An Energy Efficient Mechanism Using Genetic Algorithm for Wireless Sensor Network

[1] Swati Manapure, [2] Ajay Phulre

[1] Student, [2]Asst. Prof., CSE, SBITM COE, Betul, India
Email - [1]swatiyenurkar85@gmail.com, [2] aphulre@gmail.com,

Abstract: *Now a day's wireless technology becoming more popular, hence the two major parameters, energy and security are very important issues and difficult to handle. These issues are interrelated since because of energy issue and limited power resources there are some restrictions on implementation of security. The security issues are data integrity, Data confidentiality, service availability and energy consumption. In such case, the designing protocol for security issues must ensures minimization in energy consumption.*
This paper describes effective solution to the WSN"s energy issues and secure routing, as well as a combination of shortest path and routing algorithm is used to save time and network lifetime. Genetic algorithm is used as filter to the packet, which applies the rules on packet and checks its validity.

Keyword: *Genetic algorithm, routing algorithm, WSN.*

1. INTRODUCTION:

Sensor modes perform data processing, computing, sensing and communication with limited resources like power, memory size and bandwidth. Therefore care has to be taken while designing the network under these limitations. Most of the energy is consumed in communication of data. It is impossible to recharge the deployed node, and the lifetime of network is interdependent on battery lifetime, thus energy is vital for many applications. In WSNs energy utilization, routing, data processing, data aggregation, security etc. are related to each other. For any application if network is not secure from attack, then entire effort of transmission of data is lost. There are two types of attacks/intruder: external and internal. External intruder do not have authorize access to system and they attack by using various penetration technique. Whereas internal intruder have access permission that can perform authorized activity. These internal intruders are insider threat to the system. External intruder may attack to change the nodes to behave maliciously resulting in an abnormal behavior. The internal intruder attack to change the data processed within the nodes. In this paper we are more concern about internal attacks. Trust mechanism with the notion of trust in human society has been developed to defend against insider attacks. **In general trust mechanism works in 3 stages:** 1) Node behavior monitoring: Watchdog is a monitoring mechanism popularly used in this stage. It records each node"s behaviours such as packet forwarding. This collected data will be used for trustworthiness evaluation in the next stage. The confidence of the trustworthiness evaluation depends on how much data a sensor collects and how reliable such data is. 2) Trust measurement: Trust model defines how to measure the trustworthiness of a sensor node. There are several representative approaches to build the trust model, which include Bayesian approach, Entropy approach, Game-theoretic approach, and Fuzzy approach. 3) Inside attack detection: Based on the trust value, a sensor node determines, whether its neighbour is trustworthy for collaboration (such as packet forwarding). If a neighbour's trust value is less than a certain threshold, it will be considered as malicious node.

2. LITERATURE REVIEW:

- Pramod D Mane. [3] has created two basic models viz. Anomaly detection- build a model of normal behavior and compare with detected behavior. And it filters a large number of packet records. Misuse detection- detect attack type by comparing past attack behavior and current behavior.
- Shaila K et al. [4] proposed a HIDS system with two techniques- Cluster based and Rule based. Network is divided into cluster head (CH) and member nodes. CH transfer and collect information to and from node members. A rule based system is divided into 3 phases of intrusion detection, in first supervised node data, in second node operation failure and in third compare number of failure with estimated occasional failure in network.
- Mr. Ansar S [6] proposed an Advanced IDS which is a combination of energy prediction based IDS and hybrid intrusion detection as well cross layer IDS. The system is capable of detecting almost all intrusion but also applicable to small, medium and large sized wireless Sensor Network

3. IMPLEMENTATION RESULTS AND DISCUSSION:

The detection of any change in the data processed is difficult. Generally the analysis of data sent by each node is done by internal intrusion detection. The proposed algorithm is used for internal data analysis, where it applies the rules on data packet and checks its validity. Next it checks for node validation and select the routing path to send data packet. The routing table includes entry of valid node, their distance, and cost. The watchdog node, who doesn‟t involve in communication, will maintain the behavior

3.1 Predicted Algorithm

The implemented system uses fundamental routing protocol named Link State Routing Protocol with the exclusion of Dijkstra's algorithm. This protocol is particularly attractive in the case of Wireless Sensor Networks which have limited hardware and software features. The redundancy on applying **Dijkstra's algorithm** here reduces the routing overhead. Its absence in calculation of the shortest path is compensated using our 'Select the Most Trusted Route' (SMTR) algorithm which chooses the most reliable (or trusted) route. The initial process includes:-

For calculating the trust of node -
Initial condition:
Each node wants to communicate with other nodes in the network.
Input:
Get the source and destination of the network.
Output:
Trust value calculation and communication.

Taking routing as main objective, proposed routing mechanism dedicated for wireless sensor networks. In our proposed method, the new algorithm **SRPT (Secure Routing Path using Trust values)** has better performance as compared to existing systems. Here, in this approach, during transmission of packets, if any node in the routing path get fails to transmit the packets, that time it can automatically choose another routing path to transmit the packets to the required destination.

STEPS FOR SECURE ROUTING PATH USING TRUST VALUES (SRPT) ALGORITH

Step-1. Select source and destination node \\Routing algorithm
Step-2. If selected node is not valid then
Step-3. Source=0, destination =0
Step-4. If location is selected and both nodes are valid then
Step-5. Add all path to path dictionary
Step-6. For all path // Shortest path algorithm
Step-7. Select first two paths
Step-8. Compare shortest distance
Step-9. Set the shortest path to top
Step-10. If obstacle found
Step-11. Set another shortest path to top
Step-12. If packet found then \\Packet filtering via genetic
Step-13. Encrypt/decrypt algorithm in 3DES
Step-14. Apply filtering
Step-15. Check packet behavior and size
Step-16. Compare with last successful transmission from path dictionary
Step-17. If changed then send to abnormal file
Step-18. Else pass to next hop
Step-19. Add entry in path dictionary

The algorithm given above is the combination of routing protocol, dijkstra algorithm and genetic algorithm. All these step shows step by step implementation of secure routing path using trust value algorithm. The algorithm is useful in finding shortest path with minimum delay also checks the possibility of node attack. The trust value is increased by using genetic algorithm, that it provides encryption security to a data packet. A path dictionary is a collection of routing data used to select the best path from it.

Pseudo code for dijkstra algorithm:

```
Dist [source] =0 //distance from source to source
Prev [source] = undefined // previous node in optimal path initialization
    For each vertex v                    // initialization
        If v! = source    //v has not been removed from Q (unvisited node)
            Dist[v] = infinity                    // unknown distance from source to v
```

```
                    Prev [v] = undefined      //previous node in optimal path from source
            End if
                Add v to Q                                  // all nodes initially in Q(unvisited node)
        End for
    While Q is not empty
        u = vertex in Q with min. dist[u]
        Remove u from Q
            For each neighbor v of u                        // where v is still in Q
                        Alt =Dist[u] + Length(u,v)
                            If alt < dist[v]                // a shorter path to v has found
                            Dist[v] = Alt
                            Prev[v] = u
                        End if
                End for
    End while
    Return Dist [], Prev []
```

The pseudo code for dijkstra algorithm is given above. The algorithm makes no attempt to direct exploration towards the destination. The main process is to determine next current intersection i.e. distance from starting point. Therefore this algorithm expand outward from starting location, by considering each node closer to it in term of shortest path distance, until it reaches to destination.

The result analysis describes the result we got after running the simulation. The result is compared with other available techniques to check the reliability of this work.

3.2 Comparison of Node Failure and Recovery

Each time whenever sensor network created, the frequency count of node fail is less than node recovery by using genetic algorithm. The following time chart shows the number of occurrences of node failure. In real transaction node failure results in big delay that can destroy the whole transaction, hence users' trust towards the sent packet will reached to the destination is not sure.

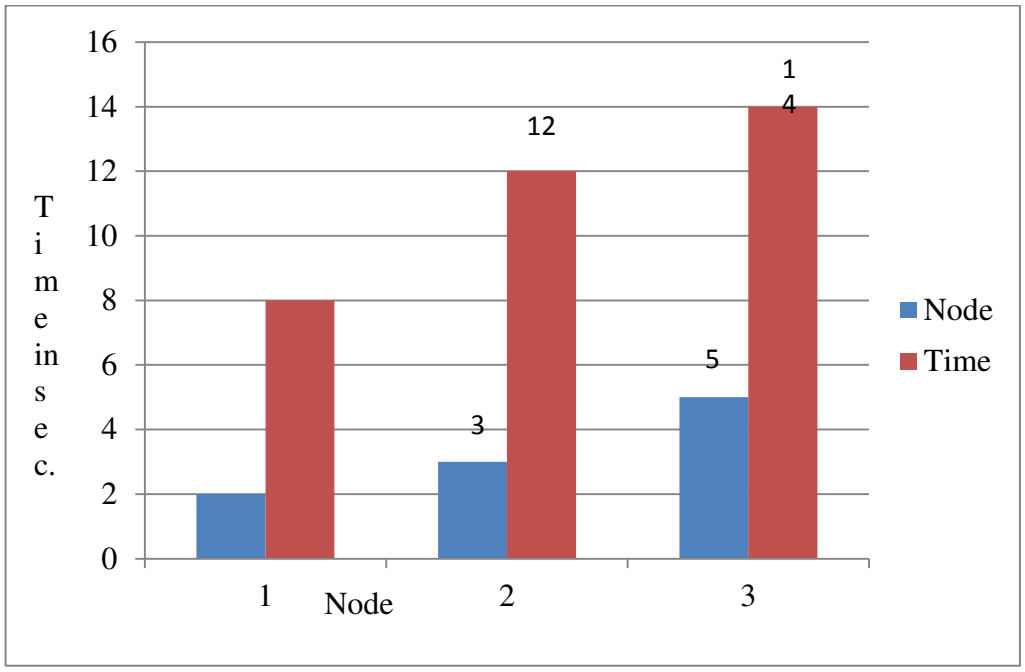

Figure : Graph Showing Node Failure and Recovery Analysis

The 'select another best path' concept makes sure the same transaction with different rout with all security that passes the packet safely to destination. The next rout assumes different nodes that are either recovered or continuously active nodes.

3.3 Comparison with other Techniques

The figure given below shows the lifetime of network by different techniques. These techniques are already implemented to measure the trustworthiness of sensor nodes.

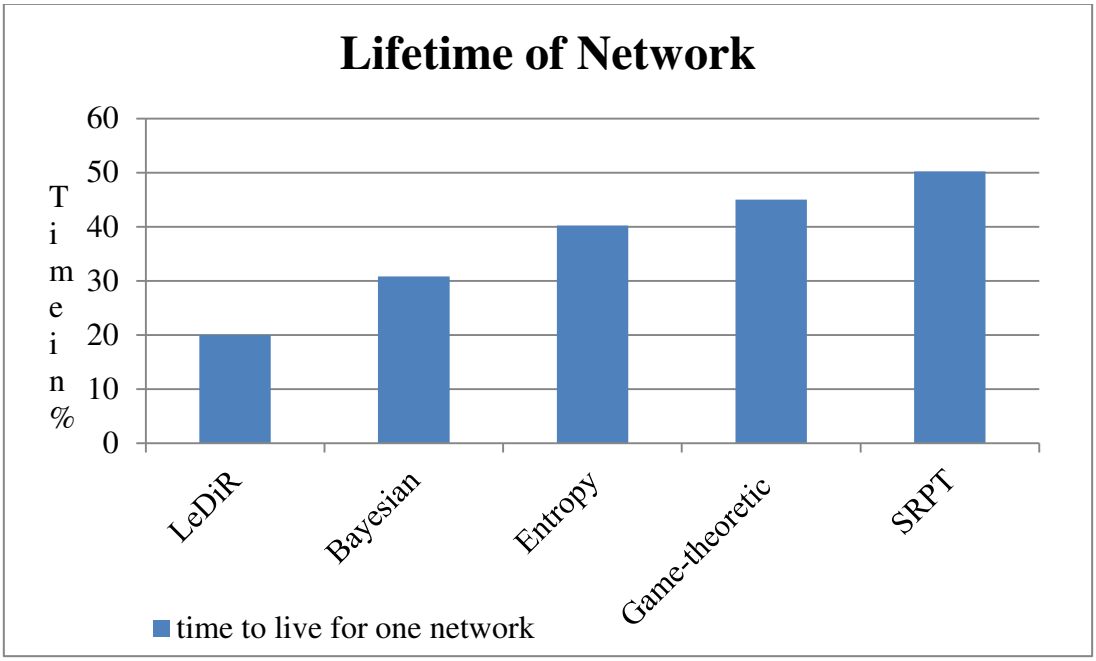

Figure : graph showing network lifetime with different techniques

The other comparative techniques are used for calculating the efficient trust mechanism; graph shows the total percent of lifetime of network with respected techniques. The SRPT algorithm is proved to be better for keeping node active for long time.

3.4 Energy Consumption Rate with Increasing Number of Packet

Following table shows the comparative analysis for proposed algorithm with other recent techniques available. The energy consumption rate is increased as the number of nodes increase. The required energy for selecting the best path can be used efficiently by using SRPT algorithm. As it already maintain all possible paths from current node to destination node.

Number of nodes	Energy consumption				
	LeDiR	Bayesian	Entropy	Game theoretic	SRPT
50	20	20	20	20	20
100	50	40	36	36	30
150	80	58	65	51	40
200	95	88	79	69	50
250	100	99	100	89	60

Table 5.1: Energy Consumption with Increasing Nodes

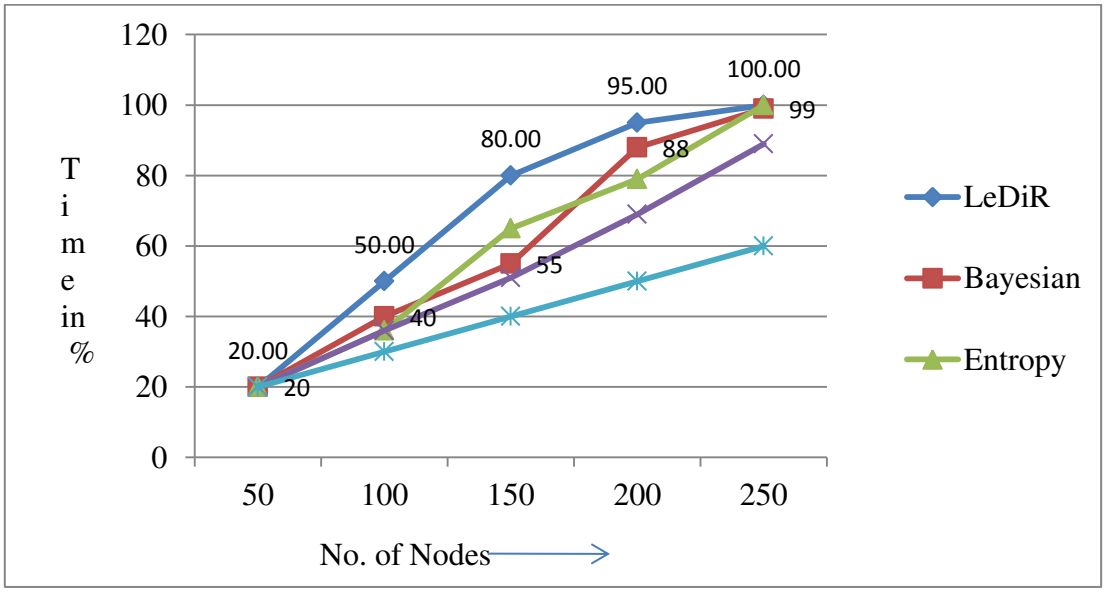

Figure : Graph Showing Energy Consumption Rate

As shown in figure as the number of nodes increased the energy consumption ratio also increased, but there is no random change in consuming the energy, but by using SRPT the analysis work shows that as the number of nodes increasing the energy remains constant. There is no random utilization for increasing nodes.

4. CONCLUSION:

In this implemented work, we applied combination of Dijkstra and link state routing algorithm for finding best and safe path among the network. A sending packet check the node index and decide the routing path, since the packet never reaches to affected node which removes the processing time required to detect and then recover the original packet. This mechanism saves time as well as increase the network lifetime. The separate defence system by using genetic algorithm is used that detect and recover the node, since affected node is out of network, no network jam occurs. The node energy is utilized efficiently as the recovery is managed in such a way that the overloaded condition occurs due to which they get time to recover from low energy state.

REFERENCES:

1. Y. Cho and G. Qu, Y Wu.(2012) "*Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks*", IEEE CS Security and Privacy Workshops.
2. Pramod D Mane, Prof. D.H.Kulkarni,(2013) "*Watchdog Three-Tier Technique to Secure Wireless Sensor Network*", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,.
3. Nidhi Aley *et al*,(October- 2014) International Journal of Computer Science and Mobile Computing, Vol.3 Issue.10, , pg. 810-813.
4. K.Q. Yan, s.c. Wang, S.S. Wang and C.W. Liu,(2010) "*Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network*", IEEE,.
5. Mr. Ansar S, Prof. Pankaj K, Prof. Hitesh Gupta,(November 2013) "*Hybrid Intrusion Detection for Anomaly & Misuse Attack using Clustering in Wireless Sensor Network*", IJARCET, Volume 2, Issue 11,.
6. Sneha Dhage, Purnima Soni,(February 2014) "*Intrusion Detection and Fault Tolerance in Heterogeneous Wireless Sensor Network: A Survey*", International Journal of Scientific and Research Publications, Volume 4, Issue 2,.
7. Joseph RishSimenthy, K. Vijayan, (April 2014) "*Advanced Intrusion Detection System for Wireless Sensor Networks*", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Special Issue 3,.
8. Ravi Kumar, Sunil Kumar, Prabhat Singh,(July 2013.) "*Enhanced Approach for Reliable & Secure Wireless Sensor Network*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7.
9. Shaila Ket al.(Feb. 2014) "*Probabilistic Model for Single And multi-sensing Intrusion Detection in Wireless Sensor Networks*", IOSR Journal of Computer Engineering, Volume 16, Issue 1, Ver. IX.
10. Hamed Khan babapour, Hamid Mirvaziri,(January 2014) "*An Intelligent Intrusion Detection System Based On Expectation Maximization Algorithm in Wireless Sensor Networks*", ICT, Volume 4,.
11. Hamed Khanbabapour Hamid Mirvaziri,(January 2014) "*An Intelligent Intrusion Detection System Based On Expectation Maximization Algorithm in Wireless Sensor Networks*", International Journal of Information and Communication Technology Research, Volume 4 No. 1,.
12. Ismail Butun et al.(2013) , "*A Survey of Intrusion Detection Systems in Wireless Sensor Networks*", IEEE,.
13. Hassen Mohammed Abduallah Alsafi.(September 2013) "*A Review of Intrusion Detection System Schemes in Wireless Sensor Network*", CIS Journal, Vol. 4, No. 9.