Deployment of Mobile Sensor Node and Asynchronous Power Management

V.Amirthavalli, S.Veluchamy

Abstract— ***The main motivation is to reduce power consumption in wireless transmission networks. In Wireless transmission networks power management and node deployment are the important factors in wireless transmission networks. In the previous methods, power can be reduced even though the nodes are remains in sleep mode. But the novel approach is proposed to reduce power in active condition. The main advantage is that the nodes are deployed in automatic manner which overcomes manual deployment. Nodes are used to cover maximum area with highly accurate localization mechanism can be done by ECDH protocol. Grid deployment is used for automatic node deployment in networks. The grid with minimum value technique is the important method to place the mobile node in the networks. Node uses power only in the active condition, whenever it needs to transmit data.***

Index Terms— ***Dynamic Power Management, Grid Deployment., Mobile Sensor Node Deployment, Particle filter algorithm.***

I. INTRODUCTION

Wireless Sensor Network (WSN) is an evolving technology of great interest to many academic units and research centers in universal. A sensor network can be composed of more number of sensor nodes that will be communicated with each other by a wireless network. The main tasks of sensor node are to sense data, and then do some processing and storing of data. Then it must communicate with other node that is it should transmit the sensed data to base station. Sometimes sensor node can be used location finding system and mobilizer, it depends the application where to use nodes. The data of each node are integrated. Motion-less design is a communal scheme because of long-term motion will consume more energy.

Sensor network can be composed by placing more number of nodes inside the phenomenon to sense or very close to it. Sensor nodes can be placed in static or random manner. The main tasks of a sensor node in a sensor field are to sense the pre-assigned events, and then perform some quick local data processing with data storage if required, and then transmit the data. For those processes sensor nodes require energy. So Power consumption can be divided into three fields such as sensing, communication, and data processing to be done at sensor nodes. Public values can be calculated by product of randomly selected numbers with base point of elliptic curve. The sender and the receiver will use the same base point, both will independently choose their own random numbers.

Many challenges rise when the security in wireless sensor networks is taken. Such challenges are like resource limitations on sensor nodes, large and dense networks, and unknown network topology prior to deployment and high risk of physical attacks to unattended sensors [1]. Elliptic Curve Diffie-Hellman (ECDH) allows two parties Alice and Bob to use a shared secret key since it is public key agreement protocol. Implementation of Diffie-Hellman key exchange algorithm enabled by group of points on an Elliptic Curve over a Galois Field Secret key can be generated between Alice and Bob done by agreement to use the same Elliptic Curve domain parameters [2]. For resource-restricted sensor nodes, Elliptic Curve Diffie-Hellman (ECDH) key exchange is feasible one. Perfect resilience to node capture, excellent scalability, and low memory as well as communication overhead are the main advantages of using ECDH key exchange in WSNs[3].

By using the ECDH key exchange scheme, one of the possible key management schemes is to permit every lower end sensor node set up shared keys with each of its neighbours. The entire nodes are obtusely deployed in the field where as in many existing reliable sensor networks [4]. In nodes' distribution coverage is the most considered factor, and there are three main deployment methods. The first method confers [5] the variety of regular deployment topologies, includes circular and star deployments, as well as triangular, square, and grid deployments, and analyzes each topology's performance. In order to find the place of all sensor nodes, virtual forces are utilized in second method [6][7][8]. The third protocol works on the on the principle of moving sensors from a heavily deployed region to a dispersedly deployed area. By including the mobility in wireless sensor network, life time of node can be improved is analyzed [9]. In which only a small percentage of network nodes are used as mobile node, and allow them to move in order to find recharge, energy, and deliver energy to immobile nodes.

Deployment of sensor network is the main issue in wireless sensor network. Designed has been carried out for distributed self-deployment protocols for mobile sensors [10]. The protocols should be calculating the target positions for the mobile node after discovering a coverage hole. Used Voronoi diagrams to discover the coverage holes and design three movement-assisted sensor deployment protocols, , VORonoi-based, VEC (VECtorbased) and Minimax based on the principle of moving sensors from densely deployed areas to sparsely deployed areas. Technical challenges and design principles are discussed in terms of system architectures, hardware development, and protocols, and software development [11].

Energy harvesting techniques, Radio technologies, and cross-layer design for IWSNs has been discussed. Coverage and uniformity increased rapidly by placing a mobile node into the monitored environment [12]. Used a novel algorithm

Manuscript received June, 2013.

P.G.Student V.Amirthavalli, Department of Electronics and Communication, Anna University Chennai: Regional Centre, Madurai, India.

Asst.Prof. S.Veluchamy, Department of Electronics and Communication, Anna University Chennai: Regional Centre, Madurai, India.

which as "Grid Method", it divided the map into many individual grids and the weighting value of each grid is determined by environmental factors. Those factors are pre-deployed nodes effect, boundary effect, and obstacles effect. The grid with minimum values is the goal of the mobile node. And the mobile node should be moved to low grid value place. This increases the coverage in wireless sensor network.

A Quality of service enhanced Base station Controlled Dynamic Clustering Protocol (QBCDCP) analyzed to suitable for the support of video and imaging traffic over resource constrained wireless sensor nodes [13]. The protocol achieved energy efficiency through a rotating head clustering approach and delegation of energy-intensive tasks to a single high-power base station, while providing quality of service (QoS) support by including delay and bandwidth parameters in the route selection process. A new approach for user authentication or server authentication by using Elliptic curve Diffie–Hellman (ECDH) and optional SIP's header is introduced [14]. The methods for improving authentication in IMS environment based on SIP protocol is investigated and analyzed. Probabilistic unbalanced distribution of keys throughout the network is demonstrated [15]. That leverages the existence of a small percentage of more capable sensor nodes can not only provide an equal level of security, but it reduces the consequences of node compromise.

II. APPLICATIONS OF SENSOR NETWORKS

Wireless sensor networks have lot of applications in various fields. The sensor networks can be used in the field of Health Care, Disaster Relief, detecting chemical, Emergency Rescue operation, Military, Environmental monitoring, Habitat Monitoring, Home networks, biological, radiological, nuclear, and explosive material etc. Some applications for different areas are Military, Medical and health systems, Industrial and home networks, Forest fire detection, Flood detection, Environmental control in office buildings, Health monitoring. For health monitoring sensor will gather data to infer activities of daily living and also give clues to a person's state of health then Monitor patients with dementia and other ills of aging. Early signs of disease are also possible and prevent its progression. One of the applications is monitoring bridges and building.

Monitoring bridges with wireless data Sensors can be done by mounted sensors on highway bridges track conditions that affect stability. For older bridges, the data provides an objective view of the bridge's condition and safety. To monitor bridge 10 to 20 sensors can be used. Wireless sensor networks applications also in various fields like Home automation, Industrial monitoring and consumer electronics, security and military surveillance, Environmental sensing. The air conditioning and heat of most buildings are centrally controlled. Therefore, the temperature inside a room can vary by few degrees. Sensors detect the events first, and then it processes them if it is possible. After processing those data it will send it to the sink. For that sensor nodes utilize its energy for sensing, processing and transmission purposes.

III. PROPOSED SYSTM OF SOFTWARE IMPLEMENTATION

System module of proposed system consist of,

- Node implementation
- Grid deployment
- Power management
- Performance evaluation

More number of nodes is implemented in a sensor environment, and also placed different mobile nodes to conserve energy. The initial check is performed that will check whether is already in grid based channels or to apply grid channels. After grid deployment it moves to awakening scheme which handles asynchronous power management for our different taken parameters such as Security, delay, loss rate and energy conservation for grid and random using x-graph as graphical tool which is implemented in Network Simulator. Proposed system is shown in figure 1.

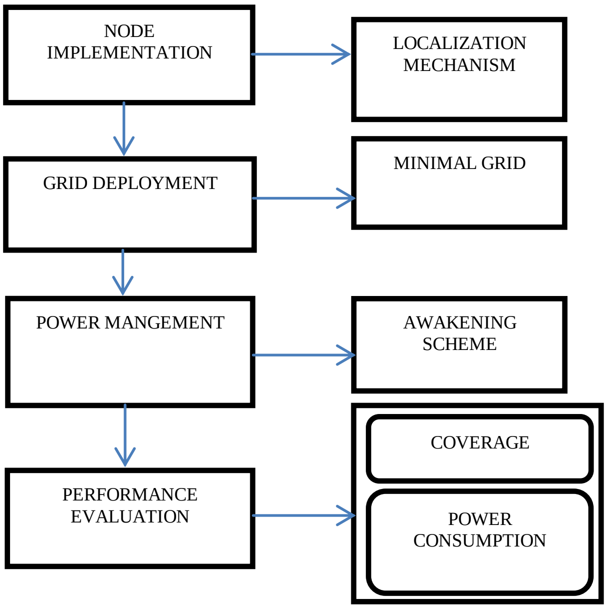


Figure 1: Proposed system

A. Node Implementation

Here some sensor nodes are implemented with initial energy and some mobility node for randomization. These sensor and mobile nodes may request to transfer the data's as per the Tcl script, so that it is easy to trace the graphical output such as NAM, Graph.

B. Researches on deployment of wireless sensor networks

Wireless sensor network deployment is one of main problem in the research of wireless sensor network, because it affects the cost and performance of network. A good deployment strategy can reduce cost of network, save the energy for communication and increase robustness of the network. Because of its various applications in wireless sensor network, various researches are going in different situations. Some of the applications, the sensors are deployed in a random manner, for example, by plane. Thus the coverage and connectivity are the most important factors. In most of the applications, the sensors may be damaged by anthropogenic or natural factors, such as battle, earthquakes or flood. As a result, the network can lose its connectivity at any time.

In some other applications, the deployment can be calculated beforehand and the sensors can survive long time in the environment. Thus performances of deployments of this kind of applications are more predictable.

C. Deployment Algorithm

Deployment algorithm proposes a framework for deployment of wireless sensor network in participatory sensing environment. It consists of several sub-models, they communicate with each other by parameters. By flexibility, means every model can be replaced by another providing the interfaces between models remain the same. This gives our deployment algorithm a good generality, which is very important due to diversity of participatory campaigns. Our framework bases on the assumption that the sensing field consists of two of three dimensional grid points, which is described in the problem formulation. Our framework concentrates on the two-dimensional cases. However, it can be generalized into three-dimensional cases straightforwardly. The distanced between adjacent grid points is determined by different campaigns. As a result, should be chosen according to practical situations. Besides this, our framework consists of following sub-models:

$$E = q2 * q1 * p(q)d(q) \qquad (1)$$

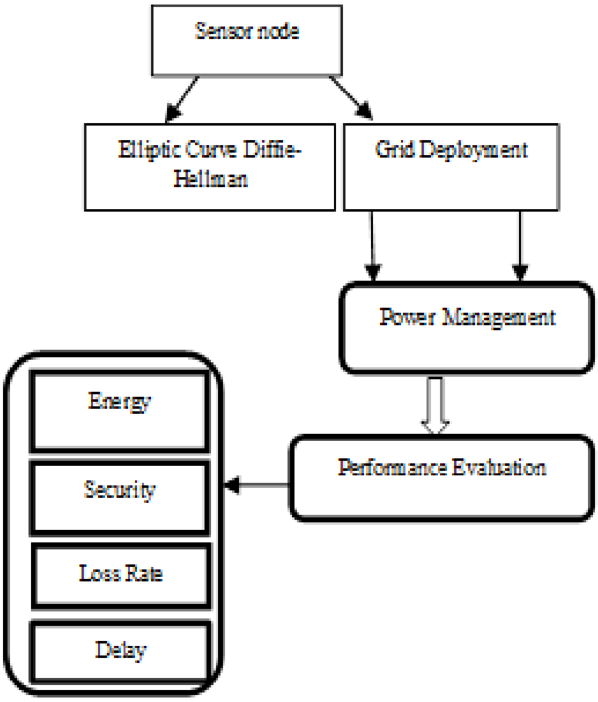


Figure 2: Deployment algorithm

- The model for sensors gives the sensing ability, by providing a detection probability matrix D. Each entry d (i,j) gives the probability that grid point g^i can be sensed by a sensor deployed in grid pointing j.
- The terrain model gives information of the sensing field, such as climates and obstacles. It affects the detection probability matrix D. For example, obstacles block the visions of some kinds of sensors and this will set some entries d(i,j) to be 0. The climates, such as fog, can decrease the detection probability. As a result, it works with sensors model together to provide the detection probability matrix D.
- The performance of every participant is described by quality evaluation model. The sensing quality is represented by marks as a real number in the range of [0, 1]. This sub model gives the probability distribution p (q) for sensing quality of every participant, based on historical data. The ensuing quality probability of next sensing action in the range [q1, q2] can be calculated by

For example, if a sensing quality probability distribution of one participant is then when this participant performs a sensing action next time, the probability that the quality of sensing result lies in the range of [0.5,1] is given by

$$E1 = 0.5 * p(q)d(q) \qquad (2)$$

- The probability that a participant performs a sensing action in grid point gi in next period is predicted by the participant's actions predication model. This model provides a vector→V, in which → Vi gives the probability that grid pointing will be visited next period.
- The deployment algorithm will take the input from above sub-models, and then calculate the grid points which will need to be monitored by extra sensor(s) and gives the minimum wireless sensors required to make sure every grid point is covered by its minimum sensing probability, as well as the locations where the sensors are deployed.

The placement problem asks how to decide the minimum number of sensors required and their locations in I to ensure that I is grid-covered and that the network is connected. Coverage is affected by sensors' sensing distance, while connectivity is determined by their communication distance. By considering that, the sensors are mobile and the area I may change over by time, and the objective of the dispatch problem is to schedule sensors to move to the designated locations (according to the result computed by the placement strategy) such that the total energy consumption of sensors due to movement can be minimized.

1. Partition the sensing field into small sub cells C^k having a regular pattern
2. i=0;
3. While termination conditions are not satisfied do.
4. Select a cell head from H_i^k the nodes which are moved to a cell C^k
5. Each node n within cell sends position P[n] to the cell head.
6. Each cell head H_i^k learn the neighboring cells information for all and constructs the adjacency list A_i^k . Each cell head H_i^k selects the victim nodes V_i^k that are to be sent to the neighboring cells
7. Assign each victim node a new position
8. Notify the adjacent cells with positions of the victim nodes.
9. All the Victim nodes will move to the new cells
10. i=i+1;
11. end

Random field to be R-covered, under the assumption that the communication distance of sensors r_c is no smaller than twice of their sensing distance $r_{s.}$ Here r_s is Random Sensing and r_c is Random communication. The work in models the sensing field by grids and considers two kinds of sensors with different costs and sensing capabilities to be deployed in the sensing field. The objective is to make every grid point

R-covered and the total cost is low. However, these both address the relationship between r_c and r_s

H_i^k represents the head node of kth cell at ith iteration and f(p) is the set of current node locations. A_i^k is the adjacent cell information of the head cell H_i^k and $V_i^{\ k}$ are the victim nodes that are targeted to the empty neighboring cells of the cell $C^{\ k}$ by the head node H_i^k.

D. Asynchronous power management

In the asynchronous protocol, if the number of buffered packets for an intended receiver exceeds a threshold L, the sender signals the receiver to remain on for the next slot. A node requested to stay awake sends an acknowledgment to the sender, indicating its willingness to remain awake in the next slot. The lifespan field in the neighbor list entry keeps the expected wakeup duration of a neighbor, and is set when the corresponding neighbor acknowledges the reservation request. If a node is not requested to stay awake by any of its neighbors, it follows its own wakeup schedule. The request is renewed on a slot-by-slot basis, i.e., the reservation only span one slot. If a neighbor is awake according to the schedule kept track of in the wakeup protocol, or it has previously acknowledged its willingness to stay awake in the current slot, then a node may deliver packets to it.

E. Mobile Configuring Deployment Algorithm for Maximum Coverage

In this section, a distributed algorithm for sensor deployment is described, considering that the space is divided into several disjoint and equal-sized hexagonal cellular regions. In which each node first elects itself as a cell head with a pre-defined probability head (Phead). If one node elects itself as a cell head, then it broadcasts its location to its neighbors. If it is not, then the node listens to the message from cell head and the node will send its location to its corresponding cell head. If any one of the head node is not elected with in a cell, then all the nodes lie in the normal state and will respond to the message transmitted by the head node.

When learning step of the deployment process, each cell head is capable of communicating with neighboring cell head/Normal nodes. If a head node is elected then all the other nodes in that cell will become as slaves. If the head node is elected, then it will execute the deployment algorithm which will uniformly spread the nodes along the given sensor field. Basically the head node will find out the position of the neighboring cells and then move redundant sensors in its cell to the unoccupied cell and this node (the node which is currently moved) will become the head node of the cell. This will be repeated till all the cells are covered.

F. ELLIPTIC CURVE DIFFIE-HELLMAN

Two communicating parties like server(s) and client(c) must agree beforehand to utilize the same curve paramenters and base point G in the elliptic curve Diffie-Hellman (ECDH) key exchange. Both the server and client must generate their private keys such as P_rS and P_rC, respectively. The corresponding public keys are given below.

$P_uS = P_rS$. G (sender) (3.1)

$P_uC = P_rC$. G (client) (3.2)

Sender will generate PrS.G as its private key and the client will generate PrC.G as its private key.They exchange their public keys, then each will multiplies its private key with the other party's public key in order to derive a common shared secret like,

$P_rC.\ P_uS = P_rS.\ P_uC = P_rS.\ P_rC.G.$ (3.3)

Attacker cannot find this shared secret from the *G,* curve parameters or the public keys of the parties. In order to achieve secure communication, Integrity, Confidentiality, authentication is the general requirement.

- Integrity and confidentiality requirements can be achieved by using encryption. It requires key(s) to encrypt or decrypt the data. Therefore key distribution mechanism is required which is suitable for the cryptographic method.
- The original user's sent message is verified by authentication of message

Elliptic curve Diffie–Hellman (ECDH) is an anonymous key agreement protocol that allows both sender and receiver having an elliptic curve public-private key pair for establishing a shared secret over an insecure channel in wireless sensor networks. This shared secret key may be directly used as a key, or it may use to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher. This is a variant of the Diffie–Hellman protocol using elliptic curve cryptography. By using ECDH approach, low number of dynamic instruction has been executed.

Key establishment protocol uses shared key that is one node wants to establish a shared key with another node, but the only channel available for them may be eavesdropped by a third party. Initially, the domain parameters (that is, in the prime case or in the binary case) must be agreed upon. Also, each node must have a key pair suitable for elliptic curve cryptography, consisting of a private key (a randomly selected integer in the interval) and a public key (where, that is, the result of adding together times). Sender's key must pair with receiver's key. Each node must have the other node's public key (an exchange must occur).Both nodes have shared secret key. The shared secret key calculated by both nodes is equal, because the only information about their private key that sender node initially exposes as its public key. So, no party other than sender node can determine sender node's private key, unless that receiver node can solve the elliptic curve Discrete Logarithm problem. Receiver node's private key is similarly secure. No nodes other than sender node or receiver node can compute the shared secret, unless that node can solve the elliptic curve Diffie-Hellman problem.

The public keys are either static or trusted, say via a certificate or ephemeral and ephemeral keys are temporary and not necessarily authenticated so if authentication is desired then authenticity assurances must be obtained by other means. The authentication is necessary to avoid Man-in-the-middle attacks. If one of sender node or receiver node's public key is static then Man-in-the-middle attacks are satisfied. Some static public keys provide neither forward secrecy nor key-compromise for impersonation resilience amongst other advanced security properties.

Holders of static private keys should validate the other public key and it should apply a secure key derivation function to the raw Diffie–Hellman shared secret to avoid leaking information about the static private key. Some of the schemes with more advanced security properties see ECMQV and FHMQV. While the shared secret may be used directly as a key or it is often desirable to hash the secret to remove weak bits due to the Diffie-Hellman exchange.

IV. PROPOSED SYSTEM OF HARDWARE IMPLEMENTATION

Assume that there have been some nodes are deployed in the monitored region. In that region mobile node should be added. The problem raises that where this mobile sensor should be placed. Ultrasonic sensor used to sense the obstacles information. Two sensors are placed for finding obstacles in front and back side of the moving node. This information is passed over the LPC 2148 processor. If any obstacles are detected, then the mobile node should avoid to be placed there. For static nodes two zigbee modules are used. Those modules are connected with computer to monitor its performance.

The mobile node is composed of sensor node and a motion control unit with LPC2148 processor. It is driven by two step motors. Two motors are used to control the front and back side movement of the node. So that mobile node can be moved to the low grid value place to increase coverage. Battery supply should be given to the Zigbee module in moving vehicle. Moving vehicle with zigbee module is considered as mobile node, since its movement in done by both motors by giving moving instructions to the motor driver.

ZigBee is one of the Advanced Wireless Technology. Its Development Kit includes the Hardware using CC2431 (latest version of CC2430) and Software to support the ZigBee Protocol. The included software helps to develop the application based on ZigBee and IEEE 802.15.4 compliant. It also helps to understand the ZigBee Protocol and IEEE 802.15.4 compliant in such a way to perform the research on these standards and protocols. ZigBee is a wireless communication protocol for low power, low rate, reliable, and secured wireless personal area network, developed by ZigBee based on IEEE 802.15.4 standard. A ZigBee network is a multi-hop network with battery-powered devices.

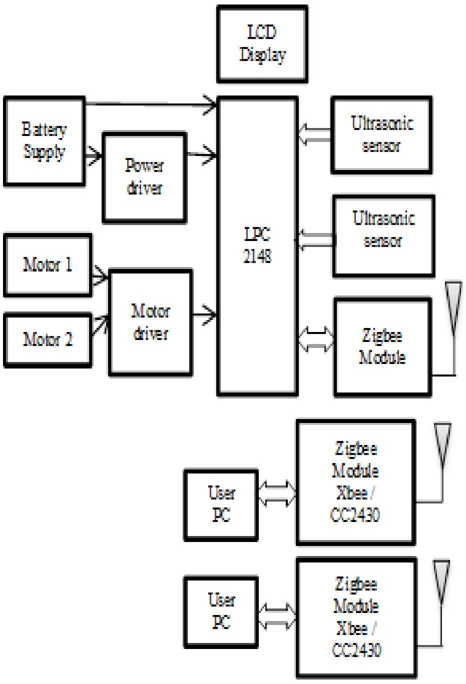
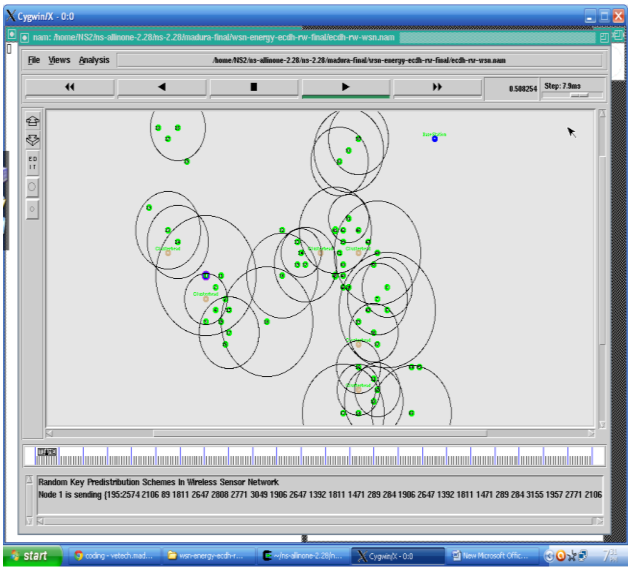


Figure 3: Deployment algorithm

Once the power level of the static node gets reduced, then the mobile node should move to that place to make transmission efficient. In that region mobile node should be added. The problem raises that where this mobile sensor should be placed. Deposition algorithm can be used with the mobile nodes to place it to monitored region. Static nodes are commercial products, micaZ, made by Crossbow. Figure 3 shows the block diagram of hardware implementation.

V.EXPERIMENTAL RESULTS

Figure 4 shows the nodes which are placed in the simulation environment. In that figure nodes are sending data's to its destination. Each grid has the same length of 1 m, each node is equipped with identical sensor, and the sensing radius is equal to 5m.


Cygwin/X - 0:0
nam: /home/NS2/ns-allinone-2.28/ns-2.28/madura-final/wsn-energy-ecdh-rw-final/ecdh-rw-wsn.nam
File
Views
Analysis
/home/NS2/ns-allinone-2.28/ns-2.28/madura-final/wsn-energy-ecdh-rw-final/ecdh-rw-wsn.nam
0.508254
Step: 7.9ms
EDIT
TIME
start
coding - vetech.mad...
wsn-energy-ecdh-r...
~/ns-allinone-2.28/n...
Cygwin/X - 0:0
New Microsoft Offic...

Random Key Predistribution Schemes In Wireless Sensor Network
Node 1 is sending {195:2574 2106 89 1811 2647 2808 2771 3049 1906 2647 1392 1811 1471 289 284 1906 2647 1392 1811 1471 289 284 3155 1957 2771 2106

Figure 4: Nodes sending data to its destination

Simulation result of ECDH for security is shown in figure 5.Security can be achieved high by using ECDH. Since ECDH uses secret key.

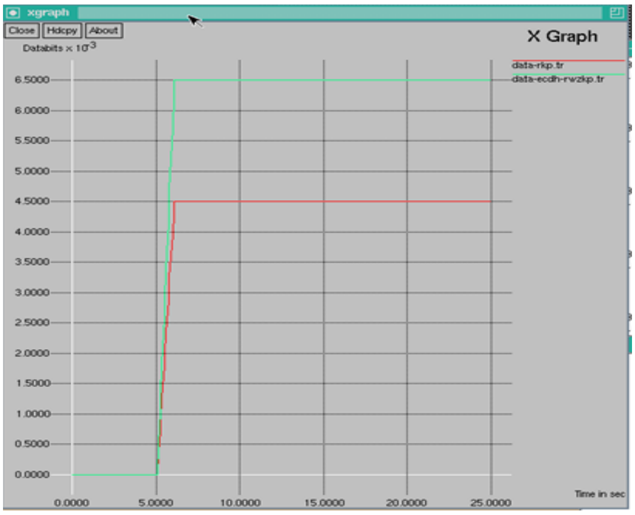


Figure 5: Analysis of Security

The result in figure 6 shows good loss rate improvement. The loss rate gets reduced with use of ECDH. Compare to previous methods this will increases the performance by reducing the loss rate.

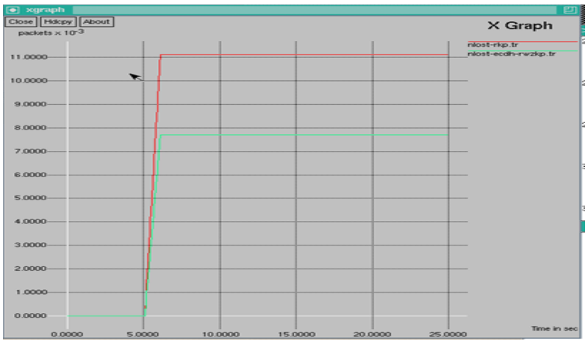


Figure 6: Analysis of Loss Rate

The result in figure 7 shows delay of receiving data. The time delay with ECDH is decreased.

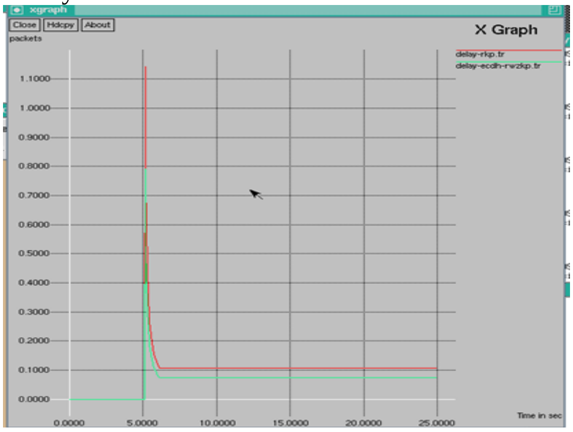


Figure 7: Analysis of Delay

It helps a lot to increase the system efficiency, improve energy conservation, and decrease the probability of missing an event.

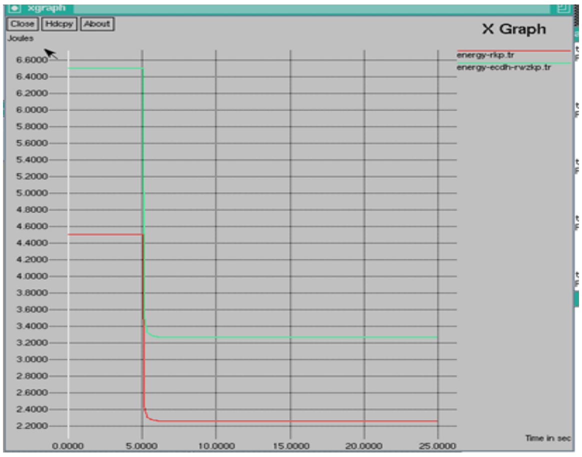
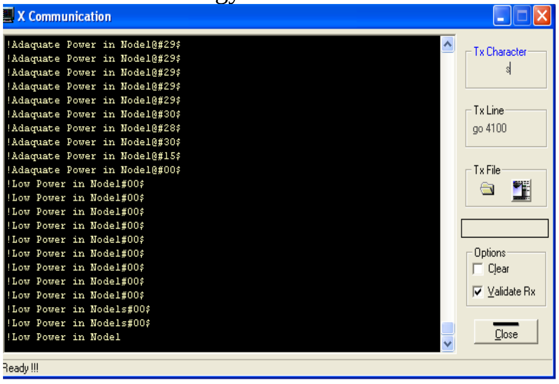


Figure 8: Analysis of Energy

Figure 8 shows the energy graph. Covering more regions with less sensor nodes means that this policy is more powerful it reduces energy.



```
!Adaquate Power in Nodel@#29$
!Adaquate Power in Nodel@#29$
!Adaquate Power in Nodel@#29$
!Adaquate Power in Nodel@#29$
!Adaquate Power in Nodel@#29$
!Adaquate Power in Nodel@#30$
!Adaquate Power in Nodel@#28$
!Adaquate Power in Nodel@#30$
!Adaquate Power in Nodel@#15$
!Adaquate Power in Nodel@#00$
!Low Power in Nodel#00$
!Low Power in Nodel#00$
!Low Power in Nodel#00$
!Low Power in Nodel#00$
!Low Power in Nodel#00$
!Low Power in Nodel#00$
!Low Power in Nodel#00$
!Low Power in Nodel#00$
!Low Power in Nodel#00$
!Low Power in Nodels#00$
!Low Power in Nodels#00$
!Low Power in Nodel
```

Figure 9: Low power in node

Figure 9 shows the low power in node. After it display low power information the mobile node should be moved to that place.

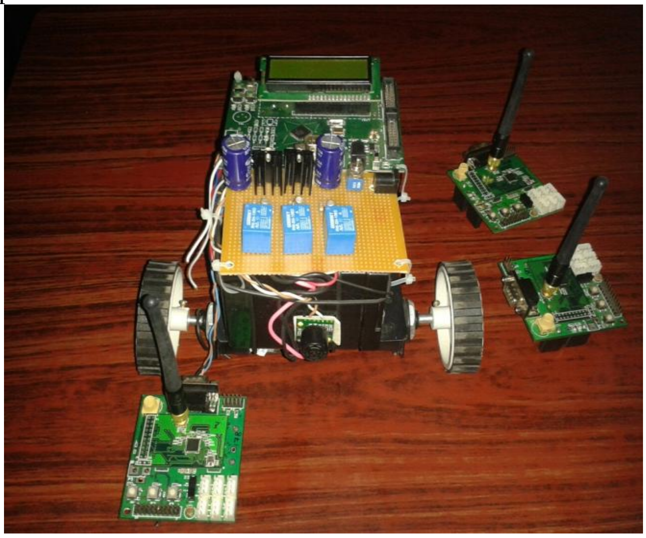


Figure 10: Hardware setup

Figure 10 shows hardware setup. It shows three zigbee modules and ultrasonic sensor.

VI. CONCLUSION

Asynchronous power management is efficient to reduce power depletion on a sensor network. In this analyze it shows that the energy conservation is achieved while deploying mobile nodes and also achieved security, improved loss rate and delay using ECDH.

REFERENCES

[1] Kejie Lu, Yi Qian, Jiankun Hu., “A Framework for Distributed Key Management Schemes in Heterogeneous Wireless Sensor Networks,” in 2006 IEEE.

[2] Makhamisa Senekane, Sehlabaka Qhobosheane, and B.M. Taele., “Elliptic Curve Diffie-Hellman Protocol Implementation Using Picoblaze,” IJCSNS International Journal of Computer Science and Network Security., VOL.11 No.6, June 2011.

[3] Christian Lederer, Roland Mader, Manuel Koschuch, Johann Großsch¨adl, Alexander Szekely, and Stefan Tillich.,“ Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks” in IFIP International Federation for Information Processing 2009.

[4] S.Pradheepkumar, V.Vijayalakshmi and G. Zayaraz, “Implementation of Pseudo-Random Route-Driven ECDH Scheme for Heterogeneous Sensor Networks” International Journal of Communication Networks and Information Security (IJCNIS) Vol. 2, No. 1, April 2010

[5] Edoardo S. Biagioni, Galen Sasaki, “Wireless Sensor Placement For Reliable and Efficient Data Collection,"proceedings of the 36th Annual Hawaii international Conference System Sciences, 2003, 6-9 Jan 2003.

[6] Heo .N. and Varshney.P.K., “A distributed self-spreading algorithm for mobile wireless sensor networks,” in Proc. WCNC, Mar. (2003), vol. 3,pp. 1597–1602.

[7] Howard.A.,Matari’c.M.J., and Sukhatme.G.S., “Mobile sensor network deployment using potential fields: A distributed, scalable solution to the area coverage problem,” in Proc. 6th Int. Symp. DARS, Jun. 25–27, 2002, pp. 299–308.

[8] Poduri.S.and Sukhatme.G.S., “Constrained coverage for mobile sensor networks,” in Proc. IEEE ICRA, May (2004), vol. 1, pp. 165–171.

[9] Rahimi.M., Shah.H., Sukhatme.G., Heidemann.J., and Estrin.D., “Studying the feasibility of energy harvesting in a mobile sensor network,” in Proc. ICRA, Sep. (2003), vol. 1, pp. 19–24.

[10] Wang. G., Cao.G., and Porta.T.F.L., “Movement-assisted sensor deployment,” in Proc. 23rd Annu.Joint Conf. IEEE Comput.Commun. Soc.(INFOCOM), Mar. (2004), vol. 4, pp. 2469–2479.

[11] Gungor.V.C. and Hancke.G.P., “Industrial wireless sensor networks: Challenges, design principles, and technical approaches,” IEEE Trans.Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. (2009).

[12] R. C. Luo, L. C. Tu, and O. Chen, “Auto-deployment of mobile nodes in wireless sensor networks using grid method,” in Proc. IEEE ICIT, Hong Kong, 2005, pp. 359–364.

[13] Abraham O. Fapojuwo and Alejandra Cano-Tinoco, "Energy Consumption and Message Delay Analysis of QoS Enhanced Base Station Controlled Dynamic Clustering Protocol for Wireless Sensor Networks," IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 10, OCTOBER 2009

[14] Maisam-Mohammadian†1Nasser-Mozayani, "2 Way Authentications for IMS by ECDH," in J. Basic. Appl. Sci. Res., 2(9)9378-9382, 2012.

[15] Patrick Traynor, Raju Kumar, Heesook Choi, Guohong CaoSencun Zhu, and Thomas La Porta., "Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 6, JUNE 2007.

Ms. V.Amirthavalli is purusing M.E degree in Communication Systems from Regional centre of Anna University Madurai. She completed her graduation in Electonics and Communication from Vickram College of Engineering, Sivagangai in 2008. She completed her diploma from Government Polytechnic College for women, Madurai.

Asst.Prof. S.Veluchamy is working as a faculty in Electronics and communication Engineering in Regional centre of Anna University Madurai. He completed his graduation from Anna University and his Master degree in Communication Systems from Anna University Chennai. He had two years of Teaching experience in Electronics and communication Engineering. Presently he is doing his Ph.D in Anna University, Chennai.