ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Sink mobility for commutative cipher based en-route filtering to prolong the network lifetime in wireless sensor networks

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

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

Manuscript Info

Manuscript History:

Received: 14 October 2015
Final Accepted: 17 November 2015
Published Online: December 2015

Key words:

Wireless sensor networks, En-route filtering, Network lifetime, Sink-mobility, Filtering-power.

Corresponding Author

Tae Ho Cho

Abstract

Wireless sensor networks (WSNs) are comprised of a large number of randomly deployed low-cost, small-size, low-energy un-attended sensor nodes. An adversary can inject a large quantities of fabricated reports towards sink(s) draining scarce energy en-route. En-route filtering schemes such as commutative cipher based en-route filtering (CCEF) are proposed to counter these attacks and hence save energy. While these schemes saves energy they may not necessarily prolong network lifetime. In CCEF, inherent limitations such as; 1) fixed paths, 2) energy inefficient routing, and 3) unbalanced communication loads leads to adverse effects on network lifetime. In order to counter these issues, we propose sink mobility based CCEF (SM_CCEF). Energy-aware routing and sink mobility help avoiding energy-hole problem which is observed in static sink based networks. Experimental results demonstrate the efficacy of our proposed method which prolonged network over three folds because of balanced communication loads over larger groups of sensor nodes.

1. INTRODUCTION

The advances in the microelectromechanical systems (MEMS) **(Deepak Uttamchandani, 2013)** have unleashed numerous new devices and applications. This technology has facilitated low-cost, low-energy, small-size, multi-purpose, untethered and unattended sensing devices. Featuring scarce resources, uncertain network conditions, and a hazardous environment, network resources should be managed wisely. However for their widespread deployment, researchers need to address energy-efficiency, network lifetime, and security requirements.

We investigated energy efficient routing for communicative cipher based en-route filtering (CCEF) **(Hao Yang and Songwu Lu., 2004)** scheme in pre-deterministic key distribution in CCEF (PKCCEF) **(Muhammad K. Shahzad and Tae Ho Cho, 2015)**. In this paper, in addition to previous work, we extend CCEF for mobile sink based networks. This further, increases the network lifetime due to the better distribution of communication loads over the network. In CCEF, inherent limitations such as; 1) fixed paths, 2) energy inefficient routing, and 3) unbalanced communication loads leads to adverse effects on network lifetime. In order to counter limitation in original scheme, we propose sink mobility based CCEF (SM_CCEF).

The main idea of existing en-route filtering schemes **(Hao Yang and Songwu Lu., 2004; F. Ye et. el., 2004; Zhen Yu, and Yong Guan., 2010; S. Zhu et. el. 2004; and Feng Li and Jie Wu., 2006)** is to counter security threats from false report attacks. These schemes with better or early detection of false reports can save significant energy. However, underlying routing might not be energy aware since residual energy level of sensor nodes is ignored while selection forwarding nodes. Moreover, these security schemes exhibit short network lifetime due to energy-hole problem in

sink based networks. This problem occurs due to faster energy depletion rate of sensor nodes closer to the BS or on critical paths.

In order to remove some of the limitations improved en-route filtering schemes has been presented **(Muhammad K. Shahzad and Tae Ho Cho, 2015; J.M. Kim et. el. 2011)**. The work **(Liu, Tao, 2012)** demonstrates that the sensor nodes closer to the sink tend to deplete their energy at a faster rate than the other nodes. In this paper, we use commonly used energy-dissemination model know as first order radio model **(Swarup Kumar Mitra and Mrinal Kanti Naskar, 2011)**. We assume Mica2 **(Crossbow, 2011)** platform for energy consumption values from research work **(Wendi et. el., 2000)**. In the past **(J. Luo, and J. P. Hubaux, 2005)**, it has been presented that sink mobility can help solving energy-hole problem by more even distribution of communication loads over the larger group of sensor nodes.

Research work **(K. Shahzad Muhammad and Cho Tae Ho, 2015)** fuzzy logic to increase the filtering capacity by network conditions to determine verification nodes. This approach better balance the communication loads to extend the network lifetime. The clocks of the sensor and other computing devices are assumed to be synchronized using an energy-efficient time synchronization protocol on wireless sensor networks (ETSP) present in **(Shahzad, Khurram, et el., 2008)**.

2. LITERATURE REVIEW

The novel commutative cipher based en-route filtering (CCEF) **(Hao Yang and Songwu Lu., 2004)** 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 **(B. Karp and H. T. Kung., 2000),** 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) **(F. Ye et. el., 2004)** 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) **(Zhen Yu, and Yong Guan., 2010)** 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 **(S. Zhu et. el. 2004)** 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) **(Feng Li and Jie Wu., 2006)**, the number of votes (i.e., MACs) is used to prevent both fabricated reports with false votes and false votes in valid report attacks.

In pre-deterministic key distribution based in CCEF (PKCCEF) **(Muhammad K. Shahzad and Tae Ho Cho, 2015)**, we have demonstrated that energy-efficient routing and pre-deterministic key distribution help balance the communication loads over the network. This approach successfully improved energy-efficiency and network lifetime. In **(J.M. Kim et. el. 2011)**, 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 low-energy adaptive clustering hierarchy (LEACH) **(Wendi et. el., 2000)** can evenly balance communication loads by random rotating the CHs inside the cluster. Data fusion is used to remove redundancy so reducing the amount of information to be transmitted to the BS. The work **(Liu, Tao, 2012)** demonstrates that the sensor nodes closer to the sink tend to deplete their energy at a faster rate than the other nodes.

In this paper in order to perform energy dissipation analysis, the first order radio model **(Swarup Kumar Mitra and Mrinal Kanti Naskar, 2011)**, has been used. Research work **(K. Shahzad Muhammad and Cho Tae Ho, 2015)** fuzzy logic to increase the filtering capacity by network conditions (i.e., false traffic ratio (FTR), residual energy of a nodes, and number of massage authentication codes (MACs)) to determine verification nodes. This dynamic path selection based approach better balance the communication loads to extend the network lifetime. The clocks of the sensor and other computing devices are assumed to be synchronized using an energy-efficient time synchronization protocol on wireless sensor networks (ETSP) present in **(Shahzad, Khurram, et el., 2008)**.

The underlying platform assumed is Crossbow Mica2 **(Crossbow, 2011)**. J. Luo et al. **(J. Luo, and J. P. Hubaux, 2005)** in the past have proposed that sink mobility can help in energy balancing and thus solving the energy-hole problem around the sink. Result have shown that this strategy can achieve a five folds improvement in network lifetime.

3. EXPERIMENTAL METHODOLOGY

In this section, experimental assumptions, network model, attack information model, and first order radio model will be elaborated with detail.

3.1. Experimental assumptions

The boot-up process is assumed to be secure for initialization process. The BS has sufficient amount of energy and cannot be compromised. The sensor nodes are static however in proposed method the BS is mobile. Unique IDs and k_n keys are preloaded in the sensor nodes. The BS knows the IDs and k_n keys of all nodes. The locations of sensor nodes can be determined by some pre-loaded location component. The energy dissipation from radio and electronics of the sensor nodes are only considered. The underlying platform for our experimental environment is Mica2 sensor motes **(Crossbow, 2011)**. The communication links are considered bidirectional.

3.2. Network model

A sensor network with random deployment of 1000 sensor nodes in a field of area (500×500) m^2 is considered in the paper. The experiments are performed in custom built C++ simulator in Microsoft Visual Studio. We perform experiments with FTR of 30%. Each sensor node has a fixed initial energy (e.g., 1 joule) and a limited sensing range of 50m. In this paper, we use the first order radio model presented in **(Swarup Kumar Mitra and Mrinal Kanti Naskar, 2011)**. 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 **(Crossbow, 2011)**. The **Table (1)** illustrate the parameters for the experimental setup that was used for performance analysis. The sensor field for our simulation experiment is shown in **Fig. (1)**.

Table (1): Experimental parameters

Parameters	**Values**	
	CCEF	**SM_CCEF**
Sensors nodes	1000	1000
Sensor field size	(500×500) m^2	(500×500) m^2
$\boldsymbol{BS}$ location	$(250, 0)$ m	clockwise
Type of $\boldsymbol{BS}$	Static	Mobile
$\boldsymbol{R_i}$	50 m	Dynamic
Cluster h/w	50 m	Dynamic
$\boldsymbol{E_{elec}}$	50 nJ/bit	50 nJ/bit
$\boldsymbol{E_{amp}}$	100 pJ/bit/m^2	100 pJ/bit/m^2
Node energy	1 Joules	1 Joules
MAC verification	20 mJ	20 mJ
Data packet	32 bytes	32 bytes
Round	128 bytes	128 bytes
FTR	30%	30%
Path loss constant (λ)	2	2

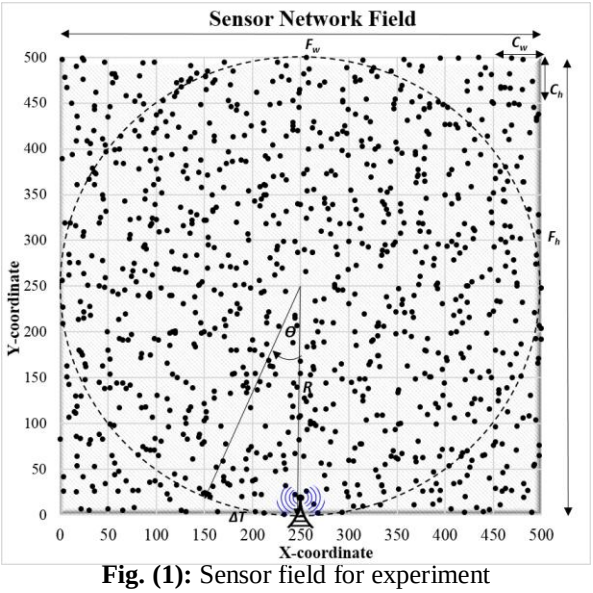

Fig. (1): Sensor field for experiment

3.3. Attack information Model

The communication in our method is query-driven in which a query message is initiated by the BS to inquire about an event in an area. For one query-response session, the BS knows the expected number of event reports from the source CH. A legitimate report received at the CH will increment the respective counter by one to determine total number such reports. For this case no extra messages or energy consumption is required at the sensor nodes. Fabricated or false reports can be dropped either en-route or at the BS.

In first case a fabricated report is dropped en-route, the BS will know report is dropped after a time window is elapsed. In second case, if a fabricated report is reached at the BS, it will be dropped after final verification. In both cases of legitimate and fabricated reports, the BS will know the total number both types of reports by their respective counters. Therefore, by using this information the value of the 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. For n events FTR is defined in **Eq. (1)**.

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

3.4. First order radio 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 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. (3)**. In order to transmit a m bits packet at a distance d between the transmitter and receiver, the transmission energy required, $E_{T_x}(l, d)$, is shown by **Eq. (2)**.

$$E_{T_x}(l, d) = E_{elec} \times l + E_{amp} \times l \times d^{\lambda} \quad (2)$$

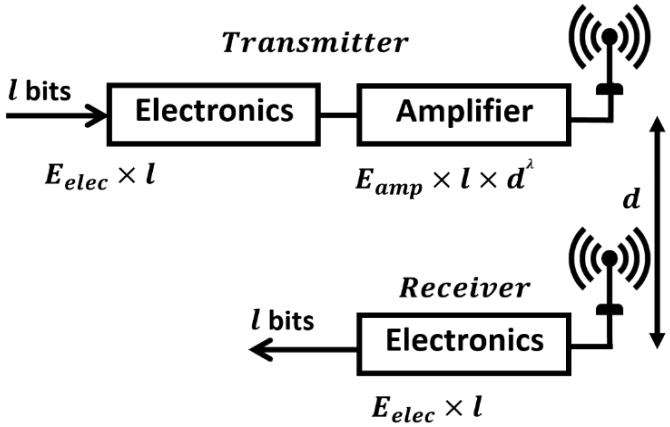

Fig. (3): First order radio model

Where E_{elec} is the energy used by the electronics of the circuit, and $E_{elec} \times l$ is the energy used by the electronics of the transmitter to transmit m bits. Moreover, E_{amp} is the energy used by the amplifier, and λ is the path loss constant. Similarly, $E_{R_x}(l)$ is the energy needed to receive k-bits in **Eq. (3)**.

$$E_{R_x}(l) = E_{elec} \times l \quad (3)$$

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 $50\ nJ/bit$.

4. PROPOSED METHOD OVERVIEW

In this section, network construction, key-distribution, path construction, and sink re-location phases are explained.

4.1. Network construction phase

A sensor field of area (500×500) m^2 with 1000 densely deployed sensor nodes is considered. 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. 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.

4.2. 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 distributed before a session in the network, while k_s is sent securely to the CH 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 using probabilistic method $p = \frac{1}{\alpha h}$; where α is design parameter and h is number of hopes.

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. The path with corresponding verification nodes as per attacks is selected dynamically. Therefore, depending upon the attack ratio, there can be different corresponding paths. A session is changed after t time or after a node is depleted.

4.3. Path construction phase

In CCEF route setup process uses GPSR for routing which is based on pure distance based routing. The energy-efficient route setup process used in proposed by selecting next forwarding node is given by the **Eq. (4)**.

$$N_n = k \times \left(1 - \frac{\beta}{2}\right) + (d + e) \times \frac{\alpha}{2} \qquad (4)$$

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.

4.4. Sink re-location phase

For the sink mobility or re-location from previous position to next in circular clockwise position is calculated with globally known information at startup. The BS initial location, and θ radius$R$ and Δt are known. If (x, y) is initial location of the BS than new location (x'', y'') after clockwise θ degrees movement can obtained by **Eq. (5)** and **(6)**.

$$x'' = x' + C_x \qquad (5)$$

$$y'' = y' + C_y \qquad (6)$$

Where $x' = x\cos\theta - y\sin\theta$,

$$y' = x\cos\theta + y\sin\theta,$$

$$\theta = (\frac{V}{R})\Delta t, V = (\frac{\theta}{\Delta t})R,$$

$$C_x = \frac{F_w}{2}$$

$$and\ C_y = \frac{F_h}{2}$$

The BSstays at subsequent position until round of data collection (i.e. 50 events) is completed. In this paper, we define $\theta = 2^{\circ}$, called degree of re-location or mobility.

5. RESULT AND DISCUSSION

In this section, performance results of CCEF and sink mobility based CCEF (SM_CCEF) are compared for network lifetime and filtering capacity.

5.1. Network lifetime

The network lifetime is compared using first node depleted (FND), half nodes depleted (HND), and percentage of nodes alive (PNA). A sensor node is considered depleted when residual energy level is reached zero due to communication after certain number of rounds. A round is defined as count four events where each event message is 200 bytes. The schemes lasting for more number of rounds have longer network lifetime. The x-coordinate indicates size of network in terms of number of sensor nodes and y-coordinate indicates number of rounds taken by a scheme before first node is depleted. The performance analysis using FND is illustrated in **Fig. (3)**, for CCEF and

SM_CCEF. The **Fig. (3)**, indicates consistently better performance of SM_CCEF as compared to CCEF scheme. On average our proposed method performs 4.4315 times (or 443.15%) better as compared to CCEF scheme.

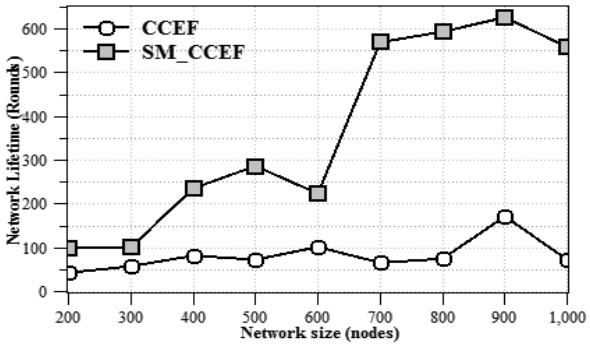

Fig. (3): Network lifetime (FND)

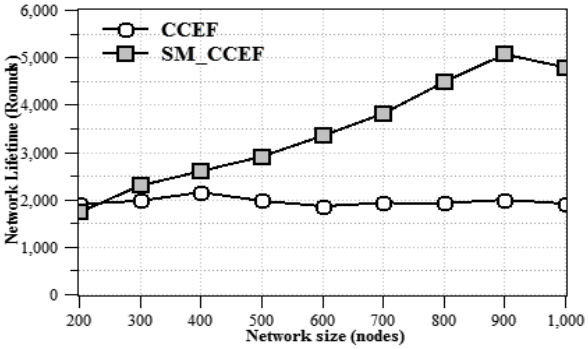

Fig. (4): Network lifetime (HND)

The **Fig. (4)**, presents the network lifetime performance of the two schemes using HND performance unit. In this case our proposed method extends the network lifetime about 1.7569 folds as compared to the original scheme. The summary of performance comparison of two schemes is presented in Table (2).

Table (2): Network lifetime performance summary

Scheme \ Matric	FND	HND	Avg.
CCEF	82.667	1966.3	1024.5
SM_CCEF	366.33	3454.6	1910.5
Extension (%)	4.4315	1.7569	309.42

Another way to measure network lifetime is number of nodes alive at the end of the simulation in each scheme. The lower the number of nodes alive means better network lifetime performance. The performance comparison of two schemes using this performance indicators is shown in **Fig. (5)**. Our proposed scheme with mobility support performs significantly better as compared to the CCEF. On average of nine cases for various network sizes 54.347%

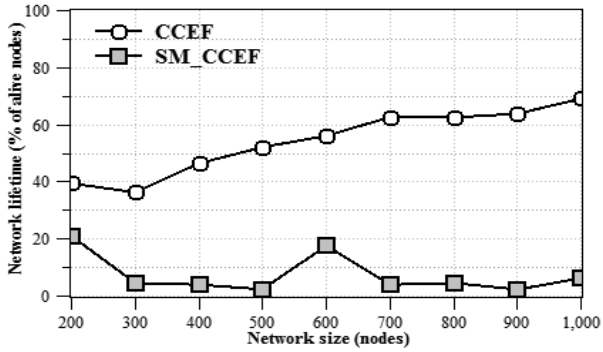

Fig. (5). Network Lifetime (PNA)

of nodes remain in CCEF whereas in SM_CCEF only 7.4435% nodes are left at the end of the simulation.

5.2. Filtering capacity

The filtering capacity performance over 30% fabricated report attacks is shown for CCEF and SM_CCEF in the **Fig. (6)**. Our proposed scheme performs better with filtering capacity of 75.63% whereas filtering capacity of CCEF is 71.31%.

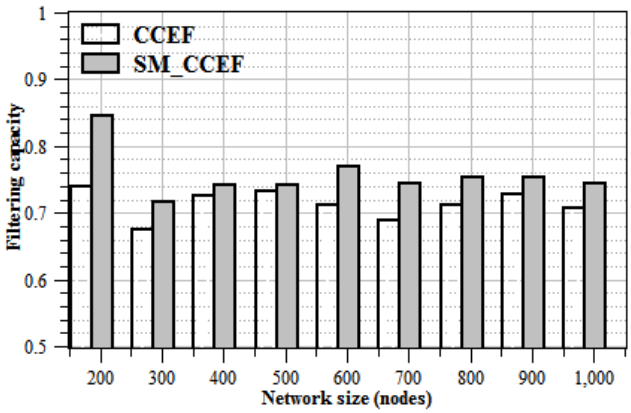

Fig. (6). Filtering capacity

6. CONCLUSIONS

Our improved CCEF for sink mobility based sensor networks avoided the energy-hole problem with balance communication loads distribution of the larger group of sensor nodes. Energy-aware routing also help balancing energy consumption with dynamic path selection in contrast with CCEF fixed path routing which is one of the reason for lower network lifetime performance original scheme.

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

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

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

Crossbow, 2011, http://www.xbow.com/

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.

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

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.

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.

J. Luo, and J. P. Hubaux, 2005, Joint mobility and routing for lifetime elongation in wireless sensor networks, In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), pp.1735–1746.

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.

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, vol 22 (8), pp. 2799-2809, DOI 10.1007/s11276-015-0941-0.

K. Shahzad, Muhammad and Cho, Tae Ho (2015), An Enhanced Detection and Energy-efficient en-route Filtering (EDEF) Scheme in Wireless Sensor Networks, Informatics Engineering, An International Journal (IEIJ), Vol. 3 (3), pp. 11-26, Sep, 2015. DOI: 10.5121/ieij.2015.3302.

Shahzad, Khurram; Ali, Arshad; Gohar, N. D. (2008), ETSP: An Energy-efficient Time Synchronization Protocol on Wireless Sensor Networks, IEEE 22nd International Conference on Advanced Information Networking and Applications (22nd IEEE AINA), Okinawa, Japan; pp. 971-976, March 23-26, 2008.

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.

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.

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.

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.

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.