Security Enhancement of N-Tier Grid Protocol Using Elliptical Curve Cryptography for WSN

Jai Prakash Prasad
Faculty, Dept. of ECE
Don Bosco Institute of Technology
Bangalore, India

Dr. Suresh Chandra Mohan
Professor, Dept. of ECE
Bapuji Institute of Technology
Davangere, India

Abstract— **A Wireless Sensor Network (WSN) is composed of large number of sensor nodes which are deployed in the field where every node consists of sensors to sense the parameters like temperature, humidity, or pressure depending on the application involved. Future WSNs are envisioned to revolutionize maintenance free and fault tolerant platform for collecting and processing information in diverse environments across various applications. A major issue in WSN is the energy constraint in a node and its limited computing resources, which may pose an operational hazard on the network lifetime. Therefore, innovative routing algorithms and cryptography techniques are required to utilize the resources of WSN to improve the life time of routing path and secure of information between the sensor nodes in WSN during any kind of attacks to the WSN. Recent advances in WSN have led to many new security protocols to achieve data integrity specifically designed for sensor networks where low energy consumption is an essential consideration. This paper investigates an experimental secure dynamic N-Tier ECC-GRID based protocol to achieve energy efficient data integrity using elliptical curve cryptography (ECC) for WSN applications.**

Keywords- *Secure Routing, Sensor Networks, Network Lifetime, Grid, Energy Efficient, ECC.*

I. INTRODUCTION

A wireless sensor network (WSN) consists of a no. of tiny sensor nodes also called motes spread across an area. Each mote has intelligence of transmitting data wirelessly through a network to the base station. WSN are prone to failure due to its limited resource constrained capabilities and topological change. WSNs have a wide range of application in Medical, Environment Monitoring, Industrial, Urban monitoring and Military, which changes our life in many ways.

The elliptical curve cryptography Implementation in wireless sensor network provides a significant reduction in key size. For example ECC key of 163 bits is equivalent to RSA key of 1024 bits and ECC key of 256 bits is equivalent to RSA key of 3072 bits. It also offers advantages as:

- the high level of security with smaller key sizes
- less storage and bandwidth savings.
- Encryption, Decryption and Signature Verification speed up.
- High-speed S/W and H/W implementations.
- Find application in Smart cards, Wireless devices & Web Servers.

A regular GRID based routing protocol with n nodes located in geographical area as shown in figure 1. In this model all nodes selects a uniform range for sensed data transmission. The proposed N-Tier ECC-GRID based routing protocol assumes a network with location of n nodes at coordinates (m, n) with $1 \leq m, n \leq \sqrt{n}$ with all node range $r(n) = \sqrt{2}$ and each node has eight neighbors except on boundary of the network.

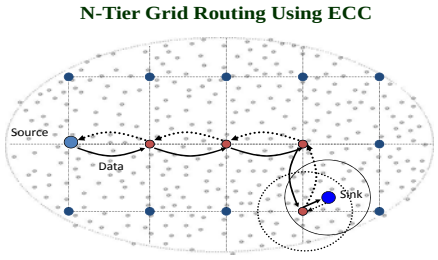

Figure 1. A grid based WSN

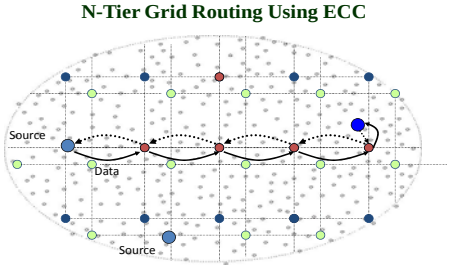

Figure 2. A dynamic grid based WSN

The battery powered sensor networks performance measurement analysis is necessary to evaluate network lifetime to provide Quality of service to end users. The sensor network lifetime is the time span from the deployment to the instant how long the network can perform the task. Improving network life time is crucial consideration and the proposed design of N-Tier GRID method achieves better performance for life time maximization.

II. NETWORK SECURITY REQUIREMENT IN WSN

Security in WSN required which provides confidentiality, Authentication, Integrity, Availability. Cryptography is one way to provide security. It can be provided through by symmetric key techniques, asymmetric key techniques. Since WSN are very constrained in terms of computing, communication and battery power, it requires a light weight cryptographic algorithm. Due to constraints of sensor nodes, the selection of cryptographic technique is vital in WSN.

- **Confidentiality -** Confidentiality ensures the concealment of the message from an attacker.
- **Authentication-** Authentication ensures the reliability of the message by identifying its origin.
- **Integrity -** Integrity ensures the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network.
- **Availability-** Availability ensures the services of resources offered by the network, or by a single sensor node must be available whenever required.

III. PERFORMANCE METRIC TERMS IN WSN

Packet Sent: Total no. of packets sent by source node and is obtained from NS2 trace file.
Packet Received: Total no. of packets received by destination node and is obtained from NS2 trace file.
Packet Delivery Ratio: It is defined as the ratio of packets received to packet sent.
Throughput: It is defined as average transform rate or bandwidth of route.
Average end to end delay: It is the delay (or Time) spent to deliver each data packet.

IV. ELLIPTICAL CURVE CRYPTOGRAPHY

Even though many cryptography techniques are available, to provide a better security asymmetric Elliptical Curve Cryptography (ECC) is extensively used. The benefit of this technique is that they uses smaller size key which need less storage, less bandwidth and less energy, thereby reducing processing and communication overhead, which is ideal for energy-constrained sensor nodes.

The main advantage which ECC offers over other public key algorithms is shorter key size for the same level of security. The Table 1.3 clearly shows that ECC algorithm of 571 key sizes offers the same security level which is offered by 15,360 key sizes of DH/RSA /DSA algorithms. The key size of ECC is only 3.7 % of DH/DSA /RSA key length. This short key length of ECC will help to save bandwidth of the sensor networks by reducing communication overheads. Also compared to the symmetric key algorithm, the key size is slightly bigger (44% more) but ECC will offer more security as compared to symmetric cryptography and will give more autonomy to nodes. The elliptic curve are defined over the equation as:

$y^2 = x^3 + a \cdot x + b,$ Where, $4a^3 + 27b^2 \neq 0$

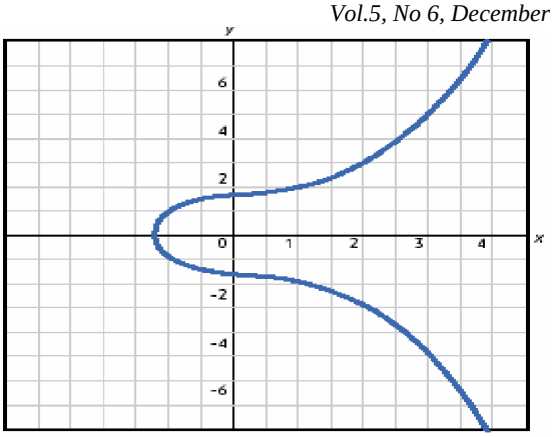

Figure 3. An example of elliptic curve

Choi et al. [1] investigated the feasibility of various cryptographic algorithms, AES, Blowfish, DES, IDEA, MD5, RC4, RC5, SEED, SHA-1 and SHA-256, for their use in WSN utilising MICAz type motes running TinyOS. The usage of resources including memory, computation time and power for each cryptographic algorithm were experimentally analysed. As a result, RC4 and MD5 turned out as the most suitable algorithms for MICAz-type motes.

Gura et al. [2] Implemented ECC on an 8 bit microcontroller by using elliptic curves GF(p) over prime integer field. They selected Elliptic Curves GF(p) over prime integer fields since binary polynomial field arithmetic specifically multiplication is insufficiently supported by current microprocessors and would thus lead to lower performance. The point multiplication of an integer and point on an elliptic curve decomposed into sequence of point additions and point doublings.

Wander et al. [3] quantified the energy cost of authentication and key exchange based on public-key cryptography; RSA and ECC on an 8-bit microcontroller platform; Atmel ATmega128 processor. A comparison has been presented on two public-key algorithms, RSA and Elliptic Curve Cryptography (ECC), and considers mutual authentication and key exchange between two un-trusted parties such as two nodes in a wireless sensor network. The ECC-based signature is generated and verified with the Elliptic Curve Digital Signature Algorithm (ECDSA). The results have shown that ECDSA signatures are significantly cheaper than RSA signatures. The experiments were conducted on the Berkeley/Crossbow motes platform, specifically on the Mica2dots. The implementation of RSA and ECC cryptography on Mica2 nodes further proved that a public key-based protocol is viable for WSNs.

Batina et al. [4] proposed a low cost public key cryptography scheme for sensor networks providing service such as key distribution and authentication. They proposed a custom hardware assisted approach to implement Elliptic Curve Cryptography (ECC) in order to obtain stronger cryptography as well as to minimize the power. The low-power ECC

processor contains a modular arithmetic logical unit (MALU) for ECC field arithmetic.

Szczechowiak et al. [5] presented results on implementing ECC, as well as the related emerging field of Pairing-Based Cryptography (PBC), on two of the most popular sensor nodes MICA2 and Tmote Sky. They showed that ECC over prime field is not always the best option as pairings over GF (2^m) seem to be more efficient on this type of architecture. They argued that fast pairing computation enables Identity Based Encryption and thus opens new ways for achieving security in sensor networks which was also argued by Oliveira et al., 2007.

Yeh et al. [6] proposed ECC-based user authentication protocol that resolves some weaknesses. The proposed rotocol provide mutual authentication to protect inside security and outside security. Also, it not only inherits the merits of ECC-based mechanism but also enhances the WSN authentication with higher security than other protocols. Therefore, the proposed protocol is more suited to WSNs environments.

V. N-TIER ECC-GRID ROUTING PROTOCOL

The proposed N-Tier ECC based GRID routing protocol is implemented using NS2 simulator. A WSN network scenario of 6*6 is constructed to measure performance metrics of sensor networks. Let $[f_1(j), f_2(j), \ldots..,f_n(j)]$ be the vector of measurements taken by the n nodes at epoch j. The proposed method perform N sets of such measurements: $[f_1(1), f_2(1), \ldots..,f_n(1)]$, $[f_1(2), f_2(2), \ldots..,f_n(2)]$, ……. $[f_1(N), f_2(N), \ldots..,f_n(N)]$. Using N-Tier GRID Routing protocol, the computational throughput L with a rate of block size N & total time $T_P(N)$ is calculated as:

$$R_L(N) := \frac{N}{TP(N)}$$

Consider a 6*6 sensor nodes ECC-Grid based routing protocol network as shown in figure-4. In this model node-36 which is a movable node acts as a source node & node-37 which is fixed node acts as a destination node. This 6*6 sensor nodes dynamically forms another stages of 6*6 sensor nodes network at different coordinates of x & y topography and simulation time as shown in figure 2. Movable or source node 36 changes is location over the topographic dimension and transmit its data to fixed node as destination node via other sensor nodes in the network using shortest path algorithm. Each sensor nodes are embedded with ECC protocol to provide encryption and decryption to data.

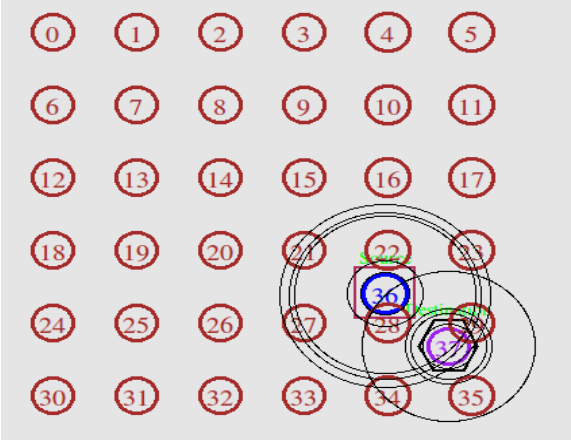

Figure 4. A 6*6 ECC-Grid Network Architecture

The method uses elliptic curve groups over the finite field F_p Elliptic curves are formed by choosing a & b within the field F_p.

Elliptic curve cryptography over the Field F_{23} is given with,
a = 9 and b = 17;
The elliptic curve equation is $y^2 = x^3 + 9x + 17$.
For example the point (3, 5) satisfies this equation since:
$5^2 \bmod 23 = 3^3 + 9*3 + 17 \bmod 23$
$25 \bmod 23 = 71 \bmod 23$
$2 = 2$
The points which satisfy this equation are:
(1, 2), (1, 21), (3, 5), (3, 18), (4, 5), (4, 18), (5, 7), (5 ,16), (7, 3), (7 ,20), (8, 7), (8, 16), (10, 7), (10, 16), (12, 6), (12, 17), (13, 10), (13, 13), (14, 9), (14, 14), (15, 10), (15, 13), (16, 5), (16, 18), (17, 23), (18, 10), (18, 13), (19, 3), (19, 20), (20, 3), (20, 20).

The point is plotted for $y^2 \bmod 23 = x^3 + 9x + 17 \bmod 23$ as follows:

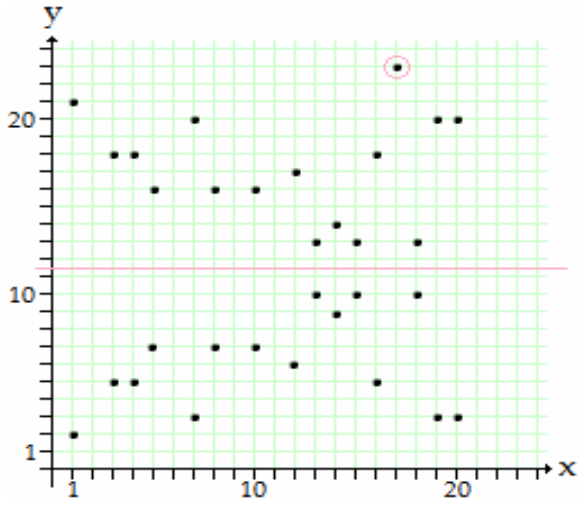

Figure 5. A plot for finite field F_{23}

VI. N-TIER GRID IMPLEMENTATIONS

The N-Tier ECC-GRID protocol performance metrics for packet delivery ratio, average throughput, end-end delay, control overheads as shown in figure below are analyzed and simulated using NS2. Performance evaluations are carried out by using various energy efficient metrics and properties to test various experimental scenarios of WSN by using simulation tool. Also, design, development and implementation of the proposed method which is novel energy efficient routing algorithm using ECC based cryptographic algorithms are performed to maximize network lifetime of WSN.

Table I: Simulation parameters for WSN

Simulation Parameters	Value
Channel type	Wireless Channel
Radio-propagation model	Propagation/Two Ray Ground
Network interface type	Phy /WirelessPhy
MAC type	Mac/802_11
Interface queue type	Queue/DropTail /PriQueue
Link layer type	LL
Antenna model	Antenna/Omni Antenna
Max packet in ifq	50
Number of mobile nodes	16/25/36/49
Routing protocol	AODV
X dimension of topography	800/ 1000/1500
Y dimension of topography	800/ 1000/1500
Time of simulation end	100
Initial energy in Joules	100
Network Type	Mobile
Connection Pattern	Random
Packet Size	512 bytes
Connection type	CBR/UDP/TCP
Pause time	0s, 20s, 80s, 110s, 140s

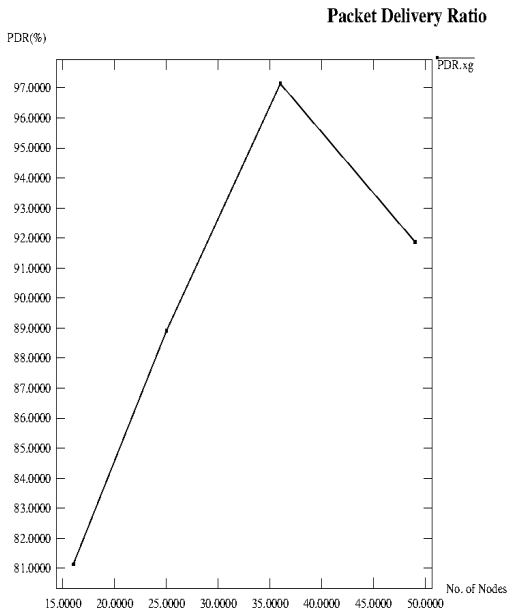

Figure 6. PDR v/s No. of nodes

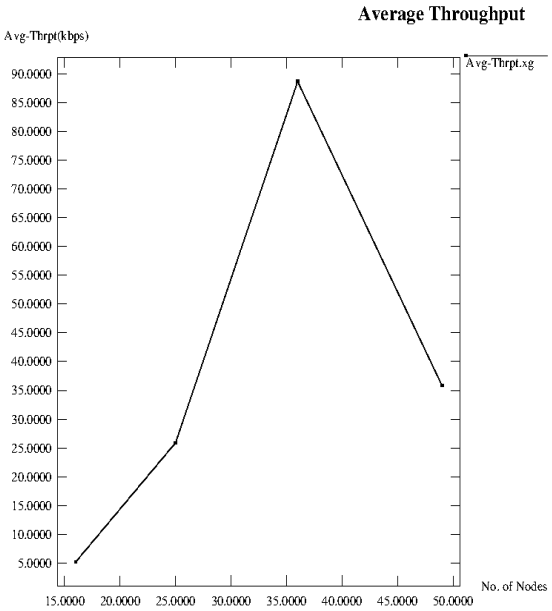

Figure 7. Avg. Throughput v/s No. of Nodes

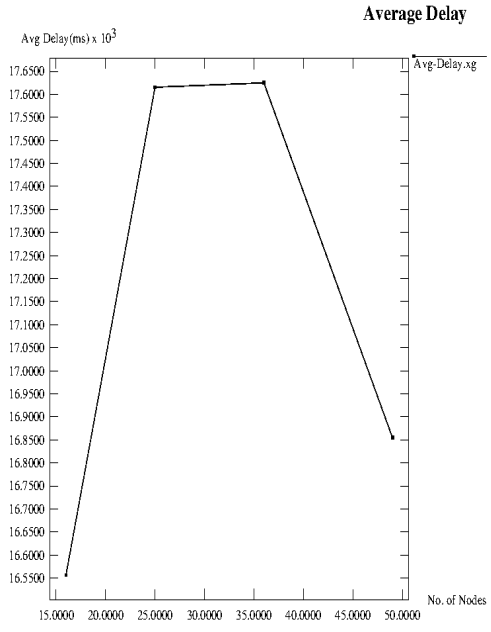

Figure 8. Average Delay v/s No. of Nodes

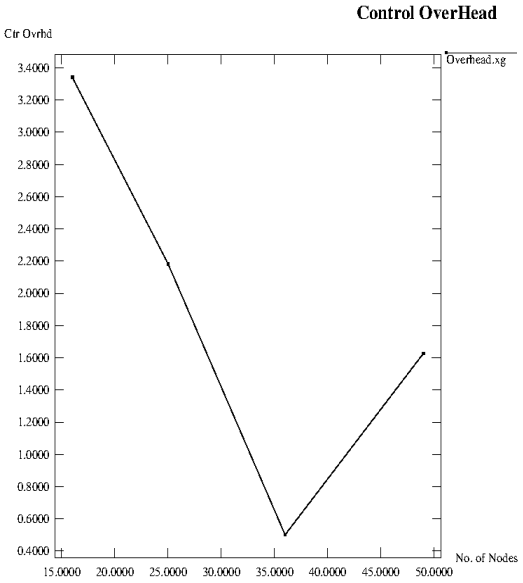

Figure 9. Control Overhead v/s No.of Nodes

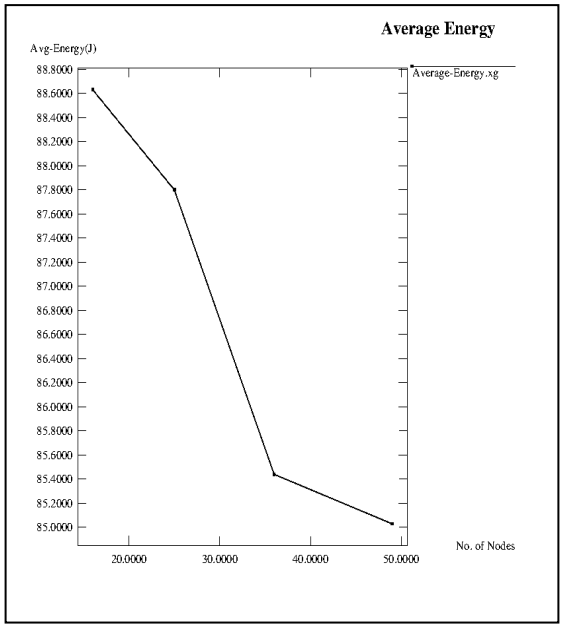

Figure 10. Average Energy v/s No. of Nodes

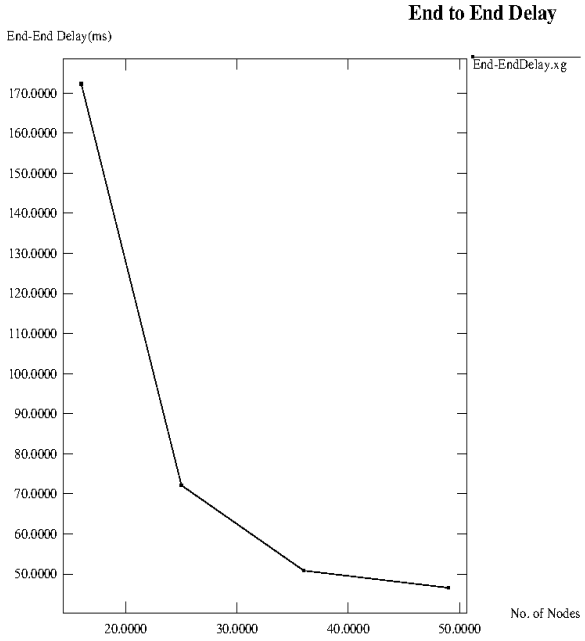

Figure 11. End-End Delay v/s No.of Nodes

CONCLUSION

The optimization of proposed routing protocol are obtained by developing novel data forwarding and secured routing scheme by considering a N-Tier ECC-GRID protocol in which each group of local sensor nodes elect a cluster head which is responsible for collecting of sensed data, performing a stage of secured data aggregation and routing first stage of data to the next stage of secured data aggregator nodes on its way to the Base Stations using ECC-GRID secure routing protocol. Among varieties of routing schemes N-Tier GRID routing protocol offers better choices to researchers to achieve better energy efficiency. The best performance to provide security can be obtained by improving the existing system based on ECC for wireless sensor networks with the following approach of requirement of security level and selection of appropriate ECC parameters set, selection of cryptographic scheme and formats for network transfer of keys.

REFERENCES

[1] Choi, K., Song, J., "Investigation of feasible cryptographic algorithms for wireless sensor network", 8th ICACT-2006, 2, 2006.

[2] N. Gura, A. Patel, and A. Wander, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs,"in Proceedings of the 2004 Workshop on Cryptographic Hardware and Embedded Systems (CHES), August 2004.

[3] Wander, A., Gura, N., Eberle, H., Gupta, V., Shantz, S., "Energy analysis of public-key cryptography for wireless sensor networks," 3rd IEEE International Conference on Pervasive Computing and Communication, 2005.

[4] Batina, L., Mentens, N., Sakiyama, K., Preneel, B., Verbauwhede, I., "Low-cost elliptic curve cryptography for wireless sensor networks", Lecture Notes in Computer Science, 4357: 6 17, 2006.

[5] Szczechowiak, P., Oliviera, L., Scott, M., Collier, M., Dahab, R., "NanoECC: Testing the limits of Elliptic Curve Cryptography in Sensor Networks EWSN 2008', 4913: 305 320, LNCS, Springer-Verlag, 2008.

[6] Yeh, H., Chen, T., Liu, P., Kim, T., Wei, H., "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", Sensors, 4767-4779, 2011.

[7] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy efficient communication protocol for wireless micro sensor networks," in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS), pp. 10–20, January 2000.

[8] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in Proceedings of the IEEE Aerospace, vol. 3, pp. 1125–1130, 2002.

[9] Choi, K., Song, J., "Investigation of feasible cryptographic algorithms for wireless sensor network", 8th ICACT-2006, 2, 2006.

[10] Yeh, H., Chen, T., Liu, P., Kim, T., Wei, H., "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", Sensors, 4767-4779, 2011.

[11] Ananthram Swami et al., "Wireless Sensor Networks: Signal Processing and Communication Perspectives", John Wiley, 2007.

[12] T.P. Sharma, R.C. Joshi, Manoj Misra, "GBDD: Grid Based Data Dissemination in Wireless Sensor Networks," In Proc. 16th International Conference on Advanced Computing and Communications (ADCOM 2008), Chennai, India, 2008, pp. 234-240.

[13] H. Eberle, A. Wander, N. Gura, S. Chang-Shantz, and V. Gupta, "Architectural Extensions for Elliptic Curve Cryptography over GF(2^m) on 8-bit Microprocessors," in Proceedings of the16th International Conference on Application-Specific Systems, Architecture and Processors (ASAP'05): IEEE, 2005.

[14] Dragoş I. Săcăleanu, Dragoş M. Ofrim, Rodica Stoian, Vasile Lăzărescu, "Increasing lifetime in grid wireless sensor networks through routing algorithm and data aggregation techniques", International Journal Of Communications, Issue 4, Volume 5, 2011.

[15] Neng-Chung Wang, Yung-Kuei Chiang, Chih-Hung Hsieh, and Young-Long Chen, "Grid-Based Data Aggregation for Wireless Sensor Networks", Journal of Advances in Computer Networks, Vol. 1, No. 4, December 2013.

[16] Yung-Kuei Chiang, Neng-Chung Wang and Chih-Hung Hsieh, "A Cycle-Based Data Aggregation Scheme for Grid-Based Wireless Sensor Networks", Sensors 2014, 14, 8447-8464; doi:10.3390/s140508447.

[17] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy efficient communication protocol for wireless micro sensor networks, in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS), pp. 10–20, January 2000.

[18] T.P. Sharma, R.C. Joshi, Manoj Misra, "GBDD: Grid Based Data Disemination in Wireless Sensor Networks," In Proc. 16th International Conference on Advanced Computing and Communications (ADCOM 2008), Chennai, India, 2008, pp. 234-240.

[19] Dragoş I. Săcăleanu, Dragoş M. Ofrim, Rodica Stoian, Vasile Lăzărescu, "Increasing lifetime in grid wireless sensor networks through routing algorithm and data aggregation techniques", International Journal Of Communications, Issue 4, Volume 5, 2011.

[20] Neng-Chung Wang, Yung-Kuei Chiang, Chih-Hung Hsieh, and Young-Long Chen, "Grid-Based Data Aggregation for Wireless Sensor Networks", Journal of Advances in Computer Networks, Vol. 1, No. 4, December 2013.

[21] Yung-Kuei Chiang, Neng-Chung Wang and Chih-Hung Hsieh, "A Cycle-Based Data Aggregation Scheme for Grid-Based Wireless Sensor Networks", Sensors 2014, 14, 8447-8464; DOI:10.3390/s140508447.