Trust based Secure and Reliable Routing Protocol of Military Communication on MANETs

[1]Uma Maheswari Arumugam and [2]Suganthi Perumal
[1] Periyar University, Salem, Tamil Nadu, India.
[2] N.K.R Govt Arts College(w), Namakkal, Tamil Nadu, India.
[1]yumaa85@gmail.com, [2]kpsuganthi74@gmail.com

Correspondence should be addressed to Uma Maheswari Arumugam **:** yumaa85@gmail.com.

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202303006
Received 15 July 2022; Revised form 20 October 2022; Accepted 12 December 2022.
Available online 05 January 2023.

Abstract - An entirely new and trendy peer-to-peer modern communications graph is called a Mobile Ad-hoc Network (MANET). The MANETs form their network without any infrastructure facilities, whenever needed. Military activities frequently need the quick and secure transfer of large quantities of data. The radio spectrum has been used by the military up until now for good communication but might have a chance to impact security problems. The security of data transfer is a major issue given the natural component of wireless networks in real-time situations. The main challenge is confirming trust across MANET nodes, as well as dealing with bandwidth, energy, and changing topology. By degrading the trust level between nodes, the malicious attitude increases poor data transmission, increases energy use, and reduces the duration of the network. To address this issue, we proposed a new protocol, Trust-based Secure and Reliable Routing Protocol (TSRRP), to increase the trust between nodes in MANETs and predict anomalous activity. This is done with the help of certain Quality of Service (QoS) metrics, such as the result analysis phase. NS2 is used to simulate the result. The simulation outcomes demonstrate how the suggested protocol performs better than the existing protocols.

Keywords - MANETs, Security, TSRRP, Military Communication, QoS Metrics.

I. INTRODUCTION

MANETs are a widely recognised type of modern cultural wireless network. Without supervision, it enables all current wireless nodes to communicate with one another anywhere and at any time. In the unpredictable dynamic topology, any node can join or disconnect from the network at any time. Due to the limited broadcast range of the wireless link, any node wishing to communicate with another node in that link needs to travel one hop with an intermediary node acting as the router. As a result, every node in MANET should concurrently act as a host and a router. Developing a reliable routing mechanism for MANETs becomes one of the most difficult problems. due to topological changes, limited node battery life, and poor wireless channel capacity [1].

A military connectivity network is used to support tactical commands and facilitate communication and cooperation. When it is destroyed during a war, the effects are severe. The network's communication nodes are impacted by the attacker; during the fight, the attacker has an impact on the network's nodes, and malevolent nodes may learn the code of communication [2, 3, 4]. Poor security data transfer affect's reliability, consumes a significant amount of energy, shortens the life of the shared network, and causes communication delays.

One of the processes is transmission power, which is comparable to connectivity, mobility, and bandwidth. Since connectedness among nodes requires transmission power to connect to other nodes, the relationship between transmission powers and linkage appears to be overly strong. It is critical for network management. The primary goal of such transmission power is to keep communication networks essential for a MANETs network.

This proposed protocol's goal is to design and increase trust among MANET nodes by utilising predicted malicious behaviour and trusted parameters to identify the best and most secure route between sources and destinations. It recognises the DN's direction and chooses the router within this direction to deliver the data. Most of the specified nodes participate in the forwarding process. All of the remaining nodes' energy is conserved. The routing overhead has been reduced. As a result, the network's efficiency improves. These works are separated into sections. The introduction portion is described in Section 1. Section II goes over the relevant works. Section III explains the trusted parameters. The proposed work process

and its phases are explained in Section IV. The simulation parameters are provided in Section V and the result analysis is illustrated and the conclusion is stated in Section VI.

II. RELATED WORK

There are different topologies for trust-based wireless ad-hoc networks. Data delivery is less secure because of the low trust level of nodes' harmful behaviour. Methods of trust management are crucial for managing these nodes. That trustworthiness was determined using two observations, both direct and indirect. When routing is involved, combining both of these procedures might increase the trust value [5]. This method contains flaws in its initial phases, so robust protection is required to assess the many security risks as they arise. [6]. In MANET, numerous attacks, including active attacks, passive attacks, external attacks, and internal attacks, are looked into [7]. Mobility, battery capacity, and bandwidth restrictions are challenges for secure network routing. Consequently, an energy-efficient routing strategy is created [8]. To reduce abnormal node involvement in MANET, security enhancement necessitates the use of a prediction technique known as trust node analysis (NTA). Authentication of networks is a critical factor to assess security via repeated activities to regulate the dependable delivery of data [9]. Because of the movement and bandwidth consumption on MANET during crisis conditions and natural disasters, some TCP/IP layers were updated, and an approach to regulating the overheads was developed [10].

Because the node could successfully access and leave the infrastructure, it opened the door to a variety of attacks. As a result, numerous strategies were applied to avoid these types of situations, and the solutions demonstrated advances in PDR and maximised throughput. [11]. Routing protocols for connectionless communication media include SLP, SAR, ARAN, SAODV, SRP, SEAD SLSP, CONFIDENT, and others. It has been done to develop a novel, undercrossed, shared secret control scheme with stable MANET networking [12]. Packets of data have been disposed of as a result of different kinds of sequence number incidents on network nodes, affecting MANET performance. As a result, a predictive method was created to reduce this [13]. A well-known estimation method called the RSSI algorithm is used to enhance each node's local decision and assess the flexibility of their surrounding nodes within the network [14]. Several legal process models have been investigated in MANET networking [15].

The trust value is estimated using a trust-based strategy. It is determined by the forwarding capacity of the packaging; thus, gained and supplied packet data are scored at every link. The higher the level, the greater the capacity of the data packets and the lower the percentage of loss. The trusted path receives more consideration than the shortest distance [16]. The AOMDV protocol is used to examine the uni-path AODV routing protocol for black hole connect identification. When comparing the multi-path AOMDV protocol to the uni-path on-demand routing AODV protocol, the PDR was higher and the delay in time was shorter [17]. A routing remedy for the Web of Things system is proposed, based on the fundamental routing protocols of MANET and WSN [18]. A novel EENRR protocol has been created by taking specific quality characteristics from existing protocols, for example, PDR and lifetime of the network, and the simulation outcomes demonstrate an increase throughout the remaining energy [19]. The s2MLBR protocol on MANET has used optimised segmentation and trust interruption (ODTI) to determine the trustworthiness of each mobile host and identify the maximum trustworthiness node for every industry as part of information transfer [20].

The MANET's communication range is constrained by its low transmission power. As a result, the algorithm's reliability is determined by the volume with the highest trust value, saving power transmission, and not focusing on the path length of the route to connect with in-network [21].Significantly raise the PDR, reduce routing overhead, and identify misbehaving wireless nodes using the new upgraded protective secret sharing scheme (NEPSSS) strategy to identify black hole attacks and also to confirm data confidentiality, integrity, and security [22]. Using team identifiers, route request packet verification is attempted. The key-encrypted onion routing and confidential validation messages are intended to keep intermediate nodes from disclosing the true target [23]. The protocol makes use of group signatures to cost-effectively achieve aspects of anonymity like unidentifiability and unlinkability [24]. To ensure confidentiality and safety and protect the network from both internal and external attackers, an on-demand location-based anonymous MANET routing protocol (PRISM) has been established [25].

III. TRUSTED PARAMETERS

These parameters are used for trust to protect against malicious nodes and ensure trust between nodes for information communication. Three crucial parameters, including neighbor node calculation, bandwidth measurement, and estimation of energy, are used by these trusted parameters.

Neighbour Node Calculation

Before gathering trust values, the neighbor node estimation is evaluated using Eq.1. The nodes with ranged trust values were chosen. To observe the reliability, the percentage of trust was measured to obtain a maximum data transmission rate. The neighbor nodes were chosen based on the distance, and the energy value was revised with the high level of trust, bandwidth frequency, and ID. Like a response, the access point with the maximum trust value is selected to transmit the packets. The ID stored in the node is considered for a specific node collecting in a one-hop distance, and the RSS is computed using the FRIIS transmission formula to determine the distance between two nodes.

$$T_p = \sqrt{\frac{GtGrPt\pi\lambda^2}{(4\pi)^2 Lpr}} \quad (1)$$

Where Pt is the power to transmit, Gt is the gain of transmit (unit less), Gr is the reception gain (unit-less),λ is the wavelength (m), L is the system loss (unit-less) and pr is the reception power.

Estimation Of Bandwidth

Its indicates the quantity of data sent during a specific period of time. More packets are transmitted when the bandwidth is higher. Therefore, when evaluating the QoS of any route in the network, bandwidth is now considered to be crucial. While evaluating the topology of a network trustworthiness, the high bandwidth rate between any two nodes should be guaranteed.

At period 't', the link (i, j) available bandwidth is calculated as L_n. Through spreading data packets, the node here uses RSS to determine the bandwidth of every collection of nodes within a one-hop distance. The amount of bandwidth and the rate at which information can be reliably transmitted over a channel are proportional. Network throughput also enhances as channel capacity does.

$$\text{Total bandwidth B(n)} = \text{c} - [\frac{\sum \text{n(s,d)}(\mathcal{L}+\beta}{\text{TCH}}]\text{bps} \quad (2)$$

Using the Eq.3, being can determine the node to node bandwidth.

$$L_n\text{=[PDR(n)-PLR(n)]}/t_c \ \{0 \leq \text{bw(n)} \leq 1\} \quad (3)$$

The PDR(n) represents the node 'n' packet delivery ratio, and the PLR(n) denotes the ratio of packet loss at the current time 't_c'. For each of the 'k' nodes, the value of the L_n is hypothesized. The 'k' is the distance in one hop from the current estimating node to the following estimating node, 'n'. The node with bandwidth L_n higher than the threshold bandwidth B_{TH} and closest to the destination has been picked as the following hop out of all 'k' nodes in the neighbor list. The action is taken up until the final destination has been reached.

Estimation of Energy

Energy refers to the capacity of those nodes to move data. The fundamental functions are detecting the neighbor's functionality and maintaining the path. This is the way the energy attribute is calculated.

$$Er(n) = E(initial), \left(\begin{pmatrix} E(receive), E(transmit), \\ E(process) \end{pmatrix}\right) * n \quad (4)$$

Where Er(n) is the total amount of energy of the nodes, E(initial) is the initial energy of the node, and E(transmit) is the energy used by a node during the next hop on the path in between the source and the final destination for transmission or forwarding. E(receive) is the amount of energy wasted by a node to receive a data packet provided by a node present at the next hop on the route between the source and the final destination.

IV. PROPOSED SYSTEM

We design an efficient and newly proposed protocol, named Trust-based Secure and Reliable Routing Protocol (TSRRP), for military communication on MANETs. This protocol ensures that nodes communicate in a secure and reliable manner. To determine the ID of every node within a one-hop distance, the proposed system collects data from the intermediate node using ID. Our protocol follows the routing principles of AODV. To be a reactive protocol, AODV obtains the most recent path to determine the destination sequence number and determine the most recent route to the location. The calculated nodes are less reliable as a result of criminal reports. In order to determine the trust value, the proposed work took into account the parameters of energy, bandwidth, and trust rate. The optimum trust value is estimated and gathered. This offers a more secure and dependable way to obtain a high level of trust. The three phases of the proposed system are cluster formation, trust analysis, and result analysis, as shown in **Fig 1. Fig 2** describes the flow chart of the proposed model.

Cluster Formation Phase

Initially, the nodes in the network are considered input. A cluster has a cluster member and a gate node. By using these gate nodes, the clusters can communicate with each other. The cluster head is chosen from among the nodes with the highest trust value. Afterward, to construct a cluster, the cluster head broadcasts the hello message to all nodes within its communication range. A few nodes would then pick a cluster head based on the received signal strength indication (RSSI) and respond to a connection packet if they had received more than one hello packet. The cluster head sends member information to the other members in the cluster. The time slot schedule is generated by the cluster head for its members according to the principles of TDMA for minimising traffic. This schedule avoids collisions between cluster heads and cluster members.

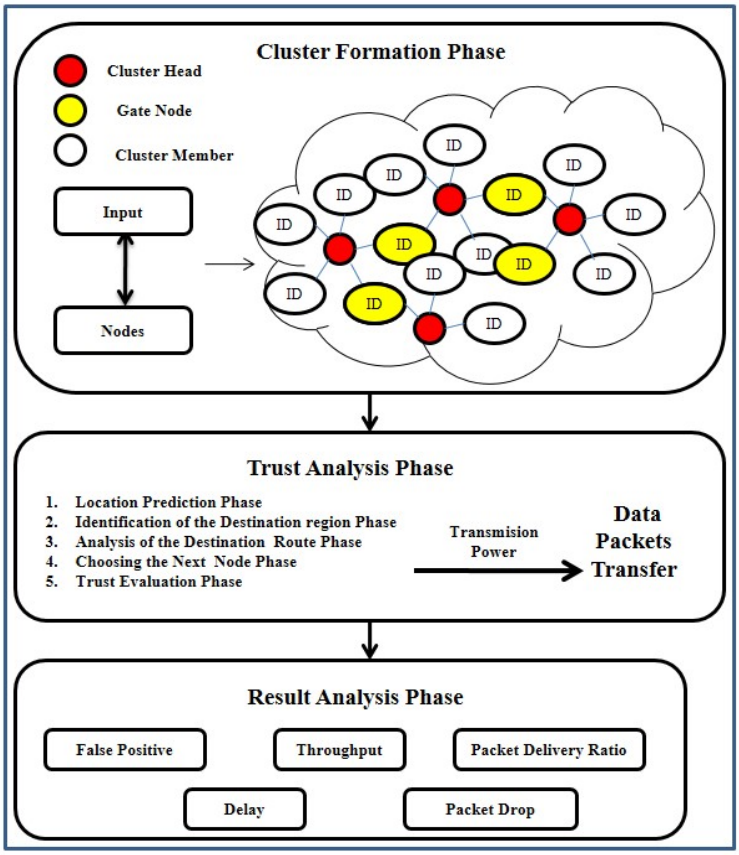

Fig 1. Architecture of Proposed Protocol

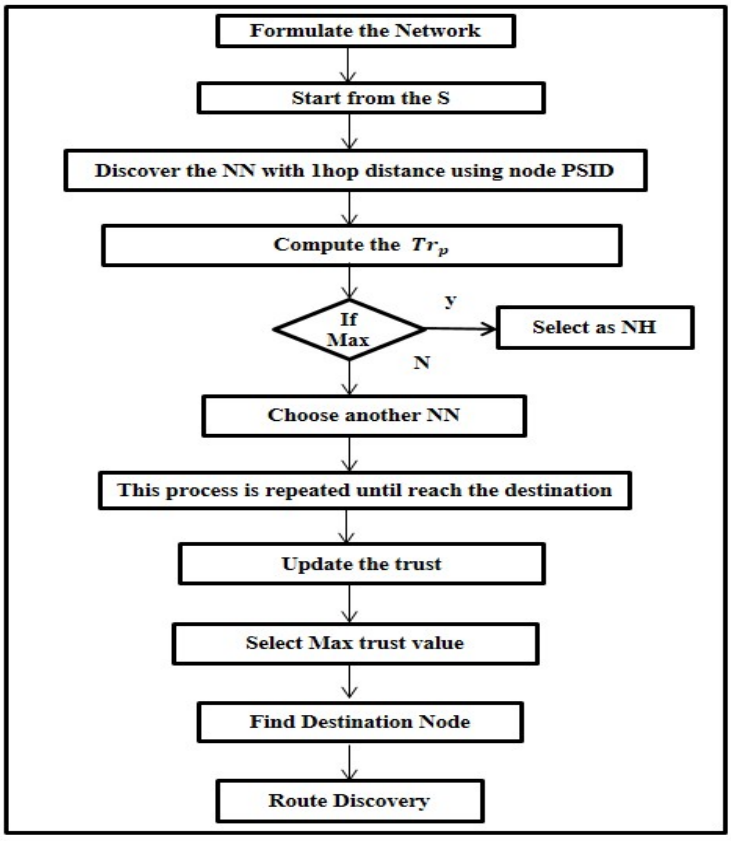

Fig 2. Flowchart of Proposed Protocol

Trust Analysis Phase

In these protocols, the trust analysis phase is classified into five phases.

- Location Prediction Phase.
- Identification of the Destination Region Phase.
- Analysis of the Destination Route Phase.
- Choosing the Next Node Phase.
- Trust Evaluation Phase.

Location Prediction Phase

In this phase, the CH stores acknowledge and save the positions of all the network nodes that are currently available. This calculation estimates the RSSI energy in free space at a distance d from the broadcaster using Eq.1. The communication range is essentially represented by the free space model as a cluster around the transmitter. A destination gathers all data packets if it is a member of the cluster. Otherwise, all packets are missed. As a result, each node in this protocol receives a ID. The destination direction is identified through the ID.

In this protocol, the CH uses a table to maintain the data for all of the nodes in the communication area. Periodically, each node transmits a signal. The node transmits its ID and the energy of the transmitted signal in points. The CH computes the node's ID from the received signal and saves it as an entry in the table.

The Smart Antenna System (SAS) on the CH allows it to determine the direction of arrival (DOA). The CH determines the direction and subsequently the geographic area where it is present according to the DOA value. The CH determines the signal's energy value from it. It determines the distance between itself and the node by using Eq.1 to calculate the transmission power.

In fact, the signal gives us information about the node's ID, energy, distance, and bandwidth. The new signal that the node sends includes ID, energy, velocity, and timestamp it starts to move. if the node's position has changed, the CH calculates that distance from its place to the desired node. The updated distance is $dist_{new}$. Old distance is $dist_{old}$, the name of the previously saved distance. It can determine the node's mobility direction from these two values. The node is moving away from the CH if $dist_{new}$ is higher than$dist_{old}$, or towards the CH if $dist_{new}$ is lower than $dist_{old}$.

The table containing the node's distance, timestamp, direction, and velocity has been updated. When the node's velocity or location changes, it will transmit a signal to the CH. No signal will be sent if not. Each node's ID is listed in the table. When the node moves among regions, the CH modifies the region value using the DOA values. On its Trust Table, the CH holds the trust value.

Identification of the Destination Region Phase

During this phase, the Source Node (SN) indicates the location of the Destination Node (DN). The source initially evaluates the distance of the neighbors before forwarding the packet. The SN transmits the packet directly if the DN is in its neighbor transmission range; otherwise, it sends the packets through the Gate Node (GN). For its neighbors, each node have a neighbor table (NT). Data from each of the node's neighbors are collected and stored in an NT. The NT contains trusted parameters in its table. The corresponding data might be erased after the neighbour node (NN) exits the cluster communication range. A new entry would be made each time a new node enters the communication range.

To identify the DN entry, the SN initially evaluates its NT. the SN can send the information directly to the DN if the entry has already been recorded. If the DN record is not found on the NT, the SN transmits a Destination ID Request Message (DIRQ) to CH to obtain the DN's ID. The DN location is included in the DIRQ message. The Destination ID Reply (DIRP) message will be used by the CH to communicate with the node. The DIRQ message contains the DN's ID.

After receiving the DN's ID, the SN initially evaluates the DN's exact location. Whereas if DN isn't changing its location, the SN has used the obtained ID for additional calculations. If the DN is changing, it must be known where it is at time T when the SN receives the ID to calculate its location. The DN's path between T_{dn} and t in terms of distance is given by Eq.2

$$QuoteDist_{T_{dn}}t\ Dist_{T_{dn}}t \qquad = (t - t_{dn}) * V_{dn} \tag{5}$$

T_{dn} Defines the time in the ID and t defines the time at which SN receives the ID.

The new position of the DN is calculated using the node's motion direction while evaluating the node's path length (D) using Eq.5.

Algorithm 1. Computation of DN's Movement Direction

Start

If D = $dist_{new}$

$$n_d = o_d - t_d$$

Else if D= $dist_{old}$

$$n_d = o_d + t_d$$

end

Where n_d denotes the actual distance between the DN and the CH, o_d is the old distance and t_d is the travelled distance. Now the DN's ID has trusted parameters. The SN seems to use this new ID for additional calculations because the DN is moving away.

Analysis of the Destination Route Phase

The DN's route is recognized by the SN as being a high trust rate node during this phase. Once receiving the DN's ID, the SN will select its Efficient Node (EN) as the Next Hop (NH) to transmit the information to the DN. One EN will be selected by the SN out of all those that are presented. To facilitate the EN selection, the SN subdivided its transmission range into four zones

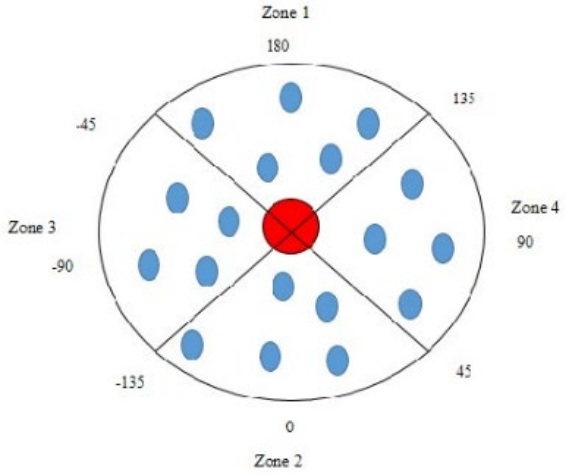

Fig 3. Circular Transmission Range With Four Zones.

Fig 3. demonstrates how the node's circular communication range is separated into four zones. It selects the best EN inside that zone after choosing the proper zone first. As in Fig.4 The SN helps reduce the estimation region to decrease overhead. The SN identifies which direction the DN is present by comparing the SN and DN IDs. According to the position of direction, this would select a specific zone for the NH selection step. It ignores the nodes in the other three zones and only considers the nodes in the zone that was selected. To determine the direction of the DN, the SN compares the ID of the received DN with its own ID.

Algorithm 2

Begin
If r(sn) =r(dn) //(both are within the circular transmission range)
If d(sn)>d(dn) then
SN selects zone 3 as the desired zone.
Else
Sn selects zone 4 as the desired zone
End
Else If r(sn) ≠ r(dn) then
If r(sn) + r(dn) = 0 or 180 then //(The circular transmission range from 0 to 180)
SN select zone 3 as the desired segment
Else compute $diff1 = |r_{DN} - r_1|$ and $diff2 = |r_{DN} - r_2|$ then
If diff1 > diff2 then
SN selects zone 2 as the desired zone
Else
SN selects zone 1 as the desired zone
End
End
End

Where r refers to the region of the SN.

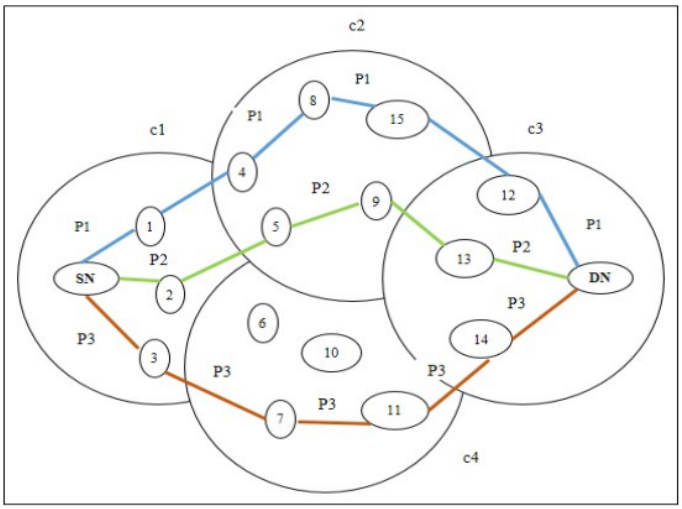

Fig 4. Packet Forwarding Route

c1, c2, c3, and c4 are clusters, whereas p1, p2, and p3 are packets. For i =1 to n, It computes Tr_p level before selecting the router with the highest Tr_p value. The optimum Tr_p trust value shows that the node is far away from SN. **Fig 4**, considers 1, 2, and 3 are maximized Tr_p values so the SN selects node 1 as NH for p1. It follows the p1 from SN-1-4-8-15-12-DN. For p2 the SN selects the route from SN-2-5-9-13-DN. To transmit the P3 the SN chooses a path from SN-3-7-11-14-DN. As a result, the burden is distributed across the participating nodes. The use of energy is managed. As a result, the network's duration will be extended.

Choosing the Next Node Phase

To communicate the necessary information during this stage, the best EN is identified as the NH. After choosing the desired zone, The SN would also pick up the NH node within it. After deciding on the portion, the SN would evaluate all of its neighbors. This would select one of them to operate as the NH and send the data packets.If a node has been used in communication, its energy will continuously decrease. If that node moves out of resources, connectivity won't exist. As a result, the transmission burden is shared equally among all of the available nodes. This algorithm is used as efficiently as feasible to select the NH node.

The SN takes the trusted parameters of each node in that specific area. Every node's Tr_p is computed by using Eq.6. The network's NH nodes will subsequently be determined by whatever node has the maximized Tr_p.

The trusted parameter result is computed using the neighbour node computation, bandwidth estimation, node energy, and distance from the SN.

$$\cdot\sum_{i=1}^{n} Tr_p = T_p + B(n) + Er(n) \quad (6)$$

Trust Evaluation Phase

The SN transmits data using the chosen NH. It determines if the accepted node is a reliable node or a malware node before sending the data. The CH sends the situation of the selected node to the SN. When a reliable node is chosen, the SN sends the information through that node. Furthermore, the malicious node is identified using the following steps.

The SN is looking forward to being acknowledged (ACK). Whether it receives an ACK, the intermediate nodes are excellent. If the CH does not obtain an ACK about any data, information will be sent to it.

An inquiry node (IN) is now assigned by the CH to identify the reason for the packet loss. From the SN, the designated IN sets out on its journey. It now requests that the SN start the transmission procedure. From the SN, information is forwarded to the Hop1 (H1) node. The transmitter address is the SN address, while the receiver address is the H1 node address. Additionally, the IN receives the data. The IN now confirms the H1 node's presence and successful data reception within the SN's transmission range.

The H1 node should now send information to the next selected node using the H1 address as the transmitter address and the H2 address as the receiver address. If the H2 transmits the data, the IN advances in that direction. If node H1 fails to send information, the IN will consider it a malicious node. Information is lost.

V. SIMULATION PARAMETERS

Through using the NS2 simulator tool, existing protocols such as GR, RBT, NETAR, and the proposed protocol TSRRP are simulated. The achievements of MANET's connections were analysed in the proposed work by comparing the

throughput, PDR, false positives, packet drops, and delay of the proposed work to GR, RBT, and NETAR to examine the trust model in **Table 1**.

Table 1. Simulation Parameters

Parameters	Values
Channel type	Wireless channel
Network interface type	Wireless-MAC
Routing Protocol	AODV
Simulation time	600s
Nodes present in network	100
MAC type	802.11 standard
Traffic Model	CBR
Simulation area	1000*800mts
Transmission Range	Omni antenna
Mobility	4-20/s

Result Analysis Phase

End-To-End Delay

The time elapsed after the final bit of a data packet arrives at its destination is known as the delay time. This has a significant impact on the mobility of certain groups of structure because some data groups are left alone for extended periods and have an impact on the result. To solve these issues, the developed approach gives high networking results in terms of delay, as illustrated in **Fig 5**.

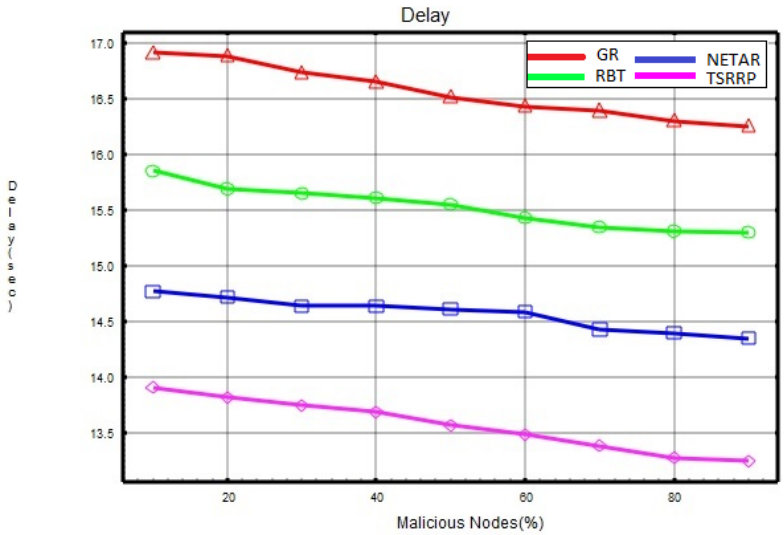

Fig 5. End-to-End Delay

The efficiency of TSRRP was 13.54%, which was lower than the existing protocols GR, which is 16.53%, RBT, which is 15,504%, and NETAR, which is 14.545%, which is higher than the proposed model and has an initial stability advantage over GR, RBT, and NETAR approaches. The suggested model has a strong ability to predict the future and is effective in reducing selfish nodes

False Positives

False positives are the results of measuring misbehaving nodes against all nodes.

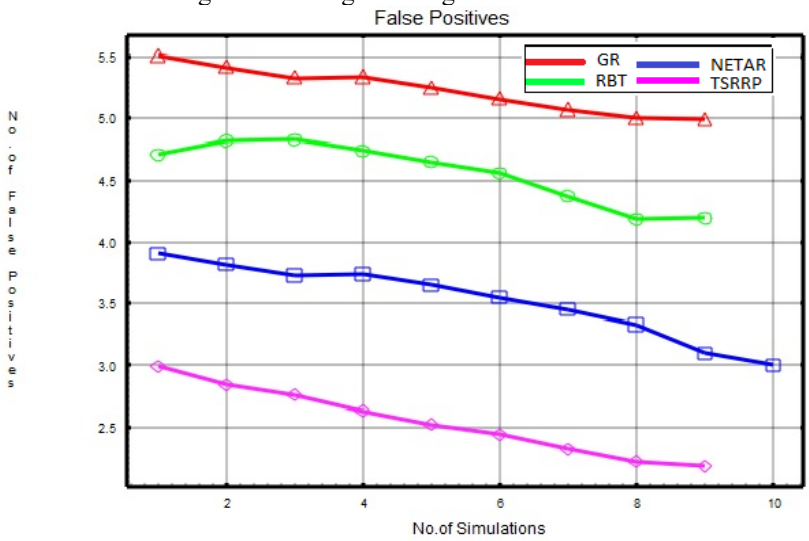

Fig 6. False Positive

Fig 6. shows the TSRRP methodology with GR, RBT, and NETAR in terms of simulation numbers. Our protocol reduces the node's irresponsibility by 2.508% compared to GR, RBT, and NETAR, where it is 5.206%, 4.524%, and 3.528%, respectively.

Packet Dropped

The ratio values differ remarkably in areas with high mobility. Some of the nodes between the clusters cause messages to be lost when nearby nodes in the clusters move outside of the transmission range. By comparing the messages lost throughout the process, it was possible to analyze packets dropped on malicious nodes.

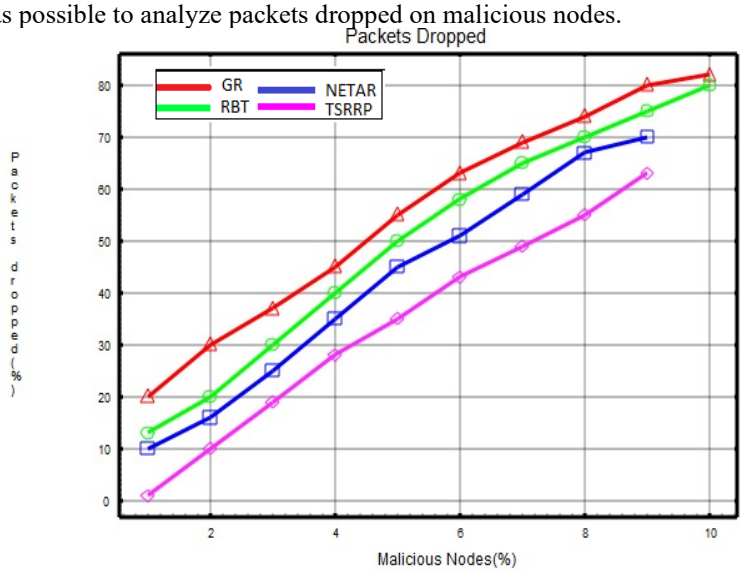

Fig 7. Packets Dropped

According to the percentage of malicious nodes, **Fig 7** demonstrates the effectiveness of the proposed protocol TSRRP is 37.19% lower than that of the existing protocols, GR, which is 55.5%, RBT, which is 50.1%, and NETAR, which is 45.177%.

Packet Delivery Ratio

The source node yields the packets of data and sends them to the destination node through the intermediate node. The TSRRP protocol is most effective in identifying the malevolent nodes and raising the range of PDR values compared with

the existing protocol. **Fig 8** illustrates how the proposed protocol TSRRP improves PDR and permits 77% better than the existing protocols GR, RBT, and NETAR, which provide 53.8%, 61.9%, and 69.8%, respectively.

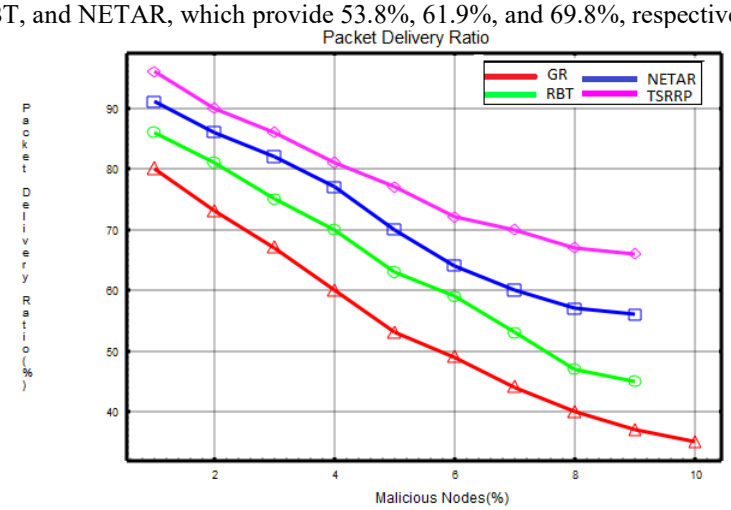

Fig 8. Packet Delivery Ratio

Throughput

It is defined as the total number of data bits correctly received by the receiver each time. The accurate and selective information provided by throughput determines whether or not data packets will reach their destination. Trusted values that have been maximised prevent harmful attempts and provide the correct result in the shortest amount of time. According to network size, **Fig 9** demonstrates that TSRRP, which is 0.746%, enhances throughput compared to GR, which is 0.357%, RBT, which is 0.442%, and NETAR, which is 0.528%.

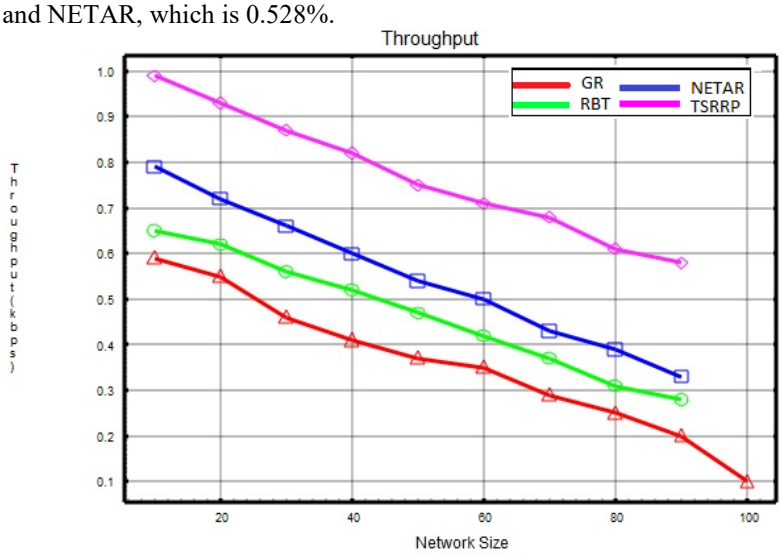

Fig 9. Throughput

VI. CONCLUSION

The performance of the network is enhanced by the proposed TSRRP protocol for military communication on MANETs. By using the available path, the protocol decreases the overhead associated with routing. The packets will be sent by the most trustworthy node. This method minimises the number of connections, mobility-related loss of data, and memory management. By distributing the load among all nodes according to their remaining energy, it extended the network's lifespan. The NS2 simulator tool is used to verify this. Compared to Novel Energy Efficient Routing Protocol (NETAR), Global State Routing (GR), and Reputation-Based Trust-Aware Routing Protocol (RBT). Future research will concentrate on optimising security with secret keys.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author(s) declare(s) that they have no conflicts of interest

References

[1]. M.S.Usha, K.C.Ravishankar. Implementation of trust-based novel approach for security enhancements in MANETs. SN Computer Science (2021)2:257.

[2]. G.M.Levchuk, F.Yu, K.R. Pattipati and Y.Levchk, "From hierarchies to heterarchies: Application of network optimization to design of organizational structures", in proc. Command control Res.Technol.Symp.,Washington,DC,USA,Jun.2003,pp. 1-11.

[3]. C.Park, K.R. Pattipati, W. An, and D.L.Kleinman, "Quantifying the impact of information and organizational structures via distributed aunction algorithm: point-to-point communication structure,"IEEE Trans.Syst., man,cybern.A.Syst.Humans, vol.42, no.1, pp.68-86,vjanv2012.

[4]. T.Maseng and C. Nissen, "Network centric military communication", IEEE Commun, Mag., vol. 44, no. 11,p.36, nov. 2006.

[5]. Dhananjayan G.Subbiah J. T2AR: trust-aware ad-hoc routing protocol for MANET. Springerplus. 2016; 5:1-16.

[6]. Jayamkumari A, Sakthivel M. Trust management model observation towards security enhancements and QoS in MANET's. Int J Innov Res Comput Commun Eng.2015; 3:1994-7.

[7]. Sharma N,Popli R. A literary review of MANET security. Int J Adv Res Ideas Innov Technol. 2019;5(2):1237-9.

[8]. Renu and Sharma S, Energy Efficient secure routing framework based on multidimentional trust evaluation for MANET. J Netw Inform Secur.2019;7(1):20-4.

[9]. Raju RL, Reddy CRK. Security Improvisation through node trust prediction approach in mobile Ad Hoc network. Int J Interact Mob Technol. 2019; 13(9):40-51.

[10]. Anjum SS. Noor RM, Anisi MH. Review on MANET based communication for search and rescue operations.Wirel Pers Commun.2015;94:31-52.

[11]. Batham G, Sejwar V.Implementation of Dempster-shafer theory for trust based communication in MANET. Int J Comput Appl.2016;150(11):27-32.

[12]. Sahadevaiah K, Prasad Reddy PVGD, Narasimha G. A new security protocol for mobile. Ad Hoc Netw. 2012;3:9-15.

[13]. Desai AM, Jhaveri RH.secure routing in mobile ad Hoc Networks: a predictive approach. Int J Inf Technol.2018;11:345-56.

[14]. Saadoune M,Hajami A and Allali H. Distance quantification algorithm in AODV protocol, Networking and Internet Architecture, Cornell University, 1-12(2014).

[15]. Yadav P and Gaur M. A survey on formal modelling for secure routing in mobile Ad Hoc networks. In: International conference on distributed computing and internet Technology. 2015: 18-23.

[16]. Dangare N.N and Mangrulkar RS.Design and development of trust based approach to mitigate various attacks in mobile Ad hoc network. In: international conference on quality up-gradation in Engineering, science and technology (ICQUEST2015).2015;27-32.

[17]. Geetha D and Revathi B.AOMDV routing based enhanced security for black hole attack in MANETs. In: International Conference on Research Trends in Computer technologies (ICRTCT-2013).2013; 20-24.

[18]. Bruzgiene R,Narbutaite L, Adomkus T.Manet network in internet of things system, peer-reviewed chapter. Ad-hoc networks, INTECH Open Sci.2017.http://doi.org/10.5772/66408.

[19]. Kothandaraman D, Chellappan C.Energy efficient node rank based routing algorithm in mobile ad-hoc networks.Int J Comp Netw Commu.2019; 11(1):45-61.

[20]. Swetha MS, Thangamani M. A novel approach to secure mysterious location-based routing for MANET. Int J Innov Technol Explor Eng. 2019; 8(7): 2587-91.

[21]. Mangrulkar RS.Chavan PV,Dagadkar SN. Improving route selection mechanism using trust factor in AODV protocol for MANET. Int J Comput Appl.2010; 7(10):36-9.

[22]. Kaur J,Singh T. A secured data transmission method using enhanced secret sharing scheme to prevent black hole attack in MENETs-a review. Int J Comput Appl.2015; 119 (10):20-8.

[23]. Liu W,Yu M.AASR: authenticated anonymous secure routing for MANETs in adversarial environments. IEEE Trans Veh Technol.2014; 63(9).

[24]. Suma CC,Gururaj HL, Ramesh M. An authenticated encrypted routing protocol against attacks in mobile ad-hoc networks. Computat Methods Soc Sci. 2016; 4(2): 5-11.

[25]. Deafawy KE, Tsudik G. Privacy preserving location-based on-demand routing in MANETs. IEEE J select Areas Commun 2011; 29(10): 1926-1934.