E-ISSN 2581 – 7957
P-ISSN 2277 – 3916
CVR Journal of Science and Technology, Volume 23, December 2022
DOI: 10.32377/cvrjst2314

Trust-based Model to Alleviate Selfish Node Attacks in MANETs

M. Deva Priya
Assoc. Professor, Sri Eshwar College of Engineering/CSE Department, Coimbatore, Tamilnadu, India
Email: devapriya.m@sece.ac.in

Abstract: **MANETs are dynamic in nature. So, they are subject to several attacks. It is always essential to ensure confidentiality, availability, authenticity and reliability of the network. Conserving energy in MANETs is an uphill task. Hence, it is mandatory to design an energy-aware inter-clustering scheme that involves Residual Energy (RE) and resources. Confirming security in MANET is another challenge. In this Paper, selfish nodes are determined based on a Trust Value (TV) that involves packet forwarding behavior, resource utilization, reliability and RE. In this paper, Reliable History dependent Resource Conscious Clustered-OLSR (RHRCC-OLSR) protocol is proposed to overcome degradation of network performance owing to selfish node attacks. It is evident that the propounded protocol offers improved PDR and throughput with reduced delay, PLR, energy and routing overhead.**

Index Terms: **Selfish node attack, MANET, Trust, Reputation, History, OLSR**

I. Introduction

As MANETS are self-organizing wireless networks and do not demand any static infrastructure for configuration, it is more appropriate to be applied in surroundings that need immediate setup. Security in MANETs is an issue which has to be addressed. The presence of selfish nodes greatly worsens the performance of the network [1, 2].

A. Ensuring Trust in the Network

A trust factor is defined to depict the security level. Researchers have focused only on subjective trust. Trust is categorized into direct as well as indirect trusts [3, 4].

- **Direct Trust:** Each node retains direct relationship with neighboring nodes. The behaviors of neighbors are observed during routing. The experience with neighboring nodes is also taken into consideration.
- **Indirect Trust:** It is determined based on nodes located outside the range of communication. Requests as well as responses may flood the network.

Trust computation consumes more time, bandwidth as well as energy. This leads to delay in discovering routes with an increase in computational overhead [5, 6].

The dynamic nature of network topology makes trust management difficult. Hence, to deal with this issue, a trust factor is added to the proposed scheme for mitigating routing attacks. TVs are computed for every node making it suitable for sending data to destination [7].

B. Selfish Node Attack

Selfish nodes focus on getting services from the network while preserving resources like battery or bandwidth. These nodes attempt to preserve communication amid nodes. But they do not collaborate to transmit packets. These nodes are involved in any one of the ensuing actions.

- Turn off power when active communication is not present
- Do not forward Route REQuests (RREQs) on receiving one
- Forward RREQ on the inverse path but not Route REPly (RREP). The source is not capable of identifying a path to destination and hence RREQ is sent again
- Do not unicast or broadcast Route ERRor (RERR) packets in case paths are not available.
- Selectively drop packets

The delivery rate is lessened by dropping packets.

C. Dynamic Reputation Management

The reputation of a node is determined based on type of packets namely, data and control packets [8]. As nodes join a network, they are ignorant of reputations of adjoining nodes. This demands assigning a default reputation to every node in the network [9]. The node reputation takes values in the range [0-2]. The corrective module includes a punishment scheme and a path administrator [10].

A node table is maintained to store the reputation of nodes. As packets are transmitted, there should be an increase in the total reputation of nodes. The status of nodes is found based on total reputation associated with a grading criterion. The path administrator takes the responsibility of removing nodes with reduced reputation from the route cache based on information obtained from the punishment mechanism [11, 12]. It ensures that packets are not forwarded through a path involving black-listed nodes.

In the proposed system, the node's trust is computed based on Residual Energy (RE), resource utilization and packet forwarding behavior along with reliability rate. The propounded Reliable History dependent Resource Conscious Clustered-OLSR (RHRCC-OLSR) protocol includes modules for detecting RE and computing trust.

In case of RE detection module, along with RE and reliability, rates of drain, packet drop and failure are determined. The rate of drain of a node is determined using an exponential weighted mechanism. The rate of packet drop is the difference amid the number of packets received as well as relayed to next hop nodes. Likewise, the failure rate is given by the sum of product of packet drop rate as well as weighted average of every session. Node reliability is determined from the failure rate of a node. TV is defined in terms of quantity of forwarded packets, RE, used bandwidth and node reliability.

CVR College of Engineering
Received on 11-05-2022, Revised on 01-11-2022, Accepted on 07-11-2022

II. Related Work

Arboit et al (2008) [13] have propounded localized certificate revocation for MANETs. The main issue related to certificate revocation is that there is no on-line acquisition to trustworthy authorities. In case of wired networks, if certificates are to be withdrawn, Certificate Authorities (CAs) add information associated with certificates to Certificate Revocation Lists (CRLs) and submit them to repositories or dispense them to suitable entities. In case of simple networks, there is no acquisition of centralized repositories or trusted authorities. Hence, the traditional method of certificate revocation is not applicable. The proposed decentralized scheme for certificate revocation allows nodes to handle challenging entities. The method is not based on input from central or external entities.

Li et al (2012) [14] have offered a framework for offering context-based security as well as trust based on some policies. The proposed scheme incorporates contextual information in terms of status of battery and communication channel including weather conditions. It is used in determining whether misbehavior is the result of malevolent action or not. It identifies malicious and malfunctioning nodes.

Eissa et al (2013) [15] have designed a trust-dependent routing scheme. The challenging problems related to routing and security are discussed. Friend Ad hoc On-Demand Distance Vector (FrAODV), a trust-based scheme, is proposed for securing AODV protocol. The routing paths are identified depending on node reputation and identity before routing data. This scheme offers a robust environment where nodes rely on one another in a secure community.

Wei et al (2013) [16] have offered cluster-based certificate revocation along with a vindication feature. Though networks offer mobility with effective positioning, they are susceptible to numerous classes of security attacks in contrast to wired networks. Secured services are to be assured. To handle this confrontation, revocation of certificates is taken as an essential integral element for securing communication. It focuses on segregating attackers from added participation in network functions. Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme offers quick as well as precise revocation. The mechanism improves reliability and accuracy. The threshold-based scheme helps in deciding whether vindictive alerted nodes are candid nodes or not before convalescing them.

Adnane et al (2013) [17] have proposed a trust dependent security for OLSR routing protocol. Trust is implicitly included in the protocols based on co-operation, particularly, amid the entities included in routing. Certainly, as the range of nodes is restricted, they jointly collaborate with their neighbors so that they extend to distant nodes and then the whole network. Moreover, trust administration allows objects to deal with trust and get decisions concerning other entities. Trust-based OLSR protocol is designed to permit every node to evaluate behavior of nodes. Once malevolent nodes are determined, preventive measures along with countermeasures to deal with irregularity are also presented.

Shurman et al (2014) [18] have proposed a co-operative reputation scheme to circumvent malevolent nodes. Routing as well as forwarding takes place through existing nodes. The BSs are concerned with route detection and maintenance, stimulating traffic along with network management. More amount of energy is spent for forwarding packets without any direct gain. A misbehaving as well as greedy node has short-term efficacy and may not contribute to routing. The proposed Reputation Approach (RAP) involves a reputation model that identifies and segregates misbehaving nodes which are not involved in collaboration for sending packets of added nodes.

Chatterjee et al (2014) [19] have designed a trust-based secure clustering framework. Secure clustering is highly essential. Conventional cryptographic solutions cannot be applied to threats from attacked nodes. Nodes' trust is computed using self as well as recommendation support of 1-hop neighbors. Based on communication as well as computational demands, the scheme is lightweight but dominant depending on flexibility in dealing with trust. Furthermore, this clustering protocol splits the network into 1-hop separate clusters and chooses nodes that are highly fit and reliable as CHs. An authentic voting scheme using parallel signatures is used for selection.

Abdel-Halim et al (2015) [20] have propounded a trusted on-demand routing protocol based on an agent. The overall routing ability is dependent on support of nodes which form the network. This behavior is handled by considering node reliability for choosing routes in addition to hop count. Trustworthiness is obtained by finding the TV of every node. This agent-based protocol is based on Dynamic Source Routing (DSR). This handles trust-dependent information with insignificant load depending on added messages as well as delay. Multi-Agent System (MAS) is used in every node. It includes monitoring as well as routing agents. A mathematical model is used for finding the TV. This method is based on the amount and size of packets which reveal selective forwarding features of a node.

Ullah et al (2016) [21] have proposed a fuzzy-based trusted model for finding selfish nodes involved in routing data. A node may not be ready to offer resources for helping others in case there is no profit for its service. Such nodes are said to be non-cooperative or selfish. This may cause partitioning of the network. Fuzzy-based analyzer is used for splitting nodes into non-cooperative and trustworthy ones. TVs are forwarded to fuzzy functions mapped to varied classes. The resulting class shows trust levels of observed nodes. Depending on computed TV, the malevolent nodes are determined and removed from active routes.

Sengathir&Manoharan (2017) [22] have focused on identifying and highlighting diverse reputation-dependent mitigation schemes for selfish node attacks along with their merits and demerits. They have presented a context-and reputation-dependent mitigation scheme categorized based on history, condition probability and futuristic probability. They have presented a review on several selfish node mitigation architectures and also aim to highlight statistical trustworthiness co-efficient which aids in efficient alleviation of selfish nodes.

Kumar & Dutta (2018) [23] have proposed an intrusion identification scheme based on dynamic trust to find and segregate selfish nodes from the network. The direct trust depending on direct communications and indirect trust depending on neighbors' endorsements are taken into

consideration to precisely find selfishness of nodes. The proposed scheme offers better results.

Nodes that are idle are considered to be selfish and are circumvented from routing. To deal with this issue, Rama Abirami&Sumithra (2019) [24] have proposed neighbor and improved neighbor credit values-based AODV routing schemes. These protocols are assessed against AODV for identification of selfish nodes. Neighbor Credit Value based AODV (NCV-AODV) protocol avoids false detection. Improved Neighbor credit value based AODV (iNCV-AODV) protocol is also proposed. In both the protocols, it is assumed that only some nodes exhibit malicious behavior.

Abdelhaq et al (2020) [25] have studied the influence of selfish node attack on AODV and DSDV to determine resilient protocol. Selfishness Attack Model (SAM) is proposed to deal with selfish node attack on routing protocols. AODV offers better performance in contrast to DSDV.

Deva Priya et al (2021) [26] have proposed Skellam Distribution Inspired Trust Factor-based Selfish Node Detection Technique (SDITF-SNDT) for ensuring efficient detection and segregation of selfish nodes from the network. The proposed scheme induces selfish node detection by finding the average packet deviance using which Standard Deviation (SD) and Variance are determined for finding Skellam Distribution Inspired Trust Factor (SDITF). This computation helps in estimating the reliability to classify them into selfish as well as co-operative nodes. From the examinations performed for the proposed scheme, an outstanding enhancement in Packet Delivery Ratio (PDR) and remarkable reduction in the amount of energy consumed are confirmed for varying amounts of nodes.

Jim et al (2022) [27] have presented a bio-inspired algorithm called Artificial Immune System Based Algorithm (AISBA) to identify selfish nodes. It is based on the principle of Artificial Immune Systems (AIS). Unlike Combined Immune Theories Algorithm (CITA), AISBA does not involve a learning stage. Two dissimilar trust models are designed to distinguish genuine and selfish nodes. The proposed scheme offers better results in terms of mean detection rate, PDR and False Positive Probability (FPP) based on weight as well as trust on threshold.

III. Proposed Reliable HRCC-OLSR (RHRCC-OLSR) Protocol

Selfish nodes are involved in discovering routes and maintaining functionalities of routing protocol. They remain idle by not forwarding packets but get benefited from other nodes. The proposed Reliable HRCC-OLSR (RHRCC-OLSR) protocol assesses the reliability of node based on RE, bandwidth utilized, quantity of sent and received packets along with reliability rate.

The proposed mechanism includes modules for RE based detection as well as computation of trust.

A node that seems to be selfish drops packets owing to limited energy and data rate, along with poor channel conditions. They can be identified by analyzing the routing table of adjacent nodes of a malevolent one. In case information related to neighbors does not get modified, the node is considered as a selfish node.

The presence of these nodes degrades network performance. These nodes do not forward packets even when they are active. Routing tables of adjoining nodes of malevolent node are not updated. Acknowledgements are not received in specified time. They drop packets which affect the dropping rate of packets. These nodes may be isolated in 3 varying ways. Firstly, TV is computed based on behavior of adjacent nodes in addition to RE. The RE of nodes is analyzed. There are chances for a co-operative node to become a selfish node. A nodes' selfish behavior is dependent on the exponential reliability factor. These nodes should be removed from the routing path.

A. Residual Energy (RE) based Detection

RE-based model for isolating selfish nodes is proposed to determine the available energy (E_A) of nodes along the path from source to destination by taking into consideration the node energy after data transmission. Energy Drain Rate (E_{DR})shows the amount of energy drained in a participating node.

The energy of a node at any instance of time 't' is given by,

$$E_A = \frac{RE}{E_{DR}} \quad (1)$$

The drain rate of a node is computed using an exponential weight-based scheme.

$$E_{DR} = \rho \times E_{DR}^{K} + (1-\rho)E_{DR}^{K-1} \quad (2)$$

$$\rho = \frac{E_{TR}}{Number\ of\ Hops} \quad (3)$$

Where

ρ - Weighted average

E_{DR}^{K}- Rate of drain of a node at session 'k'

E_{DR}^{K-1}- Rate of drain of a node at session 'k-1'

E_{TR} - Energy required for transmission

A node is said to be selfish, if 'E_A'is less than the threshold (E_{TH}).

E_{TH} - Energy level essential for a participating node (50 Joules)

Packet Drop (PD_i) is the variance quantity of packets received (P_{RC_i}) and relayed (P_{RL_i}) by a node (i) as shown in Equation (4).

$$PD_i = P_{RC_i} - P_{RL_i} \quad (4)$$

'PDR_i' of a node for session 'k' is given in Equation (5).

$$PDR_i^k = \frac{PD_i^k}{P_{RC_i}^k} \quad (5)$$

Rate of Failure (RF_i) is the weighted average of 'PDR_i'for each session.

$$RF_i = \frac{\sum_{i=1}^{k} \blacksquare PDR_i}{k} \quad (6)$$

'RF_i' is computed using PDR of node. The reputation of a node is manipulated depending on the Predicted Reliability Factor (PRF_i).

$$PRF_i = e^{-FR_i} \quad (7)$$

In casea node's reliability goes below 0.4, then it is said to be selfish and is removed from the routing path. Once they are identified, the network should be restored to increase performance.

B. Trust Computation

TV (Abdel-Halim et al 2015) is based on neighbors' REQ status. In the proposed work, reliability is measured by considering the RE, bandwidth utilized and PRF. At very node, 'RE_i' is determined. It is the difference between presently available and expended energy at a node.

$$RE_i = E_{Cur_i} - E_{Con_i} \quad (8)$$

Where,

E_{Cur_i} - Energy currently available

E_{Con_i} - Energy that is consumed

TV is given by the following formula.

$$TV = \frac{HF_i^j}{RF_i^j} \; x \; \frac{RE_i}{BW_U} \; x \; PRF_N \quad (9)$$

Where,

BW_U - Bandwidth utilized

RF_i^j - Quantity of packets requested by node 'j' to be forwarded by 'i'

HF_i^j - Quantity of packets forwarded by node 'i' and received by 'j'

Counter 'RF_i^j' is increased when 'j' sends a packet to 'i'. It is essential to make sure that node 'i' sends packets. If 'j' identifies that 'i' sends packets before a pre-determined period, then counter 'HF_i^j' is incremented.

In case the RE of nodes go below 50%, then those nodes will not be involved in routing. Increased energy reserve (RE) with better TV confirms trustworthiness of a route.

Nodes with TV<TH are identified as malicious. TH is set as 0.3 and those nodes with TV< 0.3 will not be involved in the process of routing. This overcomes packet losses as well as delays involved in data transmission.

IV. Results and Discussion

The system is implemented using ns2. It is seen that the proposed RHRCC-OLSR protocol outdoes OLSR, E-OLSR and HRAC-OLSR protocols based on diverse parameters including PDR, total energy consumption, average delay, PLR, throughput, RE and routing overhead.

The performance of the proposed scheme is compared with the above-mentioned standard protocols for varying number of nodes.

Performance depending on Varying Number of Nodes

The performance of the proposed RHRCC-OLSR is investigated by varying the quantity of nodes. It is evident from the results that the proposed scheme offers improved results in contrast to existing OLSR, E-OLSR and HRAC-OLSR protocols. The number of nodes is varied from 100 to 1000.

From Figure 1, it is evident that the proposed protocol offers better PDR for varying number of nodes in contrast to the standard protocols taken for study. With increase in the number of nodes, the schemes show a decrease in PDR. The proposed scheme is efficient in predicting the malevolent activity of nodes by considering RE and TV, thus making the system less susceptible to attacks. This facilitates the proposed system to offer greater enhancement in delivering packets when compared to benchmarked protocols. RHRCC-OLSR offers 31%, 21% and 6% better PDR when compared to OLSR, E-OLSR and HRAC-OLSR schemes respectively.

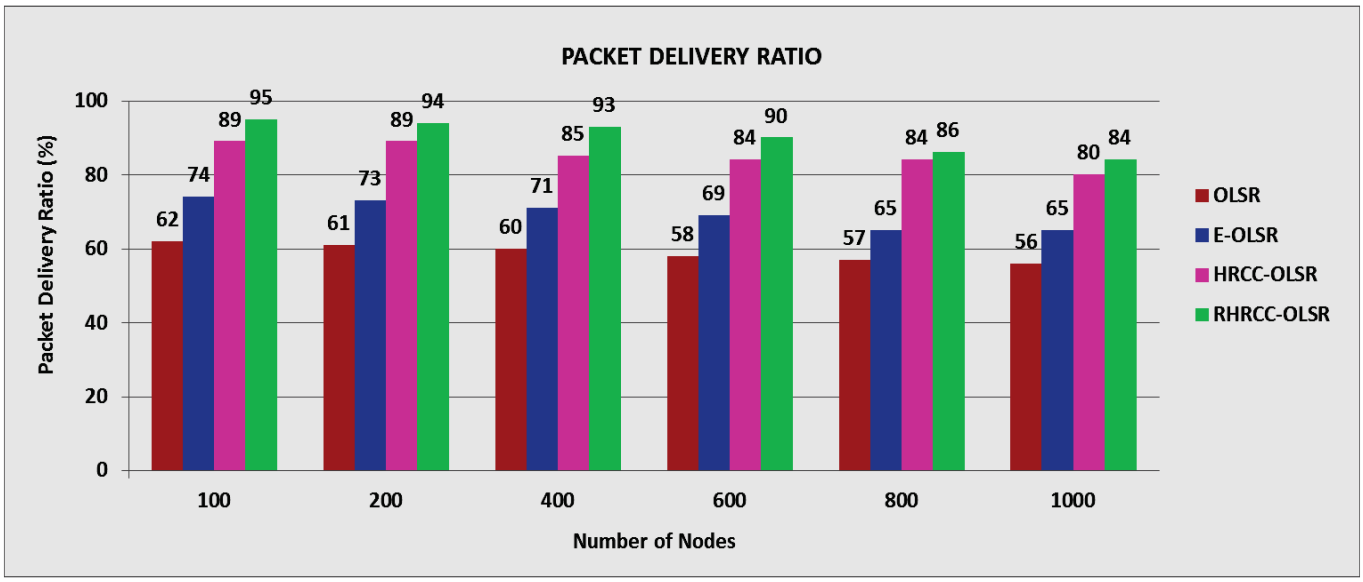

Figure 1. Packet Delivery Ratio of RHRCC-OLSR based on Number of Nodes

On the other hand, the existing OLSR, E-OLSR and HRAC-OLSR protocols offer 66%, 52% and 16% reduced throughput when compared to the proposed protocol (Figure 2). As selfish nodes are isolated from the network, they do not

CVR Journal of Science and Technology, Volume 23, December 2022
DOI: 10.32377/cvrjst2314

participate in the routing process. The reliable nodes along the path guarantees well-timed delivery of packets, thus offering increased throughput.

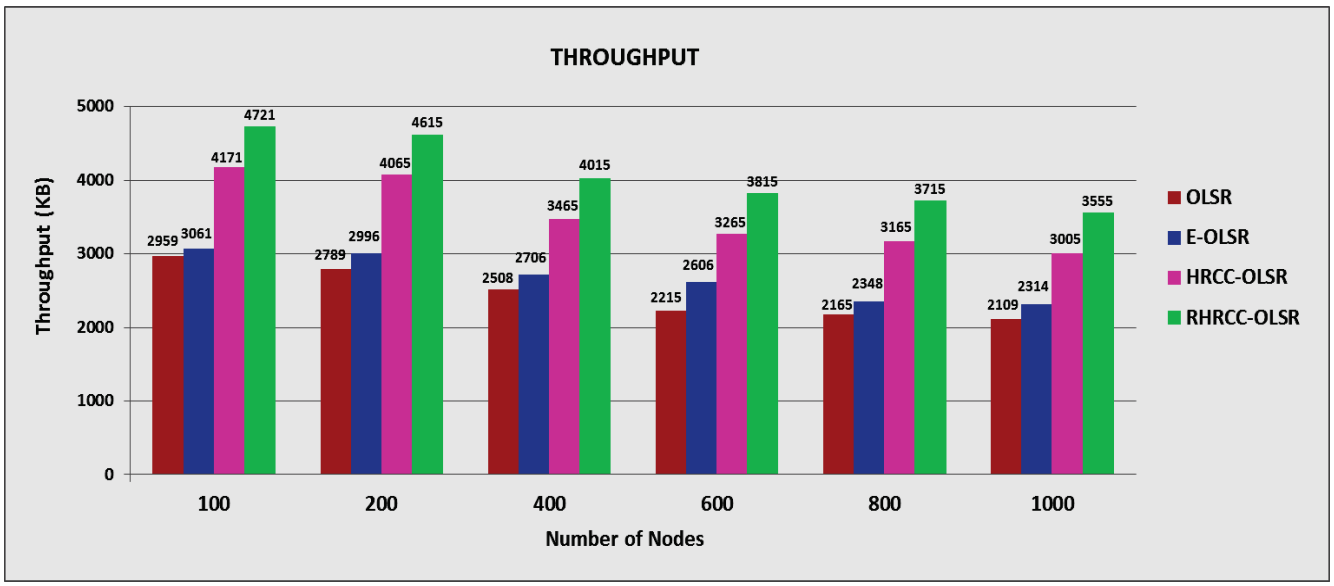

Figure 2. Throughput of RHRCC-OLSR based on Number of Nodes

From Figure 3, it is evident that performance of the proposed protocol is examined depending on RE and performance is compared with standard protocols for varying quantities of nodes. Energy consumption of existing protocols is more when compared to the proposed protocol. The RE decreases with increase in the quantity of nodes. Proposed protocol conserves energy to a greater extent and hence has increased RE in contrast to standard protocols. It has42%, 23% and 6% more RE when compared to OLSR, E-OLSR and HRAC-OLSR protocols correspondingly.

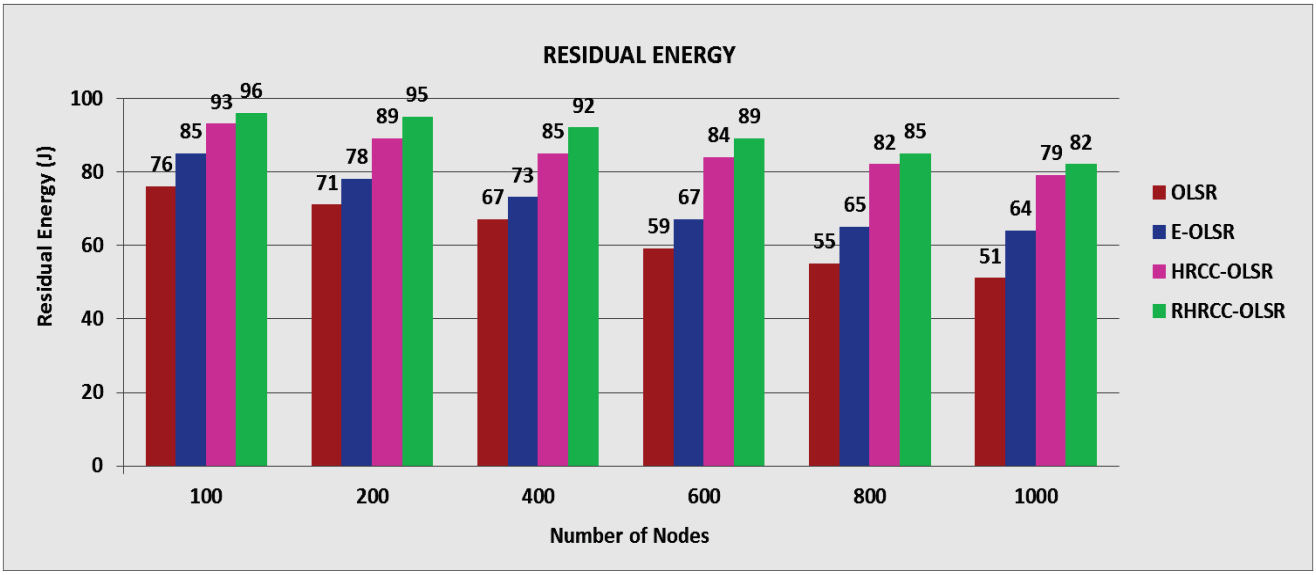

Figure 3. Residual Energy of RHRCC-OLSR based on Number of Nodes

From Figure 4, it is obvious that the proposed protocol involves lesser average delay. The existing protocols show an increase in delay in contrast to proposed RHRCC-OLSR. The malevolent nodes are isolated by determining the TV of participating nodes, which ensures route reliability. The average delays of existing OLSR, E-OLSR and HRAC-OLSR protocols are 32%, 20% and 11% more when compared to the proposed protocol.

CVR Journal of Science and Technology, Volume 23, December 2022
DOI: 10.32377/cvrjst2314

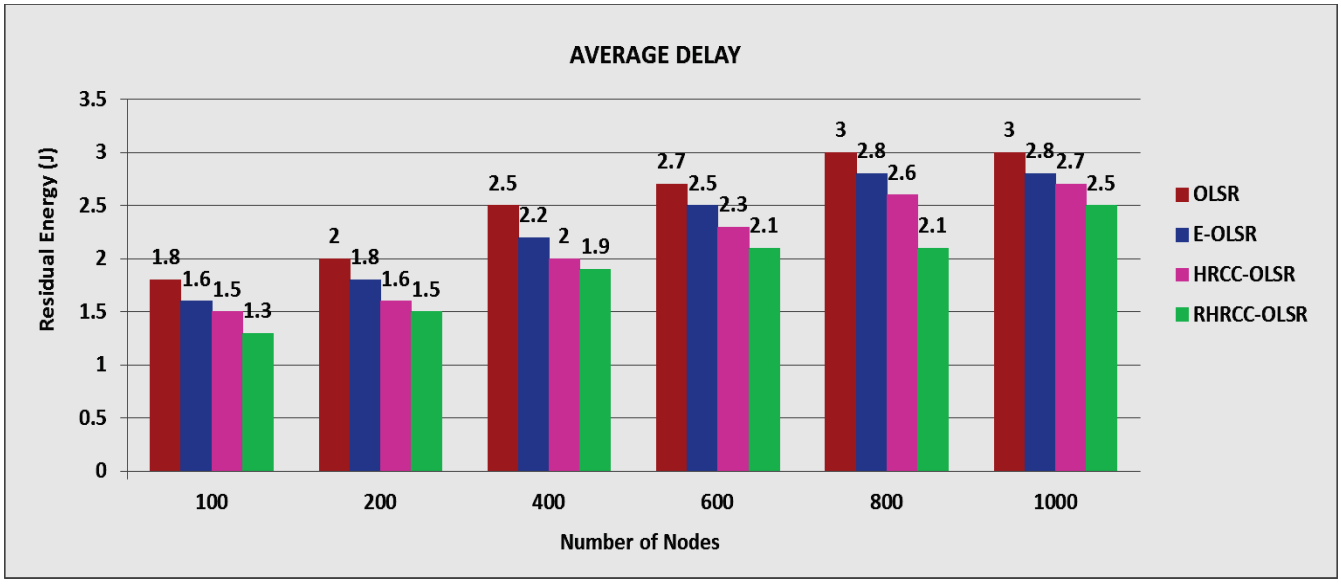

Figure 4. Average Delay of RHRCC-OLSR based on Number of Nodes

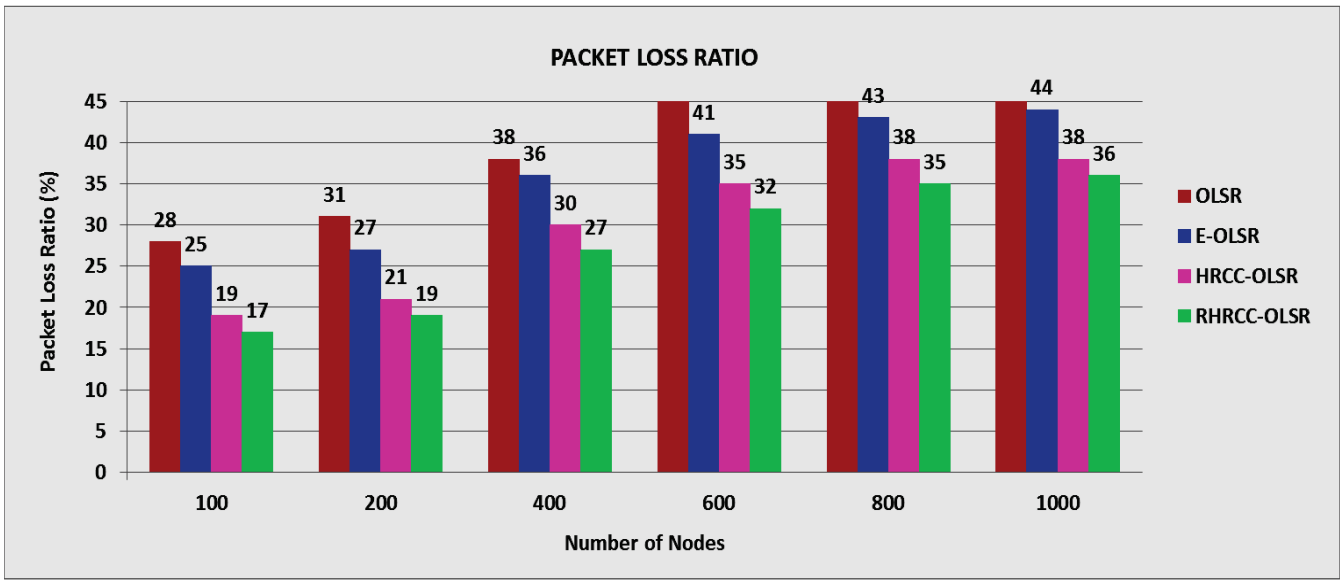

Figure 5. Packet Loss Ratio of RHRCC-OLSR based on Number of Nodes

Similarly, the proposed protocol involves reduced PLR when compared to the standard protocols. It involves 45%, 30% and 10% less PLR when compared to OLSR, E-OLSR and HRAC-OLSR protocols respectively (Figure 5).

The performance of the proposed protocol is also analyzed in terms of routing overhead and compared with standard protocols. RHRCC-OLSR involves reduced routing overhead as it permits only trusted nodes to be involved in routing, thus dropping the likelihood of performing malevolent activity. OLSR, E-OLSR and HRAC-OLSR protocols involve 32%, 23% and 7% more routing overhead when compared to the proposed protocol (Figure 6).

CVR Journal of Science and Technology, Volume 23, December 2022
DOI: 10.32377/cvrjst2314

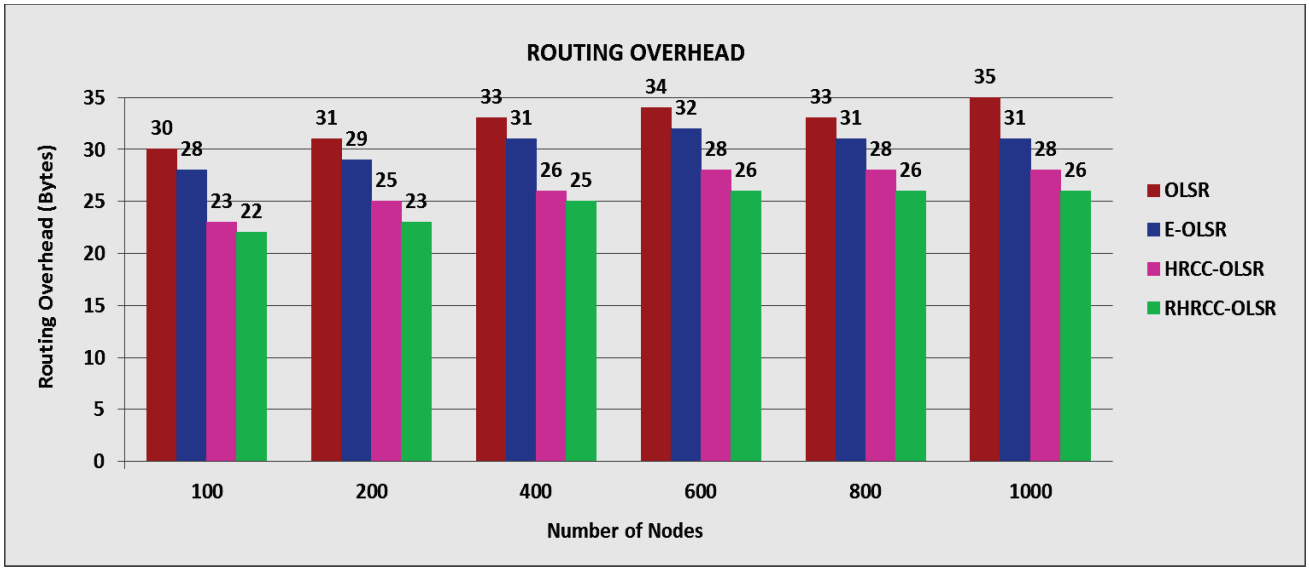

Figure 6. Routing Overhead of RHRCC-OLSR based on Number of Nodes

V. Conclusions

The Reliable HRCC-OLSR (RHRCC-OLSR) protocol propounded in this paper aids in determining the trustworthiness of mobile nodes in MANET depending on RE, bandwidth and reliability along with the quantity of packets received as well as forwarded. The selfish behavior of nodes is analyzed and TV is computed based on which nodes exhibiting such behavior are removed from the network. Residual Energy (RE)-based detection aids in determining the available energy of nodes. RHRCC-OLSR determines TV based on RE. The nodes with RE and TV below threshold limit are marked as malevolent and are not allowed to take part in routing. Computations based on energy and trust makes the system less susceptible to security attacks. The proposed scheme offers improved PDR and throughput involving reduced average delay, PLR, energy and routing overhead.

References

[1] Sheikh, R., Chande, M. S., & Mishra, D. K. (2010, September). Security issues in MANET: A review. In 7th IEEE International Conference on Wireless and Optical Communications Networks-(WOCN), pp. 1-4..

[2] Ishrat, Z. (2011). Security issues, challenges & solution in MANET. IJCST, 2(4), 108-112.

[3] Alani, M. M. (2014, November). MANET security: A survey. In IEEE International Conference on Control System, Computing and Engineering (ICCSCE 2014), pp. 559-564.

[4] Sharma, S. B., & Chauhan, N. (2015, February). Security issues and their solutions in MANET. In international conference on futuristic trends on computational analysis and knowledge management (ABLAZE), pp. 289-294.

[5] Gupta, K., & Mittal, P. K. (2017). An overview of security in MANET. International Journals of Advanced Research in Computer Science and Software Engineering ISSN, 7, 2277-3128.

[6] Roy, D. B., & Chaki, R. (2011). MADSN: mobile agent based detection of selfish node in MANET. International Journal of Wireless & Mobile Networks (IJWMN) Vol, 3, 225-235.

[7] Padiya, S. A. G. A. R., Pandit, R., & Patel, S. (2013). Survey of innovated techniques to detect selfish nodes in MANET. IJCNWMC, 3(1), 221-230.

[8] Mittal, S., & Dahiya, S. (2015). Identification technique for all passive selfish node attacks in a mobile network. International Journal, 3(4).

[9] Ramya, N., & Rathi, S. (2016, January). Detection of selfish Nodes in MANET-a survey. In 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), Vol. 1, pp. 1-6.

[10] Janakiraman, S., Priya, M., & Jebamalar, A. C. (2021). Integrated context-based mitigation framework for enforcing security against rendezvous point attack in MANETs. Wireless Personal Communications, 119(3), 2147-2163.

[11] Ghonge, M. M., Jawandhiya, P. M., & Thakare, V. M. (2017, March). Selfish attack detection in mobile Ad hoc networks. In IEEE International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1-4.

[12] Janakiraman, S., Deva Priya, M., Aishwaryalakshmi, G., Suganya, T., Sam Peter, S., Karthick, S., & Christy Jeba Malar, A. (2022). Improved Rider Optimization Algorithm-Based Link Aware Fault Detection (IROA-LAFD) Scheme for Securing Mobile Ad Hoc Networks (MANETs). In 3rd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing, pp. 155-169, Springer, Cham.

[13] Arboit, G., Crépeau, C., Davis, C. R., & Maheswaran, M. (2008). A localized certificate revocation scheme for mobile ad hoc networks. Ad hoc networks, 6(1), 17-31.

[14] Li, W., Parker, J., & Joshi, A. (2012). Security through collaboration and trust in MANETs. Mobile Networks and Applications, 17(3), 342-352.

[15] Eissa, T., Abdul Razak, S., Khokhar, R. H., & Samian, N. (2013). Trust-based routing mechanism in MANET: Design and implementation. Mobile Networks and Applications, 18(5), 666-677.

[16] Wei, L., Nishiyama, H., Ansari, N., Jie, Y., & Kato, N. (2013). Cluster-based certificate revocation with vindication capability for mobile ad hoc networks. IEEE Transactions on Parallel and Distributed Systems, 24, 239-249.

[17] Adnane, A., Bidan, C., & de Sousa Júnior, R. T. (2013). Trust-based security for the OLSR routing protocol. Computer Communications, 36(10-11), 1159-1171.

[18] Shurman, M., Alfawares, M., Al-Mistarihi, M. F., & Darabkh, K. A. (2014, February). A collaborative reputation approach to avoid misbehaving nodes in MANETs. In 11th IEEE International Multi-Conference on Systems, Signals & Devices (SSD14), pp. 1-4.

[19] Chatterjee, P., Ghosh, U., Sengupta, I., & Ghosh, S. K. (2014). A trust enhanced secure clustering framework for wireless ad hoc networks. Wireless networks, 20(7), 1669-1684.

[20] Abdel-Halim, I. T., Fahmy, H. M. A., & Bahaa-Eldin, A. M. (2015). Agent-based trusted on-demand routing protocol for mobile ad-hoc networks. Wireless Networks, 21(2), 467-483.

[21] Ullah, Z., Khan, M. S., Ahmed, I., Javaid, N., & Khan, M. I. (2016, March). Fuzzy-based trust model for detection of selfish nodes in MANETs. In 30th IEEE international conference on advanced information networking and applications (AINA), pp. 965-972.

[22] Sengathir, J., &Manoharan, R. (2017). Co-operation enforcing reputation-based detection techniques and frameworks for handling selfish node behaviour in MANETs: A review. Wireless Personal Communications, 97(3), 3427-3447.

[23] Kumar, S., & Dutta, K. (2018). Trust based intrusion detection technique to detect selfish nodes in mobile ad hoc networks. Wireless Personal Communications, 101(4), 2029-2052.

[24] Rama Abirami, K., &Sumithra, M. G. (2019). Evaluation of neighbor credit value based AODV routing algorithms for selfish node behavior detection. Cluster Computing, 22(6), 13307-13316.

[25] Abdelhaq, M., Alsaqour, R., Albrahim, N., Alshehri, M., Alshehri, M., Alserayee, S., ...&Alnajjar, F. (2020). The impact of selfishness attack on mobile ad hoc network. International Journal of Communication Networks and Information Security, 12(1), 42-46.

[26] Deva Priya, M., Christy Jeba Malar, A., Sengathir, J., & Akash, T. (2021). A Skellam Distribution Inspired Trust Factor-Based Selfish Node Detection Technique in MANETs. In Proceedings of 6th International Conference on Recent Trends in Computing, pp. 357-368, Springer, Singapore.

[27] Jim, L. E., Islam, N., & Gregory, M. A. (2022). Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes. Computers & Security, 113, 102538.