International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

Performance of Triple Umpiring System and its Enhancements in Wireless Sensor Networks

S.Ganesh[1], Dr. R. Amutha[2]
Research Scholar, Sathyabama University, Chennai-600 119, India,
Professor, Faculty of Electronics & Communication Engineering, SSN College of Engineering, Chennai-603110, India,
E-mail: [1]ganesh8461@gmail.com, [2]amuthar@ssn.edu.in

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 analyzed the performance of Triple Umpiring System and its enhancements to develop an Efficient and Secure Routing Protocol (ESRP) for WSN. Extensive investigation studies using Glomosim 2.03 simulator show that the proposed scheme helps to achieve balanced energy consumption and increases the throughput.

***Keywords*-- Wireless Sensor Networks, Triple Umpiring System, Routing Protocol, Energy Efficiency, Throughput enhancement, Glomosim.**

I. INTRODUCTION

Wireless sensor network applications include ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, and many military applications. An even wider spectrum of future applications is likely to follow, including the monitoring of highway traffic, pollution, wildfires, building security, water quality, and even people's heart rates. A major benefit of these systems is that they perform in-network processing to reduce large streams of raw data into useful aggregated information. Protecting it all is critical.

Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack. And third, sensor networks interact closely with their physical environments and with people, posing new security problems.

Consequently, existing security mechanisms are inadequate, and new ideas are needed. Fortunately, the new problems also inspire new research and represent an opportunity to properly address sensor network security from the start. 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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

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 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].In this paper, we investigate the performance of an Efficient and secure routing protocol through the improvements of Triple Umpiring System for WSN. We did a brief comparison of ESRP with Energy Efficient Sensor Routing (EESR) and LEACH, two of the popular routing protocols. 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. Simulation Results are presented in Section 4. We conclude this paper in Section 5.

II. RELATED WORK

Security is sometimes viewed as a standalone component of a system's architecture, where a separate module provides security. This separation is, however, usually a flawed approach to network security. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security must pervade every aspect of System design.

Sensor networks have also thrust privacy concerns to the forefront. The most obvious risk is that ubiquitous sensor technology might allow ill-intentioned individuals to deploy secret surveillance networks for spying on unaware victims. Employers might spy on their employees; shop owners might spy on customers; neighbors might spy on each other; and law enforcement agencies might spy on public places. This is certainly a valid concern; historically, as surveillance technology has become cheaper and more effective, it has increasingly been implicated in privacy abuses. Technology trends suggest the problem will only get worse with time. As devices get smaller, they will be easier to conceal; as devices get cheaper, surveillance networks will be more affordable. 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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

III. INTRODUCTION TO TRIPLE UMPIRING SYSTEM

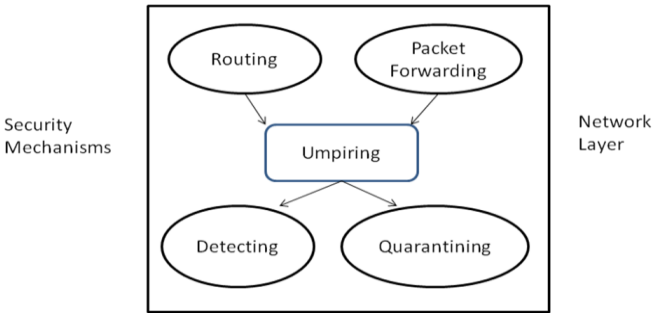

Figure1.Umpiring System

In the umpiring system [8]as shown in Fig.1 each node is issued with a token at the inception. The token consists of two fields: NodeID and status. NodeID is assumed to be unique and deemed to be beyond manipulation; status is a single bit flag. Initially the status bit is preset to zero indicating a green flag. The token with green flag is a permit issued to each node, which confers it the freedom to participate in all network activities. Each node in order to participate in any network activity, say Route Request RREQ, has to announce it's token. If status bit is "1" indicating "red flag" protocol does not allow the node to participate in any network activity. We investigate the Triple Umpiring System (TUS) for securing the Wireless Sensor Network from attacks from malicious nodes. It is assumed that the source and the destination node are not malicious.

3.1. Triple Umpiring System

The working of the Triple umpiring system is explained with reference to Fig.2. In Triple umpiring system, three umpires are used to identify and convict the guilty node. Three umpires in TUS are a node (next/previous immediate node) and two additional nodes is appointed as designated umpires i.e., Ui and Ui+1 are designated umpires for node Ni. Umpire Ui and Ui+1 are located so that they can overhear communication to Ni. Similarly Ni-1 and Ni+1 monitor the performance of Ni in the forward and reverse paths respectively. The decision can be made by all the 3 nodes involved: Ni-1 in its umpiring node in the forward path (Ni+1 in the reverse path) and Ui and Ui+1. The decision can be bound up an all of them auguring or any two of them auguring about the misbehavior of the node Ni.

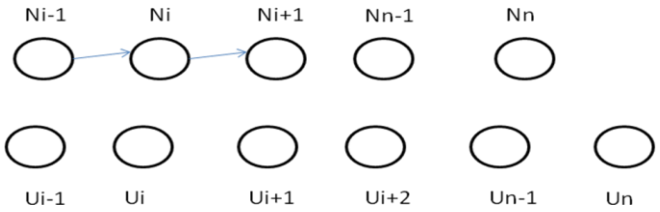

Figure2.Triple Umpiring System

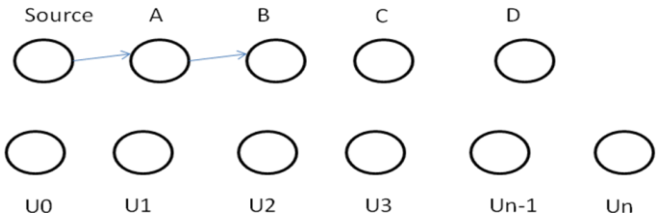

Figure3.Model of Triple Umpiring System

In the figure 3, umpire node U2 and U3 are designated umpires for node B. similarly node Un-1 and Un are designated umpires for the destination node D. Assume that node B is culprit in the Fig. 3. It is dropping the forwarded data packets given by node A. Now designate umpire node U2, U3 and node A can overheard B's transmission, the designated umpire immediately sends a M-ERROR message to the source and the status bit of culprit node is set to "1" – red flag using M-Flag message. In our system there is no change in the token – it can be used for the full lifetime of the node, if the node continuously behaves correctly. At the instance of the first offence the status of the guilty node is set to '1' preventing its further participation in the network. We assume that no node can alter its own status bit. Only the designated umpire corresponding to the forward or reverse path under consideration can change the status bit. For example the status bit of B in Fig.3 can be changed only by A in the forward path and only by C in the reverse path. It is also assumed that a node cannot announce wrongly its token particulars – NodeID and status bit.

3.2. Modified Triple Umpiring System

TUS can be modified [9] to enable path accumulation during the route discovery cycle. When the Route Request (RREQ) and Route Reply (RREP) messages are generated or forwarded by the nodes in the network, each node appends its own address on these route discovery messages. Each node also updates its routing table with all the information contained in the control messages.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

As the RREQ messages are broadcast, each intermediate node that does not have a route to the destination forwards the RREQ packet after appending its address in the packet. Hence, at any point the RREQ packet contains a list of all the nodes traversed. Whenever a node receives a RREQ packet, it updates the route to the source node. It then checks for intermediate nodes accumulated in the path. Before making an entry, we propose differentiation between the so-called 'good' neighbors and 'bad' neighbors. Classification is done dynamically based on the SNR (Signal to Noise Ratio) value that is measured whenever a packet that contains a TUS message is received. Neighbors are typically classified as 'bad' if the quality of the interconnecting channel is poor, i.e., it is not good enough to carry broadcast and unicast messages with sufficient quality regardless of transmission rate or coding technique. We also did a modification in TUS link breakage recovery mechanism. In TUS, the source node broadcasts RREQ message to find a new route to the destination when the link break is occurred. As an improvement of TUS, Self Recovery TUS takes the intermediate node, which detects the link break, to repair the break route. Once the intermediate node cannot repair the route in time, the backward pre-hop node tends to find a new route instead. TUS tends to repair break route if the broken node is near to the destination node. Otherwise, if the break node is far away from destination node, a RRER message is sent back to source node and the source node rebroadcast RREQ to find a new route. Unlike TUS [10], Self Recovery TUS can repair break route without considering the distance between the broken node and the destination node. Because of the intermediate nodes are usually nearer than the source node to the destination, the intermediate nodes on the data flow are more suitable than the source to broadcast RREQ to repair or find a route to destination. Based on this idea, the Self Recovery TUS algorithm improved the TUS algorithm by adopting intermediate nodes instead of the source to repair a route to destination. In the worst situation, each intermediate node cannot repair the break in the link and cannot find a new route to the destination. Then, the source node will receive a RR message. In this case, Self Recovery TUS and TUS have the same operations. The source broadcasts a RREQ message to find a new route to the destination.

3.3. MTUS with optimal SNR based power control

In wireless signal Transmission, one of the major sources of loss is attenuation. Basically the communication range decreases as the transmission data rate increases.

One of the important parameter of interest is BER (Bit Error Rate). The desirable BER value can be mapped in to a desirable SNR value for a given modulation scheme. The desirable SNR value required by a given data rate increases with the data rate [11]. That is, if data rate increases, the probability of error also increases and a higher SNR value is required at the transmitter to achieve the same BER at the receiver. Hence power supply increases with the SNR value.

The relation between transmit power P_S and the SNR value at the receiver ($SNR_{Rx)\ is}$ given by

$$\mathbf{SNR_{Rx} = \frac{P_S \ .A}{N}} \qquad \mathbf{(1)}$$

Where 'A' is the channel attenuation factor including antenna gain in transmission.

The noise power 'N' can be expressed as

$$\mathbf{N = N_0 . R_S} \qquad \mathbf{(2)}$$

N_0 is the noise power density .The transmission symbol rate is given by

$$\mathbf{R_S = R / b} \qquad \mathbf{(3)}$$

Where 'R' is the transmission rate and 'b' is the modulation constellation size.

$$\mathbf{SNR_{Rx} = \frac{E_b}{N_0} . \ b} \qquad \mathbf{(4)}$$

Where 'E_b' is Energy per bit $\mathbf{E_b = P_S * T_b}$ **(5)**

The transmission time of each bit $\mathbf{T_b = 1/ R}$ **(6)**

Hence the optimal transmission in terms of specific desirable BER at the receiver end can be expressed as :

$$\mathbf{P_S = SNR_{Rx} . N . \frac{1}{A}} \qquad \mathbf{(7)}$$

$$\mathbf{P_S = \frac{SNR_{Rx} . R_S . N_0}{A}} \qquad (8)$$

$$\mathbf{P_S = \frac{R_S . b \ \frac{N_0}{A} \ \frac{E_b}{N_0}}{}} \qquad \mathbf{(9)}$$

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

Where the factor 'A' is the product of antenna gain and channel loss.

$$A = K * L^{-1} \quad (10)$$

The relationship between BER and SNR for QPSK (Quadrature Phase Shift Keying) is given by

$$BER = \tfrac{1}{2}\, erfc \sqrt{E_b / N_0} \quad (11)$$

Hence the ratio E_b / N_0 can be calculated from BER.

$$\frac{E_b}{N_0} = [\, erfc^{-1}(2 . BER)\,]^2 \quad (12)$$

From Equ (9)

$$P_S = R_S . b . (N_0 / A) [\, erfc^{-1}(2 . BER)\,]^2 \quad (13)$$

The signal strength at the receiver can be calculated as follows: In a receiver, this concept involves the following parameters:

Minimum Detectable Signal power (MDS): dependent on the modulation type as well as the noise specs of the antenna and receiver.

Maximum Allowable Signal power (MAS): limited by the compression or third-order intercept points.

Minimum Detectable Signal (MDS): For a given receiver noise power, MDS determines the minimum signal-to-noise ratio at the output of the receiver (SNRo). Typical minimum SNR for QPSK with $P_e = 10^{-5}$ is 10 dB .

$$S_{imin} = KT_0FB(S_0/N_0)_{min} \quad (14)$$

In dB

$$S_{imin}\,(dBm) = -174 + B_{(dBHz)} + F(dB) + (S_0 / N_0)_{min\ dB} \quad (15)$$

Where 'K' is the Boltzmann constant, 'F' is the receiver noise Figure, B is the receiver bandwidth, and $T_0 = 290$ K.

The Receiver Dynamic range (DR_r) can be calculated as

$$DR_r = MAS / MDS \quad (16)$$

The measured receiver signal strength (aggregated value) can be fed back in the beacon message to let the transmitter to know the received signal strength. Based on the receiver feedback, the transmitter either increases or decreases the transmit power P_S there by achieving optimal power reduction.

3.4. ESRP with Two level Intrusion Detection Mechanism ESRP-TLIDM

Efficient and Secure Routing Protocol through two level intrusion detection mechanisms (ESRP–TLIDM) will detects the intruders at the first level as shown in Figure. 4**.** The first level detection is based on the well established Triple Umpiring System and its subsequent modification for WSN. The structure of a data packet is shown in Figure 5 Once the initial intruders have been identified, we forwarded the data packets since the route has been established as shown in Figure 6. We used Modified Triple Umpiring System (MTUS) as the routing protocol to find the shortest path between the sensor node and the sink. We used Cluster based data forwarding. For clustering various parameters has been taken into consideration . In this work, we have utilized the most popular clustering mechanism LEACH along with LEACH-C has taken residual energy level of the nodes for cluster head selection for creating clusters.

Fig. 5 Structure of data packet

Source address	Destination address	Recorded path	Hop count	Status bit	Original/ Dummy packet

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

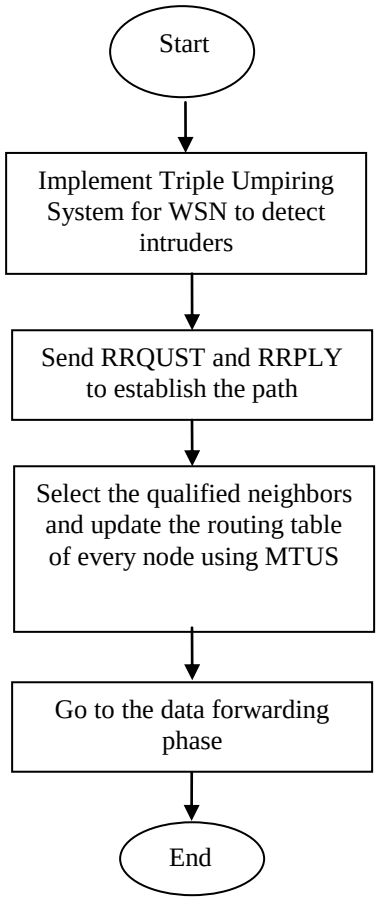

Fig. 4 Flow chart of ESRP-TLIDM Level 1

It has been achieved by setting the probability of a node, becoming a Cluster Head (CH) as a function of a nodes energy level relative to the aggregate energy remaining in the network rather than purely as a function of the number of times the node has been cluster-head:

$$P_i(t) = E_i(t) * k / E_{total}(t) \quad (17)$$

Where $E_i(t)$ is the current energy of node *i*, and

$$E_{total}(t) = \sum_{i=1}^{N} E_i(t) \quad (18)$$

The Current CH (CCH) creates the dummy packet while forwarding the data as shown in Figure 5, only when the SNR value is above the specified threshold value. For SNR threshold calculation, we proposed a method in Figure 6 shows the data forwarding phase and the flowchart for second level intrusion detection is shown in Figure 7.

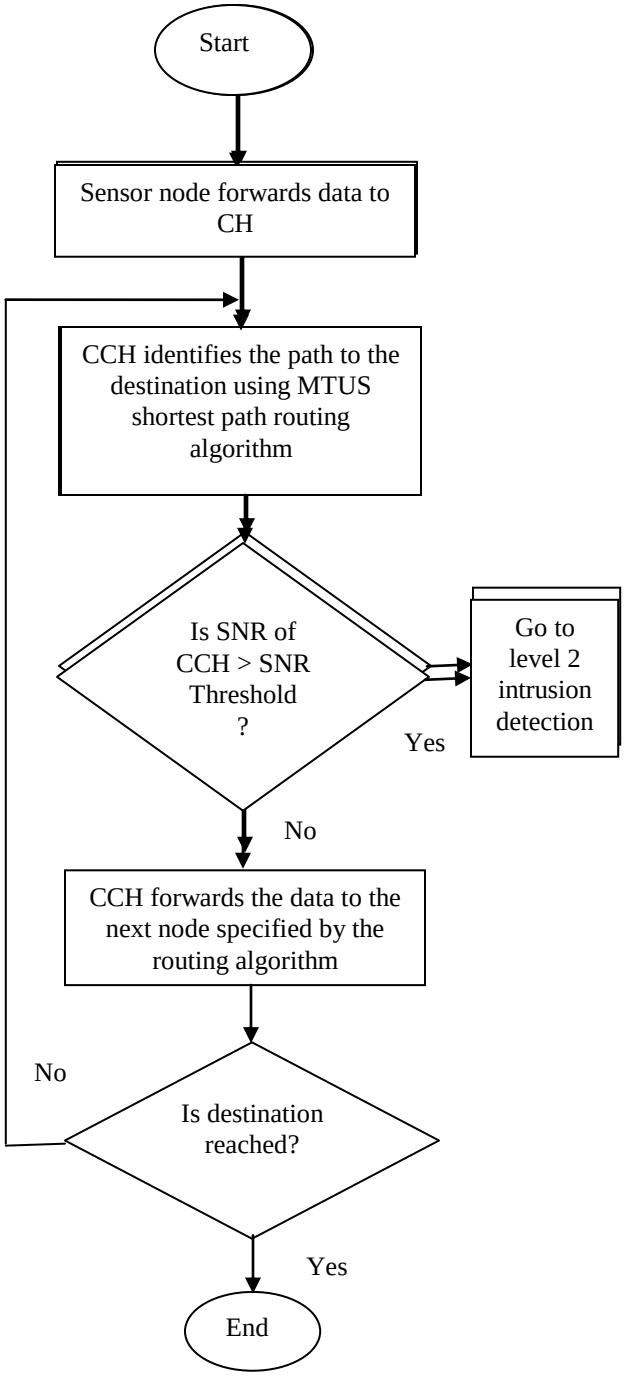

Fig. 6 Flow chart of data forwarding phase

In figure 5 ,the status bit is set to '1' after the first level of intrusion detection if found intruder.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

In the proposed protocol, every node can find whether the packet is original or dummy packet using the field 'original/dummy packet'. If this field is set to '1', then the packet will be dummy packet. This information will be used by every node when it becomes a CH and forwards the original and dummy packets accordingly.

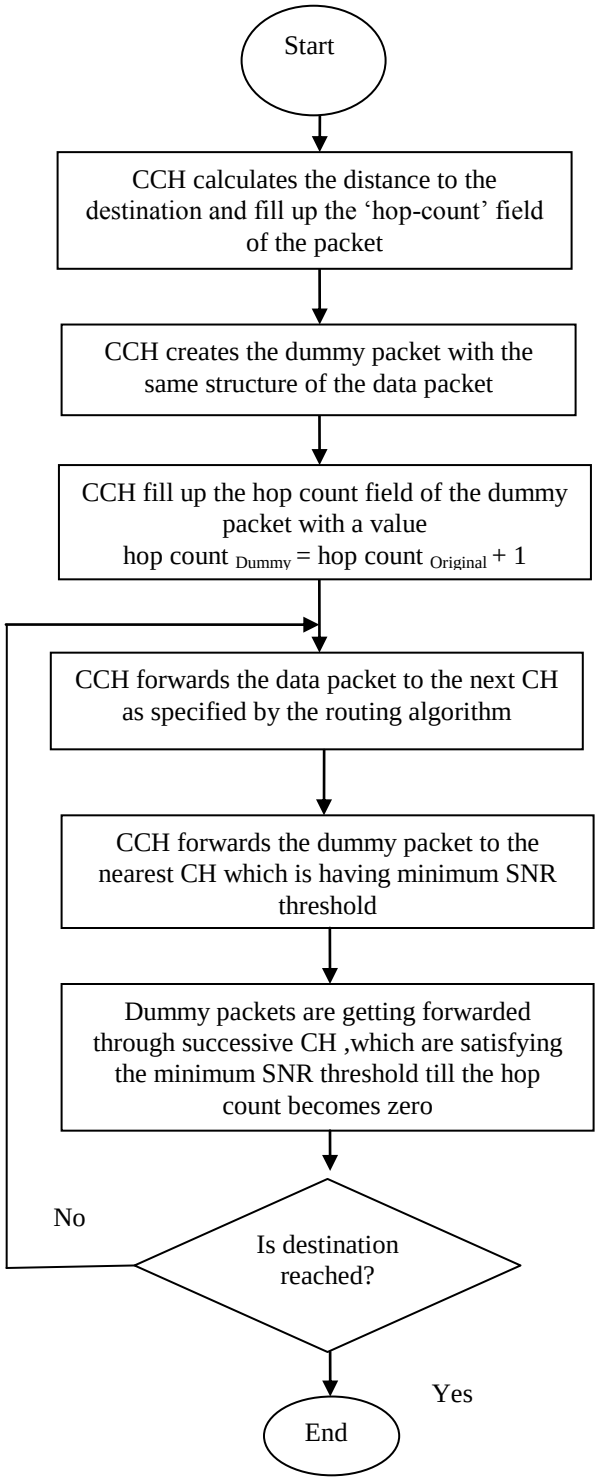

Fig. 7 Flow chart of ESRP-TLIDM Level 2

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

IV. Simulation Results

We use a simulation model based on Glomosim-2.03 in our evaluation. Our performance evaluations are based on the simulations of 500 wireless sensor nodes that form a wireless sensor network over a rectangular (1000 X 1000 m) flat space. The MAC layer protocol used in the simulations was the Distributed Coordination Function (DCF) of IEEE 802.11. The performance setting parameters are given in Table 1.

TABLE 1
Simulation Parameters

Area of sensing field	1000 *1000 m
Number of sensor nodes	500
Simulation Time	600 s
Frequency	2.4 GHz
Bandwidth	2Mbps
Traffic Type	Constant Bit rate (CBR)
Payload Size	30 to 70 Bytes
Number of Loads	200 Packets
Number of Nodes	500 nodes
Propagation Limit (dbm)	-111.0
Path loss model	Two ray model
Location of the BS	(50, 75)
Number of clusters	20
Initial energy of nodes	2J
Antenna Type	Omni directional
Channel Bandwidth	20Kbps
Routing Protocol	AODV based MTUS
MAC layer protocol	IEEE 802.11

We compared our ESRP-TLIDM with two different transmission power levels based on the following output parameters:

1.Packet Delivery Ratio

It is the ratio of the number of data packets successfully delivered to the destinations to those generated by the sources.

PDR = *Nr/Nt.*

Where *Nr* is the number of data packets successfully received and *Nt* is the number of data packets transmitted

2. End to End Delay (Seconds)

It indicates the time taken for the message to reach from source to destination.

3. Energy Consumption in mWH.

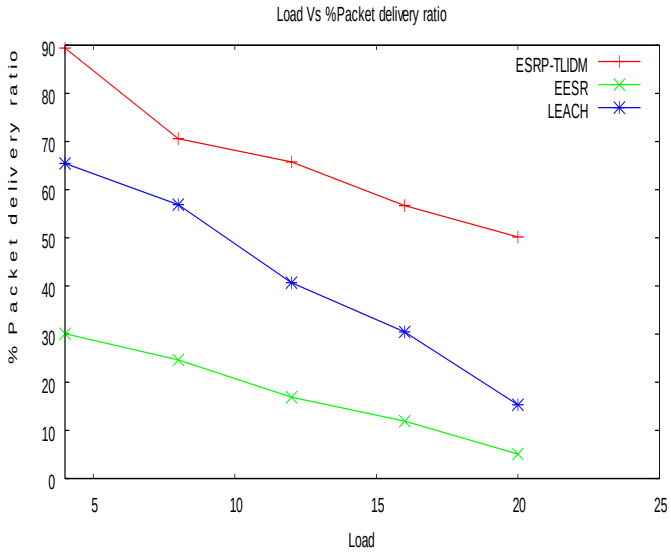

Fig. 8. Load Vs %Packet delivery ratio

As shown in Figure 8, the packet delivery ratio decreases as the load increases, but ESRP-TLIDM still can maintains appreciable % packet delivery ratio as compared to EESR and LEACH.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

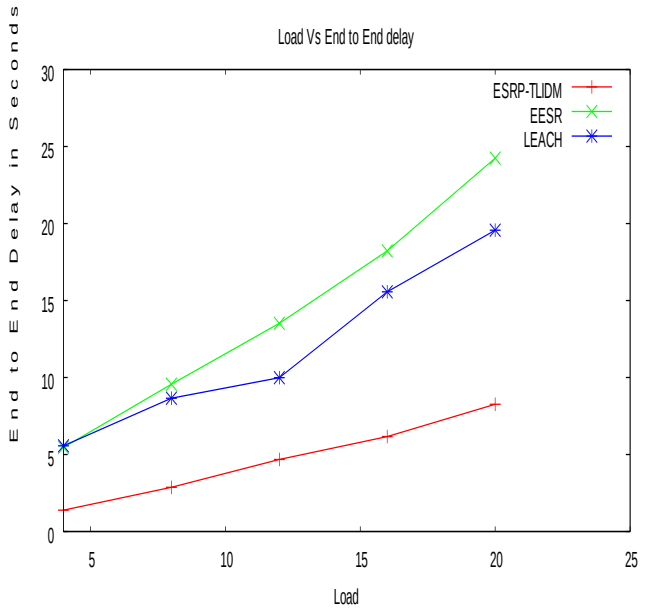

Fig. 9. Load Vs End to end Delay

Figure 9, shows that the end to end delay increases when load increases and even though it is small in ESRP-TLIDM, it is considerable in the case of real time applications. Figure 10, shows that there is a considerable power reduction in ESRP-TLIDM as compared to the other two protocols This justifies our trade off between energy reduction and increased delay.

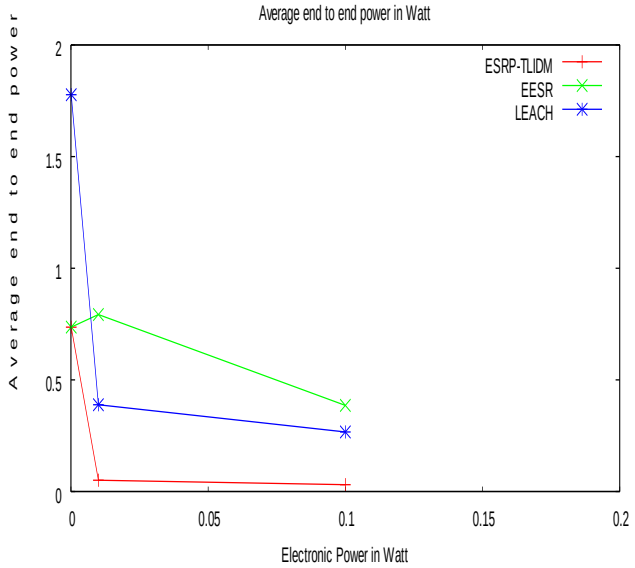

Fig. 10.Average end to end power in Watt

V. CONCLUSIONS

WSN is vulnerable to various attacks [12] 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 through the enhancement of triple umpiring system for WSN. 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-TLIDM 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 [13] 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 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 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 ComputerScience,PurdueUniversity,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] 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.

[9] 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

[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] 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

[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.