A NETWORK APPROACH FOR LOAD BALANCING AND PRIVACY PATH SELECTION IN WIRELESS COMMUNICATION

Dr. R. Jayaprakash, *Assistant Professor, Department of Computer Science, NGM College,Pollachi.*
Ms. A. Kalaivani, *Assistant Professor, Department of Computer Science, NGM College, Pollachi.*
jpinfosoft@gmail.com

Abstract: A Load Balancing in Privacy Path Selection (LBPPS) in wireless Network process for searching straight paths to transfer packets from source to destination through cluster head with the selected base station is implemented. This LBPPS method performs gateway mobility load balancing in the network order to achieve higher aggregated throughput among data transfer. The Load Balancing in Privacy Path Selection (LBPPS) detection scheme path grouping protocol examines every node in the network and monitors its neighbours' behaviour. Also, it detects any abnormal action of neighbours' to ascertain whether the node abnormally behaving is indeed malicious. As a result, the abnormal node is considered as a malicious node.

Key words: Load Balancing, Privacy, Preserving, Routing, Gateway.

INTRODUCTION:

Mechanism of Load Balancing in Privacy Path Selection (LBPPS) is a key component in traffic and refers to distributing traffic load more evenly in the network. Uneven load distribution is caused by varying user demands or uneven node distribution, where the latter may be a consequence of the unplanned and mobile nature of MANETs. Furthermore, specific network nodes are more vulnerable to become congested than others due to their location or assigned role. Nodes located in the centre of the network tend to be more congested than nodes in the periphery, either because most packets have to traverse these central nodes or contend with a higher number of neighboring nodes for the medium. Nodes having the role as *gateways* between network domains may be more congested since all inter-domain traffic has to traverse through them.

Avoiding congestion at such key nodes is critical in maintaining network connectivity and the services they provide. Figure 1.1 describes the Mechanism of Load Balancing in Privacy Path Selection process flow. Existing load balancing protocols adjust the routes dynamically to balance the traffic load based on current load distribution knowledge.(Broch et al. 1998) used multi-path routing to share the traffic equally to different nodes or path, which introduces much additional overhead. A novel approach (Hasanpour et al., 2017) is developed in targeting load balancing in ad hoc networks using quantum game theory's properties. The Quantum Load Balancing (QLB) algorithm proposed is implemented, and significant gain is stated about the QoS metrics such as delay and jitter.

REVIEW OF LITERATURE

Nodes in wireless sensor networks, which are difficult to replenish with limited energy consumption. If the energy consumption is fast, the unbalanced load will reduce the node lifetime and affect the network performance. Therefore, it is essential to study how to reduce sensor nodes' energy consumption and improve nodes energy use rate to prolong the network lifetime. Wang et al. (2020) proposed load balancing routing method for cluster head optimization in WSN. It helps to calculate an optimal number of clusters. CH selection uses unequal clustering algorithm for unbalanced nodes. The experimental results showed that the proposed algorithm when compared with LEACH and UCDP algorithm, will balance the loading and effectively extend the life cycle of wireless sensor network. The algorithm was divided into two stages: unequal clustering and establishing paths between clusters. In order to solve the problem of unbalanced, the nodes were formed as clusters. The study used tiny OS2 simulator. The simulation results showed that the method could save the sensor nodes energy consumption in a cluster. Wajgi and Thakur (2012) proposed a load balancing technique using the cluster to increase network scalability. The model used backup nodes and increase the network lifetime and provides high throughput. The proposed approach assumes a heterogeneous network with the sensor nodes having

The existing models did not efficiently address QoS improvement and energy efficiency. Motivated by this, the study presented a novel hybrid approach for improving those parameters. The model has link estimation and learning of network techniques for achieving excellent performance. Simulations have been done for varying scenarios such as speed, and the number of nodes. The analysis was done on throughput, delay analysis and packet delivery ratio for different methods. The proposed load balancing approach shows improved performance when compared to existing methods.

METHODS AND FINDINGS

LOAD BALANCING IN PRIVACY PATH SELECTION (LBPPS)

In the Mobility model, *V_{max}* and *T_{pause}* are the two relevant key parameters determining nodes' mobility behaviour. If the *V_{max}* is small, and the pause time *T_{pause}* is long, Ad Hoc networks become stable. If the node movement is faster (i.e.,*V_{max}* is large) and the pause time *T_{pause}* is smaller, the topology is highly active. The variation of these two parameters, especially the *V_{max}*, the Random Waypoint model generates several mobility scenarios with different levels of nodal speed.

The Mobility metric captures and quantifies this nodal speed. The measurement of the relative speed between node *i* and *j* at time *t* is given by,

$$\boldsymbol{Speed(i,j,t) = \left|V_i(t) - \frac{V_j(t)}{M}\right|} \qquad \textbf{eqn. (1.1)}$$

The Mobility metric is then calculated as relative speed averaged over all node pairs and overall time. The definition is given as follows,

$$\boldsymbol{M = \frac{1}{|i,j|}\sum_{i=1}^{N}\sum_{j=i+1}^{N}\frac{1}{T}\int_0^T Speed(i,j,t)dt} \qquad \textbf{eqn. (1.2)}$$

where |*i*, *j*| is the number of diverse node pair (*i*, *j*), *n* is the total number of nodes in the field (i.e., ad hoc network), and *T* is the time required for simulation.

Gateway load balancing refers to distributing inter-domain traffic more evenly and intelligently between the gateways to achieve higher aggregated throughput. The prerequisite is two or more gateways deployed in the network, providing connectivity to external network domains such as the global Internet. Since all inter-domain traffic has to traverse the gateway nodes, they are consequently more vulnerable to congested. So it is necessary to deploy multiple gateways in the network to increase the overall capacity and alleviate the probability of congestion. Also, it provided redundancy and increased robustness. Furthermore, it can also lead to fairness improvement, i.e. with only one gateway; different nodes enjoy different capacities depending on their proximity to the gateway. However, with multiple gateways, the average distance to the available gateways is the same for all nodes.

Although the deployment of multiple gateways provides several advantages, it also introduces several issues and challenges that need to be addressed effectively to exploit these advantages effectively. They may cause a gateway to be overloaded, while others may be strongly underused, either due to uneven node distribution or user demands. Hence, without proper load balancing, a potential risk for degradation in the performance.

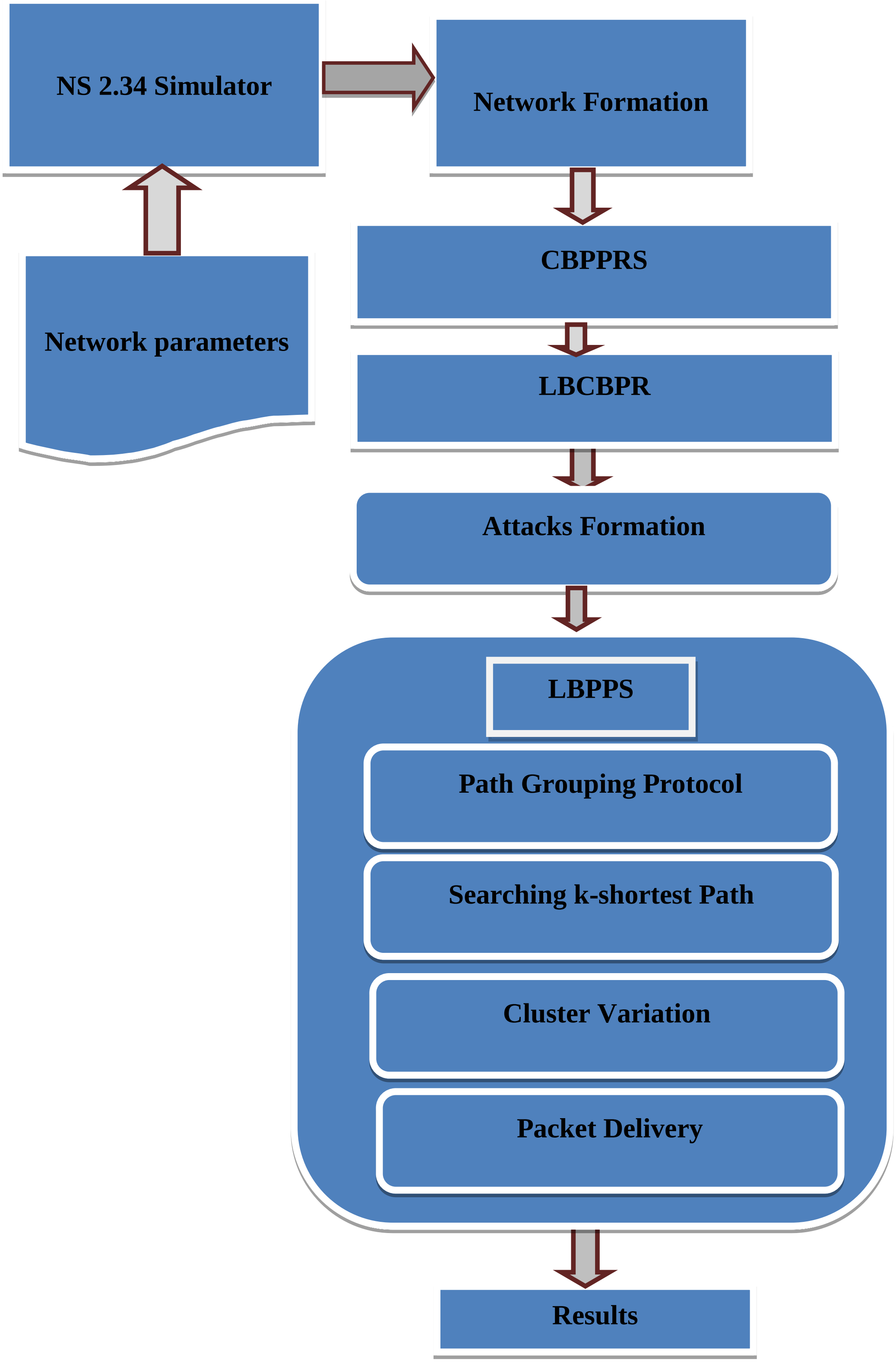

Figure1.1 Mechanism of Load Balancing in Privacy Path Selection (LBPPS)

The LBPPS searching the k-path in the mobile ad hoc network can be either unidirectional or bidirectional. The control messages are transmitted periodically one hop away for sensing the neighbouring nodes so that they are not forwarded further. When the first host receives the Hello message, it sets the second host's status to uneven in the routing table. When the first host sends control message including the message of the link it has to the second host to be asymmetric, the second host automatically set the first host status to symmetric in the routing table.

LBPPS algorithm predicts the distributed attacks in a mobile ad-hoc network. In the detection scheme path, grouping protocol examines every node in the network and monitors its neighbours'behaviour. In detecting any abnormal action by its neighbours', a distributed algorithm is raised to determine whether the node behaving is malicious. The protocol works by combining some security components present in each node in the networks. These components are as follows: (i) detection, (ii) privacy collector, (iii) privacy manager, (iv) Privacy propagator.

MECHANISM OF LOAD BALANCING IN PRIVACY PATH SELECTION (LBPPS) ROUTING

Algorithm 1: ***Mechanism of Load Balancing in Privacy Path Selection Routing***

```
Intialize CH← 0; LBCPR← 0; LBPPS← 0;
Process
Step 1: source node needs a route to the destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighbouring nodes
Step 2: Searching the neighbour cluster list present source to destination.
Step 3: Check gateway mobility balancing (gmb)
Step 4:ifgmb ≠ CH then
    CH = CH + 1
end if
Step 5:ifgmb_count>nodecount_thresh then
    //declare the target node and their previous hop nodes are attacker nodes.
    forward (attacklink);
    break;
end if
Step 6: select privacy cluster path for packet delivery
```

Meanwhile, the algorithm establishes detection, privacy collector privacy manager and privacy propagator to complete the privacy path selection. An experimental result shows that the proposed algorithm better outperforms than existing HsecGR and Trust-ECC methods. Routing overhead, insufficient packet delivery ration and other QoS parameters are some of the flaws in an inefficient load balancing scheme. Primary research is being done on the problem through congestion estimation and traffic control. Some methods use energy and power metrics for making routing decision for load balancing. Clustering-based approaches are one among them (Whaiduzzaman et al., 2014).

The primary research challenges for MANETs are QoS improvement and energy efficiency. Existing methods did not efficiently address these. Therefore, this research became a motivation by presenting a novel hybrid approach for load balancing, which improves QoS and energy efficiency performances. The primary aim of this research addresses a novel algorithm for efficient load balancing. This proposed method addressed both load balancing and energy efficiency in parallel.

For securing an ad hoc network, the attributes to be considered are Availability, confidentiality, integrity, authentication and no repudiation (Zhou and Hass, 1999; Kar, 2017). Availability ensures the survival of the network even after the denial-of-service attacks. Confidentiality ensures the disclosure of information to unauthorized entries. Integrity guarantees that no transmitted message is corrupted. Authentication ensures the identity of the node to which it communicates. Non repudiation ensures the origin cannot deny the transmission. The ad hoc networks' features pose many challenges and no standard routing protocol that resolves all the issues.

ILLUSTRATION OF RESULTS

Packet Delivery Ratio

The Energy packet delivery ratio is the percentage of the number of packets received by the destination node to the number of packets generated by the source node. The Proposed system performs the best in terms of packet delivery ratio followed by distributed weight cluster manner.

$$\boldsymbol{EPDR} = \left(\frac{\boldsymbol{Amount\ of\ Sending\ \ messages}}{\boldsymbol{Amountof\ Receive\ messages}}\right) \times \mathbf{100} \qquad \textbf{eqn. (1.3)}$$

Table 1.1: Comparison of Packet Delivery Ratio between Existing Trust-ECC and Proposed LBPPS Algorithm

Number of Nodes	**50**	**100**	**150**	**200**
Trust- ECC	98.25	91.5	88.23	85.99
LBPPS	99.02	93.47	90.09	87.88

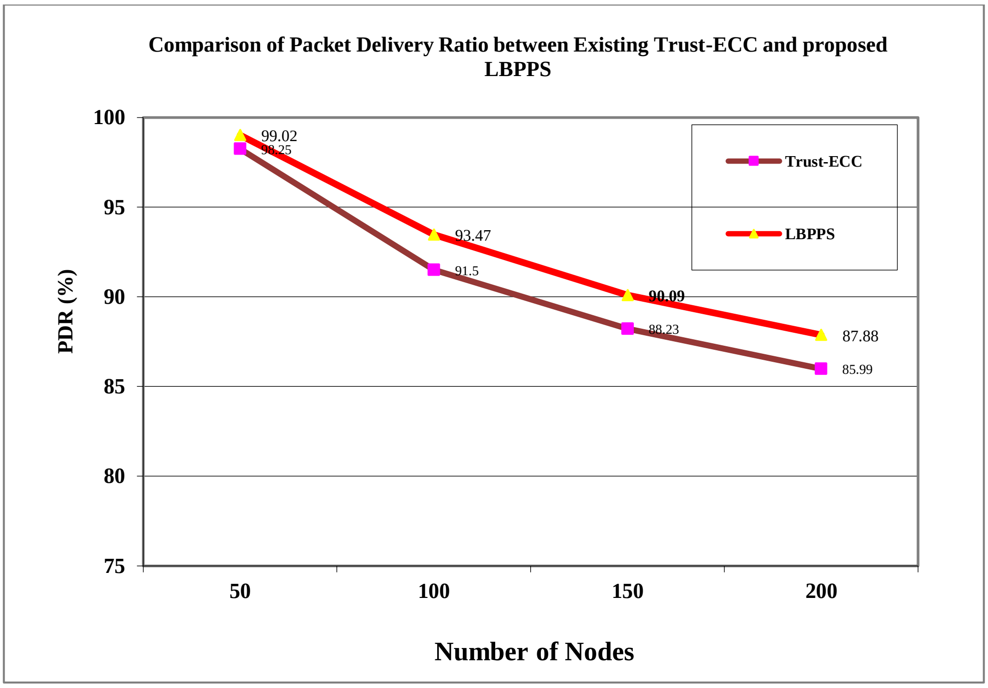

Figure 1.2: Packet Delivery Ratio

Throughput

Comparing the energy throughput of the network is given using Figure 1.3 shows the proposed algorithm's performance of the traditional cache management technique. The Y-axis shows the throughput, and the X-axis shows the Time duration in-network experimentations to represent the network's performance.

$$\boldsymbol{EX = \frac{Number\ of\ message\ requests}{Total\ Time\ duraiton}} \qquad \textbf{eqn. (1.4)}$$

Table 1.2: Comparison of Throughput Ratio between Existing Trust-ECC and Proposed LBPPS Algorithm

Number of Nodes	**50**	**100**	**150**	**200**
Trust- ECC	25.5	26.8	19.5	17.5
LBPPS	24.47	25.18	19.06	15.33

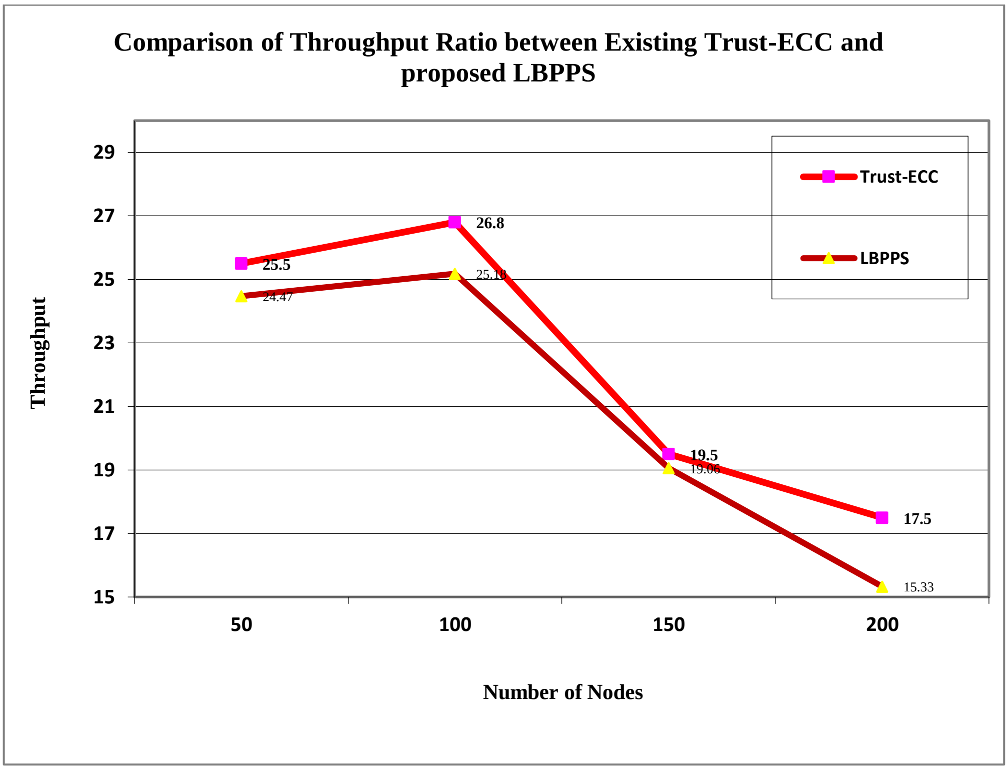

Figure 1.3: Throughput Performance

Routing Control Overhead

Routing control overhead is a measure of the total number of forwarded packets in the network i.e. the number of times it is forwarded. In order to find routes, routing protocols used to send control information (packets). This control information includes route request sent, route reply send and route error sent packets. Routing overhead can be defined as a ratio of the total number of control packets sent to the total number of data packets delivered successfully.

$$\boldsymbol{Routing\ Control\ Overhead} = \frac{\boldsymbol{Total\ number\ of\ control\ packets\ sent}}{\boldsymbol{Total\ number\ of\ successfully\ delivered\ data\ packets}} \quad \textbf{eqn. (1.5)}$$

Table 1.3: Comparison of Routing Overhead between Existing Trust-ECC and Proposed LBPPS Algorithm

Number of Nodes	**50**	**100**	**150**	**200**
Trust- ECC	2.5	8.5	13	15.6
LBPPS	1.8	6.2	10.4	12.4

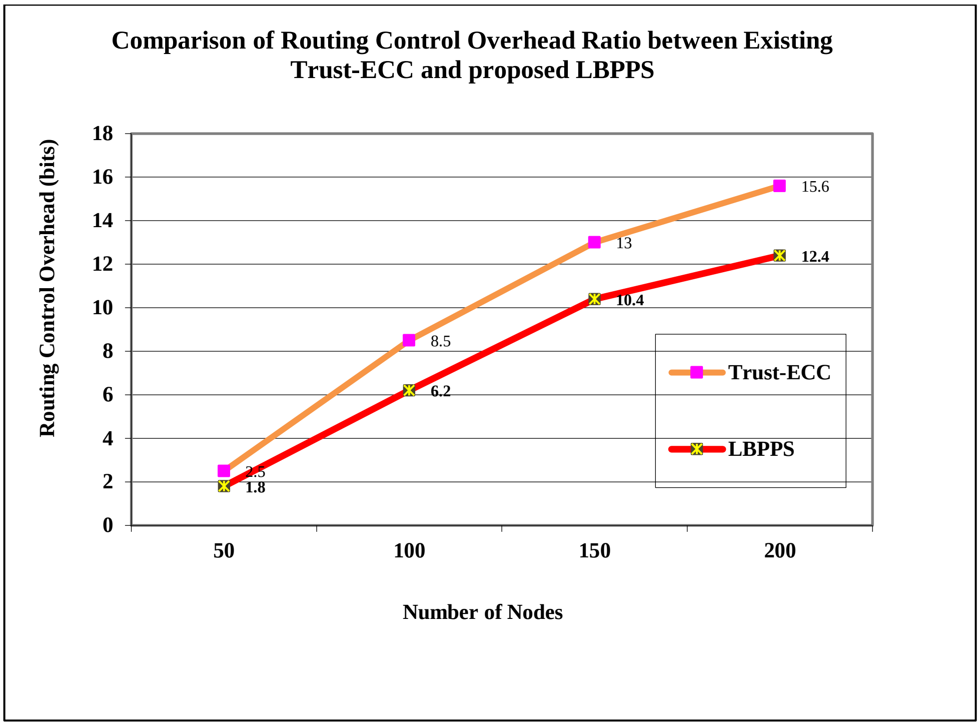

Figure 1.4: Routing Overhead

Packet Loss Rate

The Packet Loss Rate (PLR) is an important performance measure for Wireless networks. Since these data flows are guaranteed, the number of packets lost or dropped during transmission must be kept low. In a transmission interval, the PLR can be calculated as follows:

$$\boldsymbol{PLR} = \frac{\boldsymbol{N^{tx} - N^{rx}}}{\boldsymbol{N^{tx}}} \times \mathbf{100}\ \% \qquad \textbf{eqn. (1.6)}$$

Table 1.4: Comparison of Packet Loss Rate between Existing Trust-ECC and proposed LBPPS Algorithm

Number of Nodes	**50**	**100**	**150**	**200**
Trust- ECC	4	14	18	22
LBPPS	3	11	14	16

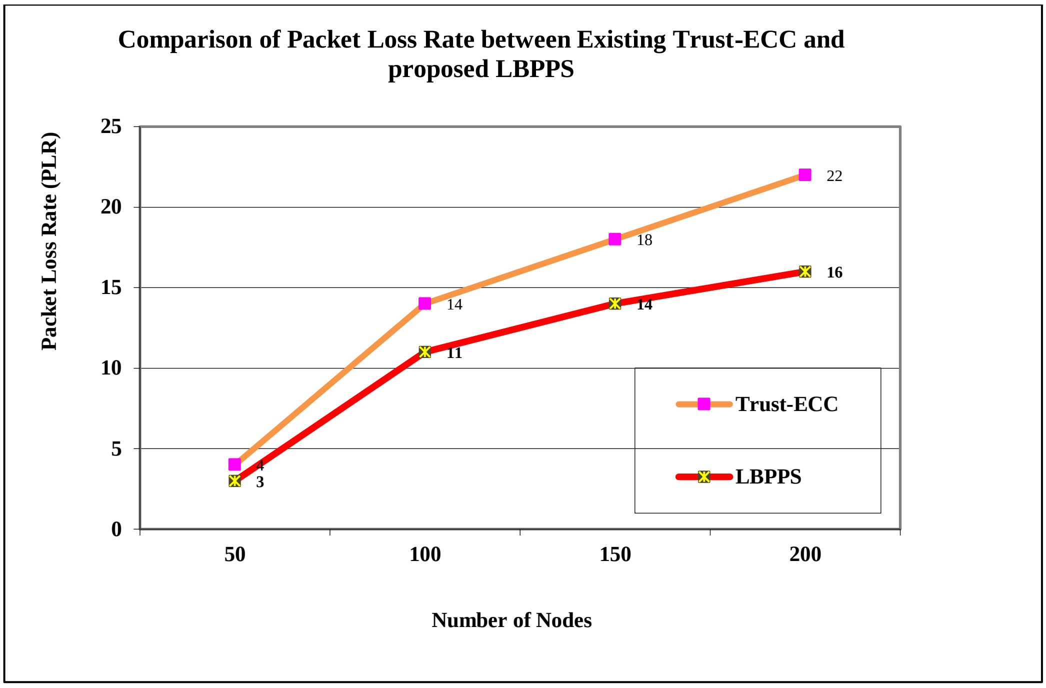

Figure 1.5: Packet Loss Rate

Average Delay

The delay of a packet in a network is when it takes the packet to reach the destination after it leaves the source. The average delay averages the overall transmitted packets in the network. The queuing delay is not considered. A source node sends the packet directly to the destination if it is within the transmission range else it forwards it to the relay nodes.

Table 1.5 Comparison of Average Delay between Existing Trust-ECC and LBPPS Algorithm

Number of Nodes	50	100	150	200
Trust-ECC	0.35	2.42	5.8	8.6
LBPPS	0.32	2.19	4.86	7.2

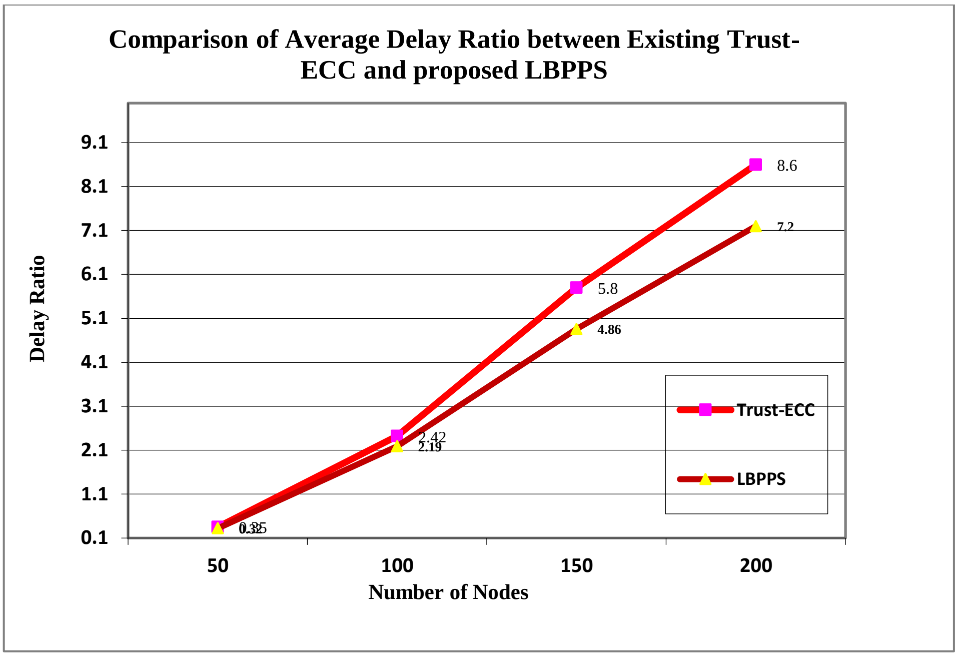

Figure 1.6: Average Delay

CONCLUSION

Wireless systems carry confidential information, and the broadcasting nature makes the transmitting information vulnerable to eavesdropping. This dynamic secret key formed for all the nodes in this research work certainly reduces the threat given in the routing protocol's path. Establishing trusts among sensor nodes can be a practical approach to counter attacks. This is commonly obtained by a system that measures the trustworthiness by a rating system. The load-balancing cluster-based privacy routing model presented handles the load imbalance in the network by the distributing equally to the nodes centrally placed. The research model decides a path which occupies mobile nodes with fewer load using routing metric and a minimization principle.

Through LBPPS load balancing and prevention of attacks are accomplished. The model compared with Trust-ECC methods. The proposed algorithm provides complete privacy path selection, and through trusted key management the quality of secure communication is achieved.

REFERENCES

1. Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y. C., & Jetcheva, J. (1998). A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking* (pp. 85-97).

2. Hasanpour, M., Shariat, S., Barnaghi, P., Hoseinitabatabaei, S. A., Vahid, S., & Tafazolli, R. (2017). Quantum load balancing in ad hoc networks. *Quantum Information Processing*, *16*(6), 148.

3. Wang, Q. W., Shi, H. S., & Qi, Q. (2010). A dynamic probabilistic broadcasting scheme based on cross-layer design for manets. *International Journal of Modern Education and Computer Science*, *2*(1), 40-47.

4. Wang, Y. (2017). Revised Quantum Resistant Public Key Encryption Scheme RLCE and IND-CCA2 Security for McEliece Schemes. *IACR Cryptol. ePrint Arch.*, *2017*, 206.

5. Wang, Y., & Singhal, M. (2007). On improving the efficiency of truthful routing in MANETs with selfish nodes. *Pervasive and Mobile Computing*, *3*(5), 537-559

6. Wang, Z., Ding, H., Li, B., Bao, L., & Yang, Z. (2020). An energy-efficient routing protocol based on improved artificial bee colony algorithm for wireless sensor networks. *IEEE Access, 8*, 133577-133596.

7. Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R. (2014). A survey on vehicular cloud computing. *Journal of Network and Computer Applications*, *40*, 325-344.

8. Yi, X., Paulet, R., & Bertino, E. (2014). *Homomorphic encryption and applications* (Vol. 3). Heidelberg: Springer.

9. Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. *IEEE Network*, *13*(6), 24-30.

10. Zia, T., & Zomaya, A. (2006). Security issues in wireless sensor networks. In *2006 International Conference on Systems and Networks Communications (ICSNC'06),* IEEE, pp. 40-40.

11. Naveed Asghar, M., Fleury, M., & Ghanbari, M. (2012). Key management protocols for secure wireless multimedia services: a review. *Recent Patents on Telecommunication*, *1*(1), 41-53.

12. Odeyemi, K. O., Owolawi, P. A., & Olakanmi, O. O. (2020). Reconfigurable intelligent surface assisted mobile network with randomly moving user over Fisher-Snedecor fading channel. *Physical Communication*, *43*, 101186.

13. Olakanmi, O. O., & Dada, A. (2020). Wireless Sensor Networks (WSNs): Security and Privacy Issues and Solutions. In *Wireless Mesh Networks-Security, Architectures and Protocols*. IntechOpen.

14. Olanrewaju, R. F., Khan, B. U. I., Anwar, F., Khan, A. R., Shaikh, F. A., & Mir, M. S. (2016). MANET–A cogitation of its design and security issues. *Middle-East Journal of Scientific Research*, *24*(10), 3094-3107.

15. Olanrewaju, R. F., Khan, B. U. I., Mir, R. N., & Shah, A. (2015). Behaviour visualization for malicious-attacker node collusion in MANET based on a probabilistic approach. *American Journal of Computer Science and Engineering*, *2*(3), 10-19.