Reliable Energy efficient Protocol for searching optimal path using Cuckoo Search algorithm

[1]D.Sivakumar, [2]J.Jegan, [3]Dr.S.Selvakumar
[1] [2]Research Scholar, Manonmaniam Sundaranar University, Tirunelveli, India &Assistant Professor
Kings College of Engineering, Pudukkottai, India
[3]Associate Professor, Annamalai University, Chidambaram, India

Abstract: Numbers of sensor nodes are fixed to form the wireless sensor network and the monitor information's are sending to the centralized node called sink. Compared to the wired network, the WSN is more vulnerable to hack the information. More number of protocols was proposed to provide the security for the safe data transmission. These issues need to be resolved in order to gain an improved focus of researchers and users to deploy the features of WSN often. The most critical task in the WSN is data transmission which cannot be done securely and reliably due to improper route existence. Thus the focus on the better route discovery can resolve these issues in the optimized way. In this paper, the wormhole attack is to be considered, and proposed the new routing protocol to find the optimized route and protect the data from wormhole attack. The new protocol cuckoo Reliability aware energy and trust based routing protocol CRETRP is proposed to solve the issues in existing protocols. This method focus improving the network performance in terms of clustering the group of similar nodes for which optimized cluster head would be selected using the modified genetic algorithm. So that data transmission can be optimized. At the time of route establishment, reliability of the nodes also considered with the trust and energy consumption factor. In the proposed research work, cuckoo search Algorithm is used for trust and reliability aware route establishment. After route establishment, worm whole attacks are discovered using expected packet transmission count value. The experimental evaluation of this research work is conducted in the NS2 simulation environment from which it is proved that the proposed research work can provide an improved security.

Keywords: attack, energy, reliability

I. INTRODUCTION

A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or pre-determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out Simple computations and transmit only the required and partially processed data.The above described features ensure a wide range of applications for sensor networks. Some of the application areas are health, military, and security. For example, the physiological data about a patient can be monitored remotely by a doctor. While this is more convenient for the patient, it also allows the doctor to better understand the patient's current condition. Sensor networks can also be used to detect foreign chemical agents in the air and the water. They can help to identify the type, concentration, and location of pollutants. In essence, sensor networks will provide the end user with intelligence and a better understanding of the environment. We envision that, in future, wireless sensor networks will be an integral part of our lives, more so than the present-day personal computers.

Now a day, in the wireless communication networks field the topic of trust and statue will be applied to observe the different kind of characters of sensor nodes and counter node unwanted steps. Trust is a novel method to given that the security without the help of cryptography methods [1]. In the wireless communication network field the trust can be described as amount of dependability of another nodes to perform the process [2]. In the trust method, based on the previous information the upcoming process can be predicted and help to take the efficient resolution for identification of suspicious nodes characteristics. Additionally, this trust based methods are appropriately for the security planning of sensor network [3].

Many number of trust based and power constrained secure routing protocol has been introduced by the scientist [4], [5], [6] to counter node fault process. On the other hand, the results cannot be applied to the wireless sensor networks directly owing to the restricted possessions on part of sensor nodes.

In this present work, for the wireless sensor network the new method is developed to give the security and dependable trust based power consumption routing protocols. The following steps are used to get the secured protocol transmission with more dependability, power utilization and trust value for this structure.

Cluster head decides the successful transmission of the data points across various data nodes. The optimal cluster head selection is done using the algorithm called the modified genetic algorithm. The constraints considered for the cluster head selection are energy, trust value and its reliability.

Better route establishment is done for performing the successful data transmission which is done in this work using the methodology called the cuckoo search Algorithm which will establish the route where the nodes involved should ensure the high level trust value, reliability and enough energy resource.

After route establishment, the data transmission is secured in run time by preventing the worm whole attack which might lead the data packets to the malicious nodes. This is done via calculating the expected packet transmission count value.

The entire process of this proposed work is given as follows: To get the optimal route establishment by using the different parameter has been conducted in a variety of research work. This process is discussed in Section 2.The overall process is explained in detailed manner in Section 3. The experimental appraisal of the present work is explained in section 4. At last, the conclusion with the advantages and disadvantages of the proposed work is described in detailed manner in section 5.

II. RELATED WORKS

Kong, et al. [3] have studied denial-of-service (DoS) attacks (including wormhole attacks) on underwater sensor networks. Because these networks typically use acoustic methods to propagate messages, the detection techniques cannot be applied directly to wireless sensor networks.

Hu and Evans [2] have attempted to detect wormholes by equipping network nodes with directional antennas so they can all have the same orientation. Lazos and Poovendran [8] have applied a similar idea in their secure localization scheme called SeRLoc. SeRLoc employs about 400 anchor nodes (called “beacon nodes”) in a 5,000-node network. Each anchor node has a directional antenna and knows its physical location. Other nodes in the network use anchor nodes to locate themselves. Since a wormhole produces shortcuts in a network, the directional antennas deployed at anchor nodes help detect the attack; nodes can then defend against the attack by discarding incorrect localization messages. However, SeRLoc is unable to detect wormhole attacks when anchor nodes are compromised, especially nodes located near one of the ends of a wormhole.

To estimate the dependability of the sensor nodes in MANET the researcher [1] was implemented a dynamic trust prediction method. This method is based on the chronological characteristics. The direct simple path is chosen by using the Trust-based Source Routing protocol (TSR) for the transfer of data packets. In this present work, the analysis process show that this prediction method is improving the delivery ratio of the packet and decreasing the average end-end delay. To identify the black hole attacks the researchers [4] recommended a Grade Trust routing protocol. The Grade Trust protocol improving the packet delivery ratio by compared to the existing protocols like On-demand Distance Vector (AODV) and Fisheye State Routing (FSR)protocol.

To calculate the trust value of the mobile nodes the researchers [5] introduced a trust based routing mechanism. The unwanted nodes were prohibited to calculate the path with the utmost path trust. For implementing a secure route, the novel Optimized Link State Routing Protocol (OLSR) was integrated. This work has been done in simulation process and the outcome is proved that the new FPNT-OLSR created optimal packet delivery ratio, overhead values and the average latency than the existing OLSR method. The path with more number of trusted nodes was selected using the AODV protocol. Instead of choosing the shortest path, the proposed protocol chose the trusted path for transferring the packets. Experimental study proved that the proposed protocol leads to reduce packet drop.

To evaluate the trust level between the sensor nodes, the researchers [5] recommended a trust based QoS model. This QoS model generating a tradeoff between the trust level and connection delay. The new routing algorithm generating a better average end to end delay, overhead, delivery ratio of the packetcompared to the existing Watchdog-Dynamic Source Routing (DSR) and QAODV. In the next section detailed discussion of the proposed research framework is given with the clear explanation and the required example scenario.

III. PROPOSED METHODOLGY

Wormhole attacks can destabilize or disable wireless sensor networks. In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wired or wireless link with less latency than the network links, and relays them to another point in the network. This paper describes secured reliable trust based routing and wormhole attack detection.

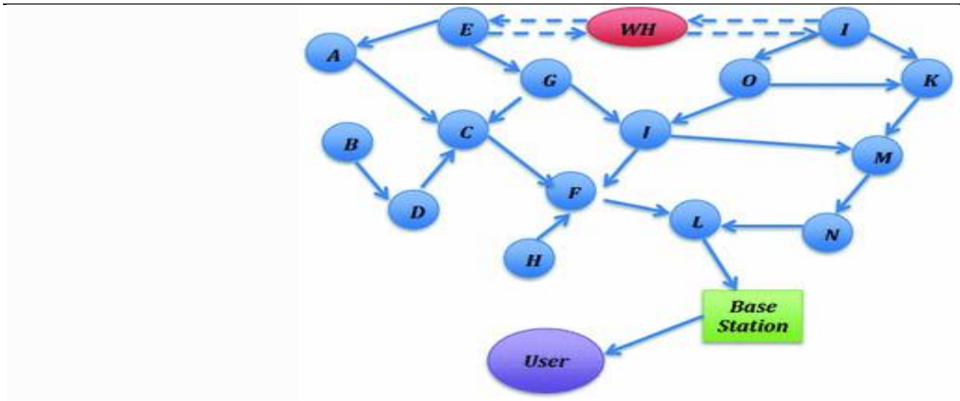

Figure1: wormhole attack

3.1 Cuckoo Reliability aware energy and trust based routing protocol

The cuckoo bird is put down their eggs in some other crowed bird nest after estimating the host bird's nest. This estimation process is done based on the colors and features of the eggs of a particular selected other bird. It decreases the probability of the eggs being discarded and, consequently, improves the re-productivity scrounging cuckoos habitually select a nest where the other bird putdown their own eggs. The cuckoo eggs produce the eggs before the host eggs. When the baby cuckoo bird is hatched, the initial process is to throw out the host eggs by propelling the eggs out of the nest. After this process, the baby cuckoo bird gets the chance to take the food provided by its host bird.

The name of Wireless Sensor Networks (WSN) is Wireless Sensor and Actuator Networks (WSAN). In this network are circulated to the independent sensor to observe corporal or ecological conditions like sound, pressure and temperature and so on. The Routing method is used to choose the greatest path in the wireless sensor network. In the previous method, the routing is used to forwarding network traffic in the middle of the networks. On the other hand, concluding function is improved the forwarding function. Routing process is common for the different types of wireless sensor network such as electronic data networks (internet), transportation network and telephone networks (circuit switching). This structure performs following actions to achieve the secured transmission of protocols with more reliability, energy consumption and trust value.

Cluster head decides the successful transmission of the data points across various data nodes. The optimal cluster head selection is done using the algorithm called the modified genetic algorithm. The constraints considered for the cluster head selection are energy, trust value and its reliability

Better route establishment is done for performing the successful data transmission which is done in this work using the methodology called the cuckoo search Algorithm which will establish the route where the nodes involved should ensure the high level trust value, reliability and enough energy resource

After route establishment, the data transmission is secured in run time by preventing the worm hole attack which might lead the data packets to the malicious nodes. This is done via calculating the expected packet transmission count value

The entire process of secured and reliable data transmission is illustrated in Figure 1 and this process is decreasing the data loss and achieves the packet transmission. In the following subsection, the overall process is described in detail.

To detect the fault movement of the sensor nodes by using the topic of trust in this present work. The identification of the trusted nodes and the congestion positions are calculated correspondingly. The fault nodes having the trust value and this is not used by the data packet routing process, owing to the some nodes this congestion metric process is not calculated. This process makes a lessening in the computation overhead and by this means enhances battery life time. By using the three trust metrics such as remaining node energy (N¢*e*), packet transmission ratio (P¢TR) and packet latency ratio (P¢L), the trust value of the sensor node is estimated. Scientifically, equation (1) is used to estimate the net trust of node *i* leading node *j* as follows:

$$\mathrm{T_{ij}} = \frac{\mathrm{A_1 * N_e' + A_2 * P_{TR}' + A_3 * P_L'}}{\mathrm{A_1 + A_2 + A_3}} \qquad (1)$$

The overall flow of the research work is given in the following diagram

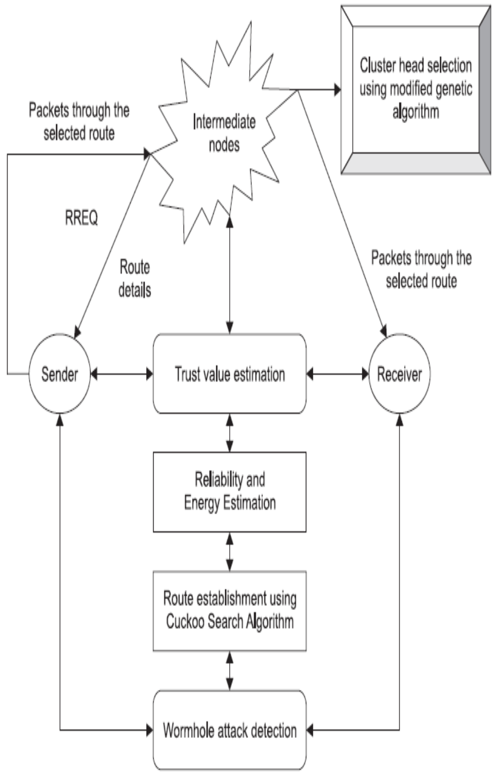
Packets through the selected route
Intermediate nodes
Cluster head selection using modified genetic algorithm
RREQ
Route details
Packets through the selected route
Sender
Trust value estimation
Receiver
Reliability and Energy Estimation
Route establishment using Cuckoo Search Algorithm
Wormhole attack detection

Figure 2: overview of the proposed research work

In the above equation, A1, A2 and A3 are represented as the analogous weights used for N¢*e*.The congestion status of a suitable node is calculated by using the parameter. This process is called Congestion Index. Consider each and every sensor nodes manage a queue to store the data packets in its buffer. Sequentially, the data packets are transferred from one node to the next node and automatically the storage space of the buffer is cleared and the data packets are waiting in the queue to leave the empty buffer space of the sensor node. Compared to the packet transmission rate, the packet received rate is higher means, the queue length, buffer overflow and congestion status of the sensor nodes are also increased. Suppose, the node is not moving to the next stage from the queue means then the particular node waiting in the pre-defined cycles in some amount of time (WCmax) and maintain the packets in every cycle in anticipation of the packets are lastly dropped. It means, at the finishing stage of WCmax cycles. The following equation is used to calculate the congestion index of the *k*th node.

$$\mathrm{CI_k} = \frac{\bar{\mathrm{r}}^{\mathrm{k}}_{\mathrm{in}} + \mathrm{Q^k(c-1)} - \bar{\mathrm{r}}^{\mathrm{k}}_{\mathrm{out}}}{\bar{\mathrm{r}}^{\mathrm{k}}_{\mathrm{in}} + \mathrm{Q^k(c-1)}} \qquad (2)$$

3.2 Wormhole Attack Detection

Worm hole attack is malicious threat in which additional malicious route would be established which will redirect the path of packet flow which might cause the information loss. This problem is resolved in the existing work by introducing the distributed worm hole detection algorithm. The entire process is explained in the following points:

To give the protected communication among the sender and the receiver encryption based data transmission is completed. That is All the valid nodes in the environment should register with the public server before transmitting their packer for secured transmission Assume the source node A need to transfer the data packets to the destination nodes B. after this process, the uniqueness particulars on node B obtained from the civic server. By using these information it will encrypted the data to be transmitted which will be send to the receiver node By receiving data from node A, receiver B will attempt to check, whether the message is received from valid node or not To do so, it will request the identity details of node A from the public server by using which verification would be done If it is valid, then the further process would be continued

The steps provide the secured communication establishment between the sender and receiver node. This steps would be followed when the information about the malicious nodes are transmitted and shared between nodes. For example consider, in your network there are five nodes present name 1, 2, 3, 4, 5 where 1 is sender node, 2, 3, 4 are intermediate node and 5 receiver node. Here 2 is an malicious nodes which is found by node 4.When node 4 found about the malicious node information it will forward about it to the neighboring node called 4 in the encrypted format as mentioned above. The node 4 will believe this information only when it is proved that the message is received from the valid node. This verification process is would be proceeded based on the procedure mentioned in the above steps.

Now, worm hole attack detection procedure is explained below: In this work, worm hole detection approach is found by using the parameter called the ETX (Expected transmission count). The ETX is nothing but the probability of number of packets that can be send or receive by the nodes. It is assumed that, whenever the data's are forwarded from one node to another node, it must receive innovative packets. Innovative packets are nothing but the new packets which cannot be found in the previously received packet values.

Worm hole detection in the existing mechanism is done in two phases. Those are

- Report phase
- Detect phase

Report phase

In the report phase, ETX count of all the nodes will be calculated by using the formula given in the paper.

The packets are transferred from the source node to the destination node. This information will be stored in the ETX count.

```
By receiving the packets from sender, the receiver node will check whether the innovative packets present
    o If it is present then it will compare its ETX rate with the sender node ETX rate
        If the sender node has higher ETX rate than the receiver node then
            Receiver will mark it as worm hole node
            Then it will create the resport contains that the sender node id which is found as
                malicious along with signature values
            This report would be encrypted which will then be forwarded to all the neighboring
                nodes
        End if
  o End if
```

Detect Phase

In the detect phase, nodes will receive the report which contains the information about the worm hole nodes from all judge nodes present in the environment in the encrypted format. Then it will be verified whether these information are received from the valid node or not by getting identity information from the public server. If it receives the information about the malicious nodes from majority of judge nodes then it will be concludes that the worm hole is present then those transmission of packets through those nodes would be avoided in the future.

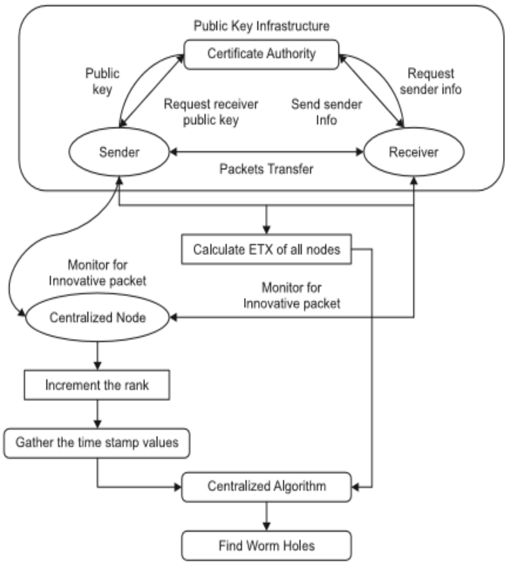

Figure 3: overview of the wormhole attack detection

IV. EXPERIMENTAL RESULTS

The performance evaluation of TERP is performed using popular network simulation (NS-2). In all the experiments, the initial energy of nodes is taken as 50J, energy threshold is set to 20% of initial energy and the trust threshold ( ) is set to 0.6. All nodes are initialized with neutral trust value 0.5. The network topology includes 100 sensor nodes deployed randomly over an area of 1200x800m2. The numbers of malicious and faulty nodes are varied from 1 to 10. The comparison is made between the methodologies Cuckoo Reliability aware energy and trust based routing protocol (CRETRP) and Trust and Energy aware Routing Protocol (TERP). The performance parameters considered in this work for performance evaluation are

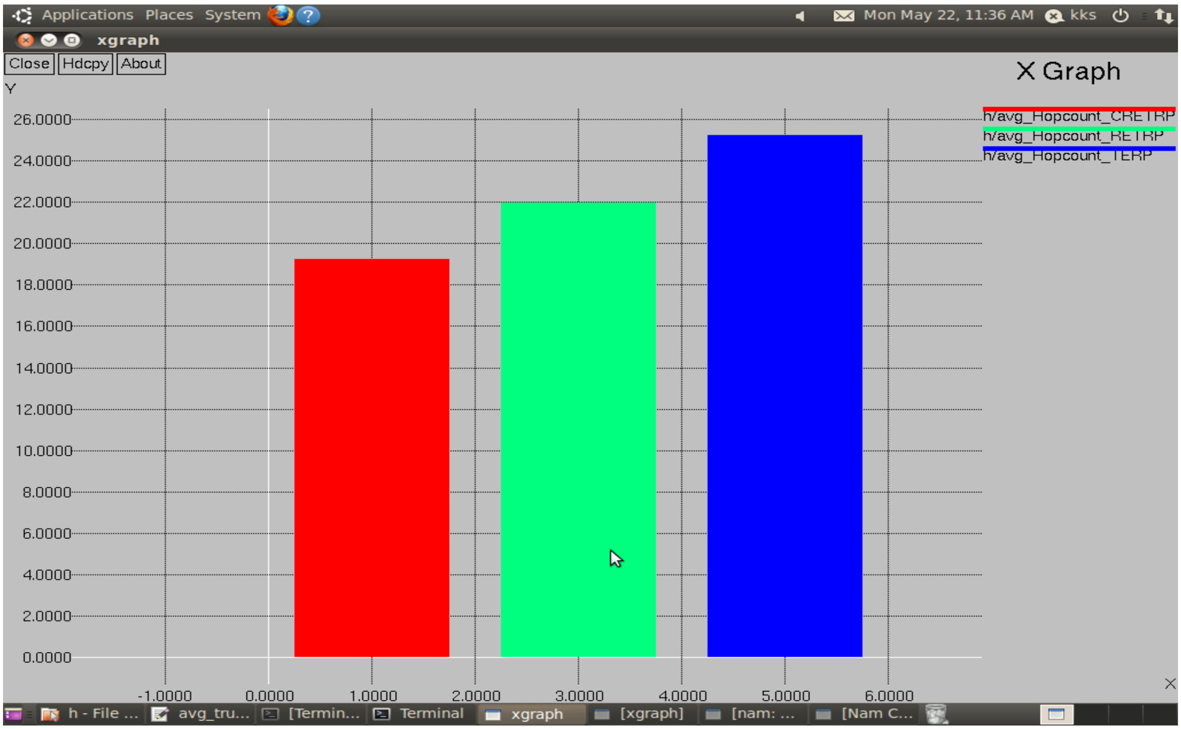

Figure: Hop Count

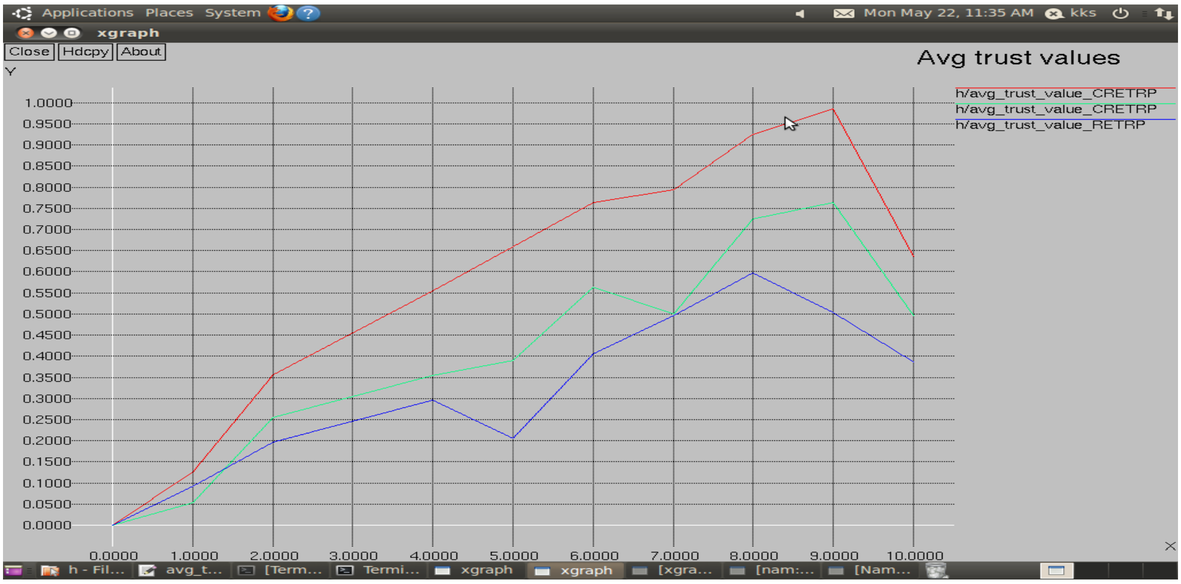

Figure: Trust Value

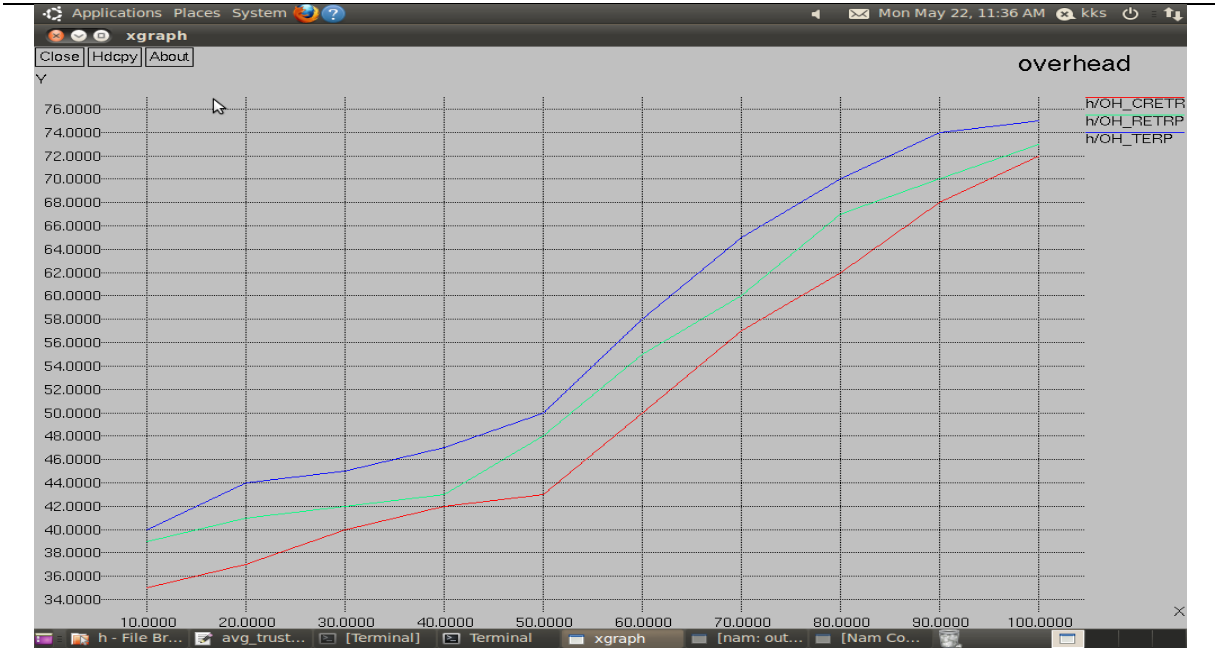

Figure : Control Overhead

V. CONCLUSION

In wireless sensor network, routing is a major task for the transferring the packets between the number of nodes for achieving the successful and secured data transmission. There might occur many issues while forwarding the data through the unsecured nodes. In this present work, the Reliability aware energy and trust based routing protocol (RETRP) is developed and it concentrate the implementation of the secured route path between the source node and the destination node. In addition to that worm hole attack are discovered at run time for avoiding the packet loss rate. The experimental evaluation is conducted in the NS2 simulation environment which shows better performance is attained in the proposed methodology.

REFERENCES

[1] W. Du, L. Fang and P. Ning, LAD: Localization anomaly detection for wireless sensor networks, Journal of Parallel and Distributed Computing, vol. 66(7), pp. 874–886, 2006.

[2] L. Hu and D. Evans, Using directional antennas to prevent wormhole attacks, Proceedings of the Eleventh Network and Distributed System Security Symposium, pp. 131–141, 2004.

[3] J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia and B. Bhargava, Lowcost attacks against packet delivery, localization and time synchronization services in underwater sensor networks, Proceedings of the Fourth ACM Workshop on Wireless Security, pp. 87–96, 2005.

[4] D. Liu, P. Ning and W. Du, Attack-resistant location estimation in sensor networks, Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks, pp. 99–106, 2005.