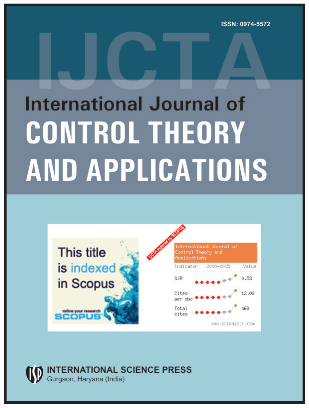

ISSN: 0974-5572

IJCTA

International Journal of
CONTROL THEORY
AND APPLICATIONS

This title is indexed in Scopus

INTERNATIONAL SCIENCE PRESS
Gurgaon, Haryana (India)

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 12 • 2017

Cuckoo Search Based Reliable Energy and Trust Aware Routing Protocol (CRETRP) for Wirless Sensor Network

D. Sivakumar[a], J. Jegan[b] and K. Selvakumar[c]

[a,b] *Assistant Professor, Kings College of Engineering, Thanjavur*
[c] *Associate Professor, Annamalai University*

Abstract: Varying deployment usage of wireless sensor networks leads to an increased problems such as security threat, lacks of the resource availability and so on. 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 the existing work, Trust and Energy aware Routing Protocol (TERP) is introduced for achieving the secured and energy concerned packet transmission which attempts to select the route in terms trust, energy and hop count of nearest nodes. However this lacks in its performance in terms of reliability due to not considering the reliability factor of nodes. And also existing work focus on only the status details of the current node and not considering the other nodes misbehavior attacks which might lead to the security violation data corruption. These issues are resolved in this work by introducing the novel framework for the route establishment namely Reliability aware energy and trust based routing protocol (RETRP). 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.

1. INTRODUCTION

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. And also it is used to transfer the data to the corresponding destination by using the network. In present, the networks following the bi-directional model and also manage the sensor movement. The improvement of Wireless Sensor Network is provoked by armed applications for example combat zone observation. In present days, the wireless sensor networks is used in more number of applications like apparatus health monitoring and manufacturing process monitoring and control.

By using the wireless sensor networks the information's are collected and these information are stored in a central base station in numerical data form. Moreover, the Open Geospatial Consortium (OGC) is used to specifying the principles for interoperability interfaces and metadata encoding and it also permits the amalgamation of heterogeneous sensor webs into the specified network. In this method is permitting the persons to observe or manage the wireless sensor networks all the way through a web browser. The consumption of sensor nodes is processing in an ad hoc approach in more number of wireless sensor network applications without cautious preparation and commerce. Once the sensor nodes implemented in the network means the sensor nodes can automatically employed into a wireless communication network. Sensor nodes can operated without presence for a many number of years and it is battery-powered. Some of the sensor nodes, it is very complex to replace or revitalize batteries. The wireless sensor networks are differentiated the sensor nodes based on the sensor level such as energy of server, consumption of sensor nodes, advanced unpredictability of sensor nodes, requirement of memory space and calculation speed.

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.

2. RELATED WORKS

In a wireless sensor network the trust based methods is a novel mechanism of the literature topic. Even though, in the wireless sensor networks as many number of power consumption routing protocols are presented. In this routing protocol, some particular routing protocol cannot consider a security of network, position of the faulty nodes and the trouble of congestion in their domain. For example, in MRP [7], based on the dynamic clustering and ACO a multi path routing protocol are explained and it increase the effectiveness of the data aggregation, in that way decreasing the utilization of the power. In TRANS [8] and TILSRP [9], the routing protocols with trust management are explained in detailed manner. On the other hand, the entire above mentioned protocols do not face the trouble of congestion. This congestion and trust based detail are explained in [10-12]. In the wireless sensor network, for the congestion control the FCC protocol [10] was developed to estimate the fuzzy based trust by Zarei et. al., the alteration form of FCC is FCCTF protocol [11]. In this case, the decision is taken by using the entry Trust Value. In the existing work, the Link State Routing Protocol is implemented to transfer the data from the server mentioned in TFCC protocol [12].

To estimate the dependability of the sensor nodes in MANET the researcher [13] 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 [14] 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 [15] 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 [17] 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 packet compared 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.

3. SECURED RELIABLE TRUST BASED ROUTING

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

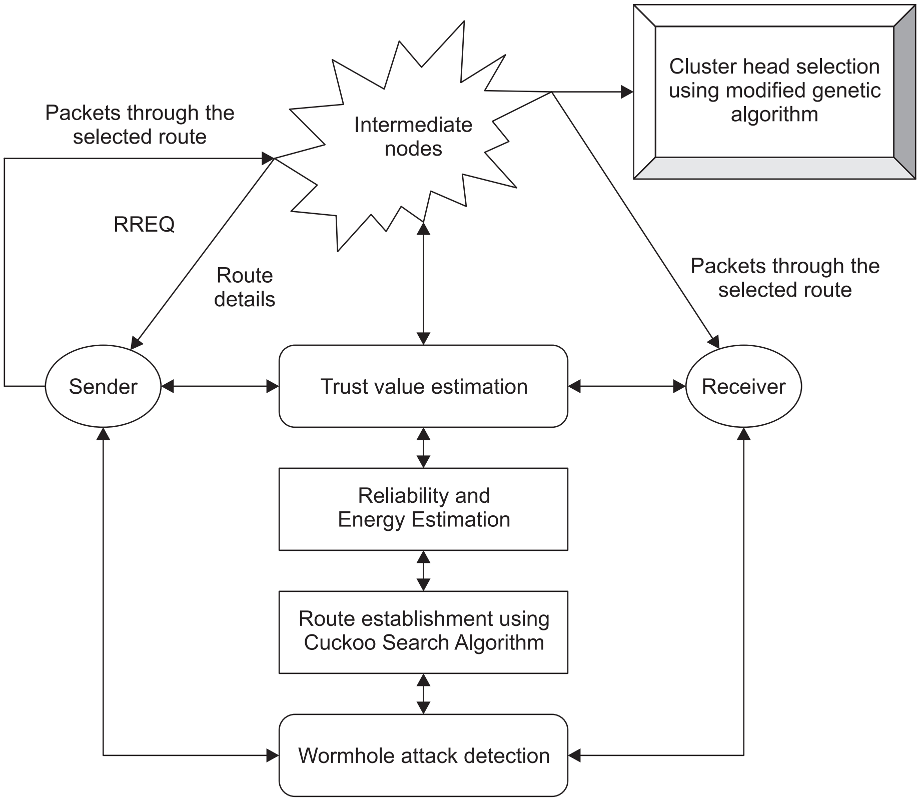
Cluster head selection using modified genetic algorithm
Packets through the selected route
Intermediate nodes
RREQ
Route details
Packets through the selected route
Sender
Trust value estimation
Receiver
Reliability and Energy Estimation
Route establishment using Cuckoo Search Algorithm
Wormhole attack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

Figure 1: Overall view of proposed research framework

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.

3.1. Cluster Head Selection using Modified Genetic Algorithm

The more number of sensor nodes are collected and to form the wireless sensor network, and to identify and transfer the data from the corresponding destination. These sensor node having the characteristics like less energy consumption, require less storage space and less calculation ability. To produce the energy in the sensor node the low energy batteries are used. In this network the energy is major trouble and to overcome these trouble the clustering models is used. By using the modified genetic algorithm the head of cluster has been chosen in the network. Based on the energy, distance between the nodes and the primary station the head of cluster has been determined. For this reason only, the wireless sensor device is known as power constraints. So that only, the highest distance node is selected for the wireless sensor device instead of minimum distance node with limited low power consumption.

In this present work the modified genetic algorithm is used to select the cluster head selection. For the selection process in the heuristic the genetic algorithm is used in the field of artificial intelligence. Another name of heuristic is metaheuristic and it is mainly used to optimization and search problems. Genetic algorithm is based on the evolutionary algorithms (EA) and it produces a result to the optimization trouble using some methods like inheritance, collection, cross over and mutation. The cross over operator is used in the genetic algorithm to differentiate the chromosomes process from the one age group to the next age group. It is similar to duplicate and genetic crossover, leading which genetic algorithms are based. Cross over genetic operator is defined as it is the process of taking more number of main results and produces a sub result corresponding to the main result. The traditional genetic algorithm is modified in its cross over operation by introducing the *k*-point crossover.

3.1.1. Fitness Function

For the power consumption the fitness value is assume for the optimal cluster head selection for this present work. In the EK network the k^{th} round is showed in the network current energy. The following equation is used to calculate the fitness function and to get the lowest value.

$$\text{Fitness} = \left| E^{K}_{\text{Network}} - E^{K-1}_{\text{Network}} \right|$$

3.1.2. Reproduction Operator

In the surroundings, the reproduction operator is the initial operator to choose at arbitrarily a couple of two particular strings for matching.

3.1.3. Cross Over Operator

The recombination operator is called cross over operator. The cross over operator is used to select the highest string and the position values are exchanged between the two strings. The common cross over is enlarged to *k*-point cross over and *k* represents the swap the genetic node of main two nodes to generate a novel chromosomes. The point is depending on the cross over point which is randomly selected. To estimate the many number of cross over which the cross over rate is commonly 2-5%.

3.1.4. Mutation Operator

After the cross over process is done, the mutation operator will be applied in the strings. After the mutation process is done means the bit value is changed from “0” to “1”. This process make a possibility to change the common node becomes a cluster head and the cluster head is becomes to the common node. at last, both the cross over and mutation process is completed in the server station to choose the chromosome and it has the networks with lowest power differentiation in proportion to the existing stage and make the sensor nodes as the cluster head the another nodes connected to the neighbor cluster head. Based on the power, density and the centrality using the genetic algorithm the cluster head can be selected. The present work stages can be described in the following algorithm:

Step 1: preliminary network.

Step 2: every node sends the location of itself in the network to its nearest node.

Step 3: to evaluate the cluster head of BS by using the genetic algorithm based on energy, density and centrality.

Step 4: each and every node the Cluster heads are introduced in the network.

Step 5: Each sensor node will connect to the nearest CH.

Step 6: Each sensor node transfers the data to the CH with a multiple-hop transmission.

Step 7: the entire data packets are received from the destination node after that to aggregate the entire data's of CHs by using the HYMN algorithm and then transfer into the server station all the way through a single hop transmission.

Trust Based Routing Scheme: In this proposed work, the new trust based congestion responsive energy efficient routing method for wireless sensor networks is introduced and the cuckoo search algorithm is using make the most of network duration. Assume the random exploitation of sensor nodes in the sensor ground beneath free space proliferation. There are two phases are used to complete the present algorithm. In phase 1, to estimate the trust values and the congestion position of the nodes and by this means, the trust-congestion surroundings are created. In phase 2, to use the trust-congestion metric and the distance metric by using the cuckoo search algorithm and it is developed for the data packet routing from source node to the server node. The detailed process of phase 1 & 2 is described in the following sub section 1 & 2.

3.1.5. Stage 1

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:

$$T_{ij} = \frac{A_1 \times N'_e + A_2 \times P'_{TR} + A_3 \times R'_L}{A_1 + A_2 + A_3} \tag{1}$$

In the above equation, A_1, A_2 and A_3 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.

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

The expression $\mathrm{Q}^k(c-1)$ is represented the blank space available in the queue of the k^{th} node till $(c-1)^{\mathrm{th}}$ sequence.

Each and every trusted node in the Trust Congestion Metric (TCM) is known as the legitimate node and it is calculated by following formula:

$$\mathrm{TC}_{ij} = \alpha \times \mathrm{CI}_j + (1-\alpha) \times \mathrm{T}_{ij} \tag{3}$$

The source node and the destination node are represented as i and j correspondingly. The congestion index of the destination is represented as C_{ij} and the source node i leading the destination node j trust value is represented as T_{ij}. The trust congestion coefficient constant value is represented as α and this constant value belongs to [0, 1].

3.1.6. Stage 2

By using the cuckoo search algorithm, the data routing protocol is implemented in stage 2. Another name of cuckoo search algorithm (CSA) is a meta-heuristic optimization algorithm to overcome the trouble and give the optimal result. 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.

Initialization: In the initialization process the number of nests is arbitrarily produced at the first step. In Table 3 this process is explained in detailed manner. Each and every nest the value is assigned arbitrarily "0" and "1".

Fitness selection: The critical feature of the cuckoo search algorithm is fitness selection process. It is used to calculate the better ability of persons result. Now, to identify the optimal route the lowest distance is selected as the best fitness. The fitness function is used to estimate the better path from the source node to the destination node. The fitness value is represented as f_i and i is represented as sum of the distance between the two nearest nodes n_j and n_{j+1}. The source node and the destination node is represented s and d correspondingly and the following equation is used to estimate the fitness function.

$$\mathrm{Fitness}(\mathrm{nest}_n^k) = \sum_{j=s}^{d} \mathrm{dis}(n_j, n_{j+1}) \tag{4}$$

In this present work, the trust congestion methodology is referred to as the fitness function. The following algorithm is described the cuckoo search algorithm:

Algorithm

Input: Trust Threshold Level, Trust Congestion Metric

Output: Optimal Route

Objective Function: $f(\mathrm{X}), \mathrm{X} = (x_1, x_2, ..., x_d)$

```
Generate an initial population of $n$ host nests;
While ($t <$ Max Generation) or (stop criterion)
 Obtain a cuckoo arbitrarily (say, $i$) and substitute its
   solution by performing Lévy flights;
   Estimate its quality/fitness $F_i$
   [For maximization, $F_i \propto f(x_j)$];
   Decide a nest among $n$ (say, $j$) arbitrarily;
   if ($F_i > F_j$),
      Swap $j$ by the novel result;
   end if
   A fraction (Pa) of the poorer nests is discarded and novel ones are creating;
   Maintain the best solutions/nests;
   Grade the solutions/nests and get the present best;
   Transfer the present best solutions to the next generation;
end while
```

New solution generation using Levy flight: The levy flight method is used to create the new methodologies. It is one kind of arbitrarily method. It is randomly search the length to create a new result which has a heavy-tailed allocation. Levy flight occupies the large search space in the specified region.

Both the real and the imaginary programs work at arbitrarily in step sizes. To calculate the step size the various function set are used compared to the real programming code. The following equation expresses the calculation of the step size in the real code.

$$\text{Stepsize} = 0.01 \times \frac{u}{|v|^{1/\beta}} \oplus (S_i^t - S_{\text{best}}) \tag{5}$$

where,

0.01 → a factor for controlling step size of cuckoo walks/flights,

S_i^t → is current solution i of iteration t

S_{best} → is the global best solution

Stepsize → is the length of walk step

$\oplus$ → is entry-wise product

U and v → are random value

β → Levy distribution parameter

From the above defined algorithm, better route establishment can be done effectively with the satisfaction of the research objectives namely energy, trust, reliability, trust and so on. After successful establishment of route paths, packets would be forwarded where there may be chance of the packet corruption/loss due to run time attacks such as worm hole attack. The protection of network from the worm hole attacks are discussed detailed in the following section.

3.2. Worm Hole 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 neighbouring 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 will find the existence of worm hole link and Detect phase will ensure worm hole is present and will block in the future

3.2.1. 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
    - 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 neighbouring nodes
        - End if
    - End if

3.2.2. *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.

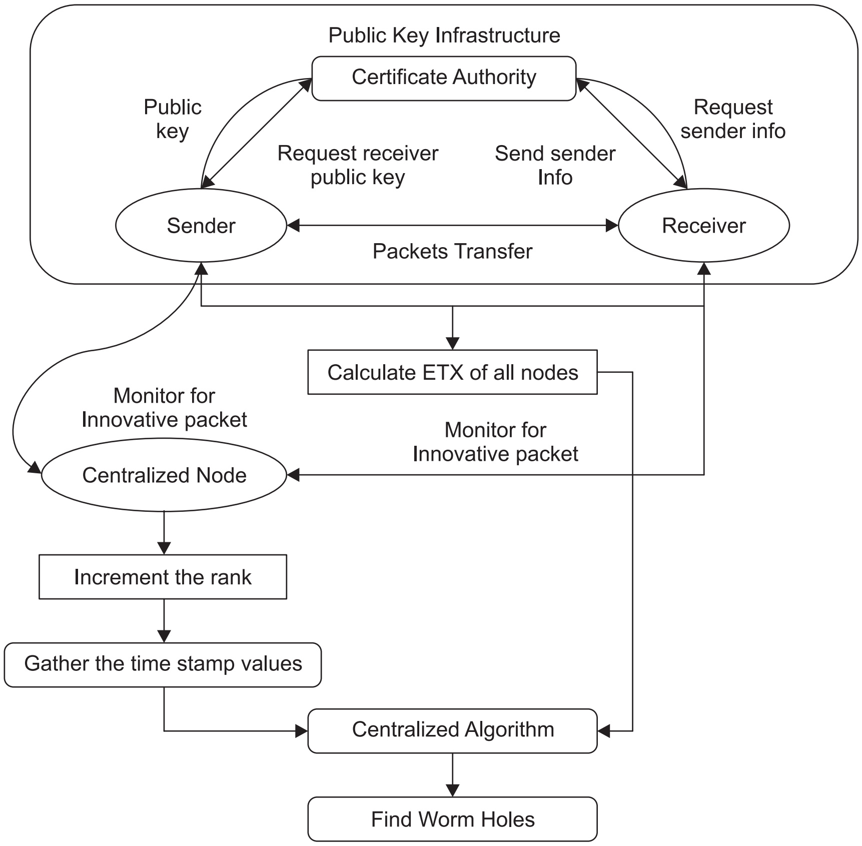

Figure 3: Overview of Wormhole attack detection

4. EXPERIMENTAL RESULTS

The network simulation (NS-2) is a very famous method of performance calculation of TERP process. In the entire work, the first energy of nodes is considered as 50 J, the energy threshold is 20% and the trust threshold is 0.6. Each and every node is assigned the trust value 0.5. Hundred sensor nodes are available in the network topology over an area of 1200×800 m^2. The unwanted and error node values are different from 1 to 10. The differentiation process is done between the Reliability aware energy and trust based routing protocol (RETRP) and Trust and Energy aware Routing Protocol (TERP). There are three parameters are used to estimate the trust value. There are,

- Control packet overhead
- Average hop count
- Average trust value of nodes

5. CONTROL PACKET OVERHEAD

Some amount of time is taken to transfer the data packets on a corresponding packet switched network and this time is referred to as the packet overhead. Every data packet need a additional bytes to store the information in the packet header and it associated with the collecting and decollating the data packets and it also decreases the entire communication speed of the original data. Packet overhead should be less for the proposed methodology for achieving the better performance. The numerical values that are obtained for the packet overhead for both the proposed and the existing methodologies are given in the Table 1.

Table 1
Packet overhead value

Number of Nodes	*Packet overhead*	
	TERP	*RETRP*
5	19500	10000
11	26000	14500
17	28900	19100
19	31000	20500
21	33000	25000

The graphical representation of the control packet overhead comparison of the proposed and existing research methodologies are given in the following Figure 3.

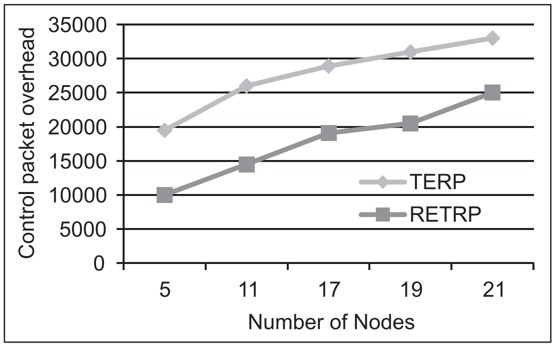

Figure 3: Control packet overhead comparison

In the Figure 3, Packet overhead comparison is done from which it is proved that the proposed methodology of the research work leads to the perform secured routing with Packet overhead is reduced considerably in the proposed research method than the existing method considerably which can be proved from the graphical representation.

6. NUMBER OF HOPS

Number of hops defines the number of hop counts required for the transmission of packets that are sending by the sender node. The lesser hop count consumed for the packet transmission would lead to better performance with improved security level. In Figure 4 illustrate the graphical representation of the hop count differentiation. Which it can be proved that the proposed method can transfer data packets with lesser hop count and more packet transmission ratio.

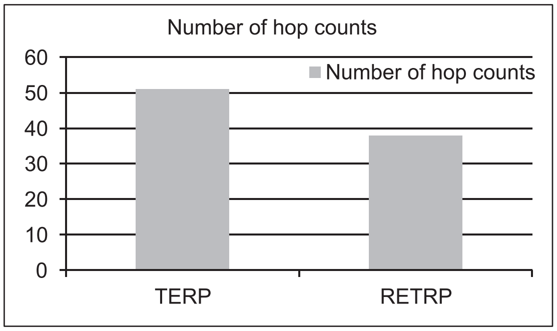

Figure 4: Average hop count comparison

In the Figure 4, average hop count comparison is given. These values are measured for the network with 60 numbers of nodes.

7. AVERAGE TRUST VALUE OF NODES

The better trust value defines the successful transmission of packets to the destination node securely without packet loss or collision. Based on the probability value the trust value is estimated. The differentiation of the calculation is illustrated in Figure 5.

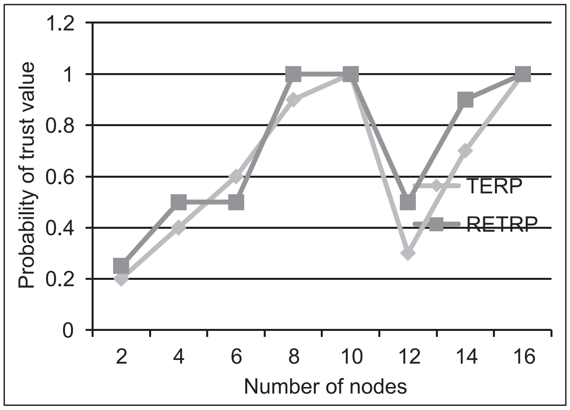

Figure 5: Trust value Comparison

8. 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.

REFERENCE

[1] J. Cordasco and S. Wetzel, “Cryptographic Versus Trust based Methods for MANET Routing Security,” Electron. Notes Theor. Comput. Sci., Vol. 197, No. 2, pp. 131-140, Feb. 2008.

[2] Y. Yu, K. Li, W. Zhou, and P. Li, “Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures,” J. Netw. Comput. Appl., Vol. 35, No. 3, pp. 867-880, May 2012.

[3] M.C. Fernandez-Gago, R. Roman, and J. Lopez, “A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks,” in Third IEEE International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU, 2007, No. SecPerU, pp. 25-30.

[4] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, “TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks,” Int. J. Distrib. Sens. Networks, Vol. 2014, No. Article ID 209436, pp. 1-14, 2014.

[5] T. Zahariadis, P. Trakadas, H.C. Leligou, S. Maniatis, and P. Karkazis, “A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks,” Wirel. Pers. Commun., Vol. 69, No. 2, pp. 805-826, Apr. 2012.

[6] T. Eissa, S. Abdul Razak, R. H. Khokhar, and N. Samian, “Trust-Based Routing Mechanism in MANET: Design and Implementation,” Mob. Networks Appl., Vol. 18, No. 5, pp. 666-677, Jun. 2013.

[7] Jing Yang, Mai Xu, Wei Zhao and Baogue Xu, “ A Multipath Routing Protocol Based on Clustering and Ant Colony Optimization for Wireless Sensor Networks”, Sensors ISSN 1424-8220, 10,4521-4540, doi : 10.3390/s 100504521’ 2010.

[8] S. Tanachaiwiwat, P. Dave, R. Bhindwale and A. Heimy, “Location-centric Isolation of Misbehavior and Trust Routing in Energy Constrained Sensor Netwoks”, IEEE International Conference on Performance Computing and Communications, 2004.

[9] A. Raha, M.K. Naskar, S.S. Babu, Omar Alfandi, and D. Hogrefe, “ Trust Integrated Link State Routing Protocol for Wireless Sensor Network (TILSRP), proceedings of 5th IEEE ANTS, Dec 2011.

[10] Mani Zarei, Amir Msoud Rahmani, Avesta Sasan, Mohammad Teshnehlab, “Fuzzy based trust estimation for congestion control in wireless sensor networks”, 2009 International Conference on Intelligent Networking and Collaborative Systems.

[11] Mani Zarei, Amir Msoud Rahmani, Razieh Farazkish, Sara Zahirnia,“FCCTF: Fairness Congestion Control for a distrustful wireless sensor network using Fuzzy logic”, 2010 10th International Conference on Hybrid Intelligent Systems.

[12] A. Chakraborty, S. Ganguly, M.K. Naskar, A. Karmakar, “A Trust Based Fuzzy Algorithm for Congestion Control in Wireless Multimedia Sensor Networks (TFCC)”, proceeding of 2nd International Conference, ICIEV, Dhaka, Bangladesh, 2013.

[13] Xia H, Jia Z, Li X, Ju L & Sha EHM 2013, ‘Trust prediction and trust-based source routing in mobile ad hoc networks’, Ad Hoc Networks*,* Vol. 11, No. 7, pp. 2096-2114.

[14] Airehrour D, Gutierrez J. & Ray SK 2015, ‘Grade Trust: A secure trust based routing protocol for MANETs’, International Conference on Telecommunication Networks and Applications Conference (ITNAC), pp. 65-70.

[15] Analysis of E-commerce challenges in INDIA by using Weka Tool, Published in IJCTA. [Scopus Indexed].

[16] Perspectives on Educational Data Mining – A Study Published in Man in india. [Scopus Indexed]

[17] Wang B, Chen X & Chang W 2014, ‘A light-weight trust-based QoS routing algorithm for ad hoc networks’, Pervasive and Mobile Computing*,* Vol. 13, pp. 164-180.

[18] Albert Mayan .J, Dr. T. Ravi, " Structural Software Testing: Hybrid Algorithm For Optimal Test Sequence Selection During Regression Testing", International Journal of Engineering and Technology, Vol : 7, Issue:1, pp: 270-279, March 2015, ISSN : 0975-4024.

[19] Mary S. Prince, Dr. Baburaj. E ," Performance enhancement in session identification ", IEEE Conference, ICCICCT-2014, pp: 837-840

[20] Zahariadis T, Trakadas P, Leligou HC, Maniatis S & Karkazis P 2013, 'A novel trust-aware geographical routing scheme for wireless sensor networks', Wireless personal communications*,* Vol. 69, No. 2, pp. 805-826.