Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 3 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Energy Efficient Elliptical Curve based Spherical Grid Routing Protocol for Wireless Sensor Networks

By Jai Prakash Prasad & Dr. Suresh Chandra Mohan
Visvesvaraya Technological University, India

Abstract- The Wireless Sensor Network (WSN) is a collection of no. of mobile nodes which communicate through wireless channel without any existing network infrastructure. Because the resource constrained nature of WSN a data packet routing requires multiple hops to exchange data across the network. In order to facilitate communication within the network, a secure energy efficient routing protocol is used to discover routes between nodes. The proposed energy efficient elliptical curve based spherical grid routing protocol for WSN provides correct and efficient route establishment between a pair of nodes so that data packets can be delivered in time to the destination. Secure route construction can be done with optimized WSN performance matrices such as packet delivery ratio, throughput, minimum energy consumptions, communication overheads & end to end delay. This proposed algorithm evaluates Spherical grid routing protocols for wireless sensor networks protocol while varying no. of nodes and pause time and results are compared with few existing routing protocols using network simulator.

Keywords: wireless sensor network, spherical GRID routing, energy efficient, packet delivery ratio, throughput. multi-tier spherical GRID, elliptical curve cryptography, scalability, routing.

GJCST-E Classification : C.2.2, I.2.9, C.2.1

Strictly as per the compliance and regulations of:

Energy Efficient Elliptical Curve based Spherical Grid Routing Protocol for Wireless Sensor Networks

Jai Prakash Prasad [α] & Dr. Suresh Chandra Mohan [σ]

Abstract- The Wireless Sensor Network (WSN) is a collection of no. of mobile nodes which communicate through wireless channel without any existing network infrastructure. Because the resource constrained nature of WSN a data packet routing requires multiple hops to exchange data across the network. In order to facilitate communication within the network, a secure energy efficient routing protocol is used to discover routes between nodes. The proposed energy efficient elliptical curve based spherical grid routing protocol for WSN provides correct and efficient route establishment between a pair of nodes so that data packets can be delivered in time to the destination. Secure route construction can be done with optimized WSN performance matrices such as packet delivery ratio, throughput, minimum energy consumptions, communication overheads & end to end delay. This proposed algorithm evaluates Spherical grid routing protocols for wireless sensor networks protocol while varying no. of nodes and pause time and results are compared with few existing routing protocols using network simulator.

Keywords: wireless sensor network, spherical GRID routing, energy efficient, packet delivery ratio, throughput. multi-tier spherical GRID, elliptical curve cryptography, scalability, routing.

I. Introduction

Wireless Sensor Network consists of no. of sensor nodes where nodes are deployed in a region to monitor its environment. Each sensor nodes consists of Microcontroller, internal & external memory, antennas, sensor and batteries as its main components to perform a specific task. Each sensor node senses its input attributes process the raw data & converts it into digital data format and then forward the data through chain of network using optimized routing scheme till the data reaches to its correct destination.

When the data is travelling through optimized routing path then there are chances of data packet to compromise from its authenticity, confidentiality, and integrity before it reaches to the destination. Therefore to overcome such threats which may exist in WSN depending on its application, there is requirement of strong cryptographic technique to counter. Wireless sensor nodes resources have its own constrained in terms of limited computational speed & battery backup. There exist plenty of energy efficient secure & routing algorithms such as LEACH, PEGASIS, TEEN, APTEEN, GBDD, TTDD, DES, AES, RSA, DSA, Elgamal encryption etc has achieved appreciable popularity for improved performance efficiency. However all the existing protocol has its own limitations and their drawbacks which has been studied & analyzed in detail for further research improvement & development in the field of wireless sensor networks.

Wireless Data Communication poses some kind of threats due to its open environment communication. To avoid compromise of data security it is required to maintain the authenticity, confidentiality and integrity of data. The elliptical curve cryptosystem provide speedy security mechanism compare to other type of public key cryptosystem and used in constrained environment conditions. Elliptical Curve Cryptography provides advantage of smaller key size that result in to faster computations, lower power consumption with savings of memory and bandwidth that makes ECC a fast, flexible, low cost security algorithm suitable for constrained environment.

Wireless Sensor Network can be deployed for Tele communication connectivity between various regions of all over the world. The modeling and placement of Wireless sensor nodes across various parts of world region for the coverage of whole world forms a cluster of networks which appears into spherical shape as shown in figure-1.

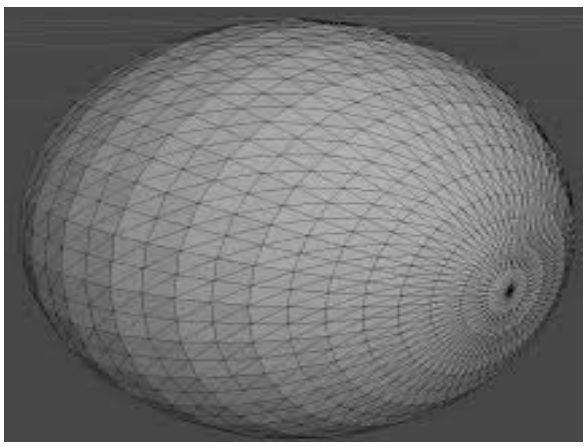

Fig.1 : Globe coverage structure using WSN's

Author α: Research Scholar, Visvesvaraya Technological University, Research Resource Centre, Belgaum, Karnataka, India.
e-mail: jaiaasu@gmail.com
Author σ: Professor, Dept. of ECE, BIET, Davangere, Karnataka, India.

The WSN find applications in,

- To monitor

Environment, parking & garden area, animals & birds, forest area, border area, Patient Health, Weather & Temp

- To Track

Nuclear mission, army movements, Production, Business, enemy

II. WSN Security & Routing: A Review

In cryptography the plaintext message content before it is sent out over the infrastructure network is encrypted, which becomes the cipher-text. At the destination side in order to read the plaintext, the cipher-text has to be decrypted. The application of wireless sensor network is wide spreading. The WSN are having limited power source, which required an ultimate power efficient routing and security protocol. There are several asymmetric cryptography schemes that are used to provide the security services. The Elliptic Curve Cryptography (ECC) performance is better for low power implementation applications. To ensure the communication network function correctly and safely, there are mainly four security requirements of WSN i.e. Authenticity, Integrity, Confidentiality, Availability.

In Wireless communication routing path is set up by establishing in either of three ways namely reactive, proactive and hybrid. Reactive protocols decide the routing path when they are ready with information to transmit. Proactive protocols calculate all the routes in advance and maintain the records in a routing table of each sensor node. If there is change in the route, the changes is updated throughout the network and due to this region proactive protocol are not suitable for WSN. Hybrid protocols join the idea of proactive and reactive protocols. Some of the routing protocols are discussed below.

Hierarchical protocols: Such protocols are suitable for higher scalability. Hierarchical protocols functions in two tier, first tier is used to decide about cluster-heads and the other tier is used for data routing. This protocol is more energy efficient and improves network scalability, lifetime and quality of service.

Location based Protocols: This protocol used nodes location information to decide the closeness among two or more nodes to estimate the energy consumptions. Two methods are used to determine the sensor node location, first one which calculates the coordinates of the neighbouring node and second one uses the global positioning system.

Ad-hoc on demand distance vector (AODV) Protocol: AODV is the energy efficient and shortest path routing algorithm widely being used for wireless network. It uses methods of path discovery and maintenance. AODV form routes between sensor nodes only when they are needed.

III. Elliptical Curve Cryptography

Elliptical Curve Cryptography (ECC) is suited for WSN applications. 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. An elliptic curve is the points in the *x-y* plane that satisfy an algebraic equation $y^2 = x^3 + bx + c$ of the form. The selection of values of *b* and *c* result different elliptic curves. The value of *x*, *y*, *b* and c are over the finite fields of F_P are commonly used in practice. An example of elliptic curve for Point addition and Point doubling is as shown below in Figure 2&3.

The equation of the elliptic curve over Prime field 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: $\lambda = ((3x^2_P + a)/ (2y_P)) \bmod p$

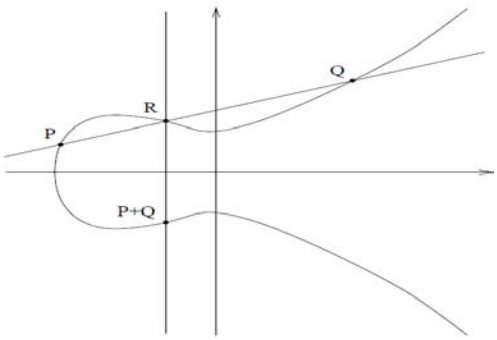

Fig.2 : Adding two points on elliptic curve

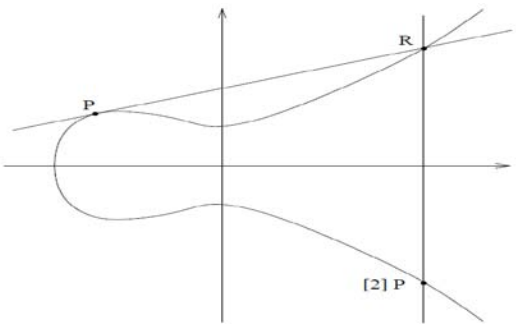

Fig.3 : Doubling a point on an elliptic curve

Elliptic Curve Cryptography technique consists of three parts: Key Generation, Encryption and Decryption. The following required inputs parameters are listed below,

1. Finite Prime Range
2. Parameters of elliptic curve equation
3. Generator Point
4. Random Numbers
5. Receiver's Public Key
6. Receiver's Private Key
7. Plain text File
8. Cipher text File

Example of an Elliptic Curve Group over F_p

As a very small example, an elliptic curve over the field F_{23} has been considered. 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 points are plotted in figure 4.

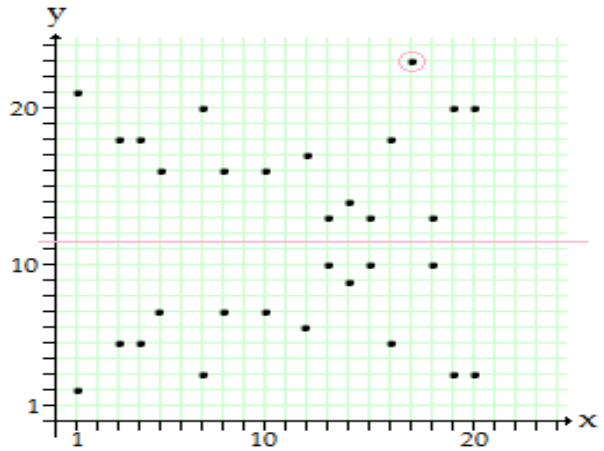

Fig. 4 : A plot on $y^2 \bmod 23 = x^3 + 9x + 17 \bmod 23$

IV. Spherical Coordinates for Ecmsgr

The proposed ECMSGR protocol is based on the concept of Cartesian Coordinates system which is consists of four basic elements: a) Choice of origin b) Choice of axes c) Choice of positive direction for each axis d) Choice of unit vectors for each axis.

Spherical Coordinates:

In the spherical coordinate system, as shown in figure 5 a point P(x, y, z) whose Cartesian coordinates are (x, y, z), is described by an ordered triple (ρ, θ, φ), where

$$\rho > 0, 0 \leq \theta \leq 2\pi, 0 \leq \varphi \leq \pi$$

are defined as follows.

- ρ = dist(P, O)
- θ is defined as the angle from zx-plane, counter-clockwise, to the half-plane originating from z-axis and containing P.
- φ = angle from positive z – axis to vector $\overrightarrow{OP}$

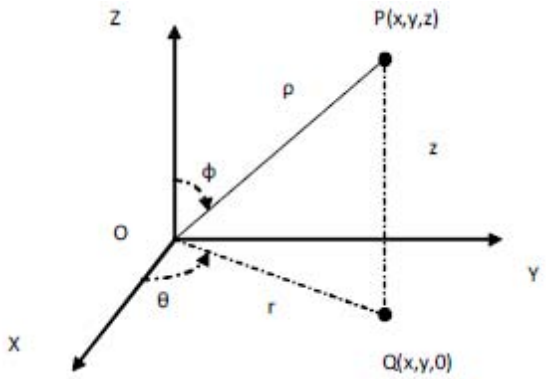

Fig. 5 : Spherical Cartesian System

Note that when P is on z – axis, φ = 0, and φ increases from 0 to $\frac{\pi}{2}$ as P moves closer to xy – plane, and φ keeps increasing as P moves below xy – plane, and φ reaches the maximum valueπ when P is on the negative z – axis.

Conversion formula (rectangular ↔ cylindrical ↔ spherical)

$$x = r\cos\theta = \rho\sin\varphi\cos\theta$$

$$y = r\sin\theta = \rho\sin\varphi\sin\theta$$

$$z = r\cot\varphi = \rho\cos\varphi$$

$$\rho = \sqrt{x^2 + y^2 + z^2}$$

$$\tan\theta = \frac{y}{z}$$

$$\cos\varphi = \frac{z}{\sqrt{x^2+y^2+z^2}}$$

To determine θ, we need to consider which quadrant the point is in. θ can be more precisely determined as,

$$\theta = \begin{cases} \arctan\frac{y}{x}, & \text{if } x > 0 \\ \arctan\frac{y}{x} + \pi, & \text{if } x > 0 \\ \frac{\pi}{2}, & \text{if } x = 0, y > 0 \\ -\frac{\pi}{2}, & \text{if } x = 0, y < 0 \end{cases}$$

φ can be uniquely determined as,

$$\varphi = \arccos\left(\frac{z}{\sqrt{x^2+y^2+z^2}}\right)$$

The coordinate system formation of the spherical grids is shown in figure 6.

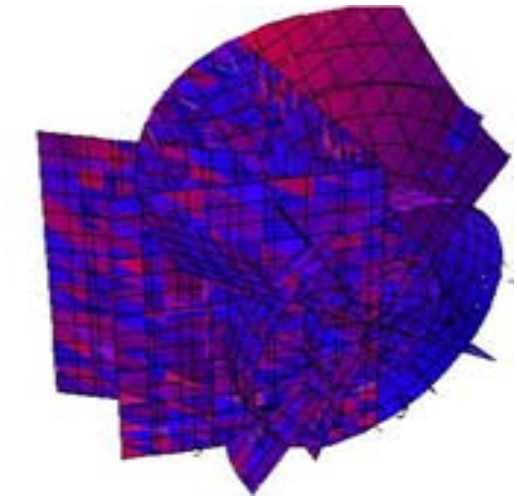

Fig.6 : A Spherical Grid

V. Elliptical Curve based Multi-tier Spherical Grid Routing (ECMSGR): A Proposed Method

The several sensor nodes are uniformly distributed across a field to form wireless sensor network for the secure routing of data packet between source and destination. Each sensor node senses its input attribute and before its send the data packet to its neighbor node it forms a routing path in spherical grid fashion with proper coordination among no. of sensor nodes. For the uniform utilization of sensor nodes, each sensor node is checked for remains energy level and no. of times used for path formation by the neighbouring sensor node as shown in figure.

In WSN multi-tier spherical grid routing path formation between two or more sensor node is calculated by determining previous and next sensor node angular position such that path formation will be in spherical fashion between starting node and destination node as shown in figure 7. Source as indication in figure 7 is sensed by a sensor node near to it. The sensed node now decides about choosing second next node with required angle and second node select third node such that the routing path formation between source and destination takes spherical shape. The red dot represent one tier spherical grid and blue dot represent second tier and so on routing path formation takes place.

The required angular position between nodes formation is shown in figure 8. The elliptical curve based multi-tier formation of spherical grid routing to cover very large area with effective & optimized utilization of sensor node is represented by figure 9.

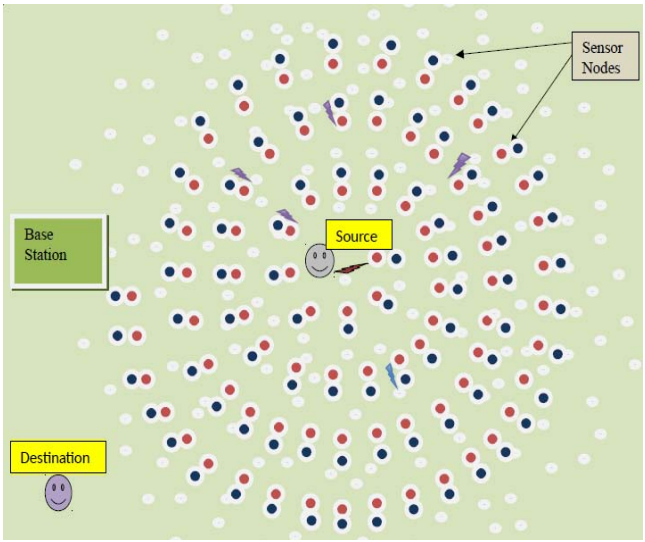

Fig.7 : Elliptical curve based Multi Tier Spherical Grid

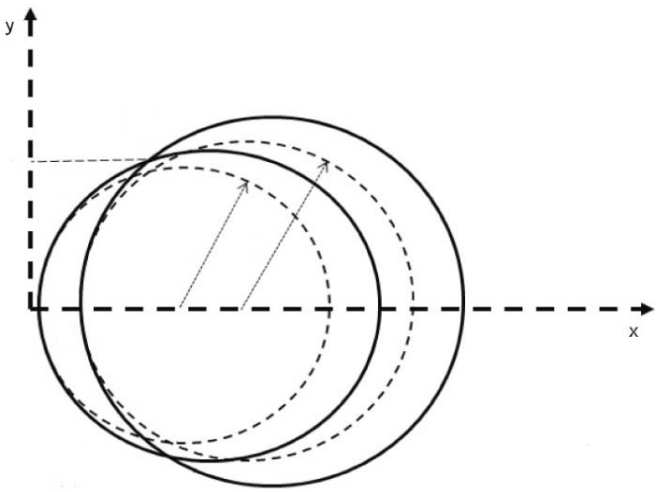

Fig. 8 : Formation of angular position between two nodes

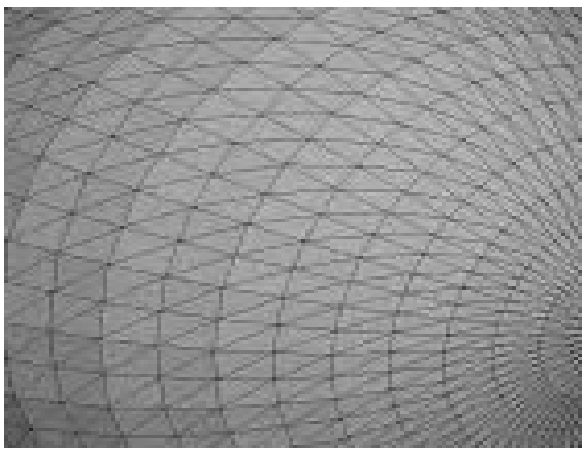

Fig. 9 : Spherical Grid formation over wide area

VI. Results & Discussions

The Proposed protocol ECMSGR is compared with LEACH and GRID protocol in network simulator 2 environment to evaluate the performance metric such packet delivery ratio, throughput, communication overhead, end-end delay and power consumption. The table I represent simulation parameter set up for NS2.

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	16/25/36/49/98/196
Routing protocol	AODV/DSR/DSDV
X dimension of topography	4000
Y dimension of topography	4000
Time of simulation end	20/40/60/80/100
Initial energy in Joules	100
Network Type	Mobile
Connection Pattern	Random
Packet Size	512 bytes
Connection type	CBR/UDP/TCP

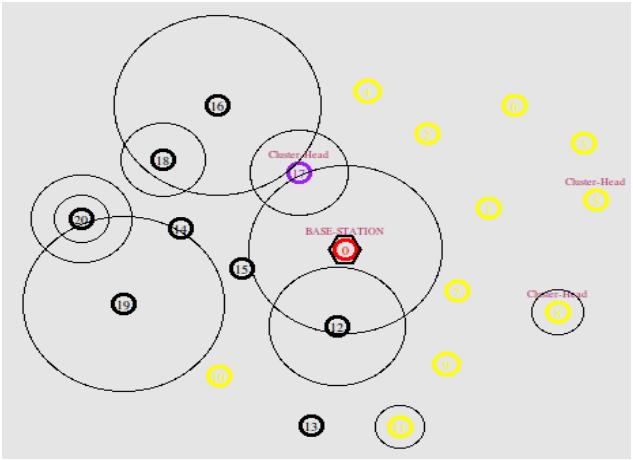

Fig.10 : M-LEACH Protocol

Figure 10 represent the M-LEACH protocol in which whole network is divided into no. of group of network. Each group of network selects their local cluster head for communication. Cluster heads are responsible for collection of data from their local sensor nodes and transmit to destination with the help of other cluster heads.

A large area is covered by a large number of sensor nodes which communicate with each other through short-range radios. Long-range data delivery is achieved by forwarding data across multiple hops. Each sensor is aware of its own location. However, mobile sinks may or may not know their own locations. When a stimulus appears, the sensors surrounding it collectively process the signal and one of them becomes the source to generate data reports. Sinks (users) query the network to collect sensing data. There can be multiple sinks moving around in the sensor field and the number of sinks may vary over time as shown in figure 11.

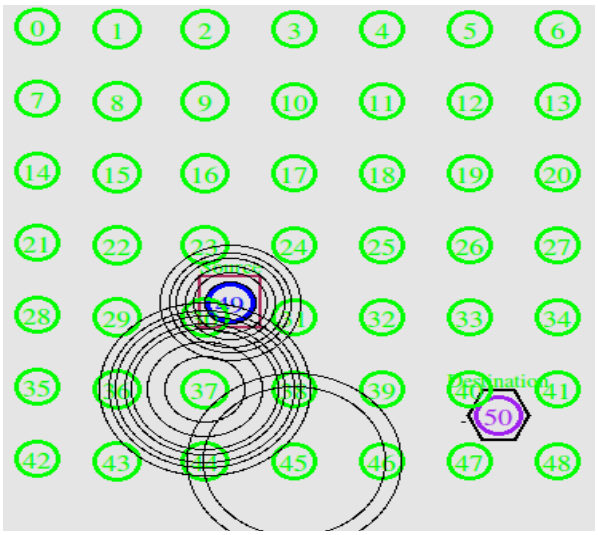

Fig.11 : 7 * 7 GBDD based Protocol

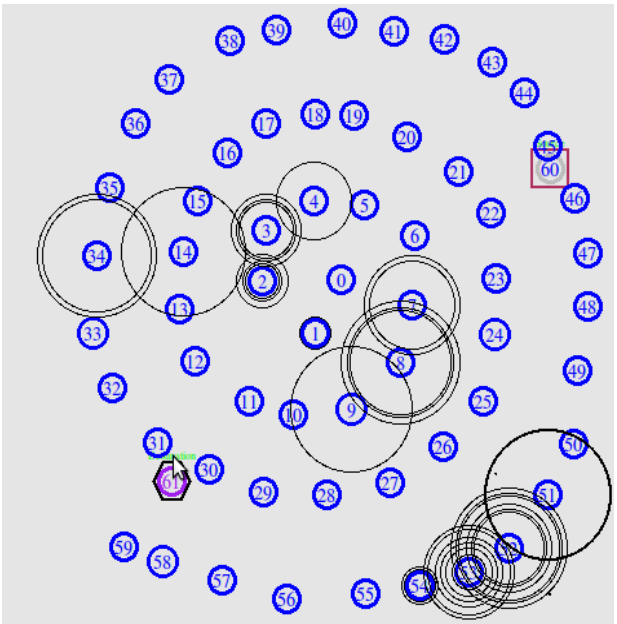

Fig.12 : ECMSGR Protocol

The ECMSGR Protocol as shown in figure 12 has been in discussed in section V. The experimental result of M-LEACH, 7*7 GBDD based protocol and ECMSGR for a network scenario as indicated in figure 10, 11& 12 and their result is compared for their transmitted packet, received packet, packet delivery ratio, average throughput and residual energy is shown in figure 13.

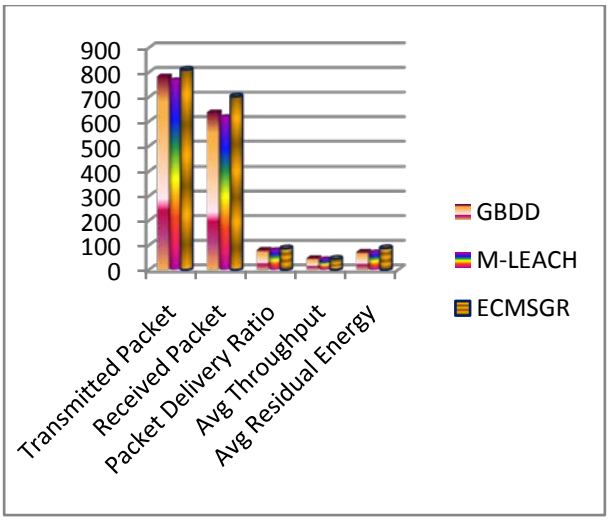

Fig.13 : A comparison between GBDD, M-LEACH & ECMSGR

VII. Conclusion

The proposed method ECMSGR provides a novel and an approach towards improvising potential WSN performance specially in terms of packet delivery ratio, throughput, communication overhead, end-end delay and power consumption. The network route formation as well as data transmission and its security are a major concern in the field of wireless sensor network. The ECMSGR protocol implementation and its performance compare to other related protocol is designed and analyzed to overcome some of the limitations of existing protocol using network simulator-2. The experimentation scenario and results shows that ECMSGR outperforms GBDD & M-LEACH. The ECMSGR protocol complexity increases when the network scalability increases at very large scale in the application of providing smart & secure gobal communication for data as well as voice communication to end users. ECC offer advantages of higher speeds, lower power consumption, and code size reductions. This concludes that ECC is best suited for wireless applications which demands speed, time and bandwidth. The results shows that optimal key generation time, encryption time and throughput using simulation. In this paper ECMSGR protocol gives an idea for researcher to explore further possible performance efficiency enhancement to offer better quality of services to provide communication coverage across globe.

References Références Referencias

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. A. Manjeshwar, D.P. Agrawal, "TEEN: a protocol for enhanced efficiency in wireless sensor networks," in *Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, San Francisco, CA, April 2001.
3. 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.
4. A. Manjeshwar and D. P. Agrawal, "APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in *Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing,* pp. 195–202, April 2002.
5. F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A two-tier data dissemination model for large-scale wireless sensor networks," in *MobiCom'02: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking*, (Atlanta, USA), pp. 148–159, ACM, September 2002.
6. Ossama Younis and Sonia Fahmy, "HEED: A hybrid, Energy-efficient, Distributed Clustering Approach for Ad-hoc Networks," *in IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366-369, Oct-Dec 2004.
7. Ananthram Swami et al., "Wireless Sensor Networks: Signal Processing and Communication Perspectives", John Wiley, 2007.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. Hoffstein J, Pipher JC, Silverman JH. Elliptic curves and cryptography. An Introduction to Mathematical Cryptography. New York: Springer; 2014. p. 299–371.
14. Vigila SMC, Muneeswaran K. A new elliptic curve cryptosystem for securing sensitive data applications. International Journal of Electronic Security and Digital Forensics. 2013; 5(1):11–24.

This page is intentionally left blank