The ICCIT International Conference Proceeding

IEEE Conference Record number: #17832
IEEE PDF Files Catalog Number: CFP1032I-ART
IEEE PDF Files ISBN: 978-89-88678-30-5
IEEE PDF Files Catalog Number: CFP1032I-PRT
IEEE PDF FilesISBN: 978-89-88678-29-9

ICCIT 2010 Vol. I

The 5th International Conference on Computer Sciences and Convergence Information Technology

November 30 - December 2, 2010,
Grand Hilton Hotel, Seoul, Korea

Sponsored by
IEEE
IEEE SEOUL SECTION
AICIT

Hosted/Co-organized by
ETRI
IEEE IRAQ SECTION

An Objective Method to Find Better RBF Networks in Classification
Hyontai Sug 373

Parallel Implementation of 2D Daubechies - D4 Transform in a Cluster
Jaumin Ajdari, Fatmir Hoxha 377

Information Retrieval using OntoSense Querying and Ontological Indexing
Iulian-Florin Toma 383

CUDA Implementation of McCann99 Retinex Algorithm
Hyoseok Seo, Ohyoung Kwon 388

Data Structures for Mixed Workloads in In-Memory Databases
Jens Krueger, Martin Grund, Martin Boissier, Alexander Zeier, Hasso Plattner 394

Nonlinear Adaptive Joint Filter for Narrowband Interference Suppression in GPS Receiver
Wang Qiang, Jiashu Zhang, Yang Jing 400

Improving the Reception Quality of CMMB by Utilizing TD-SCDMA Networks
Xiaodong Yang 405

High-Rate Full-Diversity Multiuser Space- Frequency Codes
R.S. Topu, A.U.Alam, M.A. Matin 411

A New Minimum Variance Beamforming Technique for Cognitive Radio Network
Z. Hossain, U. Habiba, M. A. Matin 417

Performance Analysis Towards a KVM-Based Embedded Real-Time Virtualization Architecture
Jun Zhang, Kai Chen, Baojing Zuo, Ruhui Ma, Yaozu Dong, Haibing Guan 421

Software Integration of Identical DLP Threads via Compilation for VLIW Processors
Maolin Guan, Nan Wu, Mei Wen, Chunyuan Zhang 427

Implementing Basic Image Processing Programs onto a Linearly Connected Parallel Processor
Hideaki Ito, Masaru Shimizu, Saburou Iida 434

An Adaptive and Reliable Data-Path Determination for Fault-Tolerant Ethernet Using Heartbeat Mechanism
Hoang-Anh Pham, Jong Myung Rhee, Yeonseung Ryu, Dong Ho Lee 440

Redesign of Grid-Based Enterprise Information Network through Servers Consolidation
Abdullah R. Abdulgafer, Paulvanna N. Marimuthu, Sami J. Habib 445

EDPPS: An Energy-efficient Data Privacy Protection Scheme for Wireless Sensor Networks
Imanishimwe Jean de Dieu, Jin Wang, Diego Jose Asturias, Sungyoung Lee,
Young-Koo Lee 451

EDPPS: An Energy-efficient Data Privacy Protection Scheme for Wireless Sensor Networks

Imanishimwe Jean de Dieu, Jin Wang, Diego Jose Asturias, Sungyoung Lee, Young-Koo Lee

Department of Computer Engineering,
Kyung Hee University, Korea
{jeanishimwe, wangjin, dasturias, sylee}@oslab.khu.ac.kr; {yklee}@khu.ac.kr

***Abstract*—In wireless sensor networks (WSNs) sensors may be deployed in unpredictable environment, a limited energy of the sensor nodes has led to the development of the Energy-efficient Data Privacy Protection Scheme (EDPPS). It is a process of ensuring privacy and security to the sensed data as well as maximizing the network lifetime. Many schemes have been proposed using symmetric key cryptography algorithm for securing data. However, a current limitation of protecting data privacy in WSNs is that the symmetric key cryptography algorithms are vulnerable to node compromise attacks. To overcome this limitation, we investigate the facts of ensuring secure sensed data in a balanced energy network backbone based on distance from the source node to base station. Specifically, a checking data integrity mechanism has been proposed in this paper. Our analysis and simulation results show that EDPPS has a better performance through four abstract parameters: anonymity of the sensor nodes, confidentiality, authenticity and integrity of the actual sensed data. It also provides a good level for energy consumption as well as maximizing the network lifetime.**

Keywords-component; Energy-efficient; Data privacy; Authentication; Wireless sensor networks

I. Introduction

Wireless sensor networks (WSNs) [1,2,3] are the most important technologies which are used in variety of applications. To impact these applications in real world environments we need more efficient strategies to guarantee secure privacy on the sensor readings as well as to prolong or maximize the network lifetime. WSNs use tiny and inexpensive sensor node devices; these multifunctional miniature devices perform limited and also specific monitoring and sensing functions [9]. They permit very low energy consumption and have very low processing power as well as low radio ranges [1]. The sensor nodes will sense, process and then transmit the data to certain remote sink node (base station) in an autonomous and unattended manner [9].

Security and privacy are important when confidential data are involved in WSNs applications [1, 4, 11]. WSNs pose unique challenges in terms of designing security mechanisms, specifically due to power, computation and communication constraints of individual sensors. As WSNs are used in everyday life, the privacy of monitored sensitive data becomes an important issue.

Our paper is mainly inspired by the work in [6] where symmetric key (shared key) was used to ensure protection of actual sensed data in WSNs. Their work was well analyzed in different challenges. However, symmetric key can be extracted by an attacker through a compromised node and without checking integrity on the receiver side; this may result on delivering a modified data to a base station (BS).

In this paper, we present an energy-efficient data privacy protection scheme (EDPPS) for wireless sensor networks which aims to achieve security and privacy for transmitted sensed data within an energy-efficient network infrastructure. Due to inherent deployment nature and energy limitation constraint of the sensors, ensuring energy efficiency together with the security and privacy of the sensed data becomes a foremost task [14]. Our scheme ensures secure transmission of data from the source sensors to the base station in a way that it can consume the available amount of energy in balanced manner within the network. We use one-way hash function and shared secret keys for ensuring security service on the sensed data. In EDPPS, a routing architecture is created as the topology of the network. The major contributions of this work are:

a) The energy balanced among the sensors in WSNs based on the distance of each node to base station. This will increase the lifetime of the whole network.

b) The privacy of the sensor readings will be achieved through a service of anonymity which results on hiding the source node identity along the transmission path and only the base station will identify the sender.

c) Providing security of the data transmission from the source node to base station through three security services: Confidentiality, Authenticity and integrity of the actual sensed data.

II. Related works

Transmission between the end nodes can occur in a single hop, or up to *N* hops [11]. Many existing researchers indicate that on multihop routing more short hops are preferable to fewer long hops, because the minimum signal-to noise ratio (SNR) along the route is larger for multihop. But as indicated in [10] this consideration does not take into account the important practical issues of resource allocation, end-to-end delay, error propagation, and interference induced by extra transmissions. Therefore, a new routing method should be adapted to prevent routing over many short hops. In [12] a hierarchical structured energy efficient routing protocol called LEACH is presented, it is a smart solution where clusters are formed to merge data before transmitting to the base station. By using the cluster-heads chosen to transmit to the base station, LEACH achieves a factor of 8 improvement compared to direct transmissions and the energy consumption is balanced via the rotation of 5% cluster heads and it is greatly reduced by data aggregation inside each cluster head. However, clustering will require more energy during rotation of cluster heads.

In [13] an Energy-Efficient Routing Schemes for Wireless Sensor Networks is proposed where after making a study on energy-optimal network configurations for manual and random placement of nodes under a natural coverage criterion; they proved that in a linear network, energy consumption is minimal when nodes are equally spaced. However, the load is not equally to all the nodes therefore energy distribution should take into account the traffic load from the source to destination.

In [14] secure energy-efficient routing protocol for densely deployed wireless sensor networks SERP is presented which aims to achieve robust security for transmitted sensor readings with an energy-efficient backbone. They proposed a network routing model which aims at minimizing the wasteful energy consumption by energy-efficient structuring of the network and then security on the sensed data transmissions from the sensors to the base station using one way hash chain and shared secret keys. Their routing model selects a minimum number of forwarding nodes in the network through energy and distance based efficient structuring of the network which helps for maximizing the lifetime of the network. However, these exchange control messages will introduce more control overheads as well as require more energy consumption and for security defense mechanism the identity of the source node is publicly known therefore, brute-force search and eavesdropping attacks are free to gain access on the system.

Energy-efficient secure pattern based data aggregation for wireless sensor networks ESPDA is presented in [15] which focused on the issue of energy-efficient data aggregation with secure data transmission. ESPDA keeps the data transmission and aggregation more secure by limiting the cluster heads to decrypt or encrypt the data received from the sensors.

Authors in [2] present an authenticated encryption scheme by using hashing method to ensure message integrity. In [5], the authors suggest using a combination of symmetric (shared key) and asymmetric (Public Key) encryption algorithms simultaneously to ensure secure protection of sensed data. As they also declared that: symmetric key cryptography can be easily extracted by an active attack. In [6], the authors propose a scheme by using two cipher algorithms (asymmetric and symmetric keys) to ensure data privacy in WSNs. The authors analyze energy consumption and time overhead of different security mechanisms in [7].

III. The Proposed Approach

The proposed approach for ensuring data privacy protection in WSNs through an energy-efficient network backbone is comprised of two phases. At the first phase we proposed a distance based energy aware routing (DEAR) algorithm. The objective of this phase is to balance the available amount of energy in the whole WSNs as well as maximizing the network lifetime. At the second phase in the proposed network routing we ensured confidentiality, authenticity and integrity security services on the sensed data. Fig. 1 shows the complete architecture of the proposed model.

A. Energy Balancing Phase

The following is the distance-based energy balanced scenario:

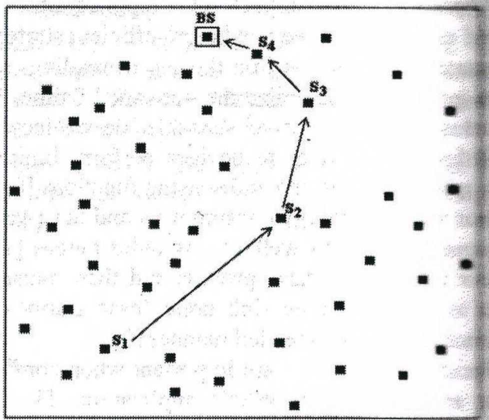

Fig.1. Distance based network model

In Fig.1 our scenario shows that when an event occurs in WSNs, the source node will transfer the data to base station (BS) in two phases: Direct transmission routing "Single hop" when the sensor node is located near the base station and Multi-hop routing when the source node is located far away from the sink node. As proposed in our previous work [9], for direct transmission routing, the nodes far away from sink node will drain out of energy very quickly due to the characteristics of wireless channel. For multi-hop routing, the nodes close to sink node will have more traffic load to forward under most routing mechanisms and also drain out of energy quickly.

Table 1 shows the energy distribution along the network from the source node to base station by considering 4 nodes to reach the sink. On the event based scenario refer to table 1 each node will require one round of an amount of energy to transmit E_{Tx} its own message and the round time for forwarding the message from previous nodes, it will increase one round per hop on the path towards the base station and this will results on more energy forwarding E_{Fx} consumption for the nodes closer to the sink (base station). Distance based energy balancing scheme is proposed to deal with this problem as well as maximizing the network lifetime.

TABLE I. TIME / ROUND TRAFFIC BASED

Sensors	Transmit	Forward
S_1	1	0
S_2	1	1
S_3	1	2
S_4	1	3

The following are the steps for distance-based energy aware routing: "This algorithm is used for balancing the energy in a whole network as well as maximizing the network lifetime".

```
Input: Sensor nodes, distance from each sensor node to base station,
base station address and distance to neighbor nodes.
Output: Maximizing network lifetime through best routing.

1./* Calculate optimal distance value, where $\alpha \in [2,4]$ $\varepsilon_{amp} = \varepsilon_{fs}$
when $\alpha = 2$ and $\varepsilon_{amp} = \varepsilon_{mp}$ when $\alpha = 4$. */
        $d_i = d_{opt} = \sqrt[\alpha]{\frac{2.E_{elec}}{\varepsilon_{amp}(\alpha - 1)}}$
2. /* Neighbors selection */
        $S_i =: select(neighbors)$
3./* Calculate distance from source to neighbors */
        $d_j =: d(S,N)$
4./* Compare optimal distance di with dj */
        $d_{temp} =: near(d_i, d(S,N).energy \geq engTh$
5. End
```

Fig.2. Algorithm for Distance-based Energy aware routing

Iteratively other nodes also repeat the same process. In Fig. 3 shows the one dimensional linear network with N sensor nodes placed along a line from source to sink node.

$$E_{Tx}(l,d) = \begin{cases} l.E_{elec} + l.\varepsilon_{fs}.d^2, & if\ d < d_0 \\ l.E_{elec} + l.\varepsilon_{mp}.d^4, if\ d \geq d_0 \end{cases} \quad (1)$$

$$E_{Rx}(l) = l.E_{elec}, \quad (2)$$

$$E_{Fx}(l,d) = E_{Tx}(l,d) + E_{Rx}(l) \quad (3)$$

Where E_{Tx} amount of energy to transmit l - bits messages over a distance d, E_{Rx} amount of energy to receive the message and E_{Fx} amount of energy to forward the message. For other parameters E_{elec} is the Energy dissipation to run the radio device, ε_{fs} free space model of transmitter amplifier, ε_{mp} multi-path model of transmitter amplifier and d_0 the distance threshold.

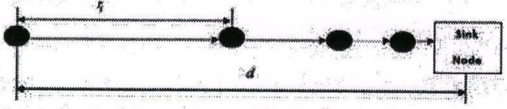

Fig.3. One-dimensional linear network

B. Data Privacy Protection Phase

Our proposed solution will ensure data privacy protection in WSNs by providing Anonymity, Authenticity and integrity on the sensed data as the services to grant full privacy. The work in [6] provides data privacy through asymmetric key for hiding sensor node identity (Anonymity) and symmetric key for securing the actual sensed data (Confidentiality). This symmetric key may be captured by one of the above attacks such as active adversary. Therefore, data integrity checking on the receiver side is needed through hashing operation by ensuring that the packet received was un-altered during its transmission from a source to destination by any intermediate sensor or malicious node.

```
Input: Sensor node identity, message, secret keys.
Output: Anonymity, Confidentiality, Authenticity and Integrity.
1. /* Anonymity provision */
        $E\ (ID_x \mid\mid R_n, K_{bs})$
2. /* Confidentiality provision */
        $E\ ((Data), K_{x,BS})$
3. /* Authenticity and Integrity provision */
        $E\ ((Data)\mid\mid H(Data), K_{x,BS})$
4. End
```

Fig.4. Algorithm for Data Privacy Protection

The following is the data privacy protection scheme proposed:

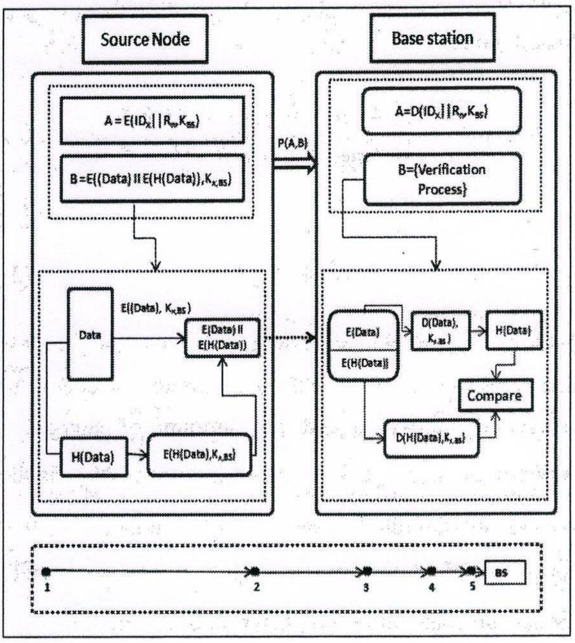

Fig.5. Energy-efficient Data Privacy Protection Scheme

A. Sender side

***E (ID**$_x$ **|| R**$_n$**, K**$_{bs}$**)**: Here we apply concatenation between the source sensor ID and random number R_n (with the same size as the sensor identity) in order to provide protection against brute-force search attacks and then we encrypt them with K_{bs} (Public Key of the base station (Receiver) to provide anonymity of the source node against some attacks from attack vector.

E ((Data), K**$_{x,BS}$**): Secondly, we encrypt the sensed data with $K_{x,BS}$ symmetric key shared between sender & base station (receiver), as secrecy of actual sensed data for providing confidentiality.

E (H (Data), K**$_{x,BS}$**): Next, we apply one way Hash function on the sensed data and to enhance data security we also encrypt the message digest by the symmetric key (shared secret key between the source node and the base station). To reach our goal of ensuring authenticity and integrity on the sensor readings from the source to destination; we concatenate the cipher-text obtained in the previous step with the later result that becomes ***E ((Data)||H(Data), K**$_{x,BS}$**)***

B. Receiver side

D (ID**$_x$ **|| R**$_n$**, K**$^*_{BS}$**): Decryption to get source node identity (*ID*) by using the private key of the base station;

Integrity and Authentication Verification: After separating the cipher text data ***E(Data)***and the cipher text message digest ***E(H(Data))*** both will be decrypted by using shared secret key between the source node and the base station. Next, we save the plain-text message digest and then one way hash function will be applied on the plain-text data obtained and finally we compare the result. Thus, the overall process results on checking data integrity to ensure that during the transmission from the source node to destination (base station) the packet has not been modified and authenticate that packet has been sent by legitimate user.

IV. Security and Performance Analysis

We analyze the security of our scheme with respect to two goals: the ability of the base station to detect an altered message and the ability of the source node to mask its identity (id) for data privacy issue.

A. Detection by the base station

EDPPS security scheme is built in a way that any fake message from a compromised node cannot successful received by the base station as real actual sensed data, instead would be detected and released by the failure of authentication check mechanism.

As any other scheme based on single shared key, EDPPS is more vulnerable against capture attack which is serious attack in sensor network, since the capture of only one sensor can compromise the shared key and then the whole network will be compromised. In our scheme to compute against this drawback we proposed checking data integrity mechanism through one way hash function. This will deal with almost all passive attacks such as DoS or side channel attacks. One way hash method will be a solution for detecting the threats and results in providing authenticity as well as integrity of those sensed data.

B. Adversary model

Assume that an adversary j has known the secret key (Shared) between source node and base station. j will have access to the concatenated data between message digest and actual sensed data. As only base station has the knowledge of the size for cipher text (E[h(data),$K_{x,BS}$]), therefore j will not be able to separate the concatenated payload. If so then the data will be stolen or only modified according to what kind of attacker, but as one way hash function has following properties:

a) H(x) = h ; where h equals to the result of one way hash function of the message x. So given h is infeasible to find x (One way property).

b) $H(x_1) = H(x_2)$ given x_1 is infeasible to find x_2 (weak collision resistance)

c) $H(x_1) = H(x_2)$, It is infeasible to find any x_1 and x_2 (strong collision resistance).

Therefore, the infeasible computational properties of one way hash function will help our scheme to identify any change that has been occurred on the actual sensed data during the transmission from the source node to the base station. Thus integrity and authenticity will be achieved.

V. Simulation Results

To understand the performance of our proposed scheme we simulated the network with two goals to achieve; Energy-efficient in the whole network for maximizing the network lifetime and the actual sensed data privacy protection along the path from the source to base station. Our energy efficient routing is a distance based scenario for balancing the consumed energy to all the nodes.

A. Energy Consumption Model

Under the event based traffic pattern, each sensor node is randomly chosen to send its sensed event to the sink node as in Fig. 1 through direct or multi-hop routing. So, the data length is same for all intermediate sensor nodes along multi-hop route.

The optimal individual distance d_i to get minimal energy consumption for intermediate nodes is:

$$d_i = d_{opt} = \sqrt[\alpha]{\frac{2.E_{elec}}{\epsilon_{amp}(\alpha-1)}} \qquad (4)$$

Where $\alpha \in [2,4]$ and $\varepsilon_{amp} = \varepsilon_{fs}$ when $\alpha = 2$, $\varepsilon_{amp} = \varepsilon_{mp}$ when $\alpha = 4$. (For more in details refer to our previous work [9]).

Our objective is not to minimize the sum of energy consumption for all nodes but to get the optimal distribution $\{r_1, r_2, \cdots, r_N\}$ when $E_1 = E_2 = \cdots = E_N$. In Fig. 6, we have 3 multi-hop routes with hop number $N = 3,4,5$. Since node j has more traffic load to forward than node i $(j > i)$, therefore node j has smaller individual distance than i $(r_j < r_i)$. We can also get the average energy value for 3 multi-hop routes as {0.0031, 0.0014, 0.0010} which validate the next hop node selection criterion of our DEAR algorithm.

B. Network lifetime

We analyzed the network lifetime with LEACH and our proposed Distance-based Energy Aware Routing (DEAR) algorithm under different node number. Our DEAR can prolong network lifetime about 80 to 100 percent than LEACH algorithm.

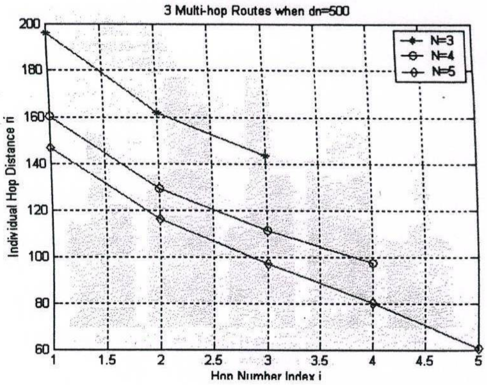

Fig.6. Optimal individual distance r_i

TABLE II. Time / Round Traffic Based

Technique	N = 100	N = 200	N = 300
LEACH	476	451	469
DEAR	854	917	953

C. Data Privacy Protection

We analyzed two existing secure energy schemes SERP and ESPDA with our EDPPS in Fig. 7, after deploying the attack vector V_i in the system. To defend V_i we considered

$$Z = \sum_{i=1}^{n} W_i * V_i \qquad (5)$$

Where Z is the defend factor and W_i is the weight ranging from 0 to 1. In our analysis the threshold value has been considered to set the range of success or fail, where the number above threshold value is considered as success and below as fail to defend against an attack vector.

Finally, the percentage of defense is delivered by:

$$S = \frac{Z}{T} \qquad (6)$$

Where S is the successful defend and T stands by the possible total attacks. We analyze the security of our scheme with respect to two goals: the ability of the base station to detect an altered message and the ability of the source node to mask its identity (id) for data privacy issue. In this case we focus on defend against insertion of malicious code as the most dangerous attack which can take an advantage of detecting the sensor node identity. This code injected in the network could spread to all nodes which results on destroying the whole network and degrading the network lifetime.

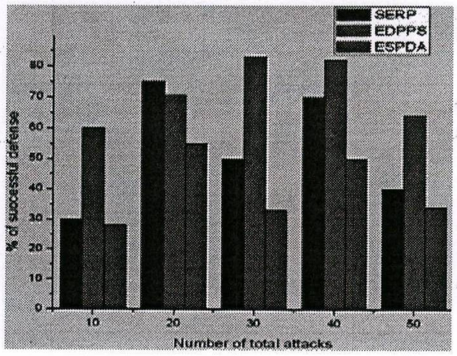

Fig.7. Defend against attack vectors

For evaluating the data privacy protection, we compare our scheme with two other low energy security schemes SERP [14] and ESPDA [15].

VI. Conclusion and Future Work

The target of our work is to provide the energy balancing on all the nodes from the source node to base station along the transmission path through a distance based energy aware routing and ensuring full protection of data privacy in wireless sensor networks through anonymity of the source node, confidentiality, authentication and integrity on the actual sensed data. This scheme will not reduce the computational complexity from the previous work but will ensure data privacy protection whenever symmetric key used to encrypt data is detected by an adversary.

In our future work, we will explore the implications of using single cipher algorithm to implement the full privacy and how the algorithm can be used to achieve better performance.

II. Acknowledgment

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National Industry Promotion Agency) (NIPA-2010-(C1090-1021-0003)).

References

[1] M. Li, and Y. Liu, "Rendered Path: Range-Free Localization in Anisotropic Sensor Networks with Holes," in Proceedings of ACM MobiCom, 2007.

[2] M. Hwang, and C. Liu, "Authenticated Encryption Schemes: Current Status and Key Issues," Journal of network security, Vol.1, No.2, PP.61-73, Sep. 2005.

[3] Yi Ouyang, Zhengyi Le, James Ford, and Fillia Makedon "PrivaSense: Providing Privacy Protection for Sensor Networks," In SenSys, Sydney, Australia, '07, November 6–9, 2007.

[4] A. T. Campbell, S. B. Eisenman, N. D. Lane, E.Miluzzo, and R. A. Peterson, "People centric urban sensing," In Proc of WICON '06, page 18, 2006.

[5] C. Xu and Y. Ge, "The Public Key Encryption to Improve the Security on Wireless Sensor Networks," In Second International Conference on Information and Computing Science, 2009.

[6] Shaikh, R.A.; Lee, S.; Brian J. d` A.; Song, Y.J.; Hassan, J. "Achieving Network Level Privacy in Wireless Sensor Networks," In Sensors 2010 ISSN 1424-8220.

[7] Trakadas, T., Zaharanadis, T., Leligou H., Voliotis, S., Papadopoulos, K., "Analyzing Energy and Time Overhead of Security Mechanisms in Wireless Sensor Networks," 2008.

[8] Javier L., Rodrigo R., Cristina A., "Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks," LNCS 5705, pp. 289–[illegible], 2009.

[9] Jin Wang, Imanishimwe Jean de Dieu, Asturias De Leon Diego Jose, Sungyoung Lee and Young-Koo Lee, "Prolonging the lifetime of Wireless Sensor Networks via Hotspot Analysis," IEICE Transactions on Communications, No. 2, pp. 305-316, 2010.

[10] M. Haenggi, "Twelve reasons not to route over many short hops," in Proc. IEEE Vehicular Technology Conference (VTC'04), Los Angeles, CA, Sep. 2004

[11] M. Sikora et al, "On the Optimum Number of Hops in Linear Wireless Networks," in *IEEE Information Theory Workshop (ITW'04)*, (San Antonio, TX), Oct. 2004

[12] W. Heinzelman, A.Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks," Proc. of the International Conference System Sciences, pp.1-10, Hawaii, Jan. 2000.

[13] M. Khan, G. Pandurangan, and B.Bhargava, Energy-Efficient Routing Schemes for Wireless Sensor Networks, Technical Report CSD TR 03-013, Dept. of Computer Science, Purdue University, 2003, p. 1-12

[14] A. S. K. Pathan and C. S. Hong, "SERP: secure energy-efficient routing protocol for densely deployed wireless sensor networks," Institut TELECOM and Springer-Verlag France (2008)

[15] Çam H, Özdemir S, Nair P, Muthuavinashiappan D, Sanli HO, "Energy-efficient secure pattern based data aggregation for wireless sensor networks" Computer Communication,pp. 446–455, 2006.