Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT AND SECURE ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS -RESULTS AND DISCUSSIONS

***[1] S.GANESH, [2] DR.R.AMUTHA**
[1] Research Scholar, Sathyabama University, Chennai-600 119, India
[2] Professor, Faculty of Electronics & Communication Engineering, SSN College of Engineering
E-mail: [1] ganesh8461@gmail.com , [2] amuthar@ssn.edu.in
[*] Author for correspondence

ABSTRACT

Advances in Wireless Sensor Network Technology (WSN) has provided the availability of small and low-cost sensor with capability of sensing various types of physical and environmental conditions, data processing and wireless communication. One of the most challenging issues so far is the extension of network lifetime with regards to small battery capacity and self-sustained operation. Endeavors to save energy have been made on various frontiers, ranging from hardware improvements over medium access and routing protocols to network clustering and role changing strategies. In addition some authors studied failures in communication regarded as error detection. Yet, only weak attention has been paid to the detection of malicious nodes and its potential for lifetime extension. In this paper, we proposed a cluster based security protocol named as Efficient and Secure Routing Protocol (ESRP). The goal of ESRP is to provide an energy efficient routing solution with security features for clustered WSN. Extensive investigation studies using Network Simulator (NS-2) shows that the proposed scheme helps to achieve balanced energy consumption and increases the throughput.

Keywords: *Wireless Sensor Networks, Routing Protocol, Energy Efficiency, Intrusion detection, Throughput enhancement, NS-2.*

1. INTRODUCTION

Wireless Sensor Network is widely considered as one of the most important technologies for the twenty-first century. The sensing electronics measure ambient conditions related to the environment surrounding the sensor and transform them in to an electrical signal. In order to realize the existing and potential applications for WSNs, advanced and extremely efficient communication protocols are required. WSNs are application-specific, so the design requirements of WSNs changes according to the application.

Hence, routing protocols' requirements are changed from one application to another [1]. However, routing protocols of all Wireless Sensor networks, regardless of the application, must try to maximize the network life time and minimize the energy consumption of the overall network. For these reasons, the energy consumption parameter has higher priority than other factors. At the network layer, it is highly desirable to find methods for energy-efficient route discovery and relaying of data from the sensor nodes to the base stations, so that the lifetime of the network is maximized.

Routing protocols are particularly susceptible to node-capture attacks. For instance, researchers have analyzed protocols for routing in sensor networks and found all are highly susceptible to node-capture attacks. In every case, the compromise of a single node suffices to take over the entire network or prevent any communication within it. Network researchers would greatly improve sensor networks by devising secure routing protocols that are robust against such attacks. Routing in WSN is very challenging [2] due to the inherent characteristics that distinguish these networks from other wireless networks like mobile ad-hoc networks or cellular networks. First, due to the relatively large number of sensor nodes, it is not possible to build a global addressing scheme for the deployment of large number of sensor nodes as the overhead of ID maintenance is high. Thus, traditional IP based

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

protocols may not be applied to WSN. Second, in contrast to typical communication networks, almost all applications of sensor nodes require the flow of sensed data from multiple sources to a particular Base Station.

Third, sensor nodes are tightly constrained in terms of energy, processing and storage capacities. Thus they require careful resource management. Further, in most application scenarios, nodes in WSNs are generally stationary after deployment except for, maybe, a few mobile nodes. Due to such differences, many algorithms like LEACH (Low Energy Adaptive Cluster Hierarchy), PEGASIS (Power Efficient Gathering in Sensor information Systems), VGA (Virtual Grid Architecture) have been proposed for the routing problems in WSNs[3].

The rest of this paper is organized as follows In Section 2, the related work is briefly reviewed and discussed. Then we describe our network model, adversary model and notations used throughout in this paper in Sections 3 and 4. Simulation and hardware results are presented in Section 5. We conclude this paper in Section 6.

2. RELATED WORK

The task of finding and maintaining routes in WSNs is nontrivial, since energy restrictions and sudden changes in node status cause frequent and unpredictable topological changes. Several layers of security are necessary to reduce the potential for malicious attacks on a system. An Intrusion Detection System (IDS) [4] is one of these layers of defense against malicious attacks. In IDS a stream of data is inspected and rules are applied in order to determine whether some attack is taking place. Intrusion Detection Systems typically operate within a managed network between a firewall and internal network elements. The idea of Intrusion Detection Systems has been around since the 1980's, beginning with James P. Anderson's study on ways to improve computer security auditing and surveillance at customer sites [5]. The IDS field has made significant advancements over the years. Today there are a number of security options available. In [6] WenShen,et.al has proposed a novel intrusion detection scheme based on the energy prediction in cluster-based WSNs (EPIDS). The main contribution of EPIDS is to detect attackers by comparing the energy consumptions of sensor nodes. The sensor nodes with abnormal energy consumptions are identified as malicious attackers. Furthermore, EPIDS is designed to distinguish the types of denial of service (DoS) attack according to the energy consumption rate of the malicious nodes. In [7] RassamM.A, Maarof, M.A, and Zainal highlighted the limitations of the state-of-the-art rule based intrusion detection schemes and they have introduced a novel framework based on rule based scheme. In [8] Yun Wang, Weihuang Fu,Dharma and P. Agrawal have analyzed the problem of intrusion detection in a Gaussian distributed WSN by characterizing the detection probability with respect to the application requirements and the network parameters under both single-sensing detection and multiple-sensing detection scenarios. Effects of different network parameters on the detection probability were examined in detail. Furthermore, performance of Gaussian distributed WSNs was compared with uniformly distributed WSNs. They analytically formulated detection probability in a random WSN and provided guidelines in selecting appropriate deployment strategy and determining critical network parameters. In[9] Fenye,Ing-RayChen, MoonJeong Chang and Jin-Hee Cho have proposed a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. They considered multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. By means of a novel probability model, they described a heterogeneous WSN comprising a large number of sensor nodes with vastly different social and quality of service (QoS) behaviors with the objective to yield "ground truth" node status. This served as a basis for validating their protocol design by comparing subjective trust generated as a result of protocol execution at runtime against objective trust obtained from actual node status. To demonstrate the utility of their hierarchical trust management protocol, they applied it to trust-based geographic routing and trust-based intrusion detection. For each application, they identified the best trust composition and formation to maximize application performance. Their results indicated that trust-based geographic routing approached the ideal performance level achievable by flooding-based routing in message delivery ratio and message delay without incurring substantial message overhead. For trust-based intrusion detection, they discovered that there exists an optimal trust threshold for minimizing false positives and false negatives. Furthermore, trust-based intrusion detection

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

outperforms traditional anomaly-based intrusion detection approaches in both the detection probability and the false positive probability. In [10] Salehian,MasoumiyanF, and UdzirN.I have provided an overview of the research on IDS in WSNs, focusing on routing protocol classification depending on network structure with respect to energy consumption as a crucial parameter in these kinds of networks. In addition, some simulation manners were reviewed.

In [11] Besson.L and Leleu.P have worked in a project funded by the European Union Information and Communication Technologies Program that was focused on security and resilience across ad-hoc personal area networks and wireless sensor networks, and provided a security toolbox for trusted route selection, secure service discovery and intrusion detection called as AWISSENET (ad-hoc personal area network & wireless sensor secure network). Their work described the intrusion detection systems for WSNs and how it is used in the AWISSENET project. In [12] Misra.S, Krishna.P.V, and Abraham have proposed a simple, low complexity and energy-aware protocol for intrusion detection in WSN. The protocol was a self-learning and distributed in nature. The distributed nature avoids all other nodes being sacrificed when a single node was compromised. The protocol exposed the concept of stochastic learning automata on packet sampling mechanism to achieve an energy aware intrusion detection system. They have rigorously evaluated the performance of their proposed solution by performing a variety of experiments and have found their solution approached to be promising. In [13] YunWang, Kelly.B.M and, Dolin.S investigated the effective intrusion detection problem in a partially connected random WSN from modeling, analysis, and simulation perspectives by integrating the K-sensing and communication tasks. Upper and lower bounds of effective K-sensing intrusion detection probability were mathematically formulated and theoretically derived. Monte-Carlo Simulations are conducted and outcomes were shown to support the theoretical analysis. In [14] ChangchunZhang, et.al has analyzed a Cognitive Radio Network (CRN) based Wireless Sensor Network (WSN). Issues addressed in that paper include experimental architecture, waveform design, and machine learning algorithm for classification. In particular, passive target intrusion was experimentally demonstrated using multiple WARP platforms that serve as the cognitive/sensor nodes. In contrast to traditional localization methods relying on radio propagation properties, the technique used in this research was based on machine learning with measured data, considering complicated multi path environment and high dimensional sensing data collected by the CRN based WSN. Preliminary experimental results were quite encouraging, suggested that a large-scale CRN based WSN supported by machine learning techniques has promising potential for passive target intrusion detection in harsh RF environments.

Sumit Gwalani Elizabeth M. Belding-Royer and Charles E. Perkins in [15] proposed a new protocol that modifies AODV to improve its performance. The protocol, AODV-PA, incorporates path accumulation during the route discovery process in AODV to attain extra routing information. They have shown from the results that AODV-PA improves the performance of AODV under conditions of high load and moderate to high mobility. Srdjan Krco and Marina Dupcinov in [16] observed a problem that affects the neighbor detection algorithm of the AODV routing protocol and has a deteriorating impact on performance of ad hoc networks that use this protocol. An improvement of the neighbor detection algorithm based on the differentiation of good and bad neighbors using signal to noise ratio (SNR) value is proposed, described and experimentally verified. Several fault detection and tolerance schemes for wireless sensor networks have been proposed in the literature. They are developed based on centralized, distributed, and hierarchical models. Due to the importance of energy efficiency, most schemes employ a distributed model, using either neighbor coordination or clustering. Ju et al. [17] proposed an improved scheme based on WTE, named weighted-trust evaluation to make a decision on the correctness of the reports. The weights assigned to sensor nodes are updated after each cycle by reflecting the ratio of the number of incorrectly reporting nodes to the total number of nodes.

3. ESRP-ALGORITHM

The following assumptions were made while designing our protocol: [18] [19] [20]

1. The locations are fixed for all nodes and known to the base station.

2. Nodes are divided into three categories; Base Station (Sink node), Cluster Head and Member Nodes.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. Each Cluster Head (CH) knows about its member nodes, while every member node known its CH. Base station stores information of all sensor nodes including CHs. Base Station maintains complete topological information about CHs and their respective members.

4. Base station is powerful enough and can't be compromised like other nodes in the network and it is connected to a PC.

5. Clustering process will be carried out initially.

6. When clusters are not feasible, that particular region will switch to a flat routing protocol using AODV.

The Protocol can be modeled as follows:

- Deploy the nodes after assigning unique ID's
- Base station will be fed with all node ID'S, their positions and initial energy values.
- Base station forms clusters
- Node with highest energy in the radio range of the sink will be deputed as CH 1 .
- Among the neighbors of CH1, the node with farthest distance from CH1 and with highest energy will be selected as CH2.
- The member nodes are selected depends upon the radio coverage range of every CH's.
- The sink will decide the membership of common nodes, based on the number of member nodes in each cluster (higher priority will be given to Uniform distribution) and also the distance to each CH.
- CH selection will be intimated to the member nodes as well as neighbor CH's.
- The non member nodes can transfer the sensed data to a nearby CH through its neighbors.

Intra Cluster routing

- Each CH will send a TDMA slots to their member nodes to collect the sensed data.
- Every CH waits for at least 2/3 of member node's report before the data aggregation.
- Each CH registers the member node ID and energy value while collecting the data.
- Each CH aggregates the collected data and form a single frame.

Inter Cluster routing

- The prover – verifier mechanism of Zero Knowledge Protocol (ZKP) will be employed, whenever a CH wants to transmit a data to a neighbor CH, which is present along the route towards the sink.
- Once the identity has been proven, then the prover will be placed in the promiscuous hearing mode to verify the acknowledgement of the forwarded packet from the verifier.
- During the data transmission, fewer CH's will randomly create a dummy packets and transmit it to the direction opposite to that of original packet to possibly trap the adversaries.
- The aggregated data reaches the sink.

CH reselection

- After few data collection, Each CH will broadcast a dummy packet and waits for 'dummy ack' packet from every member node.
- If any member nodes fail to acknowledge, then those nodes will be marked as intruder or malicious and will be reported to the sink to block any network activities of those nodes.
- The sink collects the residual energy of every cluster and selects a new CH. (Steps 3 and 4)
- No cluster will be formed in a region where 2/3 of node's residual energy are bellow 0.5 J..
- Sink informs all the nodes in that region to perform flat routing (AODV) and send the sensed information to a near by CH through its neighbors.
- The steps 5 to 17 will be repeated untill 85 % of nodes energy falls bellow 0.5 joules.

4. HARDWARE IMPLEMENTATION

We set up a WSN as shown in fig.1, with 15 nodes and a sink. The hardware consists of a Zigbee based EB051C – Coordinator Zigbee node, used to start, configure the network and allow other nodes to join

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and EB051R – Router / End device node, used to connect and communicate to networks started by a EB051C. PIC 16F877 micro controller has been used for programming.[21][22] [23].The hardware results were shown in figures 2 and 3.

5. SIMULATION RESULTS

We use a simulation model based on NS-2[24] [25] in our evaluation. Our performance evaluations are based on the simulations of 100 wireless sensor nodes that form a wireless sensor network over a rectangular (1900 X 1100 m) flat space. All network nodes start the simulation by an initial energy equal to 2 J and an unlimited amount of data to be transmitted to the base station [26]. In addition, the energy of the base station is considered as unlimited. Each node uses its limited reserves of energy throughout the duration of simulation, which involves the depletion of it. Thus, any node which has exhausted its energy reserve is considered dead. In our simulation model, we assume that there are 25 intruder nodes randomly deployed in the well field. All intruders' nodes pass through a period of passive listening and then try to connect with nodes randomly targeted.

The simulation parameters are shown in table1.

We compared our protocol with the following two other protocols.

1. A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks (LDTS) [27]

2. Secure and Energy-Efficient Disjoint Multi path Routing for WSNs (S-LEACH) [28]

The following parameters has been used for the comparison

- Number of nodes alive over simulation period
- Message overhead over simulation period
- Energy consumption over simulation period
- End to end delay
- Percentage packet delivery ratio (PDR) over simulation period

Figure 1.Hardware Setup

Figure. 2. Cluster Formation

Figure. 3.Detection of Malicious Node Through Dummy Packet Transmission

- Network life time over simulation period
- Cluster formation duration over simulation period
- Cluster head reselection time over simulation period

Table 1 Simulation Parameters

Area of sensing field	1900 *1100 m
Number of sensor nodes	100
Simulation Time	1200 s
Frequency	2.4 GHz
Bandwidth	2Mbps
Traffic Type	Constant Bit rate (CBR)
Payload Size	1000 Bytes
Propagation Limit (dbm)	-111.0
Path loss model	Two ray model
Number of clusters	5
Initial energy of nodes	2J
Antenna Type	Omni directional
Channel Bandwidth	20Kbps
Routing Protocol	ESRP
MAC layer protocol	IEEE 802.15.4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure. *4.Comparison Of ESRP Vs LDTS In Terms Of Percentage PDR*

Figure. 5.Comparison Of ESRP Vs LDTS In Cluster Formation Time

Figure. 6.Comparison Of ESRP Vs LDTS In Message Overhead

Figure. 7.Comparison Of ESRP Vs LDTS In Terms CH Reselection Time

Figure 8.Comparison Of ESRP Vs LDTS In Terms Of End To End Delay

Figure. 9.Comparison Of ESRP Vs LDTS In Terms Of Energy Consumption

Figure. 10.Comparison Of ESRP Vs LDTS In Terms Number Of Nodes Alive

Figure. 11.Comparison Of ESRP Vs LDTS In Terms Of Network Life Time

Figure. 12.Comparison Of ESRP Vs S-LEACH In Terms Of Percentage PDR

Figure. 13.Comparison Of ESRP Vs S-LEACH In Terms Of Cluster Formation Time

Figure. 14.Comparison Of ESRP Vs S-LEACH In Terms Of Message Overhead

Figure. 15.Comparison Of ESRP Vs S-LEACH In Terms Of CH Reselection Time

Figure. 16.Comparison Of ESRP Vs S-LEACH In Terms Of End To End Delay

Figure. 17.Comparison Of ESRP Vs S-LEACH In Terms Of Energy Consumption

Figure. 18.Comparison Of ESRP Vs S-LEACH In Terms Of Number Of Nodes Alive

Figure. 19.Comparison Of ESRP Vs S-LEACH In Terms Of Network Life Time

TABLE 2
Comparison Of ESRP With LDTS And S-LEACH

Table 2, shows the superior performance of ESRP compare to LDTS and S-LEACH, except in 'Percentage packet delivery ratio (PDR) .

6. CONCLUSIONS

WSN is vulnerable to various attacks [29] such as jamming, battery drainage, routing cycle, Sybil, cloning. Due to limitation of computation, memory and power resource of sensor nodes, complex security mechanism cannot be implemented in WSN. Therefore energy-efficient security implementation is an important requirement for WSN. Energy consumption is also a significant concern in sensor networks research for any routing protocols using broadcast as a component, the energy cost will be high. Regardless of which node a broadcast message originates from, it would be transmitted through the entire sensor network until every node in the network including the base station receives it. Because of the broadcast nature of wireless communications, all the nodes in the vicinity of a sender receive each packet it broadcasts. In this paper we attempted an Efficient and Secure routing Protocol to minimize node energy consumption and to increase the throughput.

The unique features are :

- Deployment level initial intrusion detection.
- SNR based neighbor selection to enable selective forwarding of control as well as data packets.
- Energy based cluster formation and CH selection
- Dummy packets were created only by nodes with optimal energy level; hence not all the nodes were participated in intrusion detection.

Based on the simulation results, we can conclude that the best routing standard in our simulation is the ESRP protocol. We note that this is very much a work in progress. We are currently trying to make the models richer and more useful for analyzing different kinds of wireless sensor networks. One significant extension [30] would be to incorporate impact of source mobility, multiple sources, and message rate from the source. In future we will be concentrating to develop a new approach in cluster formation [31] and inter cluster routing , which played a major role in this paper .

REFERENCES

[1] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy, "A Comparison of Routing Attacks on Wireless Sensor Networks," International Journal of Information

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Assurance and Security, Vol. 6, No. 3, 2011, pp. 195-215.

[2] M. Saxena, "Security in Wireless Sensor Networks: A Layer- based Classification," Department of Computer Science, Purdue University,2011,www.cerias.purdue.edu/apps/ reports_ and_ papers /view /3106

[3] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on Its Security Threats," International Journal of Computers and Their Applications, Vol. 1, Special Issue on "Mobile Ad-hoc Networks", 2010, pp. 42-45.

[4] Mohamed Mubarak.T,et.al, "Intrusion Detection: A Probability Model for 3D Heterogeneous WSN", International Journal of Computer Applications (0975 – 8887) ,Volume 6– No.12, September 2010.

[5] Kamal Kant, Nitin Gupta, "Application based Study on Wireless Sensor Network**",** International Journal of Computer Applications (0975 – 8887) Volume 21– No.8, May 2011.

[6] Wen Shen, et.al "A New Energy Prediction Approach for Intrusion Detection in Cluster-Based Wireless Sensor Networks" Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 51,2012, pp 1-12.

[7] RassamM.A, Maarof, M.A, Zainal, A. "A novel intrusion detection framework for Wireless Sensor Networks" 2011 7th International Conference on Information Assurance and Security (IAS), pp 350-353.

[8] Yun Wang, Weihuang Fu,Dharma P. Agrawal, "Gaussian Versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, 20 March 2012. IEEE computer Society Digital Library. IEEE Computer Society.

[9] Fenye ,Ing-Ray Chen, MoonJeong Chang , Jin-Hee Cho "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection",IEEE Transaction on Network and service management, June2012,Volume**:** 9 ,Issue:2 ,Page(s**):** 169-183.

[10] Salehian,MasoumiyanF,UdzirN.I, ,"Energy-efficient intrusion detection in Wireless Sensor Network" 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), **Page(s):** 207 – 212.

[11] Besson.L,Leleu.P," A Distributed Intrusion Detection System for Ad-Hoc Wireless Sensor Networks: The AWISSENET Distributed Intrusion Detection System" 16th International Conference on Systems, Signals and Image Processing, 2009. IWSSIP 2009, Page(s)**:** 1 – 3.

[12] Misra.S,Krishna.P.V, AbrahamK.I,"Energy efficient learning solution for intrusion detection in Wireless SensorNetworks",2010 Second International Conference on Communication Systems and Networks (COMSNETS)

[13] YunWang,Kelly.B.M,Dolin.S," Effective detection of a mobile intruder in a partially connected wireless sensor networks" 2012 International Conference on High Performance Computing and Simulation, Page(s): 417-423.

[14] ChangchunZhang ,ZhenHu, Guo.T.N., Qiu.R. C.,Currie.K," Cognitive Radio Network as Wireless Sensor Network (III): Passive target intrusion detection and experimental demonstration", 2012 IEEE Radar Conference, Page(s): 0293 – 0298.

[15] Sumit Gwalani Elizabeth M. Belding-Royer and Charles E. Perkins 'AODV with Path Accumulation . IEEE International Conference on Communications,ICC 2003, pp.527 – 531.

[16] Srdjan Krco and Marina Dupcinov , 'Improved Neighbor Detection Algorithm for AODV Routing Protocol', IEEE Communication letters (December 2003), Vol.7,no12, pp. 584-586.

[17] Jing Feng and Huaibei Zhou, 'A Self-Repair Algorithm for Ad Hoc On-Demand Distance Vector Routing', International Conference on

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Wireless Communication, Networking and Mobile Computing, Wicom (2006),pp 1-4

[18] S.Ganesh, Dr.R.Amutha "Network Security in Wireless Sensor Networks Using Triple Umpiring System" European Journal of Scientific Research, 2011, Vol.64, issue 1.

[19] Ganesh.S, Dr.R.Amutha "Modified Triple Umpiring System for Wireless Sensor Networks" PSG tech-National Journal of Technology, Vol.8, issue 1, March 2012, pp 48-63.

[20] Ganesh.S and Dr.R.Amutha (2012) 'Efficient and Secure Routing Protocol for Wireless Sensor Networks through Optimal Power Control and Optimal Handoff-Based Recovery Mechanism" Journal of Computer Networks and Communications, Vol.2012, Article ID 971685, 8 pages.

[21] Yi ouyang,et.al , 'Entrapping Adversaries for Source Protection in Sensor Networks', Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06)

[22] Mario Gerla Lokesh Bajaj, Mineo Takai, Rajat Ahuja, Rajive Bagrodia. GloMoSim: A Scalable Network Simulation Environment. Technical Report 990027, University of California, 13, 1999.

[23] Seo Hyun Oh, Chan O. Hong, Yoon-Hwa Choi, ' A Malicious Malfunctioning node detection scheme for Wireless Sensor Networks' ,Journal of Scientific research-Wireless Sensor Network, 2012, 4, 84-90.

[24] Djallel Eddine Boubiche1 and Azeddine Bilami, 'Cross Layer Intrusion Detection System for wireless sensor networks' International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[25] Rongrong Fu,et.al, 'Biologically Inspired Anomaly Detection for Hierarchical Wireless Sensor Networks,' Journal of Networks, Vol. 7, NO. 8, August 2012.

[26] Yi-Tao Wang and Rajive Bagrodia, 'ComSen: A Detection System for Identifying Compromised Nodes in Wireless Sensor Networks,' SECURWARE 2012 :The Sixth International Conference on Emerging Security Information, Systems and Technologies.

[27] Xiaoyong Li, Feng Zhou, and Junping Du 'LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks' -IEEE transactions on information forensics and security, vol. 8, no. 6, June 2013

[28] Soojin Lee, Yunho Lee, Sang Gunn Yoo, 'A Specification based intrusion detection mechanism for LEACH protocol'-Information technology journal 11(1) ,PP 40-48, 2012

[29] Soojan lee,Yunho lee and Sang Guun yoo, 'A specification based intrusion detection mechanism for LEACH protocol,' Information Technology Journal,Vol.11(1),pp-40 to 48,2012.

[30] Meenakshi Diwakar and Sushil Kumar , "An Energy efficient level based Clustering routing protocol for wireless Sensor networks", International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.2, April 2012.

[31] Ali tufail: 'Reliable Latency aware routing for clustered WSNs'. International Journal of distributed sensor networks, Vol.2012, pp-443-749

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

List of Figures

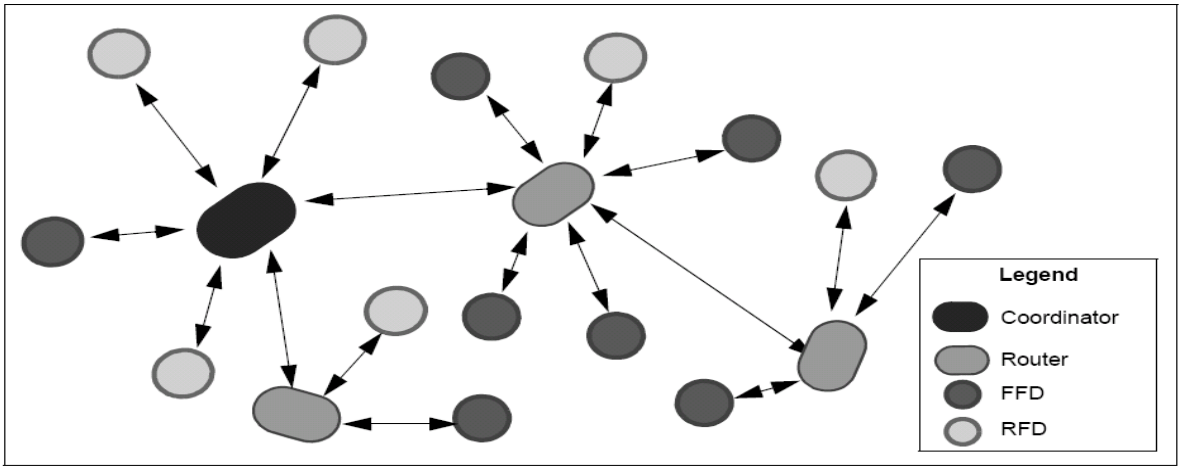

Fig. 1. Hardware Setup
FFD : Fully Functional Device, RFD: Reduced Functional Device

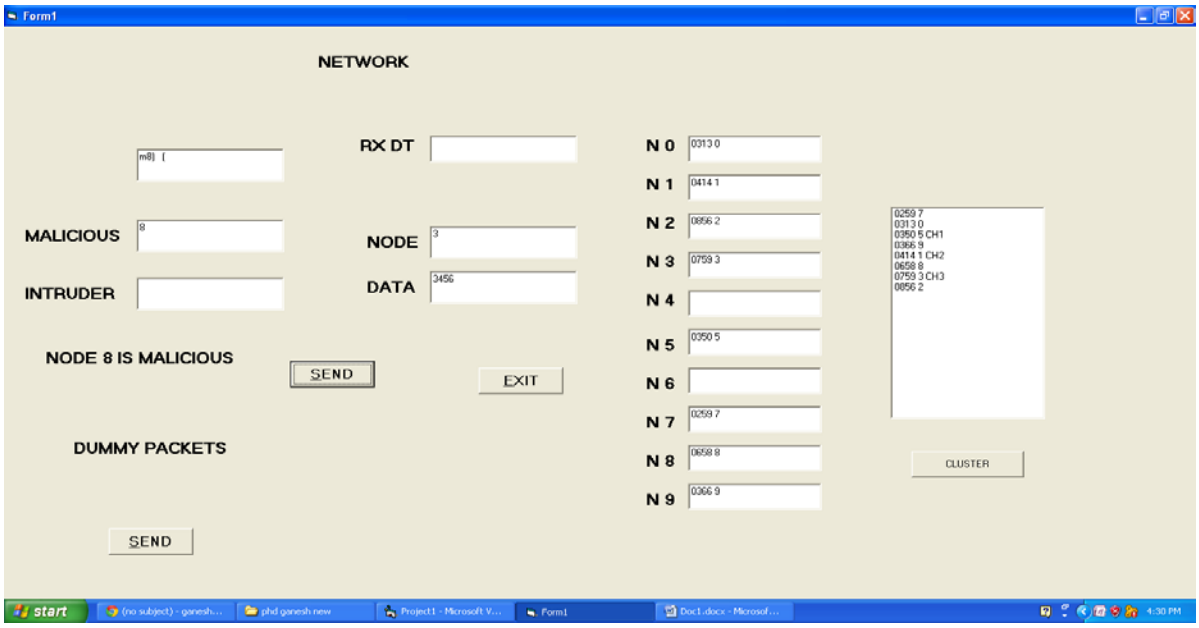

Fig. 2.Cluster Formation

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

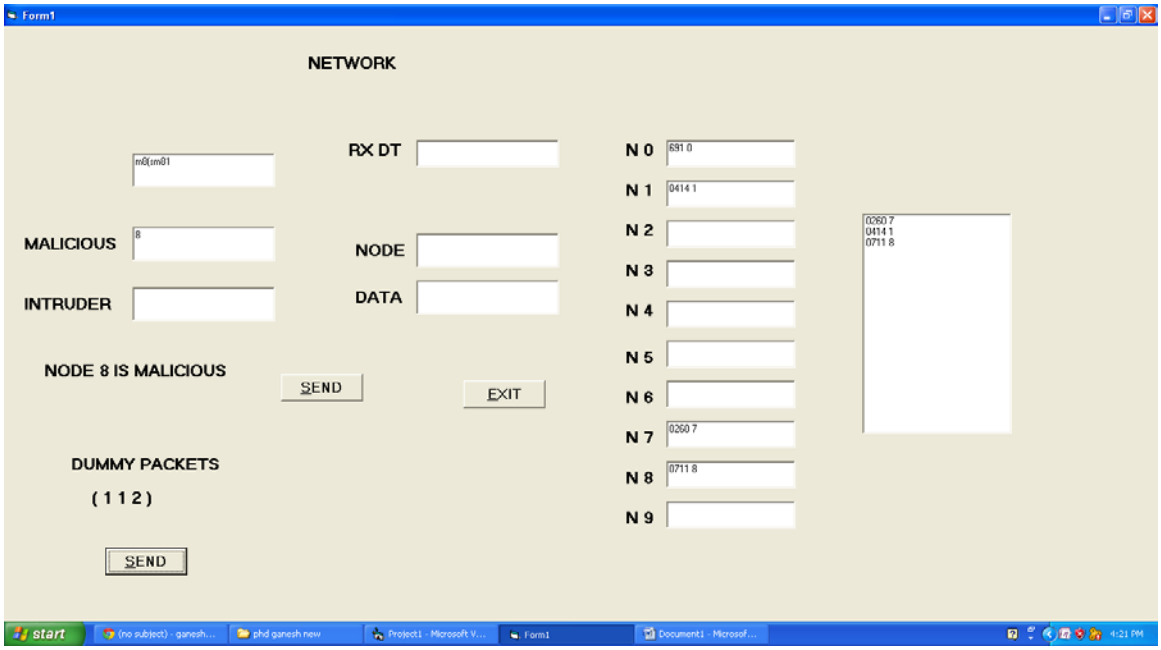

Fig. 3.Detection Of Malicious Node Through Dummy Packet Transmission

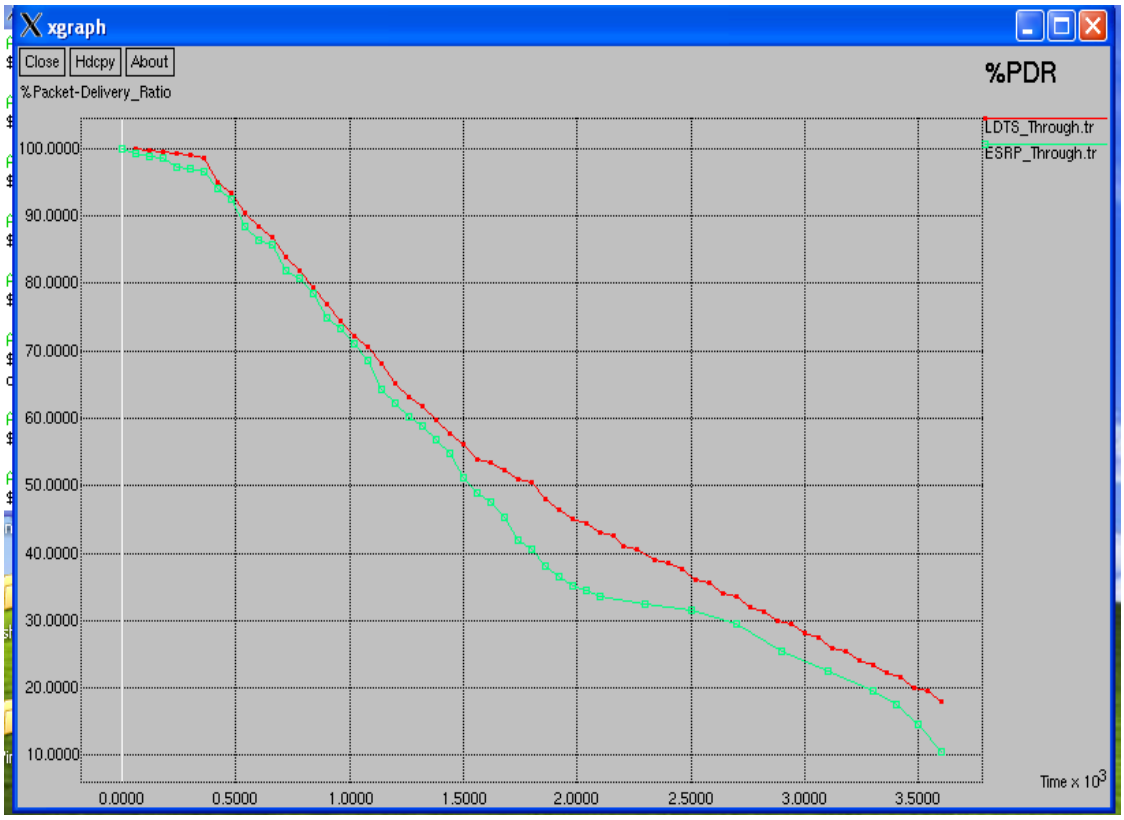

Fig. 4.Comparison Of ESRP Vs LDTS In Terms Of Percentage PDR

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

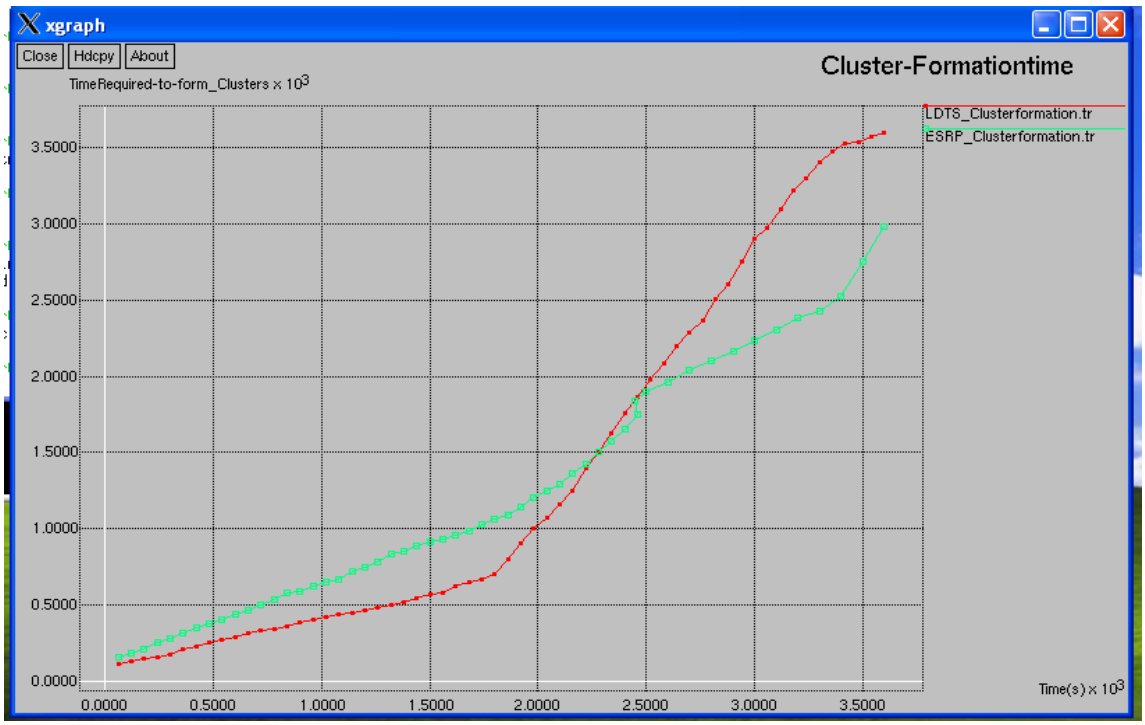

Fig. 5.Comparison Of ESRP Vs LDTS In Cluster Formation Time

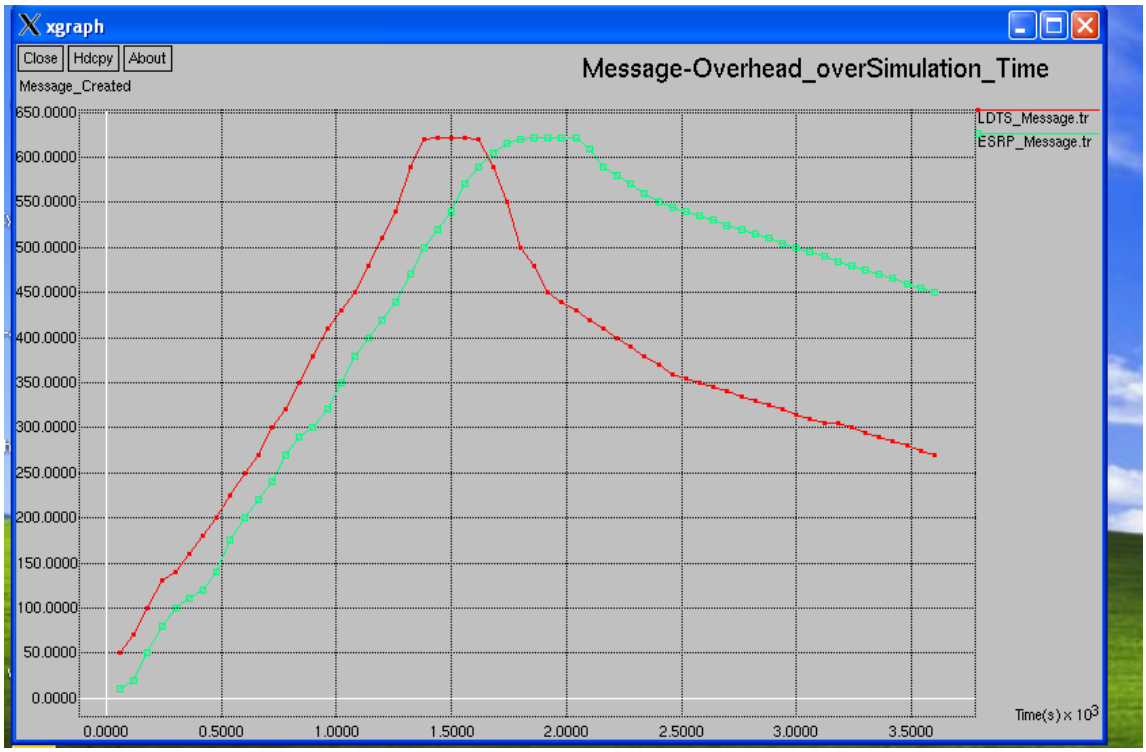

Fig. 6.Comparison Of ESRP Vs LDTS In Message Overhead

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

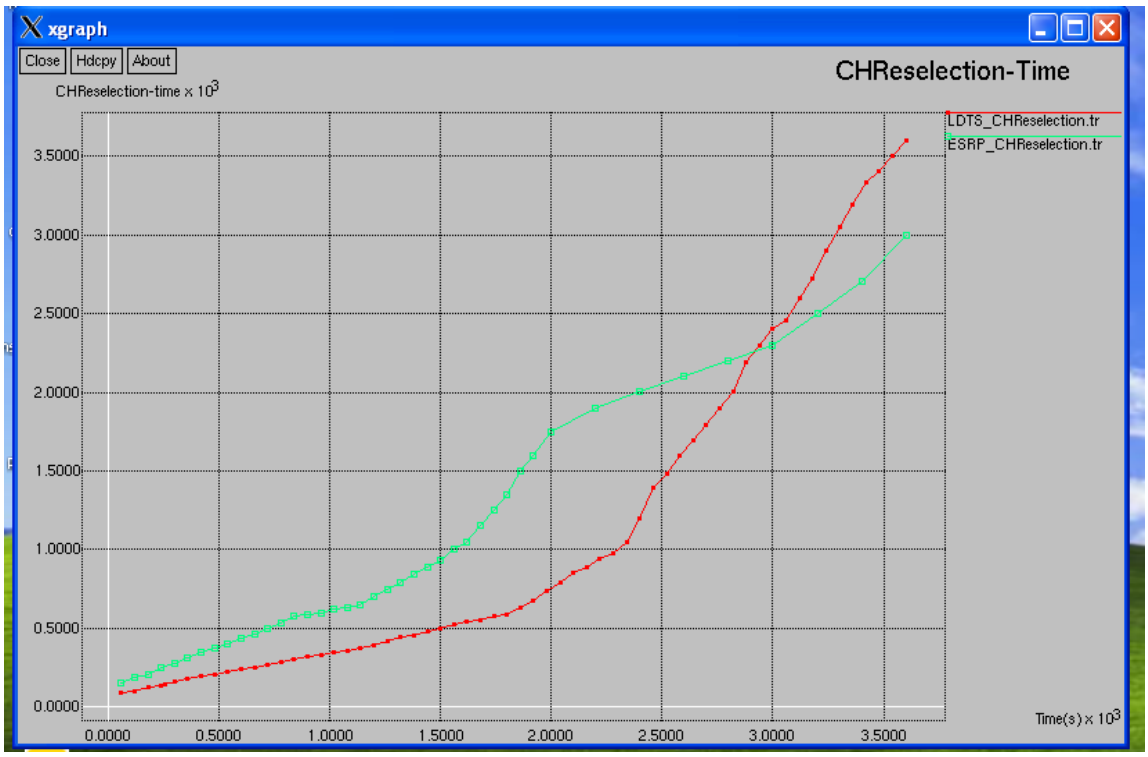

Fig. 7.Comparison Of ESRP Vs LDTS In Terms CH Reselection Time

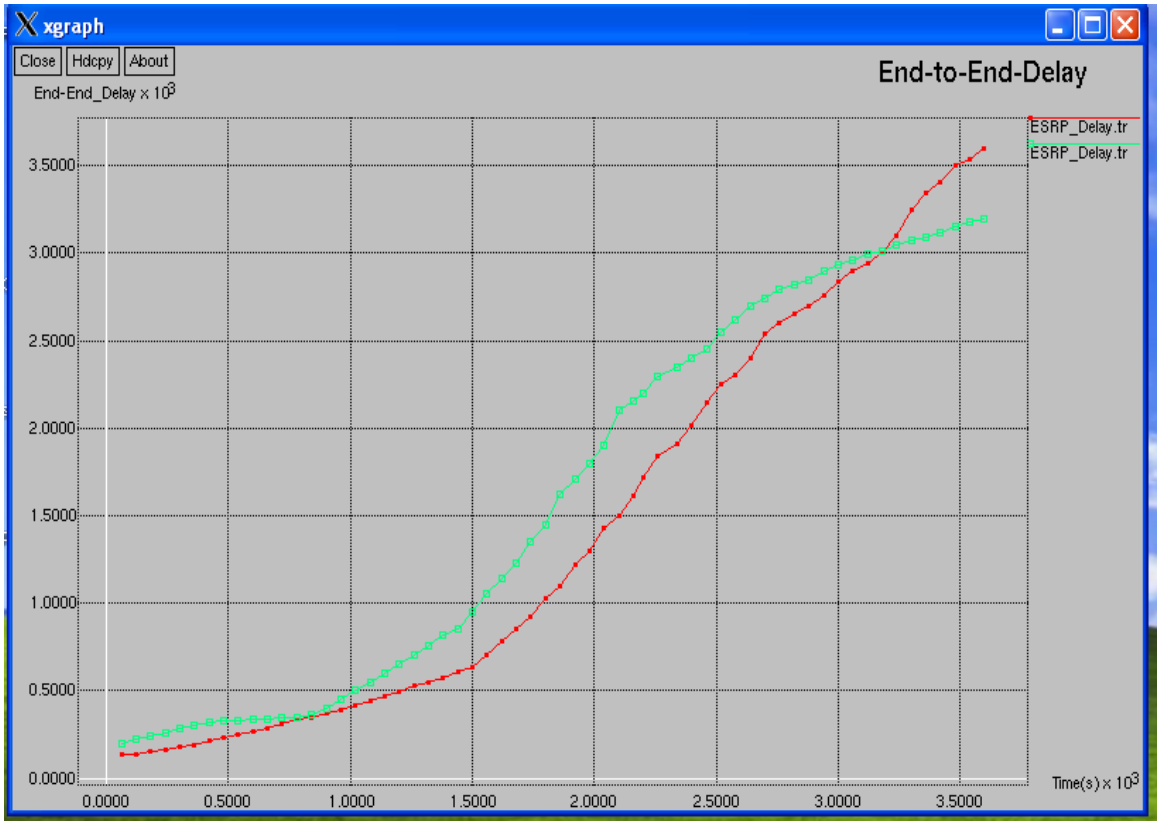

Fig. 8.Comparison Of ESRP Vs LDTS In Terms Of End To End Delay

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

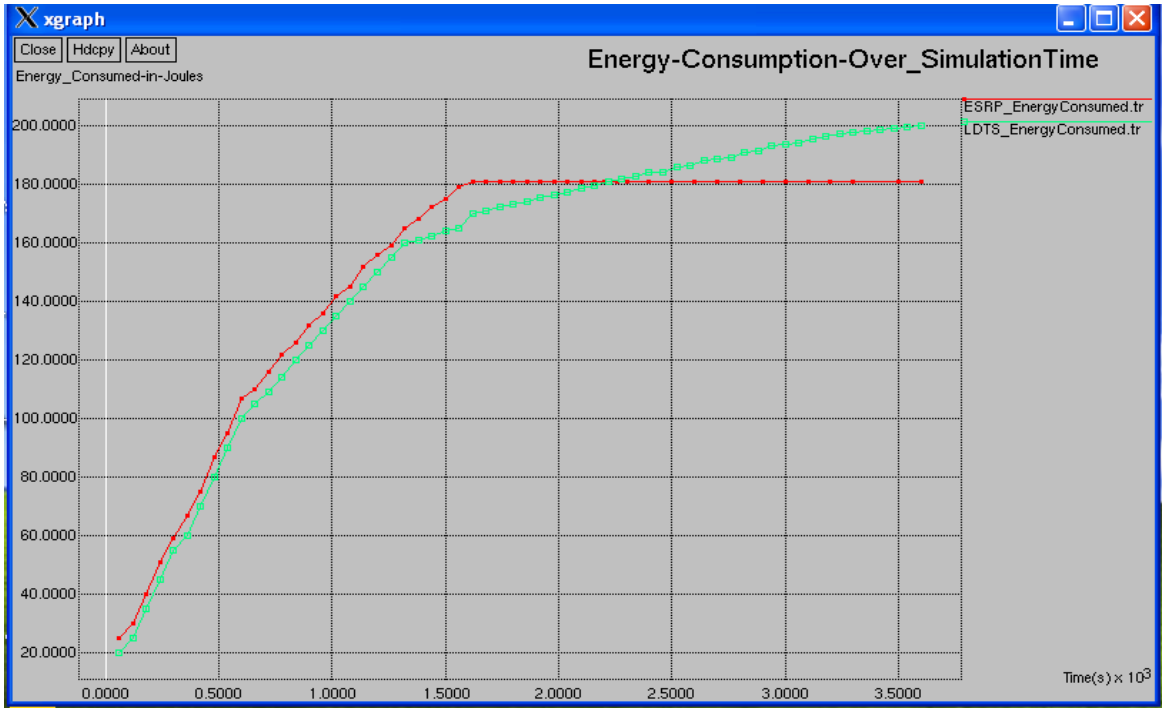

Fig. 9.Comparison Of ESRP Vs LDTS In Terms Of Energy Consumption

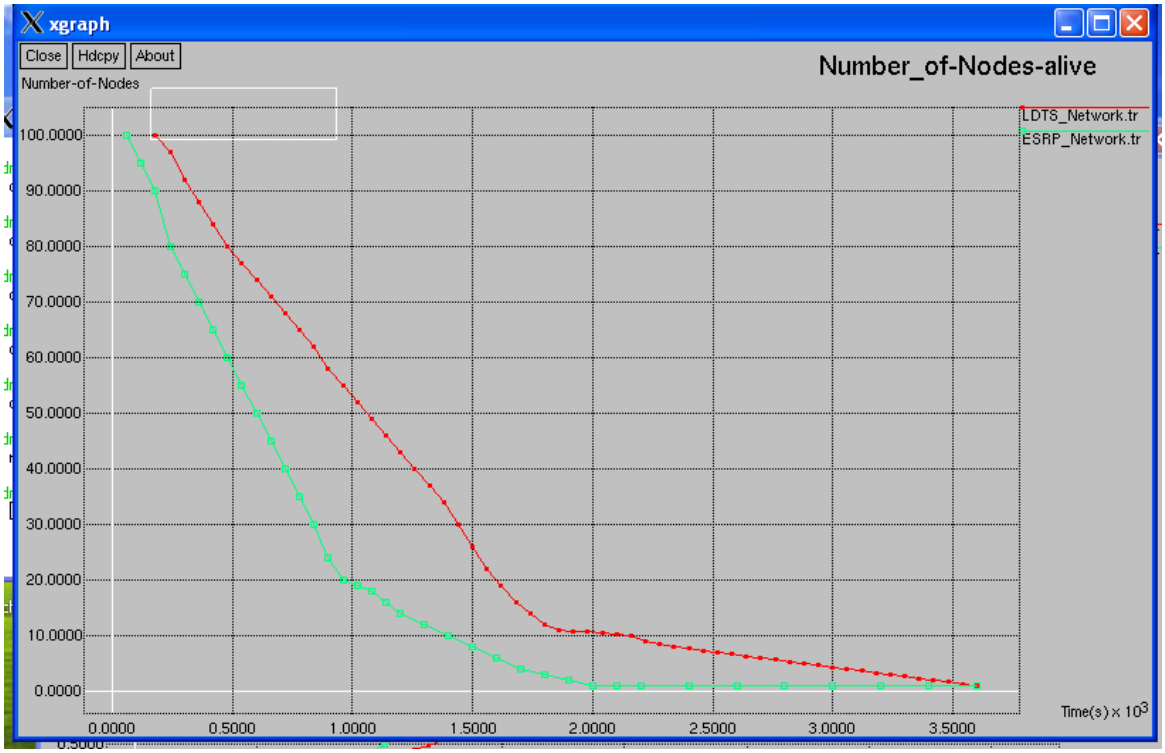

Fig. 10.Comparison Of ESRP Vs LDTS In Terms Number Of Nodes Alive

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

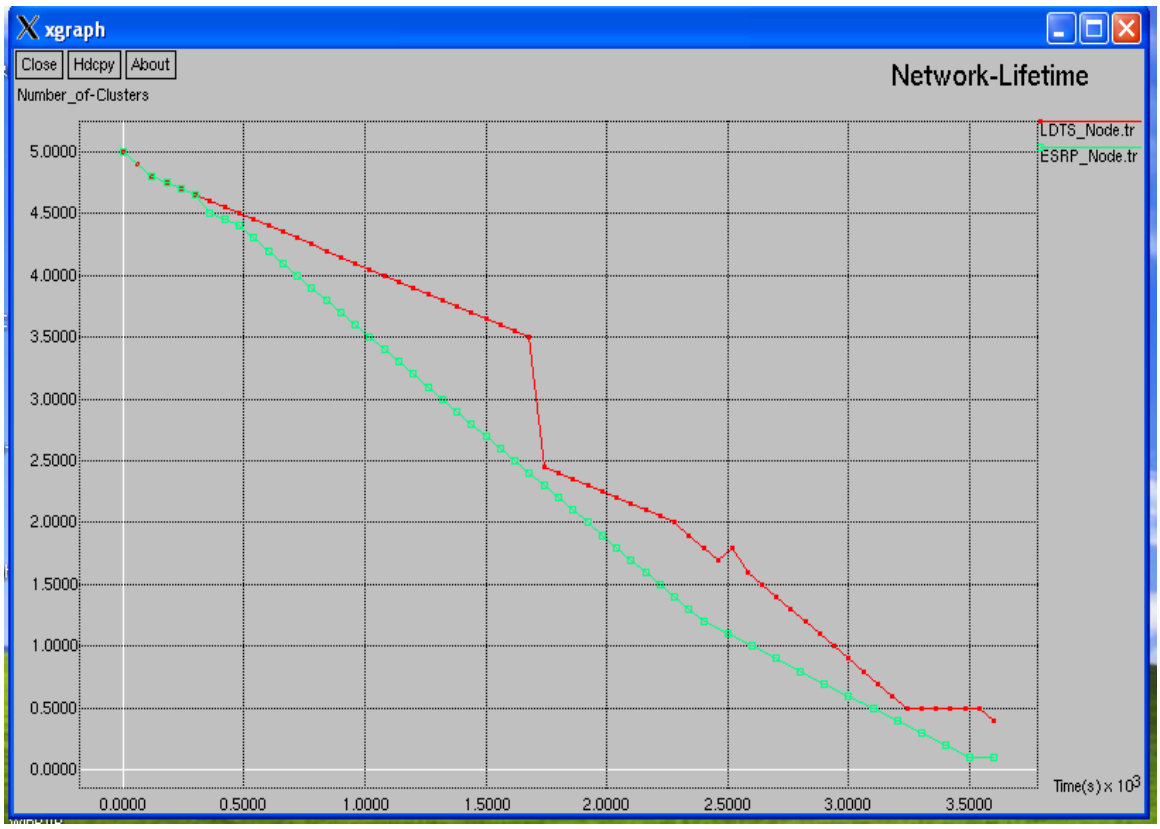

Fig. 11.Comparison Of ESRP Vs LDTS In Terms Of Network Life Time

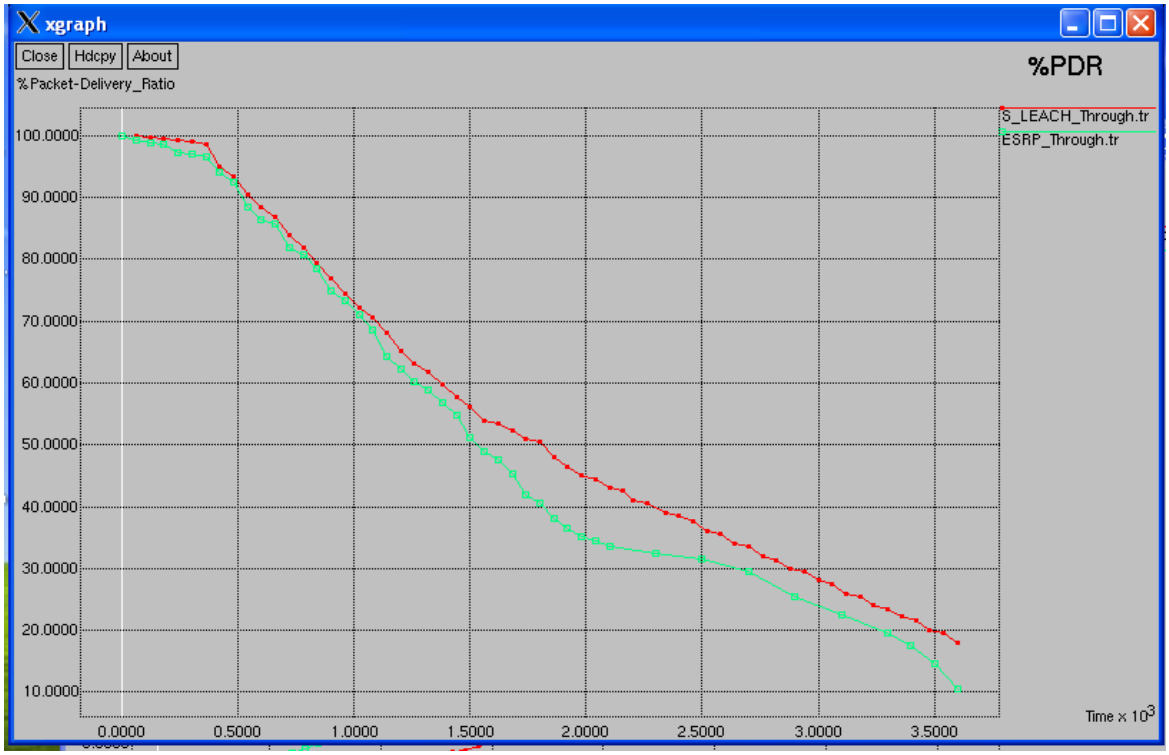

Fig. 12.Comparison Of ESRP Vs S-LEACH In Terms Of Percentage PDR

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

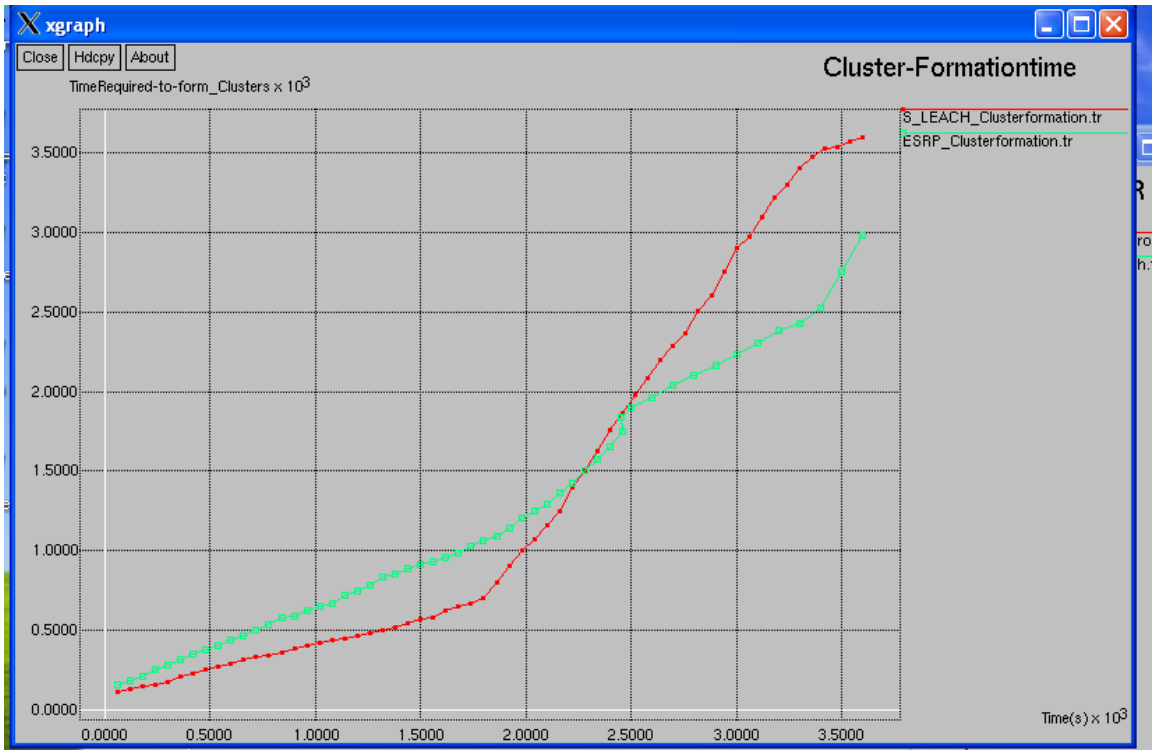

Fig. 13.Comparison Of ESRP Vs S-LEACH In Terms Of Cluster Formation Time

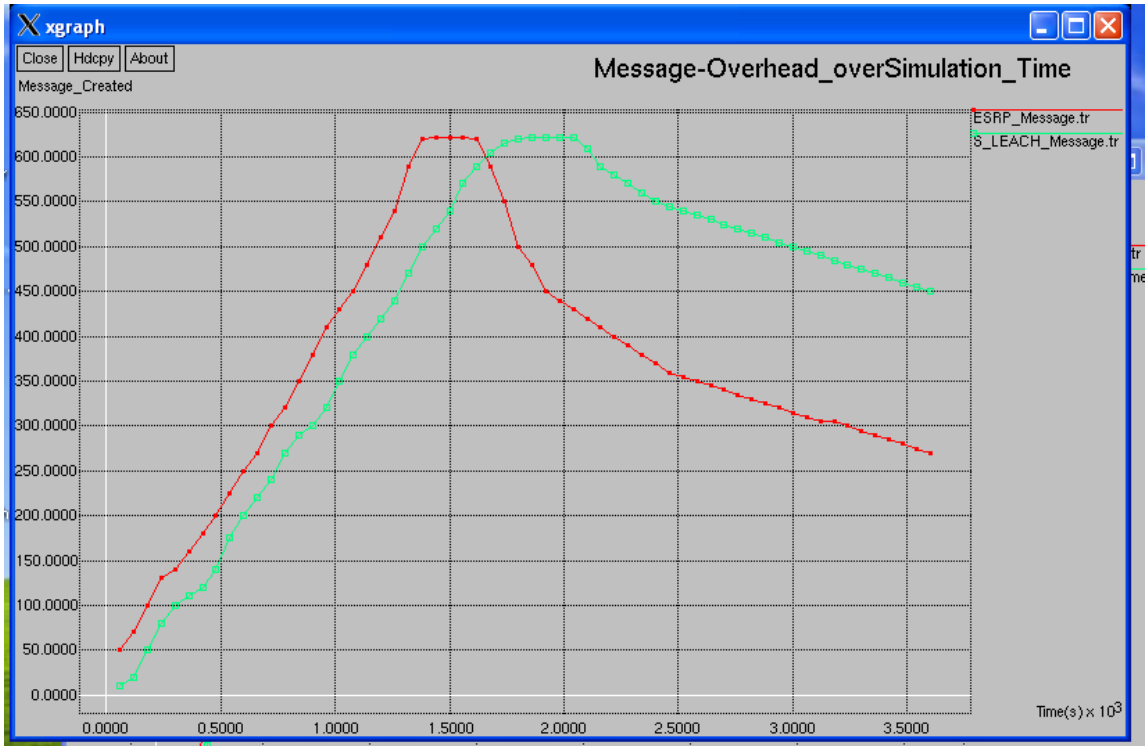

Fig. 14.Comparison Of ESRP Vs S-LEACH In Terms Of Message Overhead

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

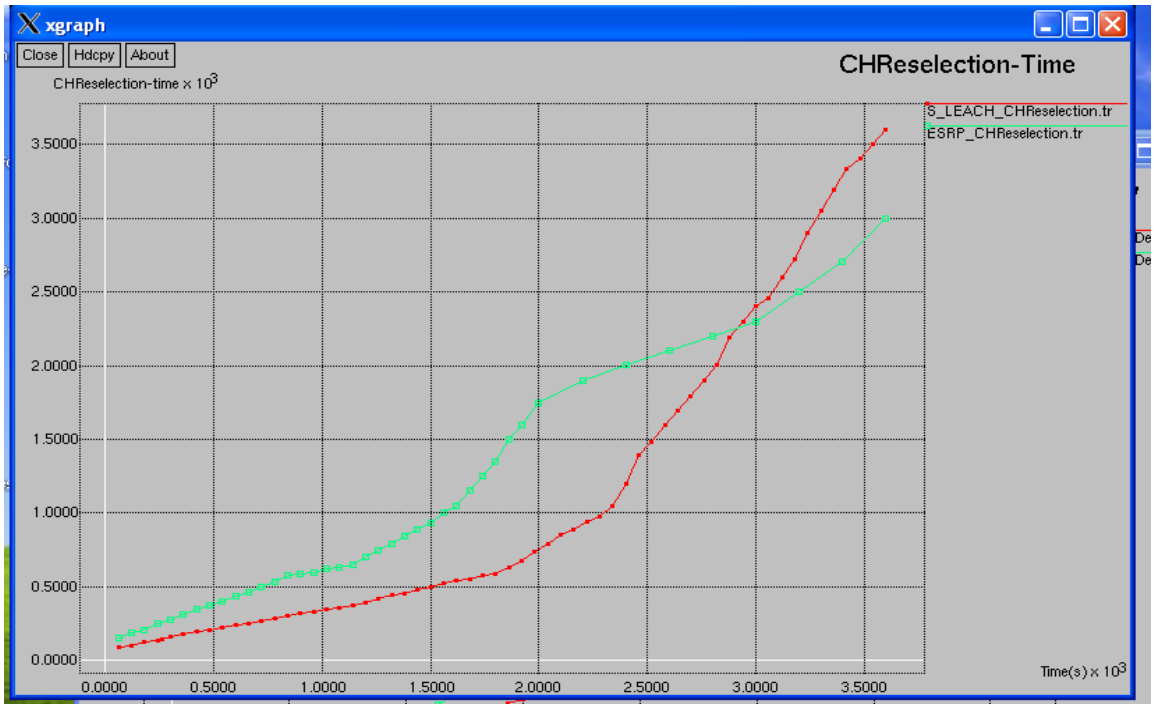

Fig. 15.Comparison Of ESRP Vs S-LEACH In Terms Of CH Reselection Time

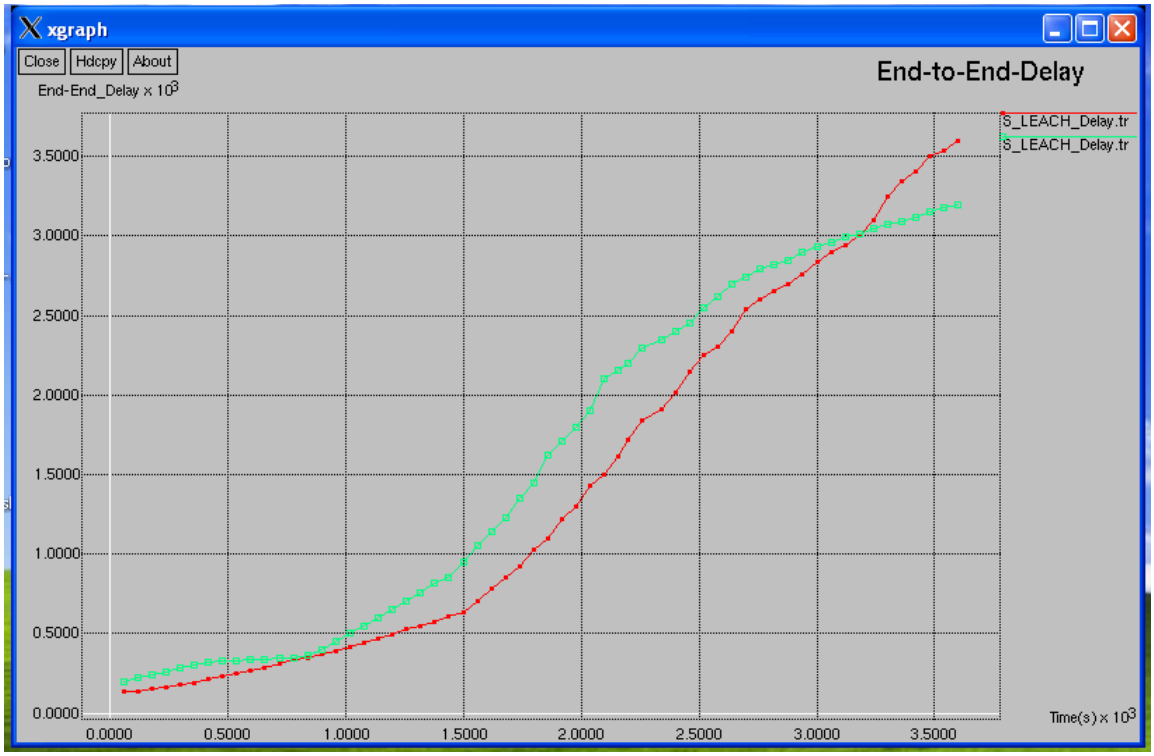

Fig. 16.Comparison Of ESRP Vs S-LEACH In Terms Of End To End Delay

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

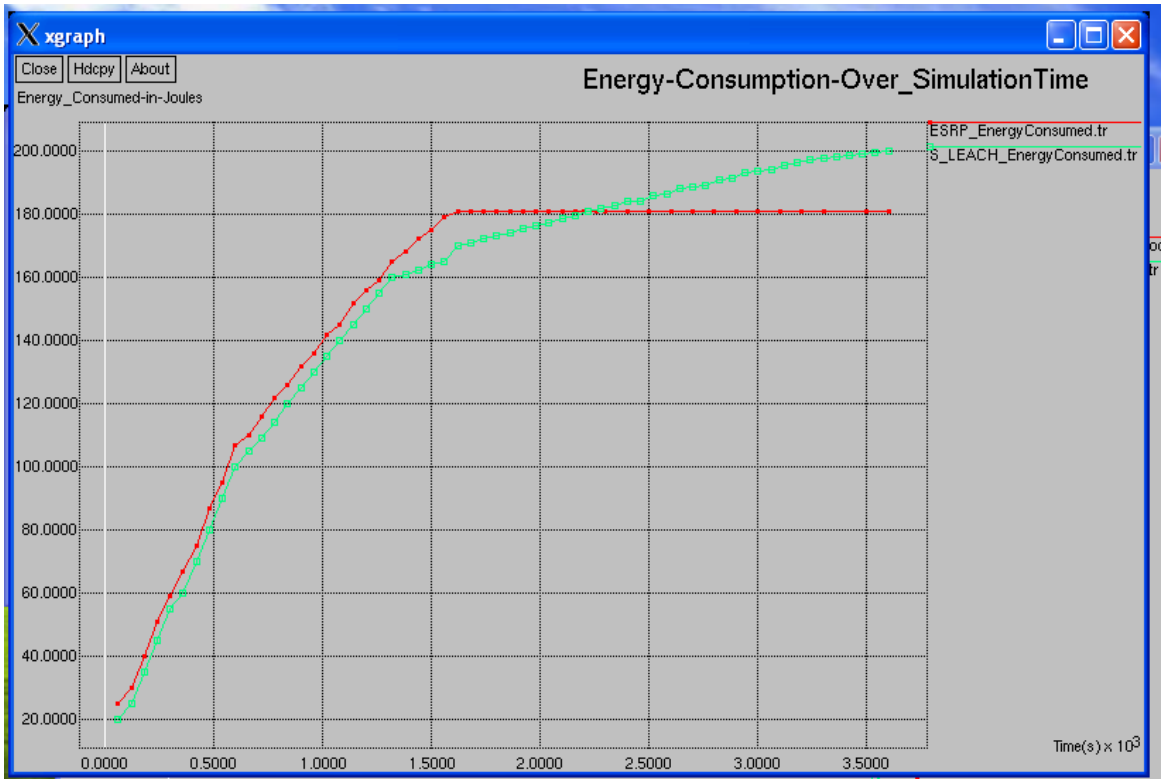

Fig. 17.Comparison Of ESRP Vs S-LEACH In Terms Of Energy Consumption

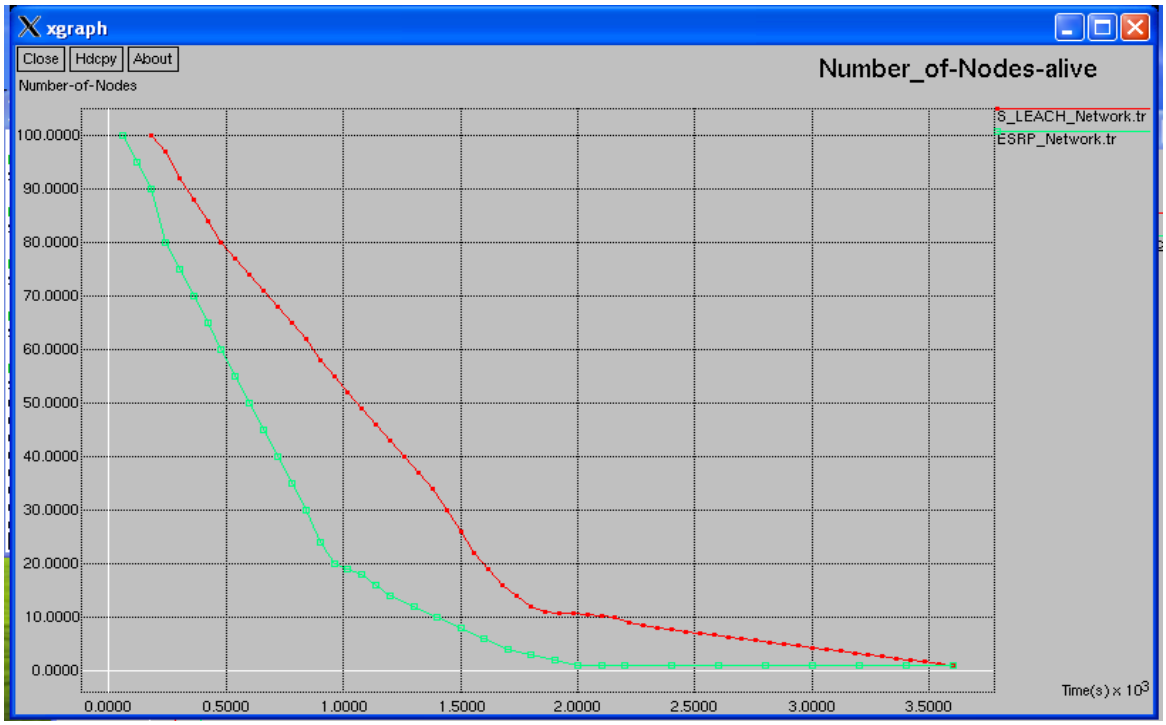

Fig. 18.Comparison Of ESRP Vs S-LEACH In Terms Of Number Of Nodes Alive

Journal of Theoretical and Applied Information Technology
20th November 2013. Vol. 57 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

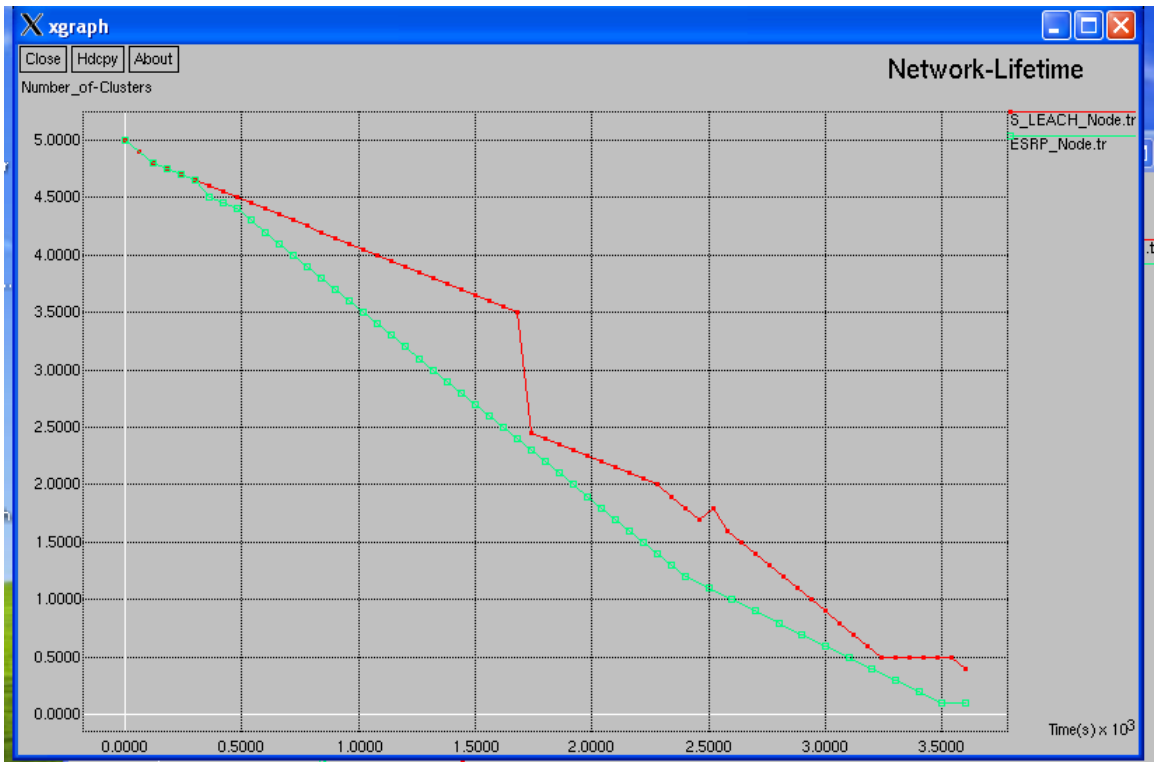

Fig. 19.Comparison of ESRP vs S-LEACH in terms of network life time

Table 2: Comparison Of Esrp With Ldts And S-Leach

Parameters for comparison	ESRP	LDTS	S-LEACH
Number of nodes alive over simulation period	Higher	Lower	Lower
Message overhead over simulation period	Lesser	More	More
Energy consumption over simulation period	Very less	Lesser	More
End to end delay	Lower	Lower	Lower
Percentage packet delivery ratio (PDR) over simulation period	Lower	Higher	Higher
Network life time over simulation period	Higher	Lower	Lower
Cluster formation duration over simulation period	Lower	Higher	Higher
Cluster head reselection time over simulation period	Lower	Higher	Higher