International Journal of Advance and Innovative Research
Volume 12, Issue 3: July - September 2025
ISSN 2394 - 7780

STRR-A SECURE TRUST BASED ENERGY EFFICIENT RUMOR ROUTING PROTOCOL FOR MANETS

[1]Divya.M.P and [2*]Dr.S.Prema
[1]Research scholar, Department of computer Science, Periyar University, Salem, Tamilnadu, India
[2]Assistant Professor and Head of computer Applications, Arulmigu Arthanareeswarar Arts and Science College, Tiruchengode
[1]divyarajesh05@gmail.com

ABSTRACT
The dynamic behavior of mobile ad hoc networks (MANETs) poses security problems and risks, which leads to a variety of attacks. The key challenge in MANETs is establishing a viable route among both the source and the destination. The Node mobility generates frequent link failures and their error rates are high, it is challenging to maintain the required Quality of service (QoS) in the network. A Secure Trust based energy efficient Rumor routing protocol (STRR) is suggested to address all of the prevalent issues concerning MANETs. Initially, the trust values are calculated using the adaptive trust value, energy trust value, and indirect trust value. The suggested STRR method is compared with the present routing method based on the parameters like as Energy consumption, packet delivery ratio, delay, network lifetime and throughput in NS2 simulator. The system had reduced delay, increased packet delivery ratio, reduced energy consumption, high network life Time, and high throughput in comparison with the existing models like trust-aware routing framework (TARF), Security Based Data Aware Routing Protocol (SDARP). The delay for 100 nodes was 18.946113 compared to values 22.864729 and 30.986795 for TARF and SDARP which was lesser than the existing system.

Keywords: *Manet, Packet delivery ratio, Network life time, Throughput.*

1. INTRODUCTION

An active, self-structuring network made up of active nodes that are free to move around is referred to as a MANET (mobile ad-hoc network).This node has an independent radio band. Because of limited radio range and mobile nodes might, in some circumstances, be unable to disseminate the information. Similar to this, if the transmission enters the appropriate radio ranges, it is kept by using next hop as a mediator.This aids in keeping wireless environments and applications operational [1]. But there are a number of security and performance issues with MANET routing due to the topology of the dynamic network, use of a resource, and open wireless media limitations [2].The fact that link breakages can cause established connections to be disrupted,however, is one of the biggest problems with MANET [3].

There has been a significant amount of work done on MANET routing design, but none of it takes into account how node distribution, which changes over time and affects route stability, may have an impact. Improved routing topology and the use of mobility prediction models research [4]. Routing problems persist despite numerous efforts to improve MANET performance. It focusses on the efficient path maintenance systems. Most often used in setting up group communications and video conferencing, one widely used technology is multicast routing. [9]. Time, delay, and bandwidth consumption are reduced by multicast routing [5]. Several defined algorithms are available for enforcing secure routing. Some algorithms consider the sensor power when choosing the reliable nodes along the route [6].

Reliability, security, access control, routing, and erg use are challenges in MANET. The solution to these problems is the secure implementation of a routing protocol that can identify abnormal nodes and can be eliminated to improve the performance. Data communication in MANETs must be secure [7]. Adopting a behavioral modelling approach is essential for protecting nodes by getting to know them better before sending a packet to them [8]. WSNs are made up of sensor nodes, which are small things with built-in sensing capabilities and form ad hoc networks. The following qualities should be present in sensor nodes: extensive coverage areas, extremely precise monitoring, self-organization, and random deployment, fault tolerance, etc. [9]. High nodal mobility and short transmission distances, however, result in rapid node-to-node communication. The calculation of best trust value for malicious node detection is one that operates in all circumstances is challenging because the behavior of nodes in MANETs can change quickly [10]. MANET has found extensive use in fields like military communications, communications in disaster zones, and emergency rescues as a result of its adaptability and dynamic nature [11].

The majority of the Manet connected devices run on batteries. Therefore, when estimating the effectiveness of routing algorithms for MANETs, the power consumption of these devices is a very important factor. A node could die very quickly as the energy level of the devices drops quickly [12].

ISSN 2394 - 7780

For network-based operations that are embarrassed by nodes, battery power is needed. In these networks, energy management was a major issue. The crucial source that can be used skilfully to prevent the nodes' early breakdown that causes the fragmentation of the trail was battery power [13]. Lot of security and performance issues with MANET routing due to dynamic network topology, application of a resource, and open wireless media limitations [14]. Congestion may occur because, if there is a link malfunction or a queue overflow, Manets operates in a smaller transmission range. Due to this congestion, there may be packet losses, increased overhead, delays when sending packets, and limited bandwidth, all of which have a substantial detrimental effect within the network's essential QoS [15]. Our research tries to address the highlighted issues in the Manets.

The contribution of the work is listed as follows:

- Make a suggestion a Secure Dependability-based Energy Efficiency Rumor Protocol for Routing (STRR) Regarding Manets using Rumor Routing protocol.
- To perform the elimination of the malicious nodes and assure a secure Routing with the help of the specially designated Monitor nodes.
- To compare the STRR systems performance with the existent trust-aware routing framework (TARF), Security Based Data Aware Routing Protocol (SDARP).

The document reminder is organized in the following order: The 2nd section illustrates the review of the recent work, Section 3 details the suggested methodology, and the 4th section explains the way the model is evaluated and discusses the results produced. The 5th section gives a briefing on the end and the upcoming projects to be done.

2. LITERATURE REVIEW

"Some of the recent research works related to secure framework based on trusted nodes were reviewed in this section"

Kasthuribai et. al., [16] suggested a routing method. They provided a particle an algorithm for route selection in multipath. The network's established routes were used to select an optimal path using the algorithm for cuckoo searches, which operates according to cuckoo behavior and addressed the issue of declination of the quality of the route link due to numerous transmissions.

Shivakumar et. al., [17] cross-layer routing protocol is a method that applies the algorithm known as particle-swarm optimization (PSO). Paths after Network layer measurements node mobility, information success rate and predicted remaining vitality. Based on the estimated remaining vitality and measured dispute, the window of contention (CW) is dispute, the window for dispute (CW)after the MAC layer has measured the conflict on the network and established the collection of routes using PSO.

Jabbar et. al., [18] have put forth a routing protocol The issues brought on by node mobility will be addressed by a lack of energy resources, causing traffic jams in MANETs when data is being transmitted. This procedure employs a node rank that combines various energy and QoS-related parameters into an all-encompassing measure to significantly the intricacy of many limited considerations is reduced, and the overhead of control brought on by independent broadcasting many parameters is avoided. These measurements are the life of the node, remaining battery power, queue, speed, and idle time size.

Bento et. al., [19] had suggested using the dynamics of fungi to develop a bio-inspired method for creating, optimizing, and choosing MANET routes. The routes are constructed like a fungal mycelium, which initially forms a number of parallel routes are formed. However, over time, biomass is only sent to the optimum routes for wall thickening and reinforcement, remaining and displaying higher flow attractiveness. Following the principle of attractiveness, the routing procedure directs data traverse areas (nodes and linkages) with higher concentration of immobile biomass, which denotes less expensive and more resource accessibility.

Alappatt et. al., [20] have put forth a mixed strategy, to increase the networks life by Combining Swarm Optimization with Binary Particles along in the optimization of ant colonies. Two modes of active and sleep states were addressed here. The shuffling both the modes was made easier for each node.

Mohsin et. al., [21] have suggested creating a mechanism to consider link quality when making forwarding decisions to raise the delivery rates within the packet while and shortest route choice was ensured, improving link stability. In order to enhance usage of limited resources on the network and consistently identify superior linkages, these two methods are suggested. Signal Strength as well as congestion Avoidance Hybrid Geo-cast

ISSN 2394 - 7780

Routing (HGR) protocol and SSCA protocol (SSCA). The most flexible and successful HGR technique uses geographic where data to limit the search space throughout the finding of the route by only to cut down on control overhead, include promising search paths.

Jamal et. al., [22] had examined all these attacks. MANETS are highly susceptible to several kinds of assaults since they are wireless. One of the black holes is the most well-known assaults against wireless networks. In which a rogue node advertises a false sequence number and hop count to draw traffic to itself. Among these Ad hoc on-demand distance vector routing and routing protocols is one (AODV). It is a very popular protocol for routing, and black hole attacks can be very damaging to it. An attack by a black hole uses a mobile node accidentally discloses the route and sinks inadvertently sending data bundles to the incorrect location instead of the intended destination.

Khudayer et. al., [23] a link failure prediction system and a Zone-based route finding system. Those seek to regulate the coding of the path requests and seek to prevent route breaks brought on by node mobility. Regarding normalized routing load, typical packet delivery ratio, and end-to-end latency, the proposed mechanisms that performance was assessed using NS3

Yu et. al., [24] had unveiled a routing measure that combines a node's requirements for dependability and performance, creating the ideal routing method. A node develops an opinion of the reliability of the nearby nodes according to its findings of the behaviors of the neighboring nodes. An illustration of such an integrated protocol, in which a node bases its routing choice on the performance and trust it has in its nearby nodes.

Jubair et. al., [25] suggested a protocol to reduce the vitality consumption of the MANET's technology known as Optimized Link State Routing (OLSR). The OLSR of MANET and the Bat Algorithm (BA) are similar in that they both use sending and receiving particular signals to determine the path. The BOLSR protocol was developed as a result of this symmetry and uses the nodes' energy dynamics to ascertain the optimal path between a source node and a destination node.

2.1 Issues in Manets in Routing:

This section discusses the aspects of MANET that make designing routing protocols more challenging and expose them to security risks. The following are problems with Manet:

- The main reason for routing is to determine the best and most precise route to a final destination. It is possible to determine the best path to a location by taking into account a number of variables, such as hop length, secure route, power consumption, and wireless link stability. Links frequently break down, and because MANET routes are mobile, they are unstable. Thus, the creation of a routing protocol capable of accommodating all routing changes is the primary requirement of MANET.
- Controlling energy sources and consumers in nodes or across the network is known as energy management, and it helps to prolong the life throughout the network. On-demand wireless networks employ nodes that perform the roles of both hosts and routers, which run on batteries and have a limited lifespan. They therefore place a high value on using and managing energy. In ad hoc wireless networks, Nodes function as both hosts routers, and they are battery-operated and have a limited lifespan. As a result, they give careful consideration to how much energy is used. Most routing and security-related network protocols, however, are appropriate for wired networks, which are assumed to have static nodes and an electricity supply, and haven't given power consumption much thought.
- Because MANET nodes are wireless, they may move both within and outside the network, causing it to continuously and dynamically change its wifi topology and connectivity. Additionally, the connection in between nodes may be either unidirectional or bidirectional.
- Wireless links between MANET nodes offer significantly less bandwidth than wired links. As a result, Congestion, noise, and interference are more noticeable in ad hoc networks, changing the available bandwidth according to the environment and frequently resulting in reduced bandwidth.
- Because of movement and a lack of infrastructure, ad hoc wireless networks are more vulnerable to attacks at the physical layer, including jamming, spoofing, eavesdropping as well as DOS (denial of service).
- Digital assistants, laptops, and cellphones are just a few examples of the compact and portable MANET hardware (PDAs). There are limitations on these devices' power supplies, processing speeds, and storage capacities.

ISSN 2394 - 7780

- Due to the absence of a stationary infrastructure, nodes that move, join, or leave the system must self-organize and reconfigure. Every node in the network is a peer node, with no hierarchy or centralized management.

3. PROPOSED METHODOLOGY

This section uses a trust-based security model to create behavioral modelling for MANET-IoT (Mobile Ad hoc Network). The model of trust, which comprises indirect, straightforward and energy trust between the various sensor nodes, verifies each node before packet transmission. The MANET nodes can function as hosts or nodes. The basic structure of MANET is illustrated in Fig 1. An interconnected system of wireless nodes known as An MANET, or mobile ad hoc network, is used for Wireless communication over links with limited bandwidth. Each wireless node has three different roles: sender, receiver, and router. When a node is a sender, it can send messages via a route to any destination node that is specified. It serves as a receiver and can take in messages from other nodes. The node can relay the packet to the destination or the following router along the route when acting as a router.

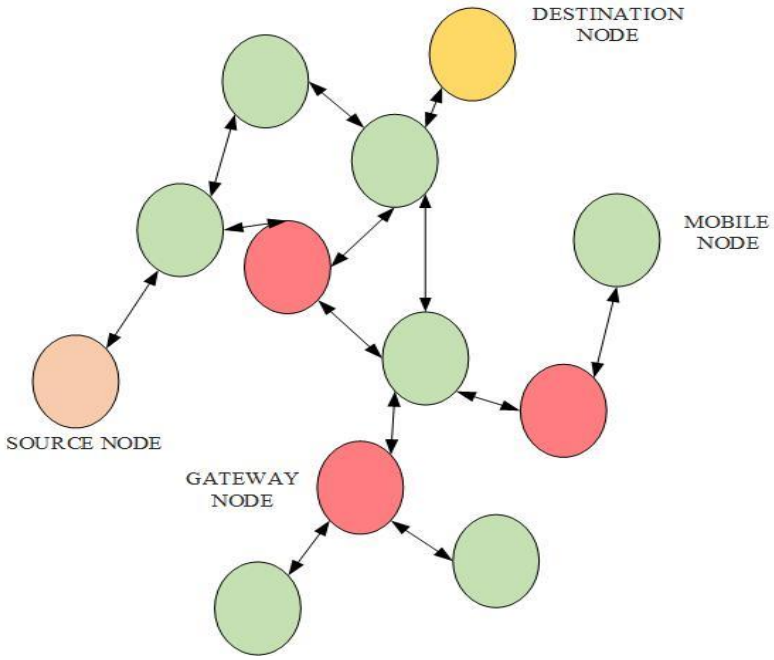

Fig1. Basic Structure of Manet

The paper suggests a Methodology for the enhancement of the security of the Manet using a secure routing system based on trust using the Rumor routing protocol. The methodology uses a model of trust to evaluate the confidence in the nodes using Direct, Indirect trust mechanisms. As Manet nodes can move around and locating the Sink nodes become an issue here, the cluster heads elect a Monitor Node to serve the functionality of a Sink node or a gateway node. This Monitor Node (MN) performs the computation of the trust values and finds the malicious node and the nodes are evaluated further using an equation to evaluate the signal strength deviation and the nodes that deviate will be detected to be malicious and are eliminated to ensure a secure routing process avoiding the nodes with worm hole attacks on the nodes. An attacked node can forward any malicious request and lead to security attacks in the network. A rumor routing protocol which is the usage of a dynamic routing system for the efficient routing process. The proposed Methodology the following steps:

1. Selection of the Cluster Head
2. Trust Model Evaluation
3. Trust Based Secure routing by the Rumor routing protocol.

ISSN 2394 - 7780

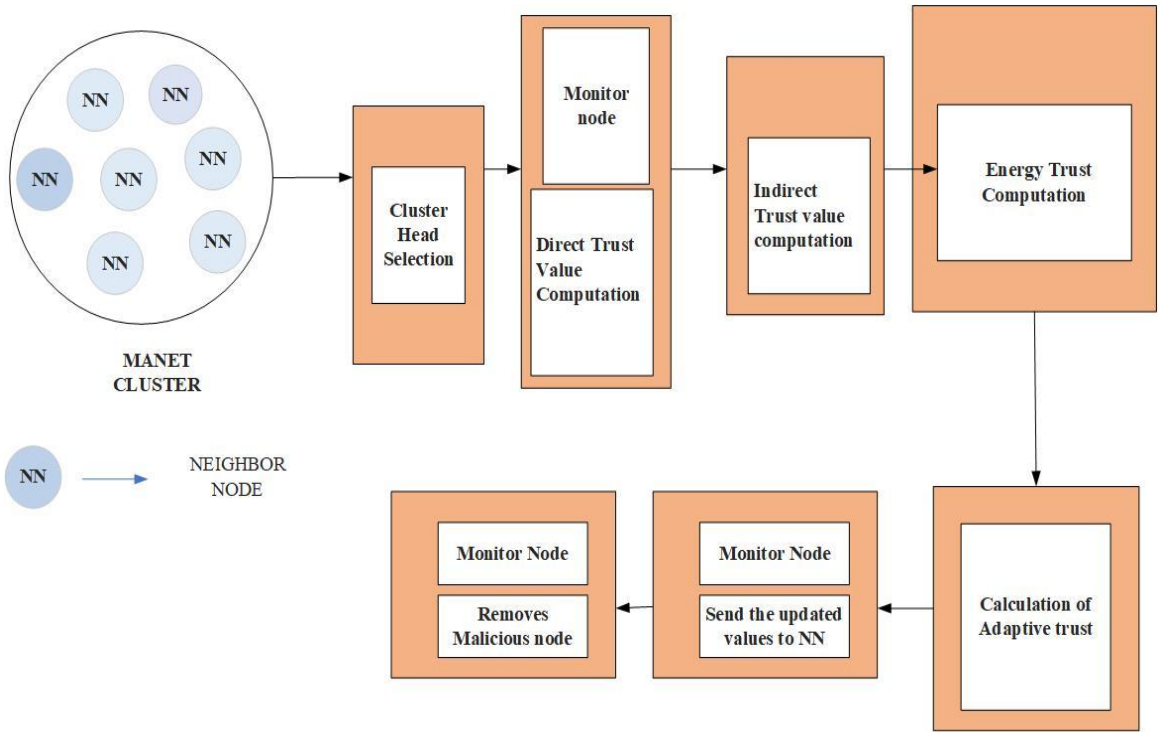

Fig2.Proposed Trust-based malicious node removal

3.2 Selection of the Cluster Head

The network is made up various clusters, as well as each cluster is made up among three different types among nodes: Neighbor nodes (NNs), CHs (cluster heads), and Monitor nodes (MNs). CHs are responsible for data forwarding both ways either within the clusters or between different clusters. Without security measures harmful nodes that turn into CHs will harm the network more than member nodes. It follows that the nodes possessing strong vitality and importance of trust must assume CHs. The detected data is sent to the CHs by NNs along with the for the energy of the neighboring nodes direct trust value. The CHS then forwards the packets of data to the sink using a combination of hops method.

The MN compute the nodes adaptive value of trust based on the direct trust value that was received and the residual energy. The updated adaptive Values of trust are then transmitted to the nodes. The high energy consumption, elevated information congestion and communication times and are therefore avoided as soon as the conventional model of trust gathers the value of trust for neighbors from nodes belonging to third parties. MN is responsible for keeping track of any changes in the cluster's signal intensity nodes to determine whether any of them are being used maliciously in wormhole attacks.

3.2.1 Monitor node election

To minimize the loss brought on by CHs or NNs being identified as affected nodes, Monitor Nodes (MNs) are in charge of monitoring the cluster's signal strength. Select the node with proximity to CH with the higher energy trust value as the MN to steer clear of the circumstance where MNs with reference to cannot identify all nodes cluster's signal strength.CH performs the MN selection by the equation:

$$K_{mn} = TR_{ij}^{t} * e^{-dist} \quad (1)$$

$$dist_{ch} = \frac{dist - dist_{min}}{dist_{max} - dist_{min}} \quad (2)$$

Here, $dist_{ch}$ refers to the normalization value of the separation within the neighboring nodes. $dist$ is the separation of the node to itself. $dist_{min}$ and $dist_{max}$ depict the least and the greatest distances from the neighboring nodes to themselves.

- NNs observed by MNs: Following selection, MNs observe the NNs in the cluster by the inequality in equation (3), allowing them to detect malicious nodes' wormhole attacks quickly by evaluating the signal strength of the nodes.

$$\left| D_R = \sqrt{\sum_{j=1}^{Mnum} (STR_j - STR_A)^2 / Mnum} \right| \leq \alpha \quad (3)$$

ISSN 2394 - 7780

Here, STR_j depicts the strength of the jth node that's monitored by the MNs and STR_A depicts the average of all the strength of the received signals of the NNs together. By determining whether its STR_j deviating from the expected range, a wormhole attack can be identified.

(b) CHs monitored by MN: It's very important to avoid malicious Cluster Heads. Wormhole attacks can also happen and it's very difficult to be traced. Our main aim is to avoid these activities. For its early identification, the following equation can be employed by the sink:

$$M_{rad} = \sum_{\substack{i=1 \\ j=i+1}}^{m_n} \frac{rad * AT^t_{m_{ni}m_{nj}}}{dist_{m_{ni}m_{nj}}} \quad (4)$$

Where, $AT^t_{m_{ni}m_{nj}}$ is the adaptive node's trust value m_{ni} for the calculation of m_{nj}, the upcoming hop from it. The maximum radius of the cluster head is given by rad and $dist_{m_{ni}m_{nj}}$ is the distance within both the hops.

The cluster heads keep checking the monitor nodes by sending packets and waiting for an acknowledgment, if it doesn't receive the acknowledgment it tries to select a new MN.

3.2.2 Trust Model Evaluation:

A node's behavior is assessed using its bundle dropped rate and package forwarded rate, packets injected falsely, packets injected falsely, and packet misrouted rate to determine the direct trust. Similar to direct trust, indirect trust is defined as the influence of a neighbor node (D) on a neighbor node (C), which includes the rate at which packets are forwarded, dropped, misrouted, and falsely injected. A detailed estimation of trust is provided. A trust-aware routing protocol can secure information delivery, protect data exchange, and uphold and protect the worth of the communicated details. Performance can furthermore suffer from node misbehavior. The system throughput is reduced, For example, by assaults that are not forwarding because packets are sent over and over again, yet are not delivered. Due to non-forwarding attacks, a compromised MANET network can be split up into several parts that can't communicate with each other. As a result, there is a need for more sensors, which leads to a change in node deployment or a rise in the quantity of sensors required to restore network connectivity. The trust values range affects the node's functionality. Due to its poor communication behavior, the malicious node always causes the trustworthiness to decline, whereas the normal node does the opposite.

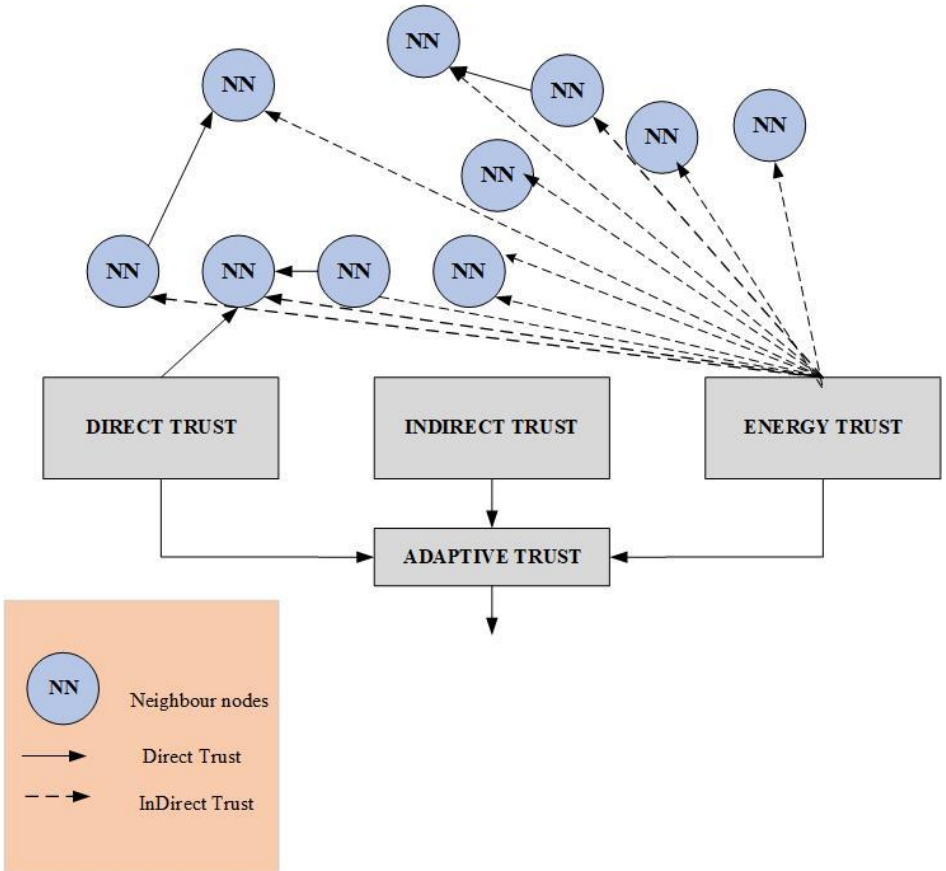

Fig 2. Diagrammatic Representation of the Trust Model

ISSN 2394 - 7780

Because of this, this paper uses centralized computing to reduce the workload on nodes and prevent the conveyance of a lot of information about queries between nodes. The MN calculates each node's indirect trust value, so every node just needs to calculate the value of direct trust of the neighboring node and send it to the MN node. To correctly calculate Node m's trust value, Node m must be aware of the direct trust value at which the third Node u evaluates Node n. direct trust evaluation model demonstrated that trust values follow the Beta distribution while evaluating the trust value. $TD_{mn}{}^{t}$, the direct node's trust value m to n is computed as shown.

$$TD_{mn}{}^{t} = E\,(Beta\,(\sigma_{mn}, \alpha_{mn})) = \frac{\sigma_{mn}+1}{\sigma_{mn}+\alpha_{mn+2}} \quad (5)$$

Where σ_{mn} and α_{mn} The original Beta-based trust evaluation model, however, does fail to consider the impact of the variables, including packet loss brought on by network congestion, on node communication interactions. Instead, it counts the number of cooperative and non-cooperative interactions among nodes, respectively. An unusual attenuation factor is presented in this paper q to enhance the initial model to address the issue. The likelihood of malevolent assaults probe is determined by the abnormal interaction among nodes, and it is calculated as follows:

$$prob = \frac{m_i}{TM_i} \quad (6)$$

m_i is the action caused by the harmful nodes behavioral impact. TM_i is the action caused through the total quantity of abnormal nodes' behavioral impact.

The impact of outside factors on the trust value can be lessened by eliminating the abnormal nodes detected by node m to compare with the original model, what the trust model is improvised.

The indirect value of trust is computed from equation (8) as follows:

$$TID_{mn}^{t} = \frac{1}{s}\sum_{v\in k_h}^{s}(TD_{mv}^{t} * TD_{nv}^{t}) \quad (7)$$

Here s depicts the neighbor trust nodes in the Manet and TD_{mv}^{t} is the worth of the direct confidence in the v node evaluated by the m node. Moreover, TD_{nv}^{t} depicts the direct trust of the n node evaluated by the node v.

➢ CALCULATION OF ENERGY TRUST VALUE

When a network node's trust value is high but its energy reserves are low, the network's overall structure and energy usage may be affected, causing the nodes death. Therefore, this paper takes the node's taking into consideration the node's residual energy when determining its trust value to balance node energy consumption while minimizing network overhead. $E_{recn} = k * E_{rcon}$ (8)

Where, E_{recn} is the receiving energy node energy consumption.

$$E_{sendn} = \begin{cases} k * E_{rcon} + k * £_{fs} * dist^2 & dist < dist_0 \\ k * E_{rcon} + k * £_{mp} * dist^4 & dist \geq dist_0 \end{cases} \quad (9)$$

Where, E_{sendn} is the sending node energy consumption,E_{rcon} refers to the radio coefficient of energy usage frequency between the nodes and k is the dimensions of the data packets and messages. $dist$ depicts the distance covered by both the node and $dist_0$ is the first node distance, $£_{fs}$ and $£_{mp}$ are two constants for energy consumption calculation, and the initial distance is calculated by the following equation.

$$dist_0 = \sqrt{£_{fs}/£_{mp}} \quad (10)$$

. The node's initial energy n is indicated by I_0 and the vitality left in the node is calculated as follows:

$$LE_n = I_0 - E_{recn} - E_{sendn} \quad (11)$$

Node n is considered eligible for the communication if it's remaining energy is greater greater than or equivalent to the cutoff; if not, regardless of the node's level of trust value, it is unable to transmit information. As a result, the value of node j's energy trust is:

$$T_E = \frac{ER_n}{I_0} \quad (12)$$

➢ ADAPTIVE TRUST VALUE COMPUTATION

Value of indirect trust, direct trust value and the Values from energy trust are utilized to calculate the adaptive worth of trust. It shows how trustworthy the nodes are. The adaptive Increases in the nodes' trust value as the

ISSN 2394 - 7780

trust level does as well. If Adaptive trust value of node n is less than the expected value of threshold, node m deems node n to be malicious and removes it, barring it from taking part in any activities. AT_{mn}^{t} is calculated as follows:

$$AT_{mn}^{t} = \sigma_1 * TD_{mn}{}^{t} + \sigma_2 * TID_{mn}^{t} + \sigma_3 * T_E \quad (13)$$

Here, $\sigma_1, \sigma_2 \; and \; \sigma_3$ depicts the Energy, indirect, and direct trust weights and the summary of $\sigma_1, \sigma_2 \; and \; \sigma_3$ gives the value 1.

3.3 Secure routing by the Rumor routing protocol.

Rumor routing is Agent-based. If the number of queries and the number of tasks is both low then performance is high. Both query flooding and event flooding are covered by this routing. The concept of an agent serves as the foundation for the energy-efficient protocol known as rumor routing. In this routing, an agent is a persistent packet that travels the network and notifies each sensor it comes across of the event. Going through several numbers of hops, the agent dies. Each sensor and the agent create an event list that contains event-distance pairs. The event and the actual distance are listed for each list. Distance is measured by how many hops there are made while maintaining the shortest route.

When an event occurs, paths to each event are built using agents by the basic rumor routing principle. The agents are network-moving persistent messages. On these agent-generated paths, future queries can be directed. The queries are first sent on a network before joining the path. An event table and a neighbors list are both kept up to date by every node in the system. Details for each event it is aware of by receiving the broadcasts and broadcasting each node's ID, the neighbor lists are created when the network is first started. At network startup, the neighbor lists are created. If the event table's storage space is limited or the events are only needed for a short time, expiration timestamps can be added to the entries.

3.3.1 Agents' role in path creation:

The paths are made by moving agents and are stored as states in single nodes. By adding a route of length 0 to the event and probabilistically creating an agent, the agents are created in the event nodes. The probability is used because, typically, a large number of nodes observe the same event, and too many paths to the same event result in an excessive amount of overhead. The agent makes a maximum number of hops while moving through the network. While traveling, it combines its event table with those of visited nodes. A path to both (or more than one) events begins to be created whenever an agent crosses a path leading there. Additionally, the agent modifies the routing table using the shortest route through the system when it finds a node with a longer path to the same event than its own. This ensures delivery when the longer path is found. The energy needed for P query routing is thus:

$$G_t(p) = G_{set} + p * (G_{th} + s * \frac{p_{tot} - P_f}{p_{tot}}) \quad (14)$$

During the query flooding process

$$G_t(p) = P * S \quad (15)$$

In the event flooding process

$$G_t(p) = T * S \quad (16)$$

Calls for a lot of communication energy and might lead to information congestion. The reason for this is that node m must first requests the neighbor node v which is publicly trusted for node n's direct trust value before it can calculate node n's indirect trust value.

3.3.2 Routing process and the Cluster head Selection:

The Monitor node is provided with limitless resources to choose a secure route so that the network's effectiveness and security can be increased. Using the M_{rad} Value can fend off wormhole attacks and cut down on nodes' energy usage during transmission. Following are examples of the steps in the proposed work:

A. The CH_m is the source transfers a request packet for the following hop to a few chosen cluster heads.

B. The selected cluster heads add their ID information on the reception of the request packet in the request packet. Then the requested packets are sent to the next hop of the cluster heads which were selected till the Monitor node.

C. The Monitor node computes the M_{rad} value using the formulation in eq.5 then the path is selected considering the longest path as the optimal one.

ISSN 2394 - 7780

3.3.3 Detailed process in the Valuation of the Trust value in the routing

The Have faith model's core calculations and focal point are utilized to calculate and update the trust value. In contrast to earlier safe routing methods based on trust, The Monitor node manages the value of indirect trust for this procedure rather than gathering a sizable quantity of direct trust values derived from neighbor nodes. As a result, when updating the trust values, this protocol minimizes overhead of communication and relieves inter-node congestion. The following list of updating procedures is detailed.

1. To assess values of the direct trust of the NNs, MNs keep track of both normal and abnormal neighbor node behavior. It determines the direct trust value use an equation (5)
2. The Monitor nodes routes are found.
3. As the data packet enters the stable phase's last time slot, NNs adds the ideals of direct trust of the calculated NNs and the energy left over in the NNs.
4. In a multi-hop process, NNs send packets to their CHs, they forward it to the MN. The MN then determines the significance of indirect trust and the adaptive trust value.
5. The Monitor Node uses multicast to send the computed adaptive trustworthiness to every CH, and after receiving it, CHs pass it on to NNs. NNs adds the neighbors' adaptive trust value. Then the equation (3) is used to evaluate the malicious node and the values are updated to the NNs. The nodes that deviate from the range are detected by the MN as malevolent nodes and eliminated through the network.

4. RESULTS AND DISCUSSION

The suggested STRR was assessed for various factors such as throughput, network life time, energy, delivery ratio, and latency. Using the NS2 simulator. Then the results obtained were evaluated for their efficiency with the existing systems like trust-aware routing framework (TARF) as well as SDARP, or Security Based Data Aware Routing Protocol. The details are discussed in this section.

4.1 Performance Metrics:

The details among the performance indicators evaluated are given below.

- **Delay**:

Delay depicts the time consumed by a packet to move the information via a network from a source to a destination. The average end-to-end delay will be obtained by averaging the end-to-end delays of all successfully delivered messages. Consequently, end-to-end delay is somewhat influenced by the packet delivery ratio. As the distance between the source and the destination rises, so does the chance of a packet drop. All possible network delays, including buffering and route-finding latency, retransmission delays at the MAC, and propagation and transmission delays, are factored into the average end-to-end delay. An equation can be used to mathematically represent it.

$$\boldsymbol{K = \frac{1}{Z}\sum_{j=1}^{Z}\left(Rt_j - Su_j\right) * 1000} \quad (18)$$

Here K shows the average delay.

j shows the packet's identification.

Rt_j shows the time it takes for a packet to be received.

Su_j- shows the time it takes for packets to be sent.

Z= No packets were delivered successfully.

- **Packet Delivery Ratio:**

One important consideration when assessing a routing protocol's efficacy in a network is the packet delivery ratio. A number of simulation-related parameters affect the protocol's performance. The most crucial elements are network topology, transmission range, node count, and packet size. The number of data packets sent from sources divided by the number of data packets arriving at destinations yields the packet delivery ratio. According to the equation, the mathematical formulation

$$\boldsymbol{P = \frac{\sum(Dn)}{\sum Sn}} \quad (19)$$

Where Dn is the total amount of packets acquired by every destination node and Sn is the sum number of the packets from the originating node

ISSN 2394 - 7780

Energy consumption:

Power is a measure of the pace at which energy is consumed. Sensor node in a specific state. Time never stops for sensor nodes in a certain state.

$$energy = power \times time$$

$$E = P * T \quad (20)$$

E stands for Energy

P stands for power

T stands for the Time

Network Lifetime:

The network lifespan is represented by the duration of the network's complete operation. To calculate the network lifetime, the number of addressed nodes that consume the least energy during transmission is compared to the total number of sensor nodes in the network. The following illustrates how Network Life Time (NLT) is calculated.

$$NLT = \frac{nodes\ with\ better\ energy\ consumption}{Total\ number\ of\ nodes} * 100 \quad (21)$$

Throughput:

The Throughput is the quantity of packets that make it to their destination. The speed at which data packets or units go from source to destination or from sender to recipient determines how much information can be transferred in a given amount of time. Often used units of measurement are bytes, bits, or packets per second.

4.2 Performance Analysis:

4.2.1 Delay: The postponement was calculated for the suggested STRR model and was in contrast to the current TARF and the SDARP models. The ideals are tabulated in a table as shown in Table 1. The tabulated values are plotted in a graph shown in Fig.4

Table 1. Delay values of the Proposed STRR and existing TARF and SDARP models

Node count	STRR	TARF	SDARP
25	0.220090	5.823892	3.458841
50	12.198368	17.810554	17.810554
75	16.322654	27.621686	27.621686
100	18.946113	22.864729	30.986795

The delay values in Table.1 of the proposed STRR showed a lesser value in comparison with the existing TARF and the SDARP model. The graph in fig 4 clearly shows a lesser curve compared to the current model curves. Hence, the suggested model shown that reduce the delay in the network traffic.

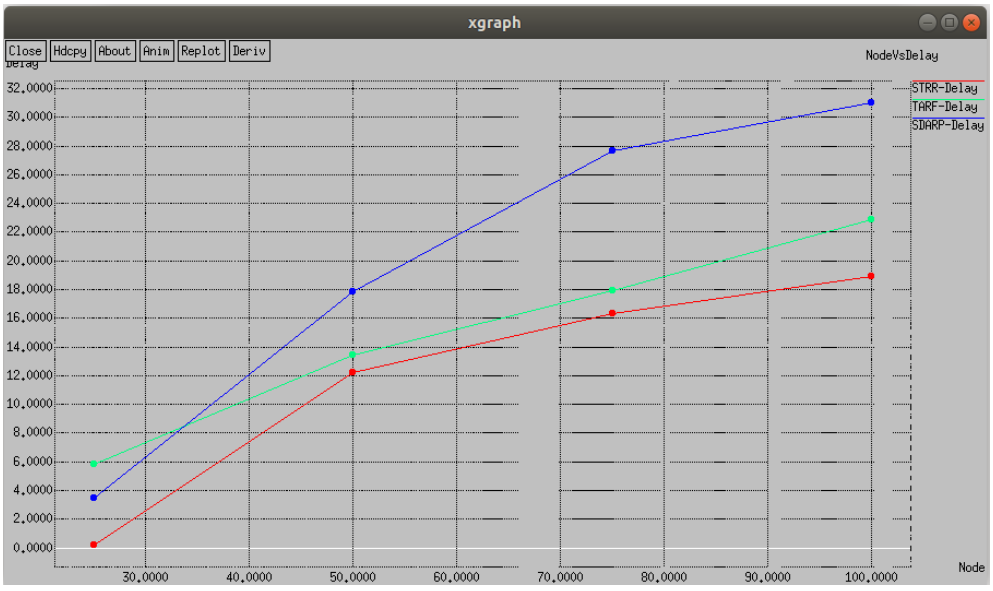

Fig 4. Graphical representation of delay values of STRR, TARF, and the SDARP models

ISSN 2394 - 7780

4.2.2 Packet Delivery Ratio:

The ratio of packet delivery was calculated for the suggested STRR model and was in contrast to the current TARF and the SDARP models. The values are tabulated in a table as shown in Table 2. The tabulated values are mapped out in a graph displayed in Fig.5

Table 2. Packet Delivery Ratio values of the Proposed STRR and existing TARF and SDARP models

Node count	STRR	TARF	SDARP
25	0.993358	0.857880	0.877415
50	0.500913	0.468752	0.367680
75	0.304422	0.253344	0.032557
100	0.224228	0.142646	0.020302

The packet delivery ratio values in Table.2 of the suggested STRR showed a greater amount in comparison with the current TARF and the SDARP model. The graph in fig 4 clearly shows a higher curve in comparison with the existing model curves. Hence, the suggested model proved to improve the packet delivery proportion within the network traffic.

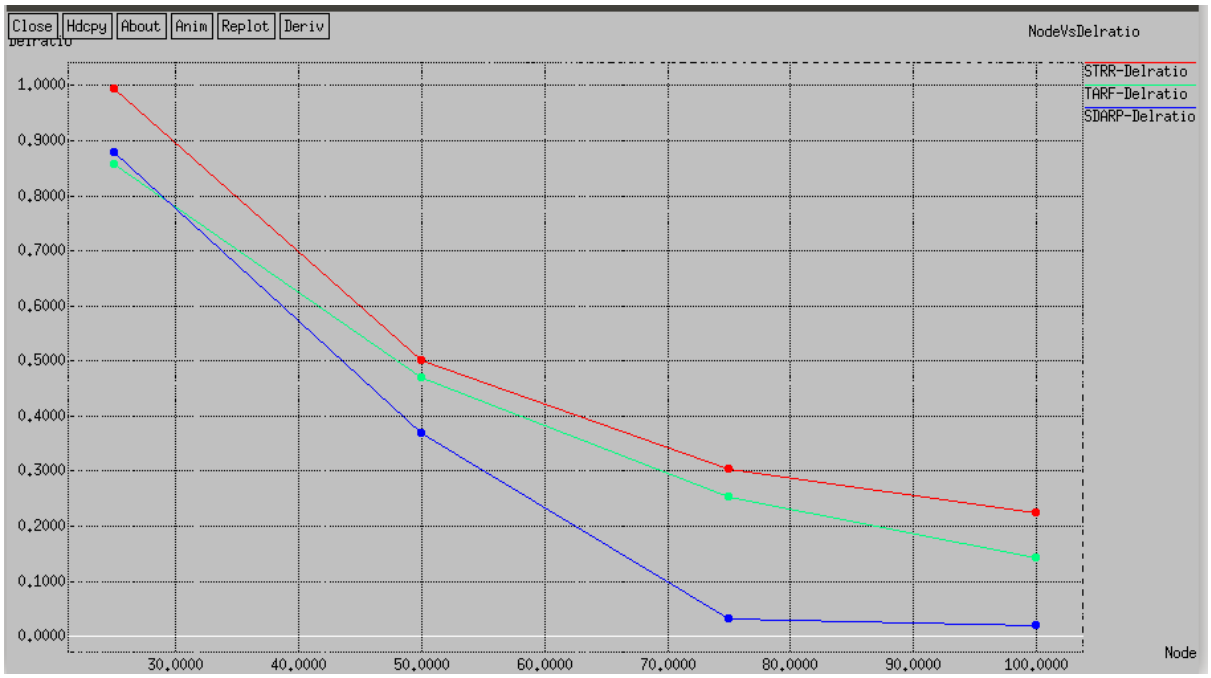

Fig 4. Graphical comparison of Packet delivery ratio values of STRR , TARF and the SDARP models

4.2.3 Energy Consumption:

The nodes' energy consumption was computed for the proposed STRR model and was contrasted with the current TARF and the SDARP models. The values are tabulated in a table as depicted in Table 3. The tabulated values are mapped out in a graph shown in Fig.5

Table 3. Energy values of the Proposed STRR and existing TARF and SDARP models

Nodes	STRR	TARF	SDARP
25	99	102	105
50	50	60	75
75	30	35	40
100	22	25	30

The energy values in Table.3 of the proposed STRR showed a lower energy consumption in comparison with the existing TARF and the SDARP model energy values.

The graph in fig 4 clearly shows a lower curve in contrast to the current model curves. Hence, the suggested model demonstrated to lower the energy consumption ratio in the network traffic.

ISSN 2394 - 7780

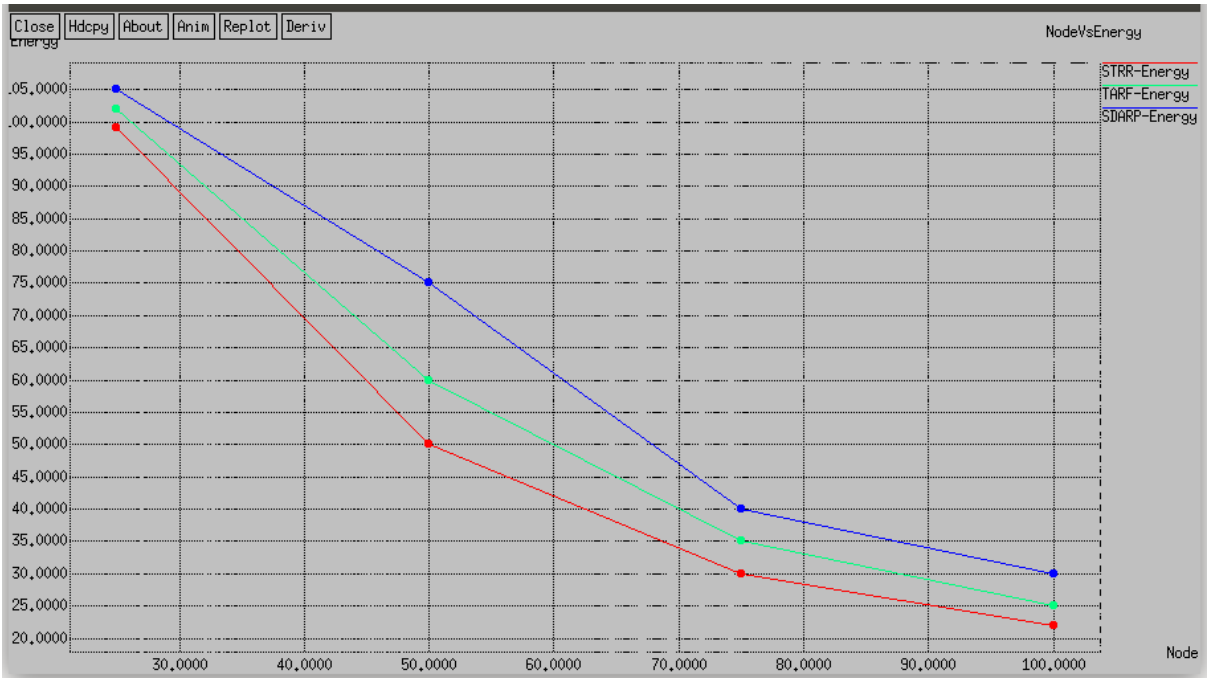

Fig 5. Graphical comparison of Energy values of STRR, TARF, and the SDARP models

4.2.4 Network Life Time:

The Life Time of the Network was computed for the proposed STRR model and was in contrast to the current TARF and the SDARP models. The values are tabulated in a table as shown in Table 4. The tabulated values are plotted in a graph shown in Fig.6

Table 4. Network Life Time values of the Proposed STRR and existing TARF and SDARP models

nodes	*STRR*	*TARF*	*SDARP*
25	549	119	61
50	306	134	47
75	184	98	0
100	133	55	0

The Network lifetime values in Table.4 of the proposed STRR showed a higher Network lifetime in comparison with the existing TARF and the SDARP model energy values. The graph in fig 6 clearly shows a higher curve in contrast to the current model curves. Hence, the suggested model demonstrated to increase the Network lifetime considerably.

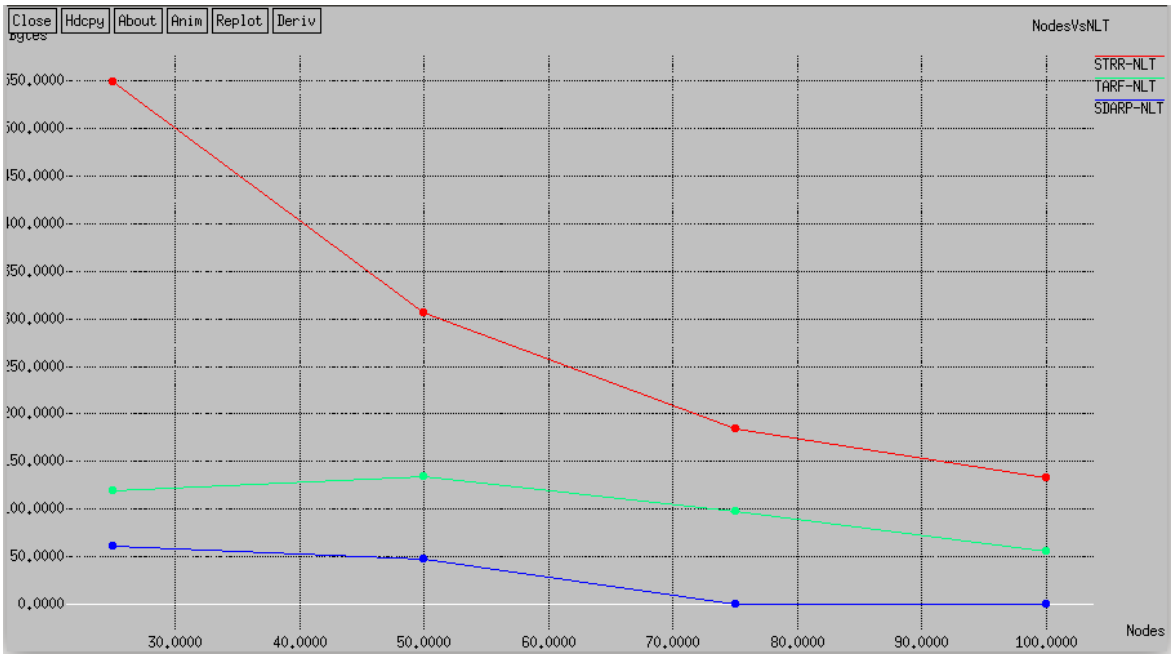

Fig6. Graphical comparison of Network Lifetime values of STRR, TARF and the SDARP models

ISSN 2394 - 7780

4.2.5 Throughput:

The proposed throughput was calculated. STRR model and was in contrast to the current TARF and the SDARP models. The values are tabulated in a table as shown in Table 5. The tabulated values are plotted in a graph shown in Fig.7

Table 5. Throughput values of the Proposed STRR and existing TARF and SDARP models

nodes	*STRR*	*TARF*	*SDARP*
25	915.320000	299.400000	305.200000
50	510.040000	335.580000	239.480000
75	307.653333	245.106667	200.960000
100	222.880000	138.490000	105.390000

The throughput values in Table.5 of the proposed STRR showed a higher Network lifetime in comparison with the existing TARF and the SDARP model energy values. The graph in fig 7 clearly shows a higher curve compared to the current model curves. Hence, the suggested model demonstrated to increase the throughput in the network traffic.

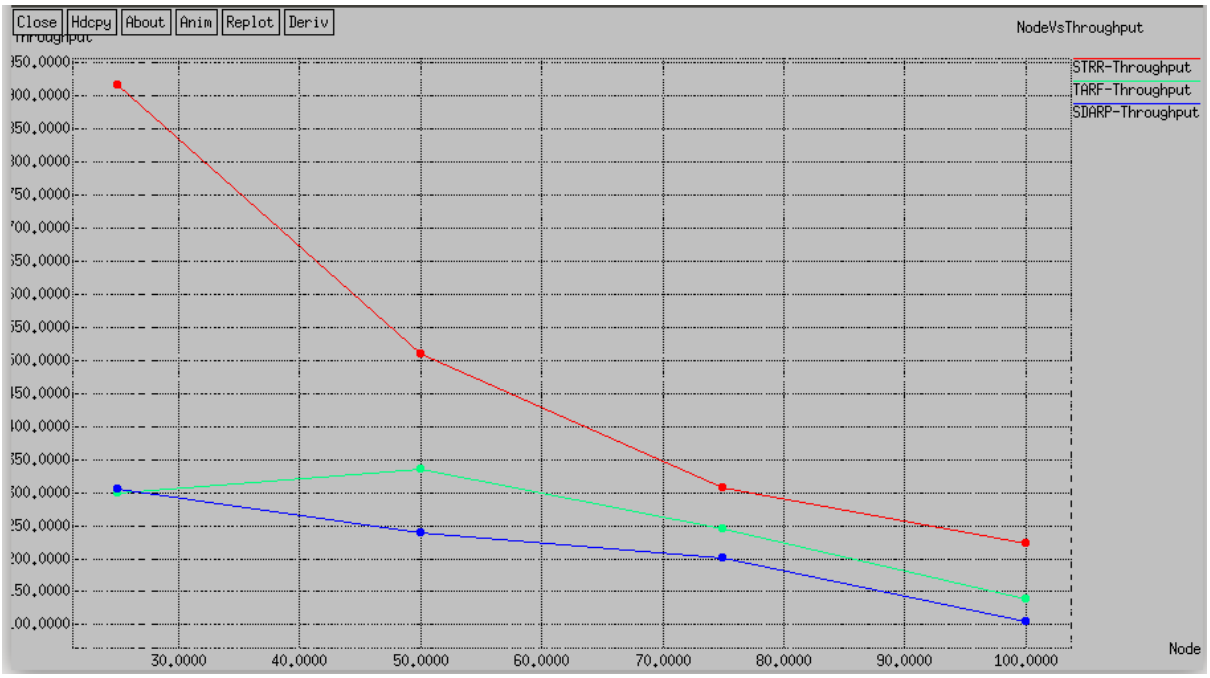

Fig7. Graphical comparison of Throughput values of STRR, TARF and the SDARP models

5. CONCLUSION AND FUTURE WORK:

Secure Energy efficiency based on trust Rumor protocol for routing (STRR) model proposed was evaluated in the NS2 simulator for the issues such as the ratio of packet delivery, Delay, Network Lifetime, Throughput, and Energy concerning MANETs. The parameters were evaluated specifically and compared with the existing models like trust-aware routing framework (TARF), and the Data-Aware Routing Protocol with Security (SDARP) for their robustness. The system had reduced delay, increased ratio of packet delivery, reduced energy usage, high network life time, as well as high flow rate in comparison with the existing models. The trust-based routing hence proved to be more efficient than the existing systems. The computation of the trust values as well as energy trust ideals along with the adaptive trust value enabled a better-secured routing process with the Rumor routing protocol which efficiently addressed the issues for the Manet than the other Routing protocols used by the existing systems. Manets are mobile and have various security-related issues. The proposed Methodology STRR addressed the existing issues available in Manets efficiently. The framework can be enhanced with more hybrid mechanisms to extend the present framework and enhance the features in the future.

REFERENCES

1. S.K, Das. &S, Tripathi. (2018). Intelligent energy-aware efficient routing for MANET. *Wireless Networks,* 24(4), Page No.1139-1159.
2. A, Malar. A. &M, Kowsigan. &N, Krishnamoorthy. &S, Karthick. &E, Prabhu. &K, Venkatachalam. (2021). Multi constraints applied energy efficient routing technique based on ant colony optimization used

for disaster resilient location detection in mobile ad-hoc network. *Journal of Ambient Intelligence and Humanized Computing*, *12*(3), Page N.4007-4017.

3. Hu, H., Han, Y., Yao, M. and Song, X., (2021). Trust based secure and energy efficient routing protocol for wireless sensor networks. *IEEE Access*, 10, Page No.10585-10596.
4. Hao, S., Zhang, H. and Song, M., (2018). A stable and energy-efficient routing algorithm based on learning automata theory for MANET. *Journal of Communications and Information Networks,* 3(2), Page No.43-57.
5. Venkatasubramanian, S., Suhasini, A. and Vennila, C., (2021). An efficient route optimization using ticket-ID based routing management system (T-ID BRM). *Wireless Personal Communications*, Page No.1-20.
6. Hema Kumar, M., Mohanraj, V., Suresh, Y., Senthilkumar, J. and Nagalalli, G., (2021). Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. *Journal of Ambient Intelligence and Humanized Computing*, 12(5), Page No.5287-5295.
7. Nandi, M. and Anusha, K., (2021). An Optimized and Hybrid Energy Aware Routing Model for Effective Detection of Flooding Attacks in a Manet Environment. *Wireless Personal Communications*, Page No.1-19.
8. Gowrishankar, J., Kumar, P.S., Narmadha, T. and Yuvaraj, N., (2020). A Trust Based Protocol for Manets in Iot Environment. *International Journal of Advanced Science and Technology*, *29*(7), Page No.2770-2775.
9. Kim, T.H., Goyat, R., Rai, M.K., Kumar, G., Buchanan, W.J., Saha, R. and Thomas, R., (2019). A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. *IEEE Access*, 7, Page No.184133-184144.
10. Khan, M.S., Midi, D., Malik, S.U.R., I Khan, M., Javaid, N. and Bertino, E., (2017). Isolating misbehaving nodes in MANETs with an adaptive trust threshold strategy. *Mobile Networks and Applications*, 22(3), Page No.493-509.
11. Shi, Q., Qin, L., Ding, Y., Xie, B., Zheng, J. and Song, L., (2019). Information-aware secure routing in wireless sensor networks. *Sensors*, 20(1), Page No.165.
12. Sharma, R.K., Sharma, A.K. and Jain, V., (2018). Genetic algorithm-based routing protocol for energy efficient routing in Manets *Next-Generation Networks*. *Springer*, Page No. 33-40.
13. Femila, L. and Marsaline Beno, M., (2019). Optimizing transmission power and energy efficient routing protocol in MANETs. *Wireless Personal Communications*, Page No.1041-1056.
14. Tripathy, B.K., Jena, S.K., Bera, P. and Das, S., (2020). An adaptive secure and efficient routing protocol for mobile ad hoc networks. Wireless Personal Communications, 114(2), pp.1339-1370.
15. Bisen, D. and Sharma, S., (2018). An energy-efficient routing approach for performance enhancement of MANET through adaptive neuro-fuzzy inference system. *International Journal of Fuzzy Systems*, 20(8), Page No.2693-2708.
16. Kasthuribai, P.T. and Sundararajan, M., (2018). Secured and QoS based energy-aware multipath routing in MANET. *Wireless Personal Communications*, 101(4), Page No.2349-2364.
17. Shivakumar, K.S. and Patil, V.C., (2020). An optimal energy efficient cross-layer routing in MANETs. Sustainable Computing: Informatics and Systems, 28, Page No.100458.
18. Jabbar, W.A., Saad, W.K. and Ismail, M., (2018). MEQSA-OLSRv2: A multicriteria-based hybrid multipath protocol for energy-efficient and QoS-aware data routing in MANET-WSN convergence scenarios of IoT. *IEEE Access*, 6, Page No.76546-76572.
19. Da Costa Bento, C.R. and Wille, E.C.G., (2020). Bio-inspired routing algorithm for MANETs based on fungi networks. *Ad Hoc Networks*, 107, Page No.102248.
20. Alappatt, Valanto, and PM Joe Prathap. "A hybrid approach using ant colony optimization and binary particle swarm optimization (ACO: BPSO) for energy efficient multi-path routing in MANET". (2020). Page No. 175-178.
21. Mohsin, A.H., Bakar, K.A. and Zainal, A., 2018. Optimal control overhead based multi-metric routing for MANET. Wireless Networks, 24(6), pp.2319-2335.

ISSN 2394 - 7780

22. Jamal, T. and Butt, S.A., (2019). Malicious node analysis in MANETS. *International Journal of Information Technology*, 11(4), Page No.859-867.

23. Khudayer, B.H., Anbar, M., Hanshi, S.M. and Wan, T.C., (2020). Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks. *IEEE Access*, 8, Page No.24019-24032.

24. Yu, M., Zhou, M. and Su, W., (2008). A secure routing protocol against byzantine attacks for MANETs in adversarial environments. *IEEE transactions on vehicular technology*, 58(1), Page No.449-460.

25. Jubair, M.A., Mostafa, S.A., Muniyandi, R.C., Mahdin, H., Mustapha, A., Hassan, M.H., Mahmoud, M.A., Al-Jawhar, Y.A., Al-Khaleefa, A.S. and Mahmood, A.J., (2019). Bat optimized link state routing protocol for energy-aware mobile ad-hoc networks. Symmetry, 11(11), Page No.1409.