International Journal of Sensors and Sensor Networks
2016; 4(1): 1-6
Published online February 13, 2016 (http://www.sciencepublishinggroup.com/j/ijssn)
doi: 10.11648/j.ijssn.20160401.11

Spherical Grid Protocol to Enhance Quality of Service to Resource Constrained Wireless Sensor Networks

Jai Prakash Prasad[1], Suresh Chandra Mohan[2]

[1]Visvesvaraya Technological University, Research Resource Centre, Belgaum, Karnataka, India
[2]Department of ECE, Bapuji Institute of Engineering & Technology, Davangere, Karnataka, India

Email address:
jaiaasu@gmail.com (J. P. Prasad)

To cite this article:
Jai Prakash Prasad, Suresh Chandra Mohan. Spherical Grid Protocol to Enhance Quality of Service to Resource Constrained Wireless Sensor Networks. *International Journal of Sensors and Sensor Networks.* Vol. 4, No. 1, 2016, pp. 1-6. doi: 10.11648/j.ijssn.20160401.11

Abstract: Wireless Sensor Network (WSN) is an emerging wireless communication networks to provide potential secure optimized data routing between source and destination. Presently the performance analysis of the Wireless Sensor Network routing technique and security protocols is the major research issues. A major issue in wireless sensor network (WSN) is the energy constraint in a node and its limited computing resources, which may pose an operational hazard or limitations on the network lifetime. Therefore, analyses of innovative secure routing techniques are required to utilize the resources of WSN to improve the life time of network in WSN. To design & develop any innovative wireless sensor network routing and security protocol, the network characteristics & its design issues are important consideration. The proposed spherical Grid Routing Protocol (SGRP) is designed and developed to enhance Quality of service to improve WSN performance using NS2 simulator compare to compared to modified LEACH techniques. The packet transmitted, packet received, average energy, throughput and packet delivery ratio are the main common performance measures that are used for performance analysis of proposed SGRP protocols.

Keywords: Wireless Sensor Network, Routing Protocols, NS2 Simulator, Packet Drop, Average Energy, Throughput, Packet Delivery Ratio

1. Introduction

In Wireless Sensor Network (WSN) each sensor node component is mainly consists of sensors, processor, memory and radio trans-receiver. Each sensor node is responsible to sense input attribute such as temperature, humidity, or pressure depending on the application involved and forward the sensed data to the destination using optimized energy efficient routing path. The figure 1 shows the general structure of WSN.

Presently there are plenty of algorithms for routing sensor sensed data in Wireless Sensor Network applications. Sensor nodes can be used for communication purposes with efficient use of their energy in various domains based on the requirement & utilization of resources more effectively to perform a specific task. Due to this WSN are extensively used in environmental monitoring, distributed control system, detection of radioactive sources, agricultural & farm practices, internet, military and surveillance. The characteristics of wireless sensor networks are summarized below:

- *Dense sensor node deployment:* Sensor nodes deployed for a specific application can be several orders of magnitudes.
- *Battery-powered sensor nodes:* Sensor nodes are deployed in an application where it is very difficult to replace or recharge the batteries.
- *Limited energy:* Sensor node batteries having limited energy.
- *Computation & Storage constraint:* Sensor nodes are having low computational & limited storage capabilities.
- *Self-configurable:* Any changes in network autonomously configure themselves into a communication network.
- *Unreliable sensor nodes:* Sensor node may fail due to its deployment in harsh or hostile environment.
- *Data redundancy:* Multiple sensor node deployed in a region have a certain level of redundancy w. r. to data.

The main design objectives of sensor networks are:-

- *Small node size:* Small node size reduces the power consumption and cost of sensor nodes.

- *Low node cost:* By designing low node cost result into the cost reduction of whole network.
- *Low power consumption:* Low power consumption of sensor node increases the lifetime of the sensor network.
- *Scalability:* Design requirement for sensor network must be scalable to grow in network size.
- *Reliability:* Proper error control and correction scheme will ensure reliable data delivery over noisy channel.
- *Self-configurability:* Sensor network must reconfigure themselves in case of topology changes and node failures.
- *Adaptability:* Network protocol designed should be adaptive to node density and topology changes.
- *Channel utilization:* Effective use of bandwidth improves channel utilization.
- *Fault tolerance:* Sensor nodes should have the abilities of self testing, self-calibrating, self-repairing, and self-recovering.
- *Security:* Security protocol which protect interception of sensor signal which causes loss of message confidentiality.
- *QoS support:* QoS is measured in terms of delivery latency and packet loss.

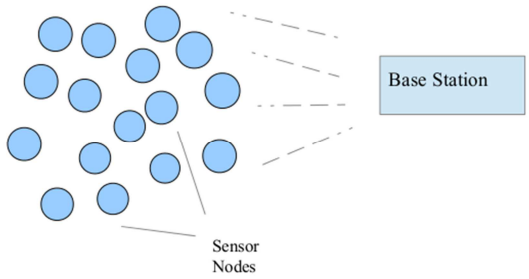

Fig. 1. *A general WSN architecture.*

The implementation of wireless sensor network in remote area and its maintenances is challenging task due to resource constrained nature of wireless sensor networks. To achieve data confidentiality and integrity in wireless sensor network there are presently available varieties of schemes in symmetric and asymmetric encryption scheme. To provide security to routed data while it is on the way from the unauthorized access by hacker there is need to design and develop optimized energy efficient secure routing protocol to improve quality of service as well as network life time compare to existing algorithm. A general public key asymmetric encryption scheme is shown in figure 2.

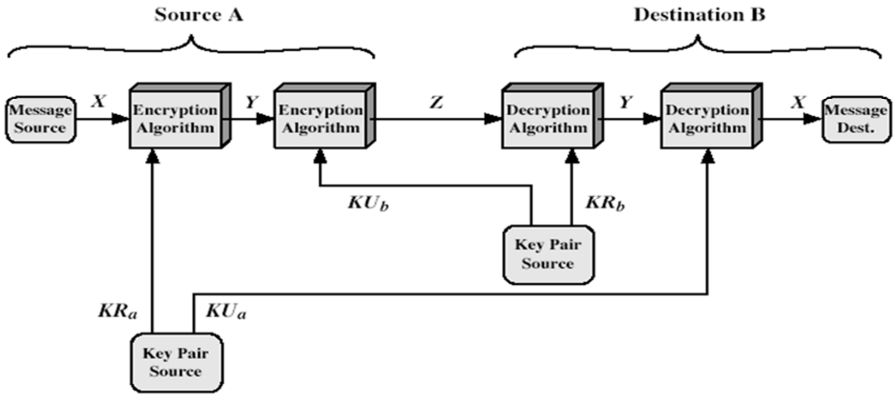

Fig. 2. *A Public Key Encryption Scheme.*

2. Traffic Patterns in WSN

There are varieties of wireless sensor network communication topological patterns as shown in figure 3. These Patterns are used to form a topology for the WSN.

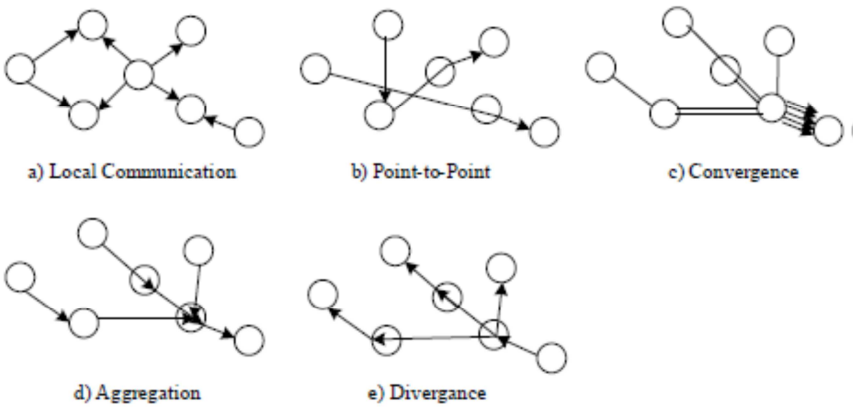

Fig. 3. *Types of Traffic Patterns in WSN.*

- *Local Communication:* Using this pattern anode information is shared among its neighbors and is used to transmit the data between the two nodes directly.
- *Point-to-Point Routing:* Here, a data packet is transmitted from a randomly chosen node to another node. It finds application in a wireless LAN environment.
- *Convergence:* Multiple nodes data packets are shared to a single base node. It finds application for data collection in WSNs.
- *Aggregation:* Processing of data packet happens in the intermediate nodes and the aggregated packet is routed to the base node.
- *Divergence:* It is used to send a request or data from a base node to another sensor node.

Table 1. *A Summary on Comparison of Grid Routing.*

Grid Routing	Present Work	Scope for future work
GBDD	• First sink appearing in the sensor field triggers grid construction with sufficiently large lifetime. • Sink constructs new grid only when no valid grid is present. • Significant overall energy savings Improvements. • Smaller average packet delay.	Packet delay is more.
GRASS	• It combines the ideas of fixed cluster-based routing together with application-specific data aggregation. • It uses optimal as well as heuristic algorithms that solve the joint problem of optimal routing with data aggregation.	Latency is more.
ARA	• It taking into account, the residual energy of the sensor nodes and creating an adaptive route path. • ARA provides a network lifetime growth of about 20% from other algorithms. • ARA can be implemented also in WSN with randomly deployed nodes.	Uses of lossless compression algorithms.
GBDAS	• It constructs a chain by linking all cell heads so that sensed data can be disseminated along the chain. • The energy consumption of sensor nodes is evenly distributed to maximize their lifetimes. • Lifetime of network is better.	Redundancy is more.
CBDAS	• Each node in a cell takes turn to be cell head and each cell head takes turn to be cycle leader • The energy depletion is evenly distributed.	Extra cell selection Overheads

3. WSN Routing Techniques: A Review

Secure Routing technique uses a strategy to ensure connectivity between the different nodes in the WSN. A number of studies as shown in table 1 that compares Grid based Routing scheme. The GRID routing comparison is made to analyze & understand its strength and weaknesses. The popular grid based routing protocols are GBDD, GRASS, ARA, GBDAS & CBDAS.

4. Elliptic Curve Cryptography [ECC]

Elliptic curves are used in public key cryptography for securing information from unauthorized access. Let assume d is a private key which is randomly selected from [1, n-1], where n is integer no. Assuming Q being public key is computed by dP, where P, Q elliptic curve points. Once the key pair (d, Q) is generated, a variety of cryptosystems such as signature, encryption/decryption, and key management system can be set up. Then dP is calculated which is known as scalar multiplication. The term dP is also for the calculations of signature, encryption, and key agreement in the ECC system.

Intuitive approach:

$$dP = P+P+\ldots+P$$

It requires d-1 times point addition over the elliptic curve. For an example, to compute $17P$, we could start with $2P$, double that, and that two more times, finally add P, i.e. $17P=2(2(2(2P)))+P$. This needs only 4 point doublings and one point addition instead of 16 point additions in the intuitive approach. This is called Double-and-Add algorithm.

Although there are many cryptography techniques are presently available, to provide a better security especially in WSN applications public key Elliptical Curve Cryptography (ECC) could be better choice for researchers. 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.

In the cryptographic schemes, elliptic curves over two finite fields are mostly used.

- Prime field F_p, where p is a prime.
- Binary field F_2^m, where m is a positive integer.

The equation of the elliptic curve over F_p is defined as:

$y^2 \bmod p = (x^3 + ax + b) \bmod p$

Where: $(4a^3 + 27b^2) \bmod p \neq 0$

$x, y, a, b \in [0, p-1]$

- Point addition for EC over F_p

$x_R = (\lambda^2 - x_P - x_Q) \bmod p$

$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$

Where: $\lambda = ((y_Q - y_P)/(x_Q - x_P)) \bmod p$

- Point doubling for EC over F_P

$x_R = (\lambda^2 - 2x_P) \bmod p$

$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$

Where: $\lambda = ((3x^2_P + a)/(2y_P)) \bmod p$

A elliptic curve E over the finite field F_2^m is given through the following equation,

$y^2 + xy = x^3 + ax^2 + b$

Where $x, y, a, b \in F_2^m$

- Point Addition and Doubling over F_2^m

Let $P=(x_P, y_P)$, $Q=(x_Q, y_Q)$ on the curve $y^2 + xy = x^3 + ax^2 + b$

The $R=P+Q$ can be computed:

$x_R = \lambda^2 + \lambda + x_P + x_Q + a$
$y_R = \lambda(x_P + x_R) + x_R + y_P$
Where: $\lambda = ((y_Q + y_P)/(x_Q + x_P))$
Then $R=2P$ can be computed:
$x_R = \lambda^2 + \lambda + a$
$y_R = x^2_P \lambda x_R + x_R$
Where: $\lambda = ((x_P + y_P)/(x_P))$

The implementation of ECC using Deffie-Hellmen algorithm as shown in figure 4 is explained below.

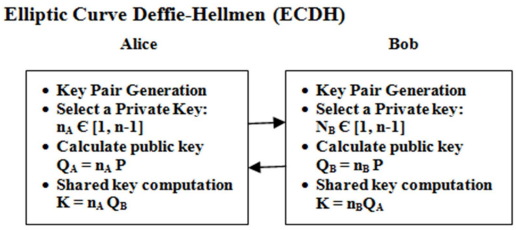

Fig. 4. *ECDH Algorithm.*

Consistency: $K=n_AQ_B=n_An_BP=n_BQ_A$

An Example of ECDH:

- Alice and Bob make a key agreement over the following prime, curve, and point.

  p=3851, E: $y^2=X^3+324x+1287$, P = (920, 303) ϵ E (F3851)
- Alice chooses the private key $n_A \epsilon 1194$,
- Computes $Q_A=1194P$= (2067, 2178) ϵ E (F3851), and sends it to Bob.
- Bob chooses the private key n_B=1759
- Computes $Q_A=1759P$= (3684, 3125) ϵ E (F3851), and sends it to Alice.
- Alice computes $n_AQ_B=1194(3684, 3125)$ = (3347, 1242) ϵ E (F3851)
- Bob computes $n_BQ_A=1759(2067, 2178)$ = (3347, 1242) ϵE (F3851)

5. Spherical GRID Routing Protocol (SGRP): A Proposed Method

The Spherical GRID routing protocol architecture is shown in figure 5. Here sensor nodes are uniformly distributed over a field to monitor its environment. All sensor nodes transmit its data to its neighbor nodes using chain route in spherical fashion.

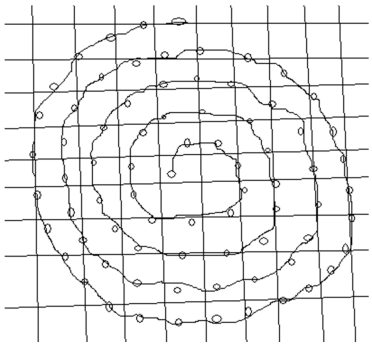

Fig. 5. *A General SGRP Networks.*

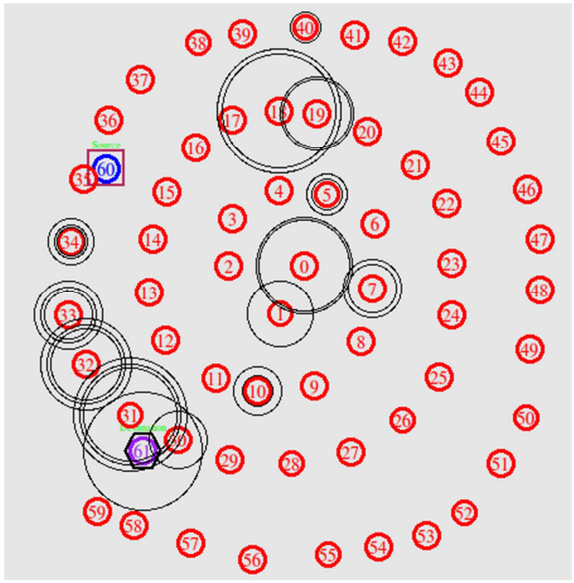

Fig. 6. *60 Nodes SGRP Network Scenario-I.*

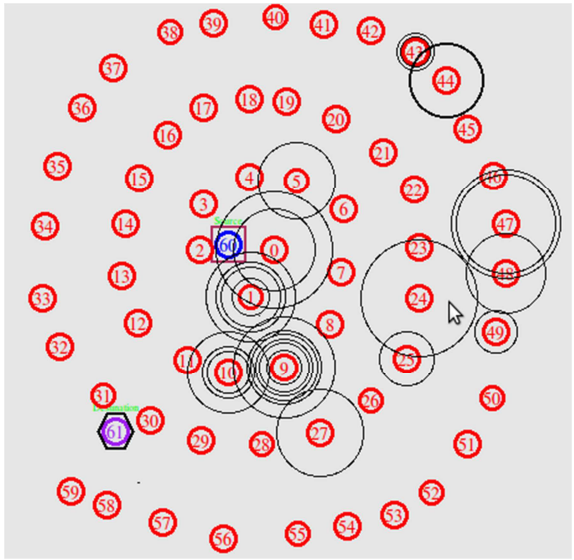

Fig. 7. *60 Nodes SGRP Network Scenario-II.*

A 60 nodes SGRP WSN network is simulated using NS-2 simulator. In network scenario-I & II as shown in figure 6 & 7 respectively, 60 nodes are arranged and distributed in spherical fashion. The source node no. 60 is indicated here as target nodes and its movement are traces by its nearest sensor nodes. The nearest node to source node 60 informs about it to the destination node no. 61 using spherical path. The performance efficiency of network is evaluated using performance metric such as transmitted packet, received packet, packet delivery ratio, average throughput and average residual energy. The simulation parameter setup of NS-2 is shown in table 2. The modified leach routing protocol & its topological setup is shown in figure 8. In modified LEACH Protocol whole network is divided into no. of clustered networks & exchange of packet takes place among clusters. Also the performance evaluation of SGRP algorithm versus modified LEACH protocol is shown in figure 9.

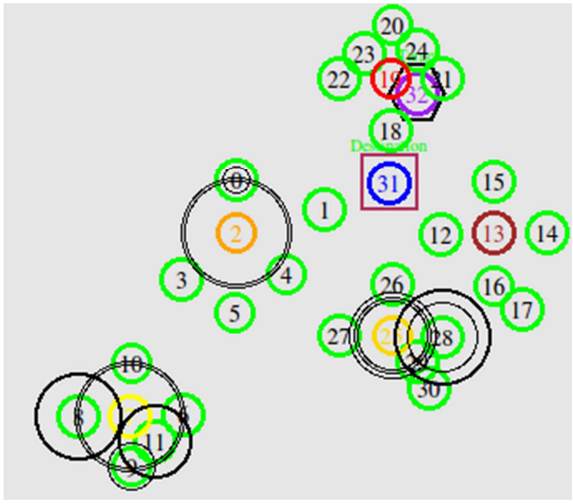

Fig. 8. Modified Leach Protocol.

Table 2. 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	2000
Y dimension of topography	1000
Time of simulation end	80
Initial energy in Joules	80
Network Type	Mobile
Connection Pattern	Random
Packet Size	512 bytes
Connection type	CBR/UDP/TCP

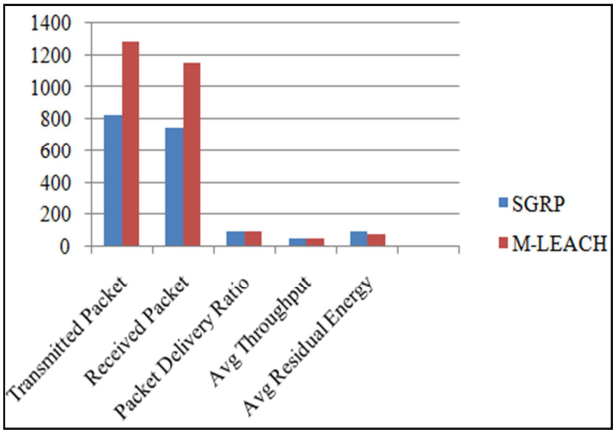

Fig. 9. SGRP v/s Modified LEACH.

6. Conclusion

The proposed Spherical Grid Routing protocol (SGRP) performance metrics are evaluated as i.e. transmitted packet, received packet, packet delivery ratio, average throughput and average residual energy and compared with the performance metrics calculations of modified LEACH Protocol. The conclusion from the analysis of results is that SGRP protocol achieves better performance compare to popular WSN modified LEACH protocol. Using these performances analysis the researchers gets better ideas to design and develop improved routing protocol by overcoming the limitations such as complete network failure due to a node energy exhaust of SPRG that can offer better PDR, Throughput, low packet drops & low power consumption in highly random mobility network. The outcomes from the result of performance metrics can adds extra life time in a node for providing better QoS in secure routing applications in real time practical applications using proposed method.

References

[1] 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.

[2] Kemal Akkaya and Mohamed Younis, A Survey on Routing Protocols for Wireless Sensor Networks, Ad hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.

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

[4] 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.

[5] Jamal N. Al-Karaki Raza Ul-Mustafa Ahmed E. Kamal, "Data Aggregation and Routing in Wireless Sensor Networks: Optimal And Heuristic Algorithms", Computer Networks, Volume 53, Issue 7, Pages 945–960, 13 May 2009.

[6] 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.

[7] 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.

[8] 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.

[9] I. F. Akyildiz et al., A Survey on Sensor Setworks, IEEE Communication Mag., vol. 40, no. 8, Aug. 2002, pp. 102–114.

[10] 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.

[11] 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.

[12] Jamal N. Al-Karaki Raza Ul-Mustafa Ahmed E. Kamal, "Data Aggregation and Routing in Wireless Sensor Networks: Optimal And Heuristic Algorithms", Computer Networks, Volume 53, Issue 7, Pages 945–960, 13 May 2009.

[13] 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.

[14] 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.

[15] The network simulator - ns-2, http://www.isi.edu/nsnam/ns/

[16] Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma, "Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless Sensor Networks", IEEE 24th International Conference on Advanced Information Networking and Application Workshops, 2010, pp. 589-592, IEEE, 2010, DOI 10.1109/WAINA.2010.47.

[17] N. Koblitz, "Elliptical curve cryptosystems", Mathematics of Computation, Vol. 48. pp. 203-209, 1987.

[18] Y. Shou, H. Guyennet, and M. Lehsaini, "Parallel Scalar Multiplication on Elliptic Curves in Wireless Sensor Networks", 14th Int. Conf. on Distributed Computing and Networking (ICDCN), LNCS 7730, pp. 300-314, Bombay, India, Jan 2013.

[19] Wenbo Shi and Peng Gong, "A New User Authentication Protocol for Wireless Sensor Networks using Elliptical Curves Cryptography" in proceedings of Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Vol. 730831, 1-7, 2013.