Wireless Personal Communications (2022) 122:1267–1281
https://doi.org/10.1007/s11277-021-08948-5

Energy and Trust Management Framework for MANET using Clustering Algorithm

C. Gopala Krishnan[1] · A. H. Nishan[2] · S. Gomathi[2] · G. Aravind Swaminathan[2]

Accepted: 9 August 2021 / Published online: 21 August 2021

Abstract

In General, Mobile Ad-Hoc Network (MANET) has limited energy resources, and it cannot recharge itself. This research goal focuses on building a power management scheme that saves energy in the MANET. Due to power instability, there is a chance that cluster heads fail and function incorrectly in cluster-based routing. As a result, instability occurs with the cluster heads while collecting data and communicating with others effectively. This work focuses on detecting the unstable cluster heads, which are replaced by other nodes implementing the envisaged self-configurable cluster mechanism. A self-configurable cluster mechanism with a k-means protocol approach is proposed to designate cluster heads effectively. The proposed k-means procedure is based on periodic irregular cluster head rotations or altering the number of clusters. We also propose a trust management mechanism in this research to detect and avoid MANET vulnerabilities. Because of the continuously changing topology and limited resources (power, bandwidth, computing), the trust management algorithm should only use local data. Consequently, compared to traditional protocols, the proposed approach with the k-means procedure and its experimental results show lower power usage and provide an optimal system for trust management.

Keywords MANET · Energy efficiency · Trust framework · k-means clustering

✉ C. Gopala Krishnan
gchandra@gitam.edu

A. H. Nishan
caaju196@gmail.com

S. Gomathi
gomathyrajah@gmail.com

G. Aravind Swaminathan
aravindcse2010@gmail.com

[1] Department of CSE, GITAM School of Technology, GITAM University, Bengaluru, India

[2] Department of CSE, Francis Xavier Engineering College, Tamilnadu, India

1 Introduction

Mobile ad hoc networks are devices that communicate through access points to the network and the base station. The complicated field of MANET embraces power and trustworthiness compared to other networks. The energy constraint of the nodes reduces the packet delivery ratio to the destination. For applications such as battlefields and emergencies, power resources are most important. The efficient use of energy resources is critical in any network since changing or recharging batteries is time-consuming [1].

The clustering process used sensors with comparable capabilities and strengths to construct clusters. Additionally, one of the nodes with better qualities selected as the cluster head, with the other nodes referred to as members. The elected leader is responsible for storing all information to be delivered and routing it to the appropriate destination. In MANETs, the optimization of energy utilization depends on the existence of the wireless nodes. Therefore, transmitting power, receiving power, residual power, and the energy consumption is managed to better energy utilization.

Typically, the MANETs are dependent on wireless communication techniques, in which secure data transfer technique plays an important role to protect the secrecy of data. Furthermore, as no central or administration node exists in MANETs, it is more important to secure the data packets secure transmission in ad hoc networks to detect or prevent security vulnerabilities and breaches or inconsistencies. Further, the literature exhibit that procedures are adequate to protect the network. However, when they are collectively layered, they are beneficial for secure routing in the network.

The clustering method proposed to utilize bandwidth and power in temporary mobile networks to overcome these limitations. Based on existing studies, it is clear that the clustering methods are suitable to solve these problems. The cluster heads can manage the entire network effectively and use intrusion detection on MANETs. Cluster approaches on the MANET divide the total nodes into smaller synchronous groups (cluster). A node acts as an organizer for controlling others in a cluster head (CH) in each group. It is not easy to maintain the members (the nodes) of clusters because of the node mobility in MANETs.

In MANET, when ineffective cluster heads are elected, they may act incorrectly due to power instability. It makes the routing failure because the elected cluster heads cannot control its member nodes and transmit their information. Thus, it affects the routing process and other network operations of the MANET. Contributions and novelty of the work are as follows:

- In the proposed research, energy management is achieved through a self-configurable cluster method with the k-means protocol.
- For identifying the unstable cluster heads in MANETs, a self-configurable cluster method was developed with the k-means protocol and cluster heads elected and designated effectively.
- A self-configurable cluster method with the k-means protocol will replace the incapable nodes with high configuration nodes.
- Trust management systems for successful packet delivery among MANET nodes are achieved through the proposed trust management algorithm.
- The proposed research work also reduces the transmission failures by detecting cluster head failure earlier.

The above section presents the challenging fields of MANET, such as power management, trust management, contemporary techniques to cope with the limitations of MANET, and the novelty of the work. Section 2 reviews previous studies of various authors. Sections 3 and 4 explain the proposed system, the trust management framework, and algorithm, k-means protocol to reduce energy consumption in MANETs. Section 5 deals with the evaluation part of the proposed work, outcomes, and comparisons discussed. Finally, Sect. 6 provides the conclusion of the research work presented.

2 Related Works

An energy-efficient routing in MANET requires MANET nodes should have an auto-organizing ability with dynamic architecture. For providing secure routing across MANET nodes, trust is necessary. The sender and recipient node's connection is characterized as trust. MANET nodes basic trust features include dynamicity, non-transitivity, asymmetric subjectivity, and context-dependency. Maintaining a high degree of trust across nodes requires trust management. The data was transmitted without any data loss if the trustworthy nodes are used.

In MANETs, the data packets are routed between sources and destinations via intermediate nodes. As a result, intermediary nodes must ensure trust. The nodes must authenticate each other before exchanging data between them. Calculating the path with the highest trust value yields the trust value. It's the recently discovered data transfer route. The routing decision is the foundation of the trust model. [2, 3].

Due to the complexity of MANETs, many techniques for energy management have limits. Easy routing, authentication, obtaining the right of the entrance to control, intrusion detection, and key management are some of the trust management approaches established for specific objectives [4]. In MANET, few authors concentrated on topics such as cooperative approaches. Collisions, limited transmission power, and node partial dropping are problems with current approaches. The methods were defined, mainly in terms of their design or model [5–8].

Muthu Raj Kumar et al. introduced a unique and safest routing mechanism called Cluster-based Energy Efficient Secure Routing Algorithm to develop a secure and energy-efficient routing algorithm, utilizing intelligent agents to make appropriate routing decisions. The routing algorithm substantially reduces service rejections. According to trials done using the trust-based secure routing mechanism, the proposed routing protocol enhances security to reduce energy consumption and routing delays [9].

Y. Hamzaoui et al. proposed an OLSR routing protocol using k-means clustering in MANETs. The author discussed QoS progress on MANETs and presented a clustering technique based on the new movement measure and the k-means approach to distributing nodes among various clusters [10].

Suyambu Karthick et al. introduced a new secure and energy-efficient routing protocol for WSN. The Trust-Distrust Protocol (TDP) routing is completed in four phases according to the suggested protocol. The most secure routing path is established in the last stage based on the quality criteria. NS2 is used to test the proposed protocol on one of the most critical types of SONs (Self-Organizing Networks), such as the WSN. Finally, the protocol suggests looping in SON, which overrides the efficacy of the present routing protocol [11].

Rao et al. proposed a hierarchical KF-MAC routing protocol for determining the energy efficiency standard and quality of services on MANETs in work. The newly introduced

KF-MAC (k-means cluster generation refers to MAC routing based on Firefly cluster head selection) minimizes the deliberation of Quality of Service elements while transmitting data from a source to a destination. In the beginning, the network is clustered into nodes using the k-means clustering approach. Then, to discover cluster heads, the Firefly Optimization Technique is used to classify and up-gradation of clustered nodes. At last, the data is transmitted within the network nodes through the TDMA- MAC routing protocol. The KF-MAC algorithm works on Quality of Service parameters like bandwidth, latency, error rate, and jitter. Furthermore, the KF-MAC method allows for conflict-free data transfer while minimizing energy consumption [12].

Maitreyi Ponguwala et al. discussed the unsupervised machine learning method. At first, the Secure Certificate-based Group Formation (SCGF) method used to construct the entire network. Then, using the recommendation filtering by the k-means method, the dependability of each group is calculated. HMAC-AES technique combines hash and cryptography capabilities. In a network simulator-3 environment, the proposed methodology achieves optimum results in terms of pocket distribution rate (96.3 percent), performance (135 kbps), latency (3.26 m), detection rate (99 percent), and power consumption (8.5 percent). Methods such as team development and trust screening help to protect the MANET-IoT network. The cryptographic function also assures data security, while the hash function maintains data integrity [13].

In wireless sensor networks, security vulnerabilities are a massive issue in data finding and dissemination. These weaknesses allow a rival to insert erroneous values into a system, remove incorrect variables, or execute DoS attacks [14, 15]. In addition, WSNs can be used to track and manage environmental factors.

The author has developed a distance-vector technique that can be implemented on computers with suitable configurations. The Direct Sequence Distance Vector (DSDV), which includes nodes, may consist of the critical paths for limited communication. It reduces memory requirements, eliminates unnecessary duplications, responds quickly to network connection failures, preserves static routes [16].

Sirisala S et al. proposed characteristics like energy, bandwidth, topological changes, continuous movement, processing power, transmission time, and channel state to evaluate trustworthiness [17]. In MANETs, trust helps nodes to deal with unpredictability and malicious nodes. However, trust calculations and management are problematic in MANET due to computing complexity limitations and many independent nodes. As a result, the data quality and reliability are impacted by such untrustworthy nodes [18].

The quality of service metrics of each multimedia stream, such as latency, bandwidth, jitter, and packet loss, was investigated as a source for the construction of sensor clusters and a link between Quality of Service for each multimedia stream in wireless sensor networks. According to the testing findings, the technique performed better in various video and audio circumstances [19].

Jose M. et al. presented energy usage in antennas during transmission from public wireless networks. Based on their findings, a new Open flow protocol extension for Software-Defined Networking networks was designed to govern the system and enhance network performance while consuming the least amount of power [20].

3 Trust Management Framework

The proposed trust management framework has three major components: gathering the information, calculating the trust level, and trust-based setup. It interacts through each node to generate trustworthy network relationships. After that, the packets are sent to the source, and the reply begins using suggestions from network clients or nodes. The neighbors of a node monitor and log all of its activity. Neighboring nodes are requested to provide their perspectives. A node is regarded as malicious if it does not reply after gathering all associate assessments. As a result, the proposed method might be precious in creating a secure wireless connection.

To identify a malicious node in this system, the CH uses a direct and indirect observer approach to send an inquiring message to the node (Fig. 1). The viewer node receives indirect observation from the nodes around it. By integrating several trust models, we can get appropriate trust values, resulting in the efficiency of the proposed methodology.

3.1 Path Discovery and Route Manager

Every route controls the routing manager in a network, tracking the route by the list, table, and path unit (Fig. 2). The path discovery method is used for determining the shortest path and the shortest path discovered by sending a route request packet to every node in the network. The routing database was updated to incorporate routes, which was commonly called pathfinding.

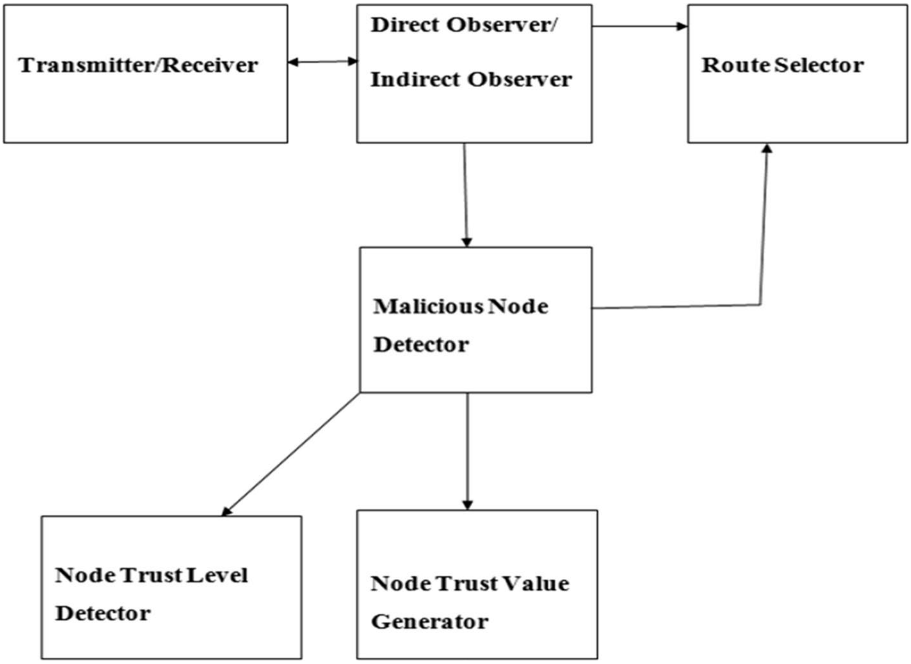


Fig. 1 Trust management framework

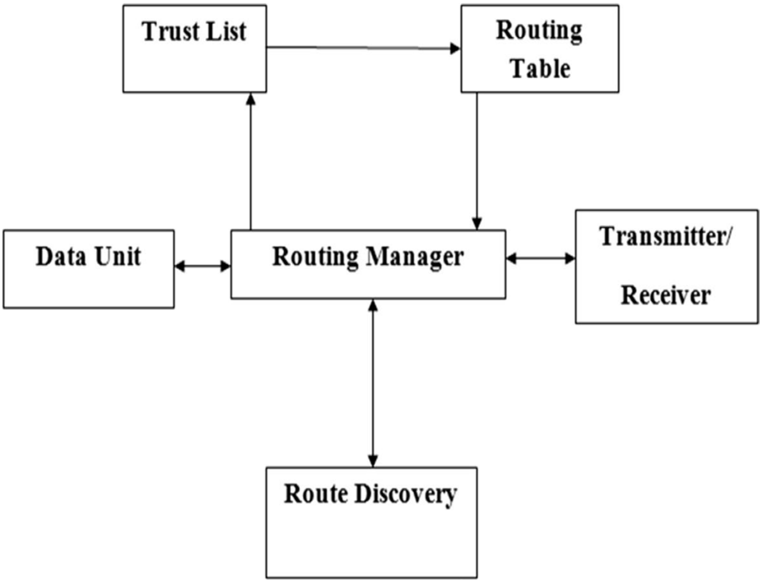


Fig. 2 Route discovery

3.2 Energy Management Through k-means Protocol

This research identifies the unstable cluster heads in MANETs through a self-configurable cluster method developed with the k-means protocol. Our approach assesses each cluster node and broadcasts the popularity levels of other CH candidates based on their activities. After that, every node collects the reputation values of all CH candidates. Cluster head arrangement is also made to accomplish speed in data transfer in groups and speed allocation in subgroups, with the possibility of selecting a leader at the end. Thus, cluster heads are selected and designated effectively through the proposed approach. When Cluster Head is not chosen in few rounds, the k-means protocol consumes substantial energy. By using a self-configurable cluster method with the k-means protocol, it can be avoided. The various steps involved in eliminating the hacker node during secure cluster head selection are shown in Fig. 3.

4 Trust Calculation Through Trust Management Algorithm

In general, wireless networks are most vulnerable to attacks. Therefore, mobile ad hoc networks require trust management and authentication system for successful packet delivery among MANET nodes. The two primary security challenges that emerge while obtaining security statistics are confidentiality and data integrity. Confidentiality confirms that the data was secure and not anywhere else, and Data Integrity ensures that the sent message has not made any changes while transmitting. The Trust Management algorithm is proposed to detect and prevent vulnerabilities in MANET. The normalized

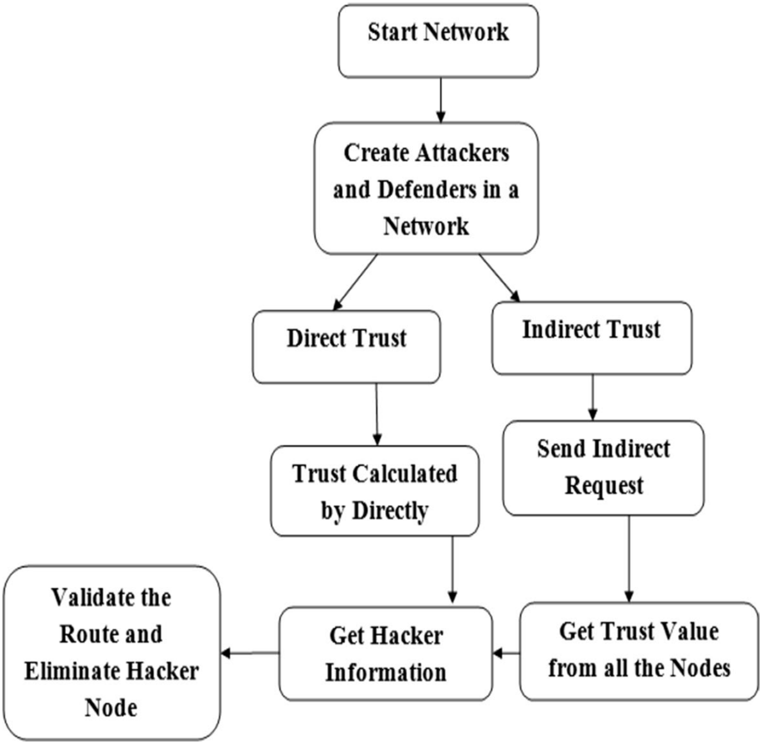

Start Network
Create Attackers and Defenders in a Network
Direct Trust
Indirect Trust
Trust Calculated by Directly
Send Indirect Request
Validate the Route and Eliminate Hacker Node
Get Hacker Information
Get Trust Value from all the Nodes

Fig. 3 Elimination of hackers node

local trust value in the algorithm makes the CH (Cluster Head) decide whether the node is a trusted or malicious node. If the node is malicious, then discard it through the trust management system. The following algorithm describes the calculation of the normalized local trust value.

Algorithm 1: (Normalized local trust value calculation)

$\mathbf{S_{x,\,y}}$ stands for the sum of ratings of individual transactions

N x, y Normalized local trust value

$\mathbf{L_x}$ stands for Local Trust value

ST (x, y) stands for Satisfactory Transactions

US (x, y) stands for Unsatisfactory Transactions

Start

Allocate parameters for Local trust value, Satisfactory Transactions, and Unsatisfactory Transactions.

Let,

For calculating $\mathbf{S}_{\mathbf{x,\,y}}$ by Eq. 1, calculate the $\mathbf{L_x}$ between the node **x, y**

Node **x** receives a data packet from node **y**. If the received data packet is good, then the $\mathbf{L_x}$ is **1,** and if the received data packet contains any harmful data, then its $\mathbf{L_x}$ value is **0**.

$$S_{x,y} = \sum L(x, y) \tag{1}$$

By Eq. 2,

$$S_{x,y} = ST(x, y) - US(x, y) \tag{2}$$

Normalize the local trust value,

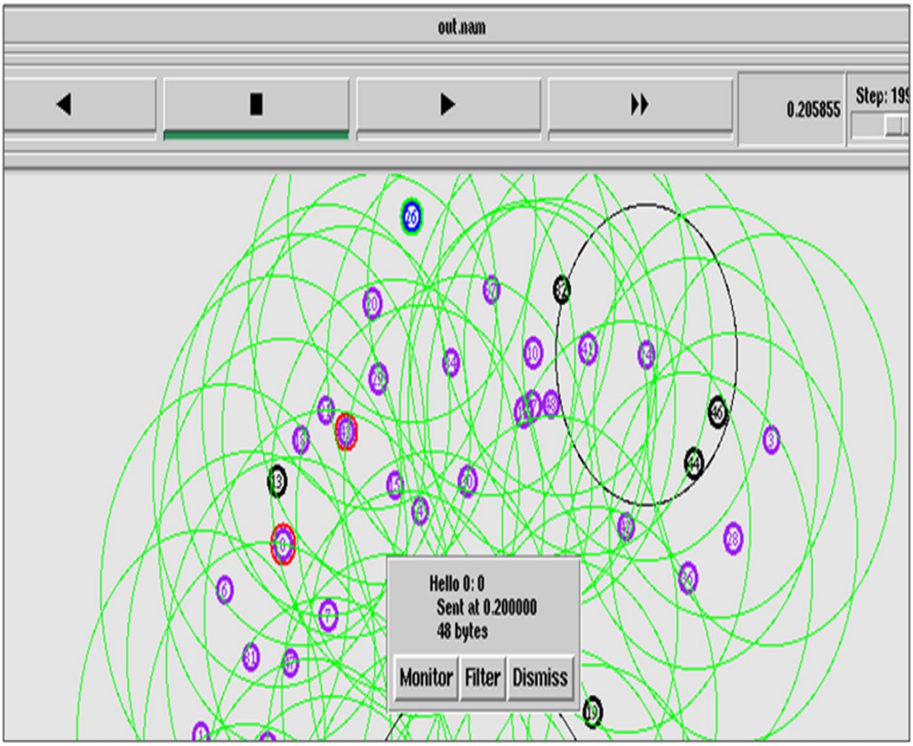
$$N_{x,y} = \frac{\max(S_{x,y}, 0)}{\sum S_{x,y}, 0} \tag{3}$$

End

In the given algorithm $S_{x,\ y}$ is the sum of the ratings of individual transactions (Satisfactory Transactions and Unsatisfactory Transactions), calculates the reputation index. S $_{x,\ y}$ was calculated either by Eq. 1 or by Eq. 2. Normalized local trust value (N x, y) is calculated by Eq. 3. This normalized local trust value and trust management framework is used to detect vulnerabilities in MANET and solve it by taking necessary actions (e.g., if the node is malicious, discard the node from the network). Thus, the proposed algorithm efficiently supports with trust management framework and provides secure communication in MANETs.

5 Results

Network simulators and NS2 gained popularity due to their recommended multipath routing protocols, cluster-based algorithms, and other features. In this research network simulator, NS2 is used to replicate the specified procedures, and Fig. 4 shows that each node



out.nam

0.205855

Step: 19

Hello 0: 0
Sent at 0.200000
48 bytes

Fig. 4 Hello messages between nodes

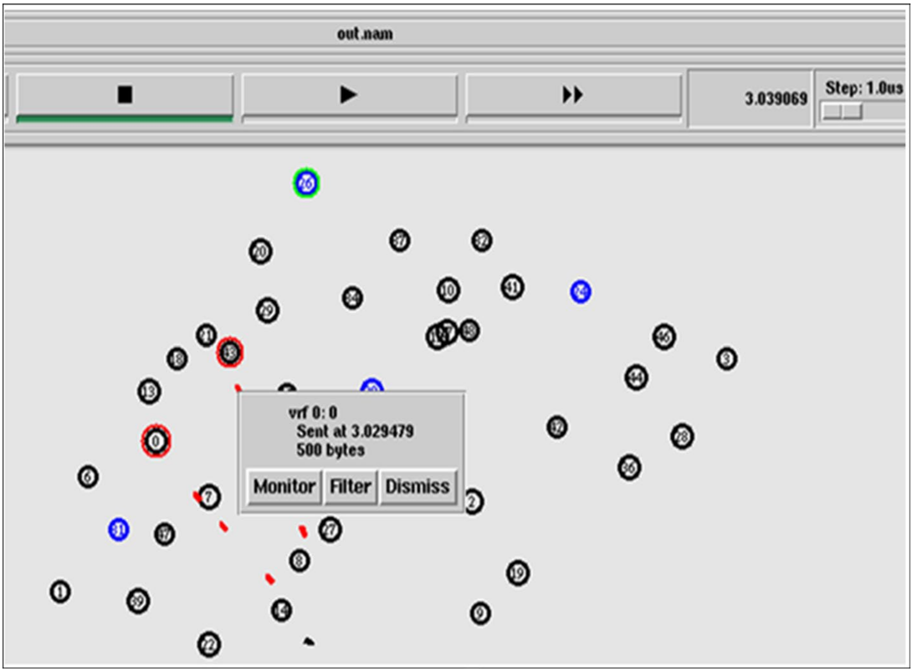
sends a single cluster head a greeting message. Other nodes are used to acquire the message from their neighbors. When every node receives the hello message in the vicinity, it enables an acknowledgment sent to each node based on its energy level.

In cluster construction, each node group is built and arranged as shown in (Fig. 5). Cluster formation is completed by communicating with other nodes, and it reduces the pace of transmission, separates groups into subgroups, and eventually selects a leader. Thus, clusters are formed, depend on the communicating range of nodes within the network.

The volume of data is combined into one or more aggregated outputs per minute using network aggregation. Then, it is used to go over the data verification message sent to BS and choose the most secure path (Fig. 6). As a result, the cluster head might be able to find out a secure path.

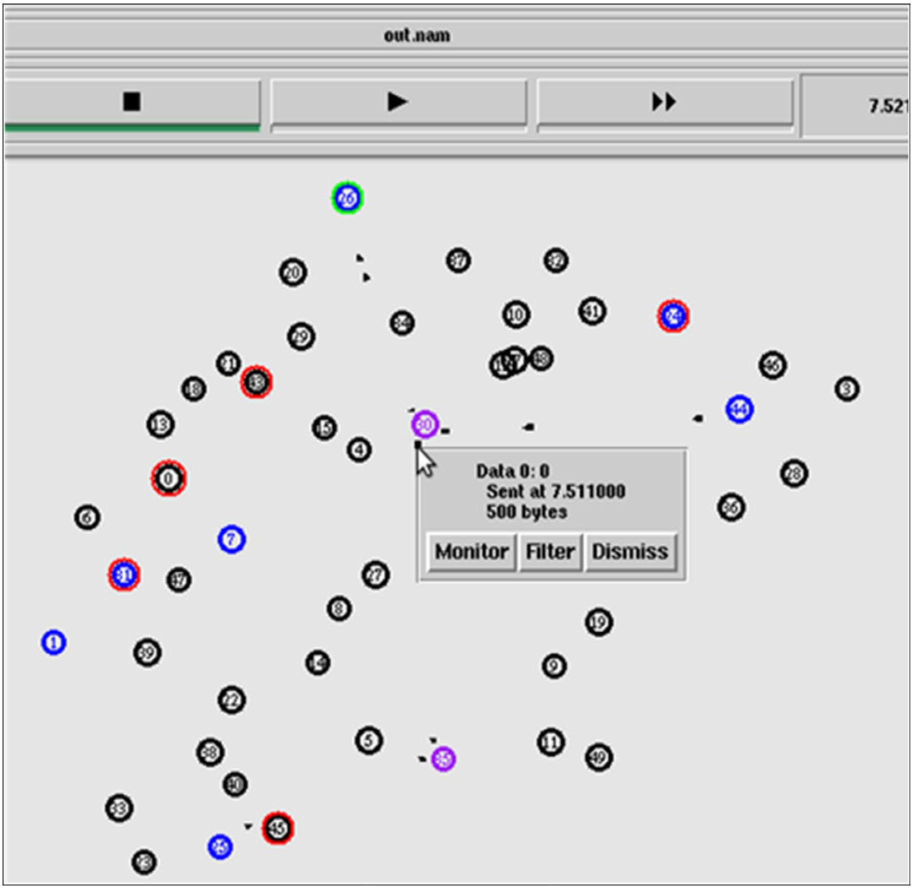
Packet Delivery Ratio: As represented in Fig. 7, the proposed approach with TSQRS (Trust-based Secure QoS Routing Scheme) protocol has the highest PDR than traditional AODV(Ad Hoc On-Demand Distance Vector) and ETRS (Enhanced trusted routing scheme)protocols. When the number of malicious nodes increases to 20, there is a significantly reduced packet delivery as 45% and 25% for AODV and ETRS protocol. In contrast, the proposed TSQRS routing protocol has 80–85 percent PDR. AODV falls to more percent of reduced PDR when the percentage of hazardous components increases. Hence, the packet delivery ratio of the proposed TSQRS routing protocol improved by 10 – 30% of PDR than the ETRS and AODV protocol.

Routing Overhead: The routing overhead of the proposed approach with the TSQRS routing protocol compared with the ETRS and AODV routing protocol, as shown in Fig. 8. we can see that the TSQRS has the lowest routing overhead at 4.96 percentage than the other existing routing approaches. When the number of malicious nodes in the network increases



vrf 0: 0
Sent at 3.029479
500 bytes

Fig. 5 Communication between nodes



Data 0: 0
Sent at 7.511000
500 bytes

Fig. 6 Find a secure path

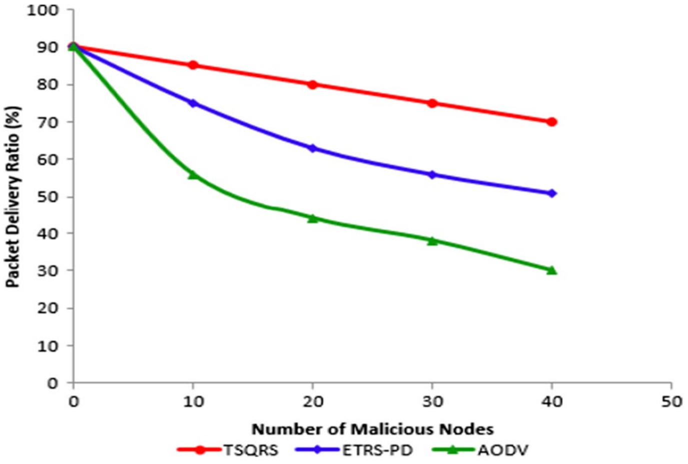


Fig. 7 PDR versus Malicious nodes

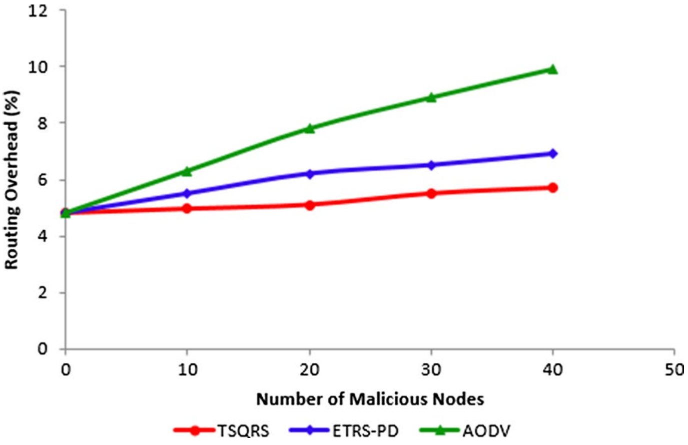


Fig. 8 Routing overhead

to 30, the routing overhead for the TSQRS routing protocol is 5.5%. On the other side, the ETRS protocol and AODV protocol routing overhead raise by a ratio between 6.5 and 9. The TSQRS routing protocol reduces routing overhead by 2–5% than ETRS and AODV protocol.

Energy Consumption: From Fig. 9, the number of malicious nodes increases the energy consumption also increases gradually. For instance, when the number of malicious nodes is 30, the ETRS consumes 313 J of energy, and AODV consumes 314.25 J of energy. In contrast, the proposed approach with TSQRS consumes less energy consumption. Similarly, the proposed approach with TSQRS consumes as low as 311.11 J of energy, whereas ETRS consumes 313.13 J of the energy and AODV consumes 314.31 J of energy. The proposed approach with TSQRS routing methodology achieves 3–5 percentage of reduced energy consumption than other approaches. As a result, the proposed techniques minimize wireless node energy consumption even with a higher number of malicious nodes in the network.

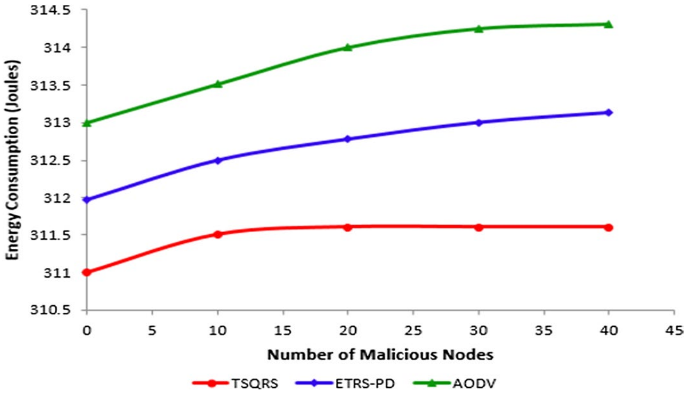


Fig. 9 Energy consumption

6 Conclusion

The complex field of MANET holds power and trustworthiness compared to other networks. The energy constraint of the nodes reduces the packet delivery ratio to the destination. This work focuses on building a power management scheme that saves energy in the MANET. Due to power instability, there is a chance that cluster heads fail and function incorrectly in cluster-based routing. As a result, instability occurs with the cluster heads while collecting data and communicating with others. This work presented about detecting the unstable cluster heads, which were replaced by other nodes implementing the envisaged self-configurable cluster mechanism. So, the self-configurable cluster mechanism with the k-means protocol approach was proposed to designate cluster heads effectively, and the Trust Management algorithm was also presented to detect and prevent vulnerabilities in MANET. Network simulator was used for its recommended multipath routing protocols, cluster-based algorithms, and other features. Finally, the proposed algorithm tested in a network simulator, and the results were observed accordingly. The experimental results showed that the proposed approach works well to minimize the energy and provide trust in MANET communication compared to other techniques. In future research, trust management can build by framing the different algorithm to overcome the real-time challenges by ensuring reputation and trustworthiness in Mobile Ad hoc Networks.

Author's Contributions **C.G:** contributed to the novelty of work, drafting of the manuscript, and analyzing the results of the study; **H.N:** contributed to the related works, comparisons of existing work, and development of trust management algorithm; **S.G:** contributed to the concepts related to energy efficiency through k-means protocol; **G.A:** contributed concepts of trust calculation through trust management algorithm.

Funding No funding received for the research presented.

Data Availability The authors confirm that the data supporting the findings of this research are available within the article.

Code Availability The coding part, algorithm code, and simulation model of the proposed research are presented within the article.

Declarations

Conflict of interest There is no conflict of interest between the authors regarding the manuscript preparation and submission.

References

1. Theerthagiri, P. (2019). "COFEE: Context-aware futuristic energy estimation model for sensor nodes using Markov model and auto-regression. *International Journal of Communication System*. https://doi.org/10.1002/dac.4248
2. He, D., Chan, S., Tang, S., & Guizani, M. (2013). Secure data discovery and dissemination based on hash tree for wireless sensor networks. *IEEE Transactions on Wireless Communications, 12*(9), 4638–4646. https://doi.org/10.1109/TWC.2013.090413.130072
3. He, D., Chen, C., Chan, S., & Bu, J. (2012). DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks. *IEEE Transactions on Wireless Communications, 11*(5), 1946–1956. https://doi.org/10.1109/TWC.2012.030812.111857
4. Zhang, D., Gao, J., & Liu, X. (2019). Novel approach of distributed & adaptive trust metrics for MANET. *Wireless Network, 25*, 3587–3603. https://doi.org/10.1007/s11276-019-01955-2

5. Vaseer, G., Ghai, G., & Patheja, P. S. (2017). A novel intrusion detection algorithm: An AODV routing protocol case study. In 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Bhopal (pp. 111–116). https://doi.org/10.1109/iNIS.2017.32
6. Lwin, M., Yim, J., & Ko, Y.-B. (2020). Blockchain-based lightweight trust management in mobile Ad-Hoc networks. *Sensors, 20*, 698. https://doi.org/10.3390/s20030698
7. Diaz, J. R., Lloret, J., Jimenez, J. M., & Rodrigues, J. J. P. C. (2014). A QoS-based wireless multimedia sensor cluster protocol. *International Journal of Distributed Sensor Networks, 10*(5), 480372. https://doi.org/10.1155/2014/480372
8. Govindan, K., & Mohapatra, P. (2012) Trust computations and trust dynamics in mobile Adhoc networks: A survey. *IEEE Communications Surveys & Tutorials*, *14*(2), 279–298. https://doi.org/10.1109/SURV.2011.042711.00083
9. Muthurajkumar, S., Ganapathy, S., Vijayalakshmi, M., et al. (2017). An intelligent secured and energy efficient routing algorithm for MANETs. *Wireless PersCommun, 96*, 1753–1769. https://doi.org/10.1007/s11277-017-4266-4
10. Hamzaoui, Y., Amnai, M., Choukri, A., & Fakhri, Y. (2020). Enhancenig OLSR routing protocol using K-means clustering in MANETs. *International Journal of Electrical and Computer Engineering (IJECE), 10*(4), 3715–3724. https://doi.org/10.11591/ijece.v10i4.pp3715-3724
11. Karthick, S. (2018). TDP: A novel secure and energy aware routing protocol for wireless sensor networks. *International Journal of Intelligent Engineering and Systems*. https://doi.org/10.22266/ijies2018.0430.09
12. Rao, M., & Singh, N. (2018). Energy efficient QoS aware hierarchical KF-MAC routing protocol in manet. *Wireless PersCommunications, 101*, 635–648. https://doi.org/10.1007/s11277-018-5708-3
13. Ponguwala, M., Sreenivasa Rao, D. R. (2019). Secure group based routing and flawless trust formulation in MANET using unsupervised machine learning approach for IoT applications. *EW EAI*. https://doi.org/10.4108/eai.13-7-2018.160834
14. Gomathi, S., & Gopala Krishnan, C. (2020). Malicious node detection in wireless sensor networks using an efficient secure data aggregation protocol. *Wireless PersCommunications*. https://doi.org/10.1007/s11277-020-07291-5
15. Ahmed, A., Abu Bakar, K., Channa, M. I., & Ahmed, A. (2014). A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. *Frontiers of Computer Science, 9*, 280–296. https://doi.org/10.1007/s11704-014-4212-5
16. Ahmed, M. N., Abdullah, A. H., Chizari, H., & Kaiwartya, O. (2017). F3TM: Flooding factor based trust management framework for secure data transmission in MANETs. *Journal of King Saud University-Computer and Information Sciences, 29*(3), 269–280. https://doi.org/10.1016/j.jksuci.2016.03.004
17. Sirisala S., & Ramakrishna S. (2019) Survey: Enhanced trust management for improving QoS in MANETs. In: Advances in Intelligent Systems and Computing (vol. 815). Singapore: Springer. https://doi.org/10.1007/978-981-13-1580-0_25
18. Cho, J.-H., Swami, A., & Chen, I.-R. (2011). A survey on trust management for mobile Ad Hoc networks. *Communications Surveys & Tutorials, IEEE., 13*, 562–583. https://doi.org/10.1109/SURV.2011.092110.00088
19. Shabut, A. M., Dahal, K. P., Bista, S. K., & Awan, I. U. (2015). Recommendation based trust model with an effective defence scheme for MANETs. *IEEE Transactions on Mobile Computing, 14*(10), 2101–2115. https://doi.org/10.1109/TMC.2014.2374154
20. Jose, M. J., Oscar, R., Jaime, L., & Juan, R. D. (2019). Energy savings consumption on public wireless networks by SDN management. *Mobile Networks and Applications, 24*, 667–677. https://doi.org/10.1007/s11036-016-0784-7
21. Nagaraju, A., Kumar, G.C., & Ramachandram, S. (2011). Ad-Hoc on demand distance vector routing algorithm using neighbor matrix method in static Ad-Hoc networks. In *Communications in Computer and Information Science* (vol. 132). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-17878-85
22. Sethuraman, P., & Kannan, N. (2017). Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. *Wireless Network, 23*, 2227–2237. https://doi.org/10.1007/s11276-016-1284-1
23. Janani, V. S., & Manikandan, M. S. K. (2018). Efficient trust management with Bayesian- Evidence theorem to secure public key infrastructure-based mobile ad hoc networks. *Journal of Wireless Communications and Networking*. https://doi.org/10.1186/s13638-017-1001-5
24. Prasannavenkatesan, T., Raja, R., & Ganeshkumar, P. (2014). “PDA-misbehaving node detection & prevention for MANETs. In *IEEE International Conference Communication and Signal Processing* (pp. 1808–1812). https://doi.org/10.1109/iccsp.2014.6950037

25. Adnane, A., Bidan, C., & de Sousa Junior , R. (2013). Trust-based security for the OLSR routing protocol. *Computer Communications, 36*, 1159–1171. https://doi.org/10.1016/j.comcom.2013.04.003
26. Krishnan, C., Rengarajan, A., & Manikandan, R. (2015). Delay reduction by providing location based services using hybrid cache in peer to peer networks. *KSII Transactions on Internet and Information Systems, 9*(6), 2078–2094. https://doi.org/10.3837/tiis.2015.06.006
27. Krishnan, C. G., Sivakumar, K., & Manohar, E. (2018) An enhanced method to secure and energy effective data transfer in WSN using hierarchical and dynamic elliptic curve cryptosystem. In *IEEE International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1–7). https://doi.org/10.1109/ICSSIT.2018.8748785
28. Tong, F., Pan, J., & Zhang, R. (2016). Distance distributions in finite AdHoc networks: Approaches, applications, and directions. *Ad Hoc Networks*. https://doi.org/10.1007/978-3-319-51204-4_14
29. Apirajitha, P. S., Gopala Krishnan, C., AravindSwaminathan, G., & Manohar, E. (2019). Enhanced secure user data on cloud using cloud data centre computing and decoy technique. *International Journal of Innovative Technology and Exploring Engineering*. https://doi.org/10.35940/ijitee.I7777.078919.
30. Gopala Krishnan, C., Golden Julie, E., & Harold Robinson, Y. (2020). Predictive algorithm and criteria to perform big data analytics. In V. Balas, V. Solanki & R. Kumar (Eds.), *Internet of Things and Big Data Applications*. Intelligent Systems Reference Library (vol. 180). Cham: Springer. https://doi.org/10.1007/978-3-030-39119-5_16
31. Pandithurai, O., Poongodi, M., Kumar, S. P., & Krishnan, C. G. (2011). A method to support multitenant as a service. In *Third international conference on advanced computing* (pp. 157–162). https://doi.org/10.1109/ICoAC.2011.6165166
32. Velu, S.G., Gopala Krishnan, C., Sivakumar, K., & Jevin, J.A. (2020). Proof of shared ownerships and construct a collaborative cloud application. In: S. Balaji, A. Rocha, & Y. N. Chung (Eds.), *Intelligent Communication Technologies and Virtual Mobile Networks. ICICV 2019. Lecture Notes on Data Engineering and Communications Technologies* (vol. 33). Cham: Springer. https://doi.org/10.1007/978-3-030-28364-3_51.
33. Prasannavenkatesan, T., & Menakadevi, T. (2020). Resource-based routing protocol for mobile Adhoc networks. *Songklanakarin Journal of Science and Technology, 42*(4), 889–896.
34. Raj, J. S. (2020). Machine learning based resourceful clustering with load optimization for wireless sensor networks. *Journal of Ubiquitous Computing and Communication Technologies (UCCT), 2*(01), 29–38.

Dr. C. Gopala Krishnan received his Ph.D. in Computer science and Engineering from St. Peter's Institute of Higher Education and Research, Chennai, India. He received his M.E. degree in Computer science and Engineering from Anna University Tirunelveli, India, and B.E. degree in Computer Science and Engineering from Madurai Kamaraj University, Madurai, India. He is currently working as Associate Professor in the Computer Science and Engineering Department at GITAM School of Technology, Bengaluru, India. His areas of interest are Mobile Computing, Operating systems, Computer Networks, Wireless Networks, Computer Graphics, Digital Principles, IOT and Cloud Computing. He has published many papers in International Conferences and International journals in various fields of advanced technologies. He is working on developing protocols for Internet of Things (IoT) where physical devices, sensors, appliances and other different objects can communicate with each other without the need for human intervention. He is a Life member of ISTE.

A. H. Nishan received her Bachelor's degree in Information Technology from Anna University, Chennai, Tamil Nadu, India. She completed her Master's Degree in Computer Science and Engineering from Anna University, Chennai, Tamil Nadu, India. Her areas of interest are Wireless Networks, Data Mining, Artificial Intelligence, Big Data, and Cloud Computing. She has published many papers in International Conferences and International journals in various fields of advanced technologies. She is working on developing software and protocols for Wireless Devices which can support file and database access. She is a member of ISTE.

S. Gomathi received her B.E from M.S. University and M.E. (CSE) degree from Anna University, Tamil Nadu. She received her Ph.D. from Anna University, Chennai. She is currently working as an Associate Professor in the Computer Science and Engineering Department at Francis Xavier Engineering College, Tirunelveli. Her research interests include wireless sensor networks, cloud computing, and big data. She has published many papers in International Conferences and journals in wireless networks and Cloud Computing.

Dr.G. Aravind Swaminathan received his B.E (Computer Science and Engineering) from Madurai Kamaraj University, India and the M.E (Computer Science and Engineering) from Anna University, Chennai, India. He has completed the Ph.D. (Information and Communication Engineering) Degree, Anna University, Chennai, India. He is currently working as a Professor in the Computer Science and Engineering Department at Francis Xavier Engineering College, Tirunelveli. He has published papers in many National and International Conferences and Journals. His major research interests are Networking,Web Technology and Software Engineering. He is a member of ISTE.