International Journal on Applications in Electrical and Electronics Engineering
Volume 9 : Issue 3 : May 2023, pp 1 – 5 www.aetsjournal.com ISSN (Online) : 2395 - 3527

Self Improved Optimal Load Balanced Routing (SI-OLBR) Approach for Reliable and Secured Wireless Sensor Network (WSN)

*[1]Dr. R.Kannan , [2]Dr.Sobha Manakkal
*[1]Department of EEE, Nehru Institute of Engineering and Technology, Tamilnadu, India
nieteeehod@nehrucolleges.com
[2]Department of EEE, Nehru College of Engineering and Research Centre, Kerala, India.

***Abstract*—** Multihop networks uses the following approaches: wireless sensor networks (WSN), vehicular ad hoc network (VANET), mobile ad hoc network (MANET) and wireless mesh network (WMN) to disseminate data from one place to another. In this paper, we consider routing protocols which uses cross-layer design, now a fundamental design concept among researchers. It considers quality of service (QoS) by analysing several network types and the challenges encountered within each. The primary performance metrics are: Minimum Throughput, Maximum Delay, Maximum Delay Jitter, and Maximum Packet Loss Ratio. Best optimal routing decision considers constraints like distance, energy and risk factor of the route obtained from Self Improved Optimal Load Balanced Routing (SI-OLBR) algorithm. For each optimal path risk factor is calculated based on the threshold and based on that the data privacy requirements are satisfied using Elliptic Curve Cryptography.

***Keywords*—** Multihop Wireless Networks, WSN, VANET, MANET and QoS

I. INTRODUCTION

WSNs :one of the most essential component of Internet of Things (IoT) Technology, it plays an interesting part in providing IoT operations employing sensor nodes such as Bio monitoring, agriculture to cultivate crops of better quality , security for unauthorized forbidden area and disaster management etc. The WSNs is the group of hardware devices and other components embedded with internet and sensors, WSNs give the relaxation to the interconnected components to monitor sense and control the framework of connections and results in direct integration of the mathematical model and the physical world.

Moreover, the internetworking gives the opportunity to transfer data with reduced human intervention. As the WSNs are vulnerable to numerous threats and attacks, we need to provide security for reliable transmission of data. Therefore, to provide better security, effective cryptographic security models are the need in today world. Due to the heteromorphic feature of WSNs, classical approach falls out unconditionally. Here, we propose Elliptic Curve Cryptographic (EEC) model to secure the network against attacks. Security issues related to verification, validation, reliableness, confidentiality is addressed through ECC model.

The major challenges that we may face in designing secured and effective routing model for WSNs are:

• Trade-off between performance and security, a determined requisite for heteromorphic WSNs

•To detect outliers i.e. Components that fluctuate from good to bad state often.

•Load balancing among cluster head of various clusters is exigent because the existing routing model every time routes packet to the node with good trust parameter increases the difficulty among cluster heads.

This research focuses to balance between reducing latency, energy efficiency and reducing difficulty in providing security for WSNs, respectively, Nevertheless, the current trust-based routing model does not separate the passive WSNs devices from the well-behaved WSNs devices and induces energy overhead. For heteromorphic wireless sensor networks, this study attempts to route packets through the least energy-intensive cluster head with the best trust parameter. This will help to provide optimal security and network longevity. The Self Improved Optimal Load Balanced Routing (SI-OLBR) Method for Dependable and Secured Wireless Sensor Network is what we present in this paper (WSN).

The Low Latency Energy Efficient Clustered Based Multipath (LLEECMP) routing technology is used by the SI-OLBR model (Gousia Thahniyath and Jayaprasad, 2018). Using different energy categories, the LLEECMP elects cluster heads (low to high). Real-time and non-real-time data packets are transmitted using distinct paths with the LLEECMP technology, with packets being routed along the shortest way (i.e., to reduce latency). Also, to increase security, LLEECMP incorporates the Elliptic Cryptographic Curve (ECC), a security mechanism used by SI-OLBR. The SI-OLBR trust metric is intended to precisely establish feedback credibility, identify oscillating devices that are changing from a good to a bad condition and vice versa, and to determine the security of the sensor devices in the future. A load balanced routing metric is also offered in the SI-OLBR model to reduce overhead among CH. The SI-OLBR model assists in giving better security with packet transmission and

energy efficient performance.

II. Literature survey

Here, we provide a thorough analysis of many current secure routing models and techniques for WSNs. For meeting Quality of Service (QoS) and security requirements for various applications, a number of trust-based models were already presented. Bayesian-based trust computational model for hierarchical routing in WSNs was developed by (Meng et al., 2018) to address the concerns mentioned. The malfunctioning sensor devices are found using the trust threshold settings, and the reliability is calculated using the packet status information.

Entropy is employed as a metric in (Zhao et al., 2019) published Exponential-based Trust and Reputation Evaluation System (ETRES) for evaluating Direct Trust (DT). Additionally, Indirect Trust (IDT) is applied to increase reliability. The trust weight can be changed at random by the model to lessen the impact of damaged sensing devices.

The multi-attribute-based trust aware routing approach for WSNs by Sun and Li (2018) uses improved sliding windows to route data utilising sensor devices that have superior quality, energy, and communication parameters. The computational model takes attack frequency into account when identifying malevolent traits in invaders.

The modern Internet of Things application must transfer packets in an unstable and unreliable environment, as demonstrated in (Sedjelmaci et al., n.d.). As a result, unstable channels can cause packet failure. Thus, these sensor nodes shouldn't be disregarded as malicious nodes. In order to overcome these issues, Lyu et al. (2019) offered a theory in which the current approaches use the Geographic Opportunistic Routing (GOR) mechanism. Nevertheless, the GOR mechanism is vulnerable to Denial of Service (DoS) attacks (Raymond and Midkiff, 2008), which occur when a hostile device sends out-of-date packets to a sensor device's receiver, impairing the wireless sensor network's ability to function normally. Lyu et al. (2019) developed Entropy-Based Selective Authentication based GOR technique, where dependability is estimated utilising wireless link, for compromising DOS attack and modelling reliable protocol.However, validating signature for every sensor nodes induces overhead of significant delay.

Comes with an upgraded beta version for detecting fraudulent sensor devices in (Umarani et al., 2016). During the transmission phase, the neighbour node is selected entirely on the basis of reliable information. The nearby sensor node is periodically updated. With this update, WSN power efficiency is improved. The trust version, however, does not take into account strength or memory limitations. Threats were discussed in (Labraoui, 2015) taking fluctuations into account. The consensus algorithm determines how much direct and indirect trust is used.

Many techniques are taken into account for performance and protection individually in (Khalid et al., 2019). A prerequisite for heterogeneous WSNs (LLEECMP (Gousia Thahniyath and Jayaprasad, 2018) model) was developed to address research challenges in bringing tradeoffs between security and performance, and this paper uses a trust-based safety model for heterogeneous wireless sensor networks in a manner similar to the prerequisite.

III. Dynamic CH Selection and Self Improved Optimal Load Balanced Routing (SI-OLBR) Approach

A. Problem Statement:

The most interesting challenges with WSNs are: For WSNs to be load balanced, selection of optimal solutions (choosing best Cluster Head) must be addressed. Only when the appropriate technique is given at-most priority, distance and energy, the network energy usage decreases randomly. Both large and small-scale WSN applications could benefit from the energy-efficient WSN. In WSN, instant transmission of data from CH to BS uses more energy. It causes the network's hot spotlight problem, which results in loss of packets. Due to node's deployment in an antagonistic and uncertain situation, the sensor node becomes inefficient and malfunctioning. More ever, while transferring data from source to their destination, the nodes' energy consumption is a major concern. As consequences of nodes' lack of energy, data packets are dropped at faster rate. The routing considers residual energy of the devices, the distance between them, and the hop count of each cluster as optimal solutions. The packet loss across network gets reduced drastically when these parameters are taken into consideration. As a result, load balanced WSN is designed to perform well in both large and small-scale WSNs.

Two factors for cargo balancing variables can be determined from the characteristics of WSNs (limited bandwidth, disconnections, etc.). The first is node communication overhead, and the second is the state of the wireless link. The first one deals with overheads that are anticipated at each node, while the second one deals with the state of wireless links between neighbouring nodes. As a result, parameters, which are essential for communication, are extracted from node data itself. a) Communication overhead parameters a) Wireless link status parameters

B. Communication Overhead:

How much overhead or load is anticipated to be induced at each node has an impact on communication overhead. The node itself provides the information on communication overhead. A node under high pressure will certainly experience congestion because of the increased traffic. Four different parameters can be used to efficiently measure communication overhead. The first is the typical number of packets received over a range of predetermined time periods. More reception entails higher overhead. The next total number of neighbours is a crucial variable in determining how much pressure (traffic) the node will experience or is already experiencing. Energy is the third criteria. Increased energy use results in higher overhead. The amount of entries in each node's current routing table is the final consideration.

The typical quantity of packets received: Every node has a

limited amount of memory. Each node stores the number of packets it handled during routing. This component gives the actual task a higher priority (i.e. the actual packet routed during communication). The node is under significant stress and will experience collision and congestion if the count exceeds a threshold limit. The full count of neighbours: Dependent on a node's number of neighbours, a node's stress level. Naturally, a node situated in a dense deployment is anticipated to engage in more packet transmission, processing requests and responses, than a node situated in a sparse deployment. Total number of neighbours, also known as node degree, is the quantity of nodes with which a node is directly connected. As a result, the level of communication overhead will change depending on how densely the network is deployed. A node's energy level is: Battery life might be a reliable indicator of a heavy communication load. A node using more energy indicates that it was handling more requests and responses. The energy level of a node is hence the third consideration for determining communication overhead. Although all sensor nodes typically begin their operations with the same battery level, a low battery level at any given time is a sign that the node is under extreme pressure and will likely fail sooner than the others. Each node's total number of entries in a modern routing table: In comparison to the first two, the third component is more specialised and is dependent on the number of routing entries on each node. Entries specify the number of nodes to connect with or the overhead used to choose the next hop. When the number of entries increases, the strain on the node increases, necessitating load balancing to alleviate congestion.

C. Wireless Link Status:

It is connected to the communication nodes' present link status. Every network is highly important, thus factors displaying Wireless link status can be checked to balance load in the network. Poor quality wireless medium can cause serious issues with communication. The time required to fully transmit the message over the link is the average retransmission time. Wireless links are highly erratic, and communication through them is not very reliable. The packet delivery ratio partially demonstrates connection dependability. In order to recover lost packets for reliable wireless communications, retransmission methods are typically used. Retransmission is necessary for an undelivered message. Retransmission techniques guarantee message delivery. Thus, the average transmission time is a substitute parameter for link Status. This value lengthens due to retransmission and queuing delay. Ratio of typical packet delivery: It displays the transmission success rate as well as the link's properties. It measures the proportion of all delivered packets to the destination. A trustworthy link that can send more packets without error has a high delivery ratio. As a result, network performance is also evaluated in terms of the likelihood of packet loss. These settings can be set, and then combined with a special greedy forwarding mechanism. We won't just utilise the distance as a parameter for packet forwarding; we'll also use the other parameters mentioned above.

D.Methodology

The Self Improved Optimal Load Balanced Routing (SI-OLBR) method will be explained in this section. We will also discuss some of the presumptions used in this work and the estimation of the cost of sending a package to its destination. In this route, greedy forwarding is used, which can cause collisions, traffic jams, and occasionally network disconnections. Our suggested technique does not just route traffic based on the shortest distance between the destination and the following hop. Now, both the greedy approach and traffic at nodes will be taken into account for packet forwarding. In SI-OLBR, we select the number of packets received in the predetermined time factor for cargo distribution from the load debating techniques. We keep a record of the traffic that went through each node. According to the overhead or load at each node we will switch to another better alternate node.

E. Assumptions for simulating SI-OLBR

We consider a number of assumptions. Every wireless sensor node is assumed to have a GPS or some other kind of localization that enables it to be aware of its location. Routing (SI-OLBR) assumes that nodes can transmit beacons to interact with nearby nodes. Beacons include data about the node's traffic volumes. Also broadcast is the distance between the base station and the node. There are additional topology considerations to be taken when the network is placed in a plane. There are bidirectional links between sensor nodes, and their distance from one another determines whether or not a link is there. A pair of nodes is considered to be in range if their distance is less than a predetermined threshold. Last but not least, we assume that each packet source is aware of the packet's destination. This data is kept in the node's cache and aids in choosing the next hop for packet forwarding.

F. Algorithm for SI-OLBR

The implementation of the SI-OLBR algorithm is divided into three main sections. The deployment of the network comes first. Next, it is determined how much it will cost nodes to deliver a packet to its final location. Third on the list is a description of the SI-OLBR algorithm. The initial step in network deployment is to randomly distribute N WSN nodes across a boundary region on a two-dimensional plane. N can be anywhere between a few hundred and a few thousand nodes. b) The transmission range places a restriction on a node's ability to communicate. As a result, a transmission range is supplied to each node. Some connections are reciprocal as well. c) Two nodes are considered neighbours if the separation between them is less than their transmission range. The distance formula can be used to compute this distance in a 2-D coordinate system. If one node's coordinates are (W1,W2) and another node's coordinates are (X1,X2), their distance from one another is: (1) Calculating the cost function choosing the following hop The cost of a node to transport a packet, which depends on the node's energy level and the distance to the base station, is also taken into account by SI-OLBR. It goes without saying that longer distances and

low energy produce high costs. The GEAR [5] formula can be used to determine how much it costs a node to send a packet. The tuneable weight value will be set between 0 and 1.

G. SI-OLBR Overview:

Each node in SI-OLBR will determine how much it will cost to send the packet to its destination. Cost is now a function of the energy level and distance between the node and base station. All node neighbours will be informed of this information via broadcast. Now, nodes will forward packets based on the load at a specific node while taking the load balancing parameter, or the amount of packets received. Traffic will be used to define load. A certain node's load has three levels. These levels depend on the state of the network. High values increase the network's vulnerability to issues like congestion and collision. This is because a system with high values might be able to withstand changes in traffic. Small values result in frequent packet routing changes. Load level is marked by LL1, LL2, LL3 etc. Each node maintains a sorted list of neighbours according to cost for delivering the packet.

H. Self Improved Optimal Load Balanced Routing (SI-OLBR) Approach

1) Algorithm:

*If X=W [0] is the next hop list, then

**When the load is at LL1 level. The load at the node is at level LL if (T.L==LL1). Next, decide which node to jump to next.

a) Find a node W[x] such that the cost of the next node should be less than the sum of its current neighbour cost and half of the deviation in costs of forwarding node and current neighbour, and load level should be LL1 when the load is at level LL2 or else if (T.L==LL2), Load at the node is at level LL2. Choose W[x] as the subsequent node.

b.) If (T.L==LL3), then when the load is at level LL3. Find a node to get the next hop list for x=0 to find a node W[x] on the nodes' next hop list such that the load level is LL1 and the cost of the next node is less than the total of its current neighbour cost and half of the variance in costs of forwarding node and current neighbour. Choose W[x] as the subsequent node.

c.) Once the load reaches level LL3 or if (T.L==LL3). Find a node with a cost lower than forwarding nodes and a load level lower than LL2 for x=0 to the node's next hop list.

A list of potential next hop nodes is kept by SI-OLBR and is arranged by cost. Now, cost-based greedy forwarding will be considered rather of only geographic distance. But before sending to the node, SI-OLBR first assesses the load there. It selects a node from a list of neighbours whose cost to send messages to the destination is the least. The load at this node will now be determined using SI-OLBR. The load at a node is determined by the packets it has received in a predetermined amount of time. The first scenario is when the load level is LL1. There were hardly any packets that the node was involved in routing at level LL1. To this node, a packet will be routed directly. Now that the load level has not increased significantly, the node is not the centre of traffic. In comparison to all of its neighbours, it also has the lowest delivery costs. While the node is only routing a small number of packets, there is no congestion at this level. Moreover, there is no collision concern. Until a better alternative is not accessible, the node will keep sending packets to the present node continually. Now imagine that the volume of traffic has increased and has reached level LL2. The node has a load of LL2, which indicates heavy traffic. Although there is extremely little possibility of a collision or congestion at this level, it is still preferable to choose a different next hop. When two nodes have identical locations, switching to another hop is necessary. Additionally, their energy levels are nearly same. Now that one node may be continuously receiving packets in this scenario, it is best to search for a different node to increase the likelihood that no single node carries all traffic. Currently, a node whose cost to supply is less than the sum of its current neighbours' cost and half of the variance in cost between it and its current neighbour may be used as the next hop criteria. If load level at this node is LL2 or LL3 then switching to alternate is not an intelligent move. Because the load is already quite severe and node is congested so no need to choose such nodes. Switching to alternative is not a wise choice if the load level at this node is LL2 or LL3. There is no need to select such nodes because the load is already pretty heavy and the node is crowded. Another requirement is that the node's load should be at level L1. Now imagine that a node is situated in a crowded area and that numerous paths lead to the destination between them. As a result, such a node will continue to grow while routing a lot of traffic. Switching to a different node is necessary when the load on such a node reaches level L3, which is when the situation becomes critical and packets may get dropped. The prerequisite for switching to an alternative node is that the new node's delivery costs must be lower than those of the forwarding node. The reason we are selecting this node is that it can divert the packet to a node that is far away from the sender. Thus, the following hop's cost should be less than the sender's own to avoid this. The load should also be at level LL2 or lower. Level LL3 is extremely important since the node is stressed out at this level. Due to the huge volume of traffic it is directing, the node's energy level is steadily decreasing, and it could soon fail. This can cause a network disconnect. Moreover, packets will be dropped owing to congestion and collision. Retransmission will therefore be available to offer trustworthy communication. This causes the network processing to lag and become slower. Collisions and congestion can be prevented by taking load—the volume of packets the node was responsible for routing—into account.

The major driving force behind the routing strategy is that state kept at nodes is essentially nonexistent, making packet delivery less expensive than with traditional routing algorithms. To enable load balancing on densely deployed wireless networks, we have introduced Geographic Load Balanced Routing, SI-OLBR, a geographic routing method. When network density rises, our approach outperforms GEAR in terms of performance. In this study, we address the greedy

forwarding limits that occur when packets always travel the same path to their destination. This stress causes energy loss at some nodes, which causes disconnections. With greedy forwarding, SI-OLBR manages collision and congestion well. In contrast to conventional greedy forwarding, this method avoids early network disconnections. To achieve load balancing, we have suggested criteria depending on communication overhead and wireless link state. The amount of state required at nodes is significantly less than in typical ad hoc techniques and is proportional to neighbours. According to simulation, SI-OLBR successfully transmits 96% of packets on average. Through this effort, we hope to explore new concepts. In networks with immobile sensor nodes, SI-OLBR manages geographic routing difficulties (collision and congestion). Since there are more and more application domains for WSNs, such as medical care and disaster management, we plan to deploy SI-OLBR for networks with mobile nodes in the future. The precision of the underlying localization technique affects the mobility accuracy in geographic networks. Hence, location estimate in SI-OLBR for adding mobility is difficult in and of itself. It is challenging to introduce mobility into this work because of time constraints, but it is possible in the future.

IV. Conclusion and Future Work:

The Self Improved Optimal Load Balanced Routing (SI-OLBR) Method for Dependable and Secured Wireless Sensor Network protocols used for network routing in IoT applications are examined in this research. This research examined ten routing protocols. The most widely used one is RPL. A distance vector protocol is used. For cognitive networks, ETRES is a nonstandard version of RPL that uses opportunistic forwarding to forward packets at each hop. For IoT sensor network applications, however, ETRES is the sole distributed hop-based routing system. Most commonly, ETRES is utilised for underwater communication. It is not yet utilised in other IoT applications because it is not standardised and has only been proposed in literature. A development on CARP, GOR is a location-free, greedy hop-by-hop routing protocol for efficiently forwarding packets from sensor nodes to the sink node. The relative importance of various qualities is not differentiated by ETRES. A more general traffic pattern is catered to by SI-OLBR. There is no single point of failure, a longer route discovery phase, and more control traffic in SI-OLBR if traffic is primarily peer to peer. SI-OLBR also offers a flexible and compressible packet format.

V. References:

1. Feeney, L, B. Ahlgren, and A. Westerlund, 2001. Spontaneous networking: an application-oriented approach to ad hoc networking, IEEE Communications Magazine, 39(6), June 2001.

2. Special issue on ad hoc networking. 2. Kuosmanen, P., 2002. Classification of ad hoc routing protocols, Finnish Defence Forces, Naval Academy, Finland.

3. Stojmenovic, I., and J. Wu, 2003. Broadcasting and activity-scheduling in ad hoc networks, in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York.

4. Belding-Royer, E.M., and C.-K. Toh, 1999. A review of current routing protocols for adhoc mobile wireless networks, IEEE Personal Communications Magazine, 46–55.

5. Freebersyser, J.A., and Barry Leiner, 2001. A DoD perspective on mobile ad hoc networks, in: Charles E. Perkins (Ed.), Ad Hoc Networking, Addison Wesley, Reading, MA, pp. 29–51.

6. Corson, M.S., J.P. Maker, and J.H. Cernicione, 1999. Internet-based mobile ad hoc networking, IEEE Internet Computing 3 (4) pp. 63–70.

7. Chlamtac, I and A. Lerner, 1986. Link allocation in mobile radio networks with noisy channel, in: IEEE INFOCOM, Bar Harbour, FL.

8. Chlamtac, I, and A. Lerner, 1987. Fair algorithms for maximal link activiation in multi-hop radio networks, IEEE Transactions on Communications COM-35 (7) pp 739-746.

9. Perkins, C.E., and P. Bhagwat, 1994. Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers, Computer Communications Review pp. 234–244.

10. Chiang, C.C., H.K. Wu, W. Liu, and M. Gerla, 1997. Routing in clustered multihop, mobile wireless networks with fading channel, in: Proceedings of IEEE SICON-97, pp. 197–211.

11. Murthy, S., and J.J. Garcia-Luna-Aceves, 1996. An efficient routing protocol for wireless networks, ACM Mobile Networks and Applications (MONET) Journal, Special Issue on Routing in Mobile Communication Networks, pp. 183–197.

12. Jacquet, P, P. Muhlethaler, and A. Qayyum, 1998. Optimized Link State Routing Protocol, Internet Draft, draft-ietf-manetolsr- 00.txt