.

[14] 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.

[15] S.V. Annlin Jeba Dr. B. Paramasivan. (2012). An evaluation of the en-route filtering schemes on wireless sensor networks. International Journal of Computer Engineering & Technology (IJCET). vol. 3(2), pp. 62-73.

[16] 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.

[17] Crossbow, 2011, http://www.xbow.com/

[18] Error Traces 802.15.4: http://wisnet.seecs.nust.edu.pk/datasets/Traces_802.15.4/

[19] ETSP: An Energy-efficient Time Synchronization Protocol on Wireless Sensor Networks. (2008). Shahzad, Khurram; Ali, Arshad; Gohar, N. D., IEEE 22nd International Conference on Advanced Information Networking and Applications (22nd IEEE AINA), Okinawa, Japan; March 23-26.

AUTHORS PROFILE

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.