Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.029345
Article

Tech Science Press

Hybrid Trust Based Reputation Mechanism for Discovering Malevolent Node in MANET

S. Neelavathy Pari[1,*] and K. Sudharson[2]

[1]Department of Computer Technology, Anna University, Chennai, 600025, India
[2]Department of Information Technology, Velammal Insitutue of Technology, Chennai, 601204, India
*Corresponding Author: S. Neelavathy Pari. Email: neela@annauniv.edu
Received: 01 March 2022; Accepted: 07 April 2022

Abstract: A self-contained connection of wireless links that functions without any infrastructure is known as Mobile *Ad Hoc* Network (MANET). A MANET's nodes could engage actively and dynamically with one another. However, MANETs, from the other side, are exposed to severe potential threats that are difficult to counter with present security methods. As a result, several safe communication protocols designed to enhance the secure interaction among MANET nodes. In this research, we offer a reputed optimal routing value among network nodes, secure computations, and misbehavior detection predicated on node's trust levels with a Hybrid Trust based Reputation Mechanism (HTRM). In addition, the study designs a robust Public Key Infrastructure (PKI) system using the suggested trust evaluation method in terms of "key" generation, which is a crucial component of a PKI cryptosystem. We also concentrate on the solid node authenticating process that relies on pre-authentication. To ensure edge-to-edge security, we assess safe, trustworthy routes to secure computations and authenticate mobile nodes, incorporating uncertainty into the trust management solution. When compared to other protocols, our recommended approach performs better. Finally, we use simulations data and performance evaluation metrics to verify our suggested approach's validity Our approach outperformed the competing systems in terms of overall end-to-end delay, packet delivery ratio, performance, power consumption, and key-computing time by 3.47%, 3.152%, 2.169%, and 3.527%, 3.762%, significantly.

Keywords: Mobile ad-hoc network; trust management; secure authentication; reputation mechanism; secure routing

1 Introduction

Over several years, experts have detected and analyzed harmful attacks on various layers of the MANET. Numerous routing techniques evolved to protect MANET packet routing and send against malicious actions. Most traditional routing algorithms rely on a central PKI to identify and protect harmful behavior through tight security or cryptosystems. Moreover, these systems provide only limited security in the early phases of controlling mobile nodes, when a malicious mobile node can threaten the channel's reputation. Even though nodes firstly act as perfect nodes in secure group interaction, and so

fulfill the strict security requirements, nodes may be subject to behavior modifications caused by malicious parties in some instances. On the other hand, these unapproved nodes could become selfish or malignant, reporting misleading facts to jeopardize the trustworthiness of group communication. Conventional cryptographic systems are incapable of detecting and preventing these frequent changes in node behavior.

In other words, rigid security protocols cannot entirely ensure connection dependability, data quality, or access management. As a result, a protection system is necessary to protect against node behavior changes, often known as mild security risks, and preserve the integrity, durability, and access management of the MANET communication process. As a result, an efficient distributed and self-organizing system based on mutual trust designs to monitor and protect misbehavior in Manets. Although cryptographic approaches to counter potential attacks might well be efficient. However, they are not ideal for practical uses where temporal value is a significant challenge/constraint because data encryption and decryption take time, raising delay at every node. With this in perspective, we present a cryptographic technique with a randomized timestamp flavor that reduces the time associated with deciphering at every node without compromising security against an outside attack. Because of the seriousness of the problem, trust connects to a unified strategy that allows for its formulation and systemization, called Trust Administration. The trust control system provides a formal foundation for trust formulation and interpretations. Surprisingly, the effectiveness of a reputation method is contingent on node coordination.

A reputation-based approach may be a security issue because of its vulnerabilities to various attacks, in which multiple hostile nodes cooperate to disrupt the network's Quality of Service (QoS) or functionality [1–3]. Each node's trust calculates by any node's trustworthiness, faithfulness, and honesty with its neighbors. Without being an egoistic node, a trustworthy node continuously works truthfully and transmits accurate data to its peers to complete tasks. Trust may be measured, but that can be adjusted or modified based on the assessments made by its neighbors. As indicated in the diagram, a trusted network represents a range of interconnected nodes. Each node has its reputation tables that store the trust entries of all other neighboring nodes. The reputation table may include criteria such as the node's integrity, closeness with the nodes, truthfulness, energy required to the node, and operational priorities. This trust database is updated whenever new information about the trust of neighboring nodes becomes available [4,5].

We concentrate on route configuration when combining the MANET system with the internet. In our proposed method, hubs divide into two categories: secure hubs, which send both secure and standard data, and ordinary hubs, which send just data. After choosing a secure hub, all must choose a secure authenticated route from the mobile node to the security hub. It is chosen based on the most trustworthy optimal routing value. It is dependent on the node's threshold, the route's trust level, and the "key" authentication [6–9]. Our research makes a significant contribution by proposing an HTRM and authentication strategy for MANET. Secure data is transmitted using this strategy's secure hub and secure verified routing. This approach also describes how the authentication system authenticates mobile nodes before data transfer.

The following is how the article's content is structured: In Section 2, we explain the relevant research. In Section 3, we implement the research work with the suggested method, in Section 4, we illustrate the outcomes and performance of the HTRM framework, in Section 5, we show the effectiveness of the simulation study, and in Section 6, we finish up the research with possible improvements.

2 Related Works

There has been a great deal of research on security measures and their deployment in a PKI-based MANET safety system during the last few years. Most of these studies [10] concentrate on routing algorithms, network layers, and packet transmission techniques. However, for MANET-based detecting and scrutinizing systems, decentralized communication is imperative. Only when all nodes behave

righteously will the interaction be effective. Because of the restricted bandwidth, nodes must interact through numerous hops. As a result, each node's availability is highly vital. As a result, an effective forwarding method needs to determine the best route between the origins and the sink. Developing several routing schemes based on trust and explored when constructing a MANET. Most trustworthy development policies were designed for collaborative routing to detect attack nodes generated by faulty nodes. Researchers analyzed opinions and connections concerning wireless nodes, among other factors, when constructing safe and secure routing methods. Several anticipated path models are created and utilized to identify different forms of security breaks objectively. Some scholars explored the concerns around essential issues relating to IoT-based MANETs.

During the development of methods, many protection and vulnerabilities issues were examined [11]. There are three types of routing algorithms: reactive, proactive, and hybrid. Routes must be updated regularly for dynamic routing systems like the Destination Sequence Distance Vector (DSDV) [12]. As a result, it produces many control datagrams, and these methods have been inappropriate for MANETs. As a result, reactive frameworks allow, like dynamic source routing (DSR) [12] and ad hoc on-demand distance vector routing (AODV) [13]. Identifying a pathway between the origin and the sink creates a necessary one. Route discovery and maintenance are the two processes in such techniques. They are using a route-discovery mechanism to calculate routes and a source and destination using a route-maintenance step to examine any modifications in structure. Develop various cryptographic algorithms and procedures to secure communication across MANET nodes. For example, Intelligent Routing Mechanism [14], Effective Certificateless Secure Communication [15], Energy-Efficient Partial Permutation Encryption (EEPPM) [16], Secure optimized routing Protocol [17,18], Secure technique for network layer attack discovery and elimination [19,20], and Lightweight reputation-based approach [21] protocols. On the other hand, these approaches are vulnerable to various security concerns and require much power from the nodes.

Based on direct and indirect evidence evaluations and a degree of reputation, a trust-based approach for MANETs on the Internet-of-things [22] forecasts its last node score. The hybrid method, the cat slap single-player technique, was applied in [23] to construct a trust-based secure energy-efficient MANET movement (C-SSA). The MANET consensus mechanism proposes multiple trust predictions based on exchanging group proposals [24]. *Trust* is defined as an individual's level of trust in any participating node's behavior [25]. Reference [26] Distinguished trust maintenance from several security measures in offering and maintaining security measures and interactions. MANETs where node compromise and attacks are more likely to develop in unrestricted contexts with no centralized command and control authority. These distinct characteristics impose appropriate limits on nodes for secure transmission, particularly in the key management framework. Consequently, quantifying each user's behavior in such cooperative dialogues is essential. Do it by evaluating node behavior using reputation, with mobile nodes arranged into groups to provide efficiency and minimize chronic node failure throughout secure group interaction.

In MANET, trust management is used to evaluate information and node belief levels, detect malicious, capable of providing security services such as key management, verification, authentication protocols, and node forfeiture [27]. As a consequence, specific computational approaches for measuring confidence are used regularly. However, apart from a wired connection, a dynamic communication system like MANET can only compute trust based on periodic measurements. Furthermore, trust computation is challenging due to unpredictable mobile nodes and the lack of a centralized authority. The MANET survey of trust management [28–30] provides an overview of several trust computation strategies. Many following schemes to consider the neighbor's opinion and direct decision-making encounters benefited from the formalizing trust method [31]. Each node calculates trust using two approaches in [32], namely the reputation structure and trust concern. In a reputation system, direct surveillance and further carry out the delivery of information. In contrast, direct interpretation and opinions from one-hop neighbors

integrate to evaluate trust relationships in trust establishment. Reference [33–35] introduces the concept of mixed trust calculation, in which the calculation of direct trust using direct observations and calculation of indirect trust using recommendations. Reference [36] discusses misbehavior verification in trust computation for noncooperation. Estimating trust in an entirely distributed network is difficult [37,38].

A trust model with Bio-Inspired Gateway Selection Scheme presents updating the reputation from direct observations [39]. In a public-key communication infrastructure [40], several trust models are discussed. They build these authentication schemes on a mobile node network that prioritizes safety. On the other side, the present frameworks for assessing each node's trust level in MANET have increasing computational power challenges. Numerous safe and power-aware multihop routing procedures have recently been developed for MANETs, including Hybrid Secure Multipath Routing Protocol (HSMRP) [23], Trust Aware Secure Energy Efficient Hybrid Protocol (TASEEHP) [24], Recurrent Reward-Based Learning (RRBL) [25], and Signcryption Technique (ST) [26]. These practices are highly successful in facing a range of security threats. Even though these methods consume less power than traditional methods, there is always room for development.

3 Proposed Work

A mitigating attack paradigm secures the whole developed methodology, providing a protective mechanism against selfish and malevolent node activity. We model the greedy behavior as exploiting the vulnerability in a group interaction across network nodes. As a result, even though the nodes act irrationally, they work together to accomplish secret-key managerial functions. Each node's power level defines as its current state. A node's trustworthiness is determined using both direct and indirect evidence, with the indirect assessments coming from the targeted node's one-hop neighbors, known as recommenders. We choose the recommenders in our strategy depending on the level of trust. For hybrid reputation management, we examine two fundamental theories. First, the chance of choosing a reputable hybrid recommendation increases when direct observations invalidate the unreliable node. Second, choosing significantly greater recommender systems implies that those recommender nodes involve effective communication. Thus associated with the destination point, however, trustworthy recommendation systems are chosen randomly to prevent undiscovered breaches that could restrict endorsed interaction.

3.1 System Model

Fig. 1 depicts the suggested framework system architecture. Its design describes the conceptual reputation management, grouping, and steps involved in constructing a secure cryptography platform in MANET. Firstly, the reliability of MANET nodes is determined using, directly and indirectly, trusting approaches, namely the Bayes and Evidence theories, accordingly. After that, the hybrid trust ratings combine direct and indirect trustworthiness. We classify nodes as reliable or unreliable during this phase, with the reputable nodes being picked and passed to subsequent network functions. Next, we segregate the system's unreliable nodes f banned further. During the next step, aggregate all the reliable nodes into clusters, with the maximum trust value as a reputable node. Then, every time nodes enter or depart the MANET. Next, we perform the steps to optimize mobile node enrollment and departure. Finally, to protect the MANET system, the grouped trust architecture is used for cryptographic functionality.

3.2 Reputation Model

There is still the possibility of considering combined direct and indirect reputation by considering trust depending on a node's behavior. In direct trust, a node earns its reputation by behaving well with its closest neighbors; in indirect trust, the node's behavior is determined by nodes apart from its closest neighbors. It

would have accumulated reputable information by routing packets for those other nodes. The functioning of the nodes in the very same MANET zone is not only geographically but also temporally connected. In another sense, the activity of a node is related not just to its history but also activity of other nodes in the same zone. The frequency with which the node's behavioral changes has statistical properties that must be discovered and assessed. Due to this behavior, the direct and indirect trust value is acquired by nodes from the same area, minimizing data transfer among several network nodes.

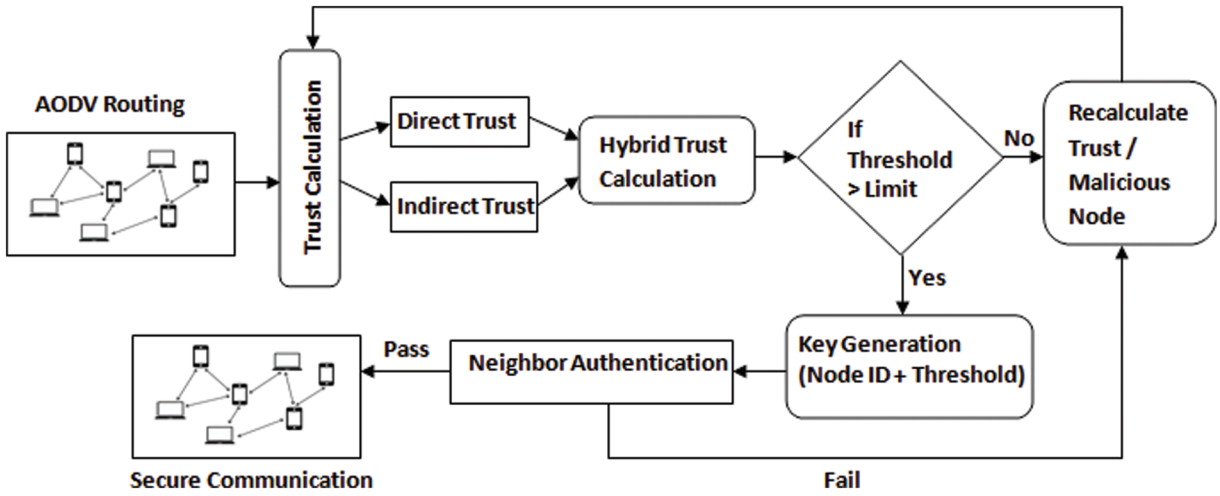

Figure 1: HTRM-system architecture

3.2.1 Trust Components

Capacity, honesty, and connectedness are the three aspects of trust that we examine. We derive connectedness characteristics from online communities while capturing capacity and honesty from wireless links. The three aspects of trust are:

1. Capacity (C): In terms of a node's team cohesion and accessibility, this relates to an object's capacity to fulfill incoming demands. Connectivity factors such as route failures, energy depletion, and deliberate or forced disconnect can affect accessibility. The proportion of positive comments to overall interactions calculates in routing packets.
2. Honesty (h): It refers to an object's truthfulness when it comes to network threat activities like fake identity distribution (e.g., compromising another node's secret key *via* an identity or Sybil attack), fraudulent referral, transaction manipulation, or forging. It is calculated by dividing positive interactions by the combined total of conversations connected to protocol conformance.
3. Connectedness (Cs): This is the set of nodes that a node interacts with over the total amount of nodes within the network throughout a trust refresh period T_{ref}. Unlike entities with weak Cs, those with strong Cs are more began to transmit data efficiently to the system. The mobility pattern of an object may impact the device's trustworthiness.

3.2.2 Trust Calculation

In this paper, we develop HTRM on top of a trust model wherein we investigated the best trust formation that optimizes trust precision (or reduces trust distortion) based on differences between accurate (measured data) and anticipated (projected) trust levels. As an actual figure, grading of trust value within 0 and 1. We use an aggregate of both direct and indirect findings to calculate the trustworthiness of each trust element. In the

trust component Tc, the trust of node b (trustee: trusted entity) is judged by node a (trustor: trusting entity) as follows.

Direct Trust:

Each node calculates direct trust using trust components and timestamp. The direct trust of node a in node b based on Tc at Timestamp (ts), $DT^{Tc}_{a,b}(ts)$, is calculate as:

$$DT^{Tc}_{a,b}(t_s) = \begin{cases} T^{Tc}_{a,b}(t_s) \; if \; Nd(a,b) == 1 \\ \lambda T^{Tc}_{a,b}(t_s - \triangle t_s) \quad otherwise \end{cases} \tag{1}$$

Node distances (Nd) is the distance between two nodes a and b. when both nodes successfully encounter one-hop neighbor at timestamp $(t_s - \triangle t_s)$, node a calculates the direct trust on node b based on its interpretation. When both nodes are separated with more than one hop distance, node "a" relies on its history of observation to recalculate the direct trust on node b.

Indirect Trust:

The Indirect trust of node b calculated by node a on Tc at Timestamp (ts), $IDT^{Tc}_{a,b}(ts)$, is calculate as:

$$IDT^{Tc}_{a,b}(t_s) = \begin{cases} T^{Tc}_{a,b}(t_s) & if \; |S| > 0 \\ \lambda T^{Tc}_{a,b}(t_s - \triangle t_s) & otherwise \end{cases} \tag{2}$$

When node a obtains accurate suggestions, it fully utilizes them to measure implicit trust. If |S| is the empty set, node a will rely on its past knowledge because no correct suggestions have been obtained.

Hybrid Trust:

HTRM is a Hybrid Trust computational model combines both direct and indirect reputations between nodes. From Eqs. (1) and (2), we can obtain the node's trust either directly or indirectly. However, combining both trusts will give more robust and accurate trust between nodes. While combining both trusts, we can use the following mathematical expressions for calculations.

$$DT^{Tc}_{a,b}(t_s) = \left(\frac{P_{a,b}}{P_{a,b} + N_{a,b}}\right) * \lambda T^{Tc}_{a,b}(t_s - \triangle t_s) \tag{3}$$

$$IDT^{Tc}_{a,b}(t_s) = \sum_{i=1}^{n}\left(\frac{P_{a,b}}{P_{a,b} + N_{a,b}}\right) * \lambda T^{Tc}_{a,b}(t_s - \triangle t_s) \tag{4}$$

In Eqs. (3) and (4), $P_{a,b}$ is the no. of positive trust (completed transactions) between node a and node b. where node b is not an immediate neighbor of node a; $N_{a,b}$ is the no. of the negative trust (incomplete transactions) between node a and node b; $\lambda T^{Tc}_{a,b}(t_s - \triangle t_s)$ is the trust degradation at timestamp (t_s) during interactions between node a and node b.

Now Hybrid Trust,

$$HT^{Tc}_{a,b}(t_s) = DT^{Tc}_{a,b}(t_s) + IDT^{Tc}_{a,b}(t_s) \tag{5}$$

Eq. (5) denotes the hybrid trust of node a in b on Tc at Timestamp t_s, which evaluates trust by combining the trust obtained from the above equations.

3.3 Security Model

These messages can be dropped whole or partial rather than delivering potentially hazardous datagram's to another hop. The purpose of the initial interaction between the sender and receiver nodes is to find malicious activity:

1. Every node calculates a trust score between 0 to 1. Each network device has a commonly specified limit as threshold, and each network node is classification as a breached or ordinary node based on that value.
2. The status power of malicious detected nodes is changed and disconnected from the network.
3. Eliminates the malicious nodes within the transmitter and the receiver, then the sender can choose a trustable path to its targeted node.

We use Asymmetric cryptography in the suggested paradigm, and we use two distinct keys, the secret key (SK) and the Exchange key (EK). For key generation and authentication, we use these two keys. As a result, all other nodes in the network must calculate SK and EK for authentication. It will aid in the tightening of node security. The SK and EK keys are determined based on their Node-UniqueID and trustworthiness factors (Positive threshold), and the EK is used to disseminate the secret keys to other nodes. In the majority of existing models, each node must create its keys.

Furthermore, security breaches will occur if any node exploits, and each node must produce credentials based on their unique-id for authentication in the suggested approach. If a node's key authentication fails, it eliminates the node immediately. Therefore, it will also not affect the network's overall security.

Initialization: In the suggested technique, a node determines an exchange/secret key pair before entering the network. When a node joins for the first time and wants to obtain many credentials for its key pair from existing nodes, it sends a key request (KREQ) signal to the system.

Key Exchange: Before seeking the key of node B, node A determines the minimum trustworthiness (threshold value) that must meet to accept that B's exchange key is trustworthy. We named this level of trust the hybrid-trust threshold exchange key-value (HTEK). It is a local assessment based on A's security needs. Node A then sends out a KREQ for B's keys, including B's address and listing all nodes K(A). The KREQ is sent as a short time to live (STTL). Finally, every intermediary node N obtains the KREQ, checks the key-pair of B, and checks its key-list.

N merely sends the request since it has no key for B or has previously responded to the KREQ. In any other case, N provides a "key" response (KRES) having a key, N authenticates the A's exchange-key (Fig. 2a). If N is unfamiliar with A, it creates a self-authenticated key and notifies A that it wishes to swap keys (Fig. 2b). These packets forward to A over several node-disjoint pathways, and N notifies B that A has demanded its exchange-key if it has a pathway to B in its cache. B answers with a "key" request for A's exchange key. Because N and B mutually authenticate, employing N's identity to safe communication between B and N.

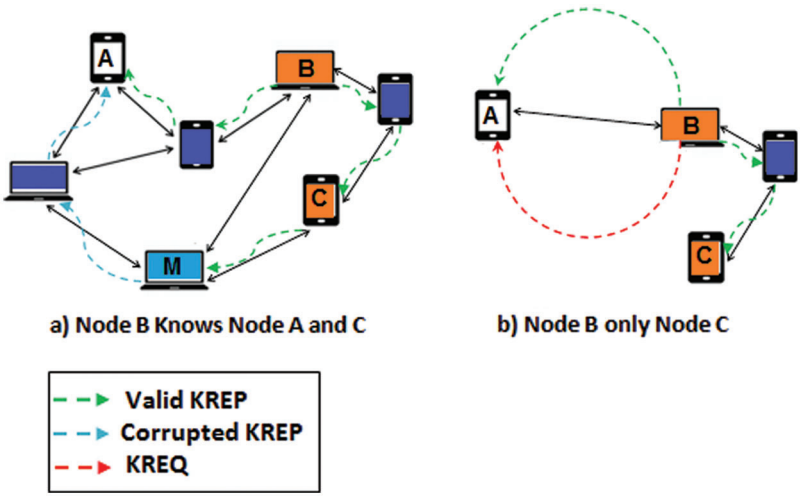

Figure 2: Security model of HTRM

As a result, no node can tamper with the key issued by N to A. B responds to the KREQ itself if it does not know a sufficient number of nodes. A repeats the transaction with a longer TTL until the requisite minimum amount of keys for B's exchange key is received. A delivers its first packet to B after obtaining the keys, which comprises a list of nodes who have supplied B's exchange-key. B obtains information about A's recognized verifiers in this manner. After sharing exchange-keys, A and B generate keys for one another. Because A and B do not have to perform any costly path discovery procedures for routing, this key exchange mechanism can now be used directly in packet forwarding [41–44].

Revocation of keys: Because authentication protocol uses nodes to keep a list of verifiers. We use an implicit revocation technique, in which each node changes its exchange-key regularly by exchanging secure-key and secure exchange communications with its neighbors.

4 Performance Evaluations

We are assessing the suggested HTRM system using the NS-3 simulator. A network of 50 nodes unevenly scattered within a 100 × 100 m region in the experimentally induced. It uses the AODV routing algorithm to evaluate essential parameters such as Packet delivery ratio, power consumption, computational time, throughput, and end-to-end delay. Tab. 1 lists the factors that must be used in a model. We use parameters like end-to-end delay, packet delivery ratio, performance, power consumption, and key-computing time to calculate the effectiveness of the proposed method in the existence of 2 types of nodes in the simulations: trust nodes and fool nodes. We compare the existing approaches such as Data Security-Based Key Management Routing in MANETs (DSBRM) [1] and Energy Efficient Partial Permutation Encryption (EEPPM) [16] protocols with our proposed system simulation results.

Table 1: Simulation factors

Factors	Values
Channel	Wireless channel
Number of nodes	50
Network size	100 × 100 m^2
Network traffic	5 pkt/s
MAC layer protocol	IEEE 802.11
Node mobility	Random mobility
Routing scheme	AODV
Dimension of (x,y) topography	1500,750
Time simulation	250 ms
Data rate	12 Mbps
Antenna type	Omni antenna
Traffic type	CBR

4.1 End-to-End Delay Analysis

In Tab. 2 and Fig. 3 compares the suggested and existing protocols such as DSBRM, EEPPM protocols in terms of end-to-end delay (in milliseconds).

Table 2: End-to-end delay analysis (msec)

Nodes	EEPPM	DSBRM	HTRM (proposed)
10	0.015	0.012	0.008
20	0.022	0.018	0.015
30	0.035	0.023	0.019
40	0.044	0.028	0.024
50	0.051	0.035	0.029

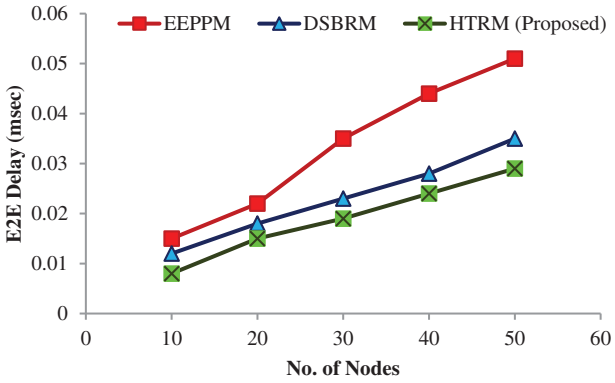

Figure 3: End-to-end delay analysis (ms)

Compared to EEPPM and DSBRM, the suggested model produces a lower end-to-end loss factor. The fundamental explanation for the difference seems to be that the suggested framework is more effective than EEPPM and DSBRM at detecting and removing fool-around nodes [45–47].

4.2 Packet Delivery Ratio Analysis

We compare the analysis of packet delivery ratio between proposed and existing DSBRM and EEPPM protocols as in Tab. 3 and Fig. 4.

Table 3: Packet delivery ratio (%)

Nodes	EEPPM	DSBRM	HTRM (proposed)
10	90	92	95
20	88	90	92
30	85	87	91.5
40	83	85	91
50	80	83	90

It shows that the suggested protocol outperforms well than the EEPPM and DSBRM in packet delivery ratio by 3.152 percent.

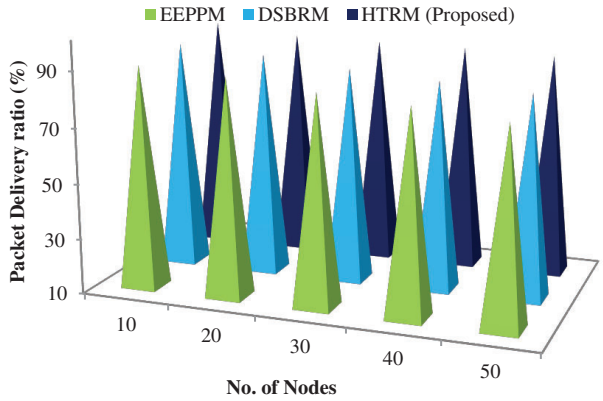

Figure 4: Packet delivery ratio (%)

4.3 Throughput Analysis

The throughput (packets/s) comparison between HTRM (proposed) and existing systems (DSBRM and EEPPM) recorded in Tab. 4 and Fig. 5.

Table 4: Throughput (pkts/s)

Nodes	EEPPM	DSBRM	HTRM (proposed)
10	95	96	98
20	92	91	95
30	90	90	94
40	87	90	94
50	86	92	95

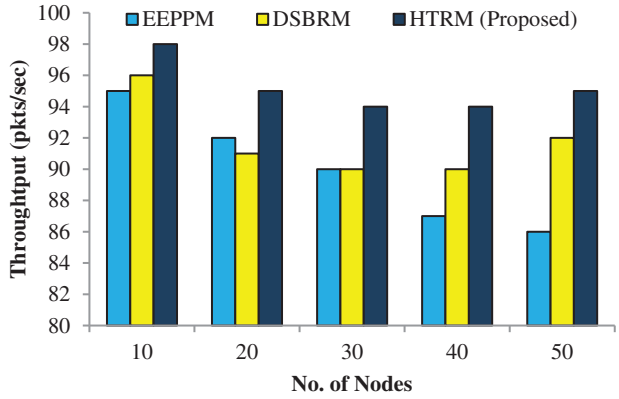

Figure 5: Throughput (pkts/s)

It depicts that the suggested mechanism outperforms DSBRM and EEPPM in terms of the system's performance. The suggested approach outperforms DSBRM and EEPPM by 2.169 percent on average throughput.

4.4 Power Consumption Analysis

The power consumption (watt-hour) evaluation depicts in Tab. 5 and Fig. 6. Compared to the DSBRM and EEPPM models, the proposed model utilizes much less power. Because all nodes in the proposed model must compute their keys, but only when they deviate from their usual behavior [48–52].

Table 5: Power consumption (watt-hour)

Nodes	EEPPM	DSBRM	HTRM (proposed)
10	5.5	3	2.5
20	7	5.5	3
30	9	5.7	3.2
40	6.5	5	3
50	9.5	8.5	3.5

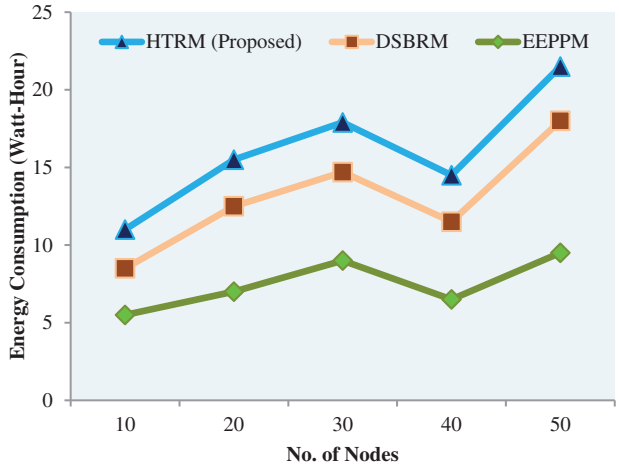

Figure 6: Throughput (pkts/s)

As a result, only nodes require power during key production and transmission periods, increasing power efficiency [53,54]. In the EEPPM paradigm, on the other hand, each time must calculate its keys, leading to higher energy use. As a result, the proposed scheme improves DSBRM and EEPPM by 3.527 percent in power-saving.

4.5 Key Computational Analysis

We show the key (microseconds) computational analysis between the HTRM and DSBRM, and EEPPM models in Fig. 7 and Tab. 6. The time required to execute the computational procedure is a key computational cost. The suggested approach requires less time to compute keys than the EEPPM model, which takes much more time.

In the HTRM approach, all nodes must compute their keys when required. It reduces key computation time instead of the EEPPM model, which requires each node to calculate its keys. Because wireless nodes have limited computing power, the key calculation time grows when the nodes are grown. Compared to DSBRM and EEPPM, the suggested protocol takes 3.762 percent less to compute keys.

Table 6: Key consumption (ms)

Nodes	EEPPM	DSBRM	HTRM (proposed)
10	0.011	0.021	0.008
20	0.032	0.031	0.024
30	0.081	0.071	0.051
40	0.071	0.081	0.051
50	0.1	0.081	0.055

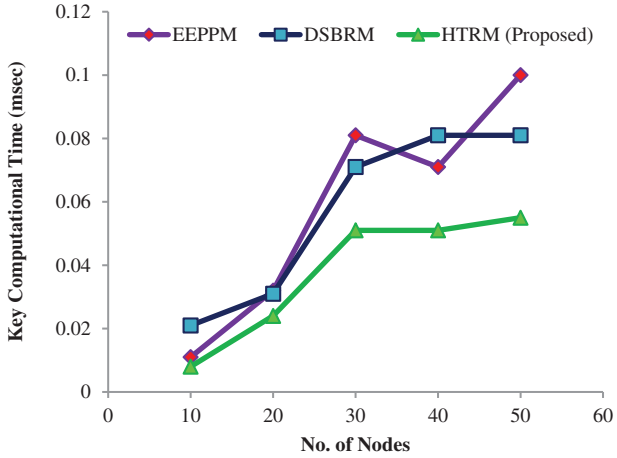

Figure 7: Key consumption (ms)

5 Conclusion and Future Work

According to the findings, MANETs are vulnerable to security attacks that are hard to counter using current protection measures. As a result, several safe routing algorithms propose to improve MANET security. The proposed HTRM methods require each node to generate and distribute its secret keys only when they authenticate a misbehaving node, resulting in reduced power distribution. Furthermore, security flaws must happen if any node exploits. We propose a safe and energy-efficient routing system associated with group key exchange to address such difficulties. Asymmetric cryptographic security was employed, which entails the employment of two distinct keys: a SK and an EK. These two components were in charge of node identification and authorization. As an outcome, neighboring nodes did not have to do any extra calculation to generate the secret keys all the moment. We carry out comprehensive tests using both the old and suggested methods. In terms of overall end-to-end delay, packet-delivery ratio, performance, power consumption, and key computational time, the suggested technique exceeds the competing protocols by 3.47, 3.152, 2.169, 3.527 and 3.762 percent, respectively. As a result, numerous optimization methodologies, such as evolutionary algorithms, will be used to optimize the hyperparameters of the suggested model. Tactical systems, Wireless Technologies, Communication Systems, Device Networks, and other real-time applications leverage our technique. Moreover, the suggested model can be applied to other applications of wireless systems in the future, like Vehicular *Ad Hoc* Networks (VANETs).

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Bondada, D. Samanta, M. Kaur and H. Lee, "Data security-based routing in manets using key management mechanism," *Applied Sciences*, vol. 12, no. 3, pp. 1041, 2022.

[2] K. V. Kumar, T. Jayasankar, V. Eswaramoorthy and V. Nivedhitha, "SDARP: Security based data aware routing protocol for ad hoc sensor networks," *International Journal of Intelligent Networks*, vol. 1, no. 1, pp. 36–42, 2020.

[3] V. S. Devi and N. P. Hegde, "Multipath security aware routing protocol for manet based on trust enhanced cluster mechanism for lossless multimedia data transfer," *Wireless Personal Communications*, vol. 100, no. 3, pp. 923–940, 2018.

[4] T. V. Suresh Kumar and G. B. Prabhu, "A secure routing protocol for manet using neighbor node discovery and multi detection routing protocol," *International Journal of Engineering Trends and Technology*, vol. 68, no. 7, pp. 50–55, 2020.

[5] A. K. Biswas and M. Dasgupta, "A secure hybrid routing protocol for mobile ad-hoc networks (MANETs)," in *2020 11th Int. Conf. on Computing, Communication and Networking Technologies*, Kharagpur, India, pp. 1–7, 2020.

[6] M. G. El-Hadidi and M. A. Azer, "Traffic analysis for real time applications and its effect on qos in manets," in *Proc. of the 2021 Int. Mobile, Intelligent, and Ubiquitous Computing Conf.*, Cairo, Egypt, 26, pp. 155–160, 2021.

[7] V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain *et al.,* "Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 21, pp. 4995–5001, 2020.

[8] K. Rukhsana, M. Alhaisoni, S. Abid Akhtar, N. Shah, A. Qamar *et al.,* "A secure data dissemination in a dht-based routing paradigm for wireless ad hoc network," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1– 32, 2020.

[9] M. Maheswari, S. Geetha, S. S. Kumar, M. Karuppiah, D. Samanta *et al.,* "PEVRM: Probabilistic evolution based version recommendation model for mobile applications," *IEEE Access*, vol. 9, pp. 20819–20827, 2021.

[10] L. E. Funderburg and I.-Y. Lee, "A privacy-preserving key management scheme with support for sybil attack detection in vanets," *Sensors*, vol. 21, no. 4, pp. 1–17, 2021.

[11] M. Mehic, P. Fazio and M. Voznak, "Usability of destination-sequenced distance vector routing protocol routes," in *2019 11th Int. Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, Dublin, Ireland, pp. 1–5, 2019.

[12] Q. Liang, T. Lin, F. Wu, F. Zhang and W. Xiong, "A dynamic source routing protocol based on path reliability and link monitoring repair," *PLOS ONE*, vol. 16, no. 5, pp. 1–12, 2021.

[13] A. R. Sangi, M. S. Alkatheiri, S. Anamalamudi, M. A. Alqarni, M. H. Memon *et al.,* "Spectrum handoff aware aodv routing protocol for cognitive radio vehicular ad hoc networks," *Complexity*, vol. 2021, no. 4, pp. 1–13, 2021.

[14] U. Allimuthu and K. Mahalakshmi, "Intelligent route discovery towards rushing attacks in ad hoc wireless networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 2, pp. 921–960, 2022.

[15] R. Rajesh, M. Ramakrishnan and B. Sugumar, "A modest approach on manet using certificateless cryptography," in *2017 Int. Conf. on Intelligent Sustainable Systems*, Palladam, India, pp. 1197–1204, 2017.

[16] A. Khan, Q. T. Sun, Z. Mahmood and A. U. Ghafoor, "Energy efficient partial permutation encryption on network coded manets," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–10, 2017.

[17] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access*, vol. 10, pp. 14260–14269, 2022.

[18] A. B. C. Douss, R. Abassi and S. G. El Fatmi, An optimized reputation-based trust management scheme for manet security. In: *Security and Privacy in Smart Sensor Networks*. Hershey, PA: IGI Global, pp. 63–85, 2018.

[19] Y. Ebazadeh and R. Fotohi, "A reliable and secure method for network layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold," *Security and Privacy*, vol. 5, no. 1, pp. e183, 2022.

[20] S. Kalime and K. Sagar, "A review: Secure routing protocols for mobile adhoc networks (MANETs)," *Journal of Critical Reviews*, vol. 7, pp. 8385–8393, 2021.

[21] A. Hammamouche, M. Omar, N. Djebari and A. Tari, "Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET," *Journal of Information Security and Applications*, vol. 43, no. 3, pp. 12–20, 2018.

[22] M. Ponnusamy, "Detection of selfish nodes through reputation model in mobile adhoc network-manet," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 9, pp. 2404–2410, 2021.

[23] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf *et al.,* "An improved hybrid secure multipath routing protocol for manet," *IEEE Access*, vol. 9, pp. 163043–163053, 2021.

[24] N. Veeraiah, O. I. Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani *et al.,* "Trust aware secure energy efficient hybrid protocol for manet," *IEEE Access*, vol. 9, pp. 120996–121005, 2021.

[25] K. S. Sankaran, N. Vasudevan, K. R. Devabalaji, T. S. Babu, H. H. Alhelou *et al.,* "A recurrent reward based learning technique for secure neighbor selection in mobile ad-hoc networks," *IEEE Access*, vol. 9, pp. 21735–21745, 2021.

[26] M. Elhoseny and K. Shankar, "Reliable data transmission model for mobile ad hoc network using signcryption technique," *IEEE Transactions on Reliability*, vol. 69, no. 3, pp. 1077–1086, 2020.

[27] J. Tu, D. Tian and Y. Wang, "An active-routing authentication scheme in manet," *IEEE Access*, vol. 9, pp. 34276–34286, 2021.

[28] F. Aftab, Z. Zhang and A. Ahmad, "Self-organization based clustering in manets using zone based group mobility," *IEEE Access*, vol. 5, pp. 27464–27476, 2017.

[29] M. Kaur, D. Singh, V. Kumar, B. B. Gupta and A. A. Abd El-Latif, "Secure and energy efficient-based e-health care framework for green internet of things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1223–1231, 2021.

[30] T. Zhang, S. Zhao, B. Cheng, M. Farina, J. Huang *et al.,* "Lightweight soa-based multi-engine architecture for workflow systems in mobile ad hoc networks," *IEEE Access*, vol. 6, pp. 14212–14222, 2018.

[31] S. Singh and H. S. Saini, "Intelligent ad-hoc-on demand multipath distance vector for wormhole attack in clustered WSN," *Wireless Personal Communications*, vol. 122, no. 2, pp. 1305–1327, 2022.

[32] T. Singh, N. Saxena, M. Khurana, D. Singh, M. Abdalla *et al.,* "Data clustering using moth-flame optimization algorithm," *Sensor*, vol. 21, no. 12, pp. 1–19, 2021.

[33] C. Gopala Krishnan, A. H. Nishan, S. Gomathi and G. Aravind Swaminathan, "Energy and trust management framework for manet using clustering algorithm," *Wireless Personal Communications*, vol. 122, no. 2, pp. 1267–1281, 2022.

[34] K. R. Shibu and R. Suji Pramila, "Load based key generation for manets: A comparative study with dsr and aodv," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1703–1712, 2021.

[35] M. Yadava, A. S. Pandey and K. Singh, "Secure and efficient wireless multicast communication using trust-based key management," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 3, pp. 711–727, 2021.

[36] D. Hurley-Smith, J. Wetherall and A. Adekunle, "SUPERMAN: Security using pre-existing routing for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2927–2940, 2017.

[37] T. Zhang, X. Xu, X. Jiang Le Zhou and J. Loo, "Cache space efficient caching scheme for content-centric mobile ad hoc networks," *IEEE Systems Journal*, vol. 13, no. 1, pp. 530–541, 2019.

[38] D. -G. Zhang, P. -Z. Zhao, Y. -Y. Cui, L. Chen, T. Zhang *et al.,* "A new method of mobile ad hoc network routing based on greed forwarding improvement strategy," *IEEE Access*, vol. 7, pp. 158514–158524, 2019.

[39] H. Xu, Y. Zhao, L. Zhang and J. Wang, "A bio-inspired gateway selection scheme for hybrid mobile ad hoc networks," *IEEE Access*, vol. 7, pp. 61997–62010, 2019.

[40] T. Dbouk, A. Mourad, H. Otrok, H. Tout and C. Talhi, "A novel ad-hoc mobile edge cloud offering security services through intelligent resource-aware offloading," *IEEE Transactions on Network and Service Management*, vol. 16, no. 4, pp. 1665–1680, 2019.

[41] N. Partheeban, K. Sudharson and P. J. Sathish Kumar, "SPEC-serial property based encryption for cloud," *International Journal of Pharmacy & Technology*, vol. 8, no. 4, pp. 23702–23710, 2016.

[42] K. Sudharson, A. M. Ali and N. Partheeban, "NUITECH–Natural user interface technique foremulating computer hardware," *International Journal of Pharmacy & Technology*, vol. 8, no. 4, pp. 23598–23606, 2016.

[43] J. Aruna Jasmine, V. Nisha Jenipher, J. S. Richard Jimreeves, K. Ravindran and D. Dhinakaran, "A traceability set up using digitalization of data and accessibility," in *2020 3rd Int. Conf. on Intelligent Sustainable Systems (ICISS)*, Thoothukudi, India, pp. 907–910, 2020.

[44] D. Dhinakaran and P. M. Joe Prathap, Ensuring privacy of data and mined results of data possessor in collaborative ARM. In: *Pervasive Computing and Social Networking. Lecture Notes in Networks and Systems*. Vol. 317. Singapore: Springer, 2022.

[45] S. Arun and K. Sudharson, "DEFECT: Discover and eradicate fool around node in emergency network using combinatorial techniques," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 10, pp. 1–12, 2020.

[46] K. Sudharson and V. Parthipan, A Survey on ATTACK–Anti terrorism technique for adhoc using clustering and knowledge extraction. In: *Advances in Computer Science and Information Technology. Computer Science and Engineering. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Vol. 85. Berlin, Heidelberg: Springer, pp. 508–514, 2012.

[47] K. Sudharson and V. Parthipan, "SOPE: Self-organized protocol for evaluating trust in MANET using Eigen Trust Algorithm," in *3rd Int. Conf. on Electronics Computer Technology*, Kanyakumari, India, pp. 155–159, 2011.

[48] N. Suganthi and S. Neelavathy Pari, "Detecting malicious nodes in MANET using rateless codes for maximum content distribution," in *2014 Sixth Int. Conf. on Advanced Computing (ICoAC)*, Chennai, India, pp. 308–311, 2014.

[49] M. Sathish, K. Arumugam, S. Neelavathy Pari and V. S. Harikrishnan, "Detection of single and collaborative black hole attack in MANET," in *2016 Int. Conf. on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, pp. 2040–2044, 2016.

[50] S. Neelavathy Pari, S. Jayapal and S. Duraisamy, "A trust system in manet with secure key authentication mechanism," in *2012 Int. Conf. on Recent Trends in Information Technology*, Chennai, India, pp. 261–265, 2012.

[51] S. Neelavathy Pari, M. Sathish and K. Arumugam, "An energy-efficient and reliable depth-based routing protocol for underwater wireless sensor network (ER-DBR)," in *Advances in Power Systems and Energy Management. Lecture Notes in Electrical Engineering*, A. Garg, A. Bhoi, P. Sanjeevikumar, K. Kamani (eds.), Vol. 436. Singapore: Springer, 2018.

[52] S. Neelavathy Pari and D. Sridharan, "Design of cross layered security architecture to mitigate misbehaving nodes in self-defending network," *European Journal of Scientific Research*, vol. 77, no. 1, pp. 37–45, 2012.

[53] M. Ali, C. Xu and A. Hussain, "Authorized attribute-based encryption multi-keywords search with policy updating," *Journal of New Media*, vol. 2, no. 1, pp. 31–43, 2020.

[54] X. R. Zhang, X. Sun, W. Sun, T. Xu and P. P. Wang, "Deformation expression of soft tissue based on bp neural network," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 1041–1053, 2022.