International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

HUMAN-CENTRIC TRUST-BASED SECURITY KEY ROUTING IN MANETS FOR SMART CITIES BY USING MACHINE LEARNING TECHNIQUES

I.JEYARAMAN SATHIAMOORTHY[1], B. PRAVEEN[2], P. SENTHILRAJA [3]
[1] Professor, Department of Information Technology, St.Joseph's Institute of Technology(Autonomous), OMR, Chennai-119, India.
[2] Research Scholar, Department of Information Technology, St.Joseph's Institute of Technology(Autonomous), Anna University, Chennai 600025 India
*Corresponding e-mail: praveen071205@gmail.com
[3] Research Scholar, Anna University, Chennai 600025 India
*Corresponding e-mail: senthilrajamtech@gmail.com

***Abstract*—With the diversification of mobile ad hoc networks into all spheres of smart city functionality, there is a need to advance communication among mobile nodes in terms of security mechanisms. This paper presents a human-centric trust-based security key routing protocol based on machine learning techniques that enhance the security and reliability of routing operations in MANETs.**

Keywords—Mobile Ad Hoc Networks, Trust-Based Routing, Smart Cities, Machine Learning, Security, Routing Protocols.

Received: 15-10-2025 Accepted: 26-11-2025 Published: 05-12-2025

I. INTRODUCTION

The development of communication networks is in itself a critical component which plays a very significant role in the infrastructure of smart cities. Many persons across the world are now interested in this concept, thereby resulting in an increase in demand for communication solutions, decentralised, flexible, and safe. MANETs, also known as mobile ad hoc networks, have emerged as an enabling technology for smart city applications (Balakrishnan, 2020). This has primarily been because of the native characteristics of self-organization, adaptability, and scalability inherited by MANETs. Despite all the benefits MANETs are providing, security is undoubtedly one of the major concerns (Banti, 2023). It is considerably more relevant in the context of MANETs due to their dynamic nature and complete absence of a centralised authority of any kind. At the core of the research focus in this study will be a human-centric trust- based routing protocol that will be reinforced through machine learning techniques to strive for maximum accessibility for securing MANETs (Baras, 2005).

A. Smart Cities and the Role of MANETs

Smart cities are those characterized by integrated systems of sensors, gadgets, and networks that work together to improve the quality of life in metropolitan areas (Basheer, 2023). Communication networks that support real-time data exchange, traffic control, environmental monitoring, public safety, and so on are very crucial to the functioning of these cities. This scenario is especially suitable for MANETs as they are adaptive and do not necessarily need any conventional infrastructure to function (Boukerche, 2007).

MANETs are also very flexible to contexts that continuously change as mobile devices are facilitated by direct interaction with one another as opposed to the traditional networks that require routers or access points (Chatterjee, 2006). In MANET, each node serves as a host and a router because it forwards data to other nodes in the network.

This architecture is known as a MANET. Because it is decentralized, the installation can be very easy, and this becomes a key characteristic for smart city applications such as emergency response, vehicular networks, and environmental monitoring (Chaudhry, 2019). However, because of their decentralized nature, MANETs are susceptible to a wide range of security risks. The reason for this is that the malicious nodes can easily invade the network and communication (Djenouri, 2008). To ensure that MANETs function well in smart city environments, the security issues regarding such must be handled..

B. Security Challenges in MANETs

One of the most important complications that have been associated with these networks is that MANETs are susceptible to

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

security flaws because of their open and dynamic architecture. That is to say, nodes in a MANET are free to join and leave the network at any time, which makes it tough to construct a permanent security perimeter (El-Sayed, 2020). This open architecture renders it susceptible to denial-of-service (DoS) attacks, Sybil attacks, man-in-the- middle attacks, and packet dropping (Ionescu, 2024). Routing may be compromised by malicious nodes: data may be lost, delayed, or even partition the network. Even though classical cryptographic security mechanisms work efficiently in static networks, they may perhaps not be ideal for the MANET due to the dynamic nature of the latter (Kumar, 2020).

Since these methods are claimed to be resource-intensive in terms of the number of processing cycles and bandwidth, they might not be feasible in such a resource-scarce and mobile environment (Li, 2019). It must also be taken into consideration that cryptographic solutions neither provide a remedy for the internal threats that stem from compromised nodes in the network (Liu, 2007). Accordingly, such security methods should be very flexible and adaptable because they have to include the kind of problems envisioned by MANETs (Mamoun, 2018).

C. Trust-Based Routing as a Solution

Trusted routing protocols prove to be a promising method of enhancing the security of MANETs because they can overcome the limitations and constraints imposed by standard security techniques (Mishra, 2003). Regarding trust- based routing, inside the network, behavior of nodes is analyzed, and routing decisions are performed based upon the trust level of the nodes within the network (Nassar, 2017). This approach is different from the cryptographic methods as it presents an approach that is much more versatile and less resource-intensive in comparison.

In a trust-based routing protocol, nodes continuously evaluate the performance metric of the neighbourhood behavior, including how often their packets get delivered, the amount of energy consumed by this process, and the amount of time it takes for a response to be given (Pirzada, 2004). It is based on this assessment that nodes are assigned trust values and routing is done with preference given to nodes holding high valued trust values. The dynamic assessment of trust thus helps the network respond in response to situations of change so as to isolate rogue nodes and therefore reduce the possibility of potential attacks (Rajasoundaran, 2021).

However, despite the fact that trust-based routing contributes to increased security, it also has its challenges. On the other side, considering the dynamic nature of MANETs, in which the behavior of nodes may change over time due to movement or environmental conditions, static models of trust have difficulties adapting to the dynamic nature of MANETs (Saxena, 2020). In addition, most of the trust-based systems currently developed do not take into account those human-like elements within decision making that may influence the evaluation of trust.

D. Human-Centric Trust Models

Human-centric aspects to trust-based routing processes add a new dimension of security to MANETs. In making decisions, humans do not merely rely on what behavior is visible but also upon subjectivity factors such as reputation, past experience, and perceived reliability (Shen, 2019). The evaluation process that is analogous to human evaluation can be mimicked to make the trust management in MANET robust and dynamic.

Within the developed human-centric trust model, nodes should assess their peers from various perspectives; objective parameters, such as packet delivery rates, and subjective characteristics, including the perceived level of trust and the number of peers already encountered. This multi- dimensional evaluation of trust can help the network to deal more effectively with complex and dynamic situations (Sun, 2008). For instance, in the near term, a node would be trusted much more if it has consistently high reliability for its data, whereas a node that performs erratically may not be trusted as much even though it may have the same packet success rate. This is due to the fact that the former continuously provides data with high reliability (Yang, 2004). This human-centric trust management approach thus yields a better, more subtle understanding of the node behavior and leads to routing decisions that are best informed and more reliable.

E. Integrating Machine Learning for Enhanced Security

Trust based routing protocols may be adaptive, yet lightweight solutions to protect MANETs, but machine- learning approaches can significantly improve the performance of these protocols by automatically detecting malicious behavior and enhancing the accuracy of trust evaluation (Yang Y. X., 2021). The machine learning models aid in the real-time analysis of large volumes of network data and thereby derive knowledge about patterns that may not intuitively be

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

discernible by straightforward observation. We use the machine learning techniques, in this particular case a Random Forest classifier, in the methodology we have suggested to make predictions about malicious nodes based on an analysis of their behavior. This classifier is trained on multiple characteristics, such as the percentage of successful packets, the amount of latency, the energy amount consumed, and trust recommendations from neighbouring nodes. By using the power of machine learning, the system will be able to classify suspicious behaviour by simply tweaking the values based on this behavior. This reduces the dependency of the system on the thresholds to be static and enhances its adaptability in real-time network conditions. The combination of machine learning with human-centric trust models results in an effective framework that is liable to enhance the security and dependability of MANETs used in smart cities. Since machine learning is dynamic, the system can increase its detection accuracy continuously (Zhao, 2018). The human-centric trust model also possesses this feature of routing decisions based on a deeper understanding of the node's behavior.

F. Significance of the Study

The rapid growth of smart cities, spurred by the advancement in technology, including the Internet of Things and wireless communication networks, is posing an increasing requirement to have infrastructure that is highly secure and dependable enough to support applications being developed in large numbers. MANETs, which are the abbreviation for mobile ad hoc networks, form a crucial part of this concept because they offer decentralized and self- organizing capabilities necessary in dynamic environments such as smart cities. The implementation of MANETs, however is deemed to undertake pretty significant dangers because of inherent vulnerabilities possessed by these networks, including the possibility of being exposed to malicious attacks and breaches in security. This study is of great importance because it introduces a novel trust-based security key routing protocol human-centric and machine learning boosted to overcome these difficulties. This work improves the dependability, adaptability, and security of MANETs by integrating human-like trust variables into the network decision-making process and applying machine learning techniques for the real-time detection of hostile nodes. The research also uses machine learning. The approach that has been provided not only contributes to academic discussions under way concerning trust-based security in dynamic networks but also offers solutions applicable to the kind of infrastructures found in the real world, those of smart cities. Finally, the results of this work could significantly contribute to enhancing the resilience of MANETs while ensuring safer communication in applications such as traffic management, emergency services, and environmental monitoring, thus contributing to the advancement in the development of smart cities.

G. Problem Statement

MANETs have found their place because they are decentralised and dynamic, thus an alternate in the field of smart cities, where there is a great requirement of communication networks that should be secure as well as efficient. MANETs notwithstanding all these advantages, they are extremely vulnerable to a wide variety of security risks. The other threats are packet dropping, malicious node actions, and denial-of-service (DoS) attacks, which indeed can seriously degrade the functionality of the network. This makes typical cryptographic techniques less suitable for dynamic and resource-constrained scenarios like MANET even though they are used in most static networks. They introduce high computationally and bandwidth-intensive overheads that disqualify them. What is not captured by those trust-based routing protocols which, in the absence of adaptation to complex and developing security risks, fail not only to respond but crash into the first instance that the protocols themselves were not designed to accommodate is a critical aspect of human-like decision-making elements, namely perceived reliability and previous behavior. Hence, a need arises immediately for a better routing protocol that includes a more sophisticated trust evaluation with machine learning-based approaches to dynamically discover and counter the harmful behaviors occurring within MANETs. The current research aims to bridge this gap by inventing a human-centric trust-based security key routing protocol using machine learning. This protocol will provide a solution more flexible and efficient in ensuring secure communication in MANETs for applications related to smart cities.

II. RELATED WORK

Muzammal, Murugesan, and Jhanjhi (2020) proposed the concept of IoT as a network which interlinks and integrates various devices, including sensors, actuators, smartphones, and wearables. The authors emphasized that WSNs, as a component of IoT, ensure data forwarding

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

once sensed and collected. However, the scalability and heterogeneity of IoT systems created tremendous security risks, making it prone to various attacks; many of them are inherited from WSNs. Moreover, the authors noted that also, IPv6 Routing Protocol for Low Power and Lossy Networks, which is adopted as standard protocol for IoT was suffered by various security risks due to its intrinsic features. It investigated a few mitigating mechanisms targeted for securing the IoT networks along with their routing protocols, marking greater direction towards trust-based approaches as an emerging solution for improving security. Of these, the trust models were SecTrust, DCTM-IoT, and CTRUST, all designed specifically to cater to the demands of IoT's system security necessities (Muzammal, 2020). The research further dug into security issues produced by Blackhole attacks, Spoofing, and Rank with mitigation strategies. Lastly, they discussed the trust metrics relevant to IoT environments and drew focus to open research challenges while emphasizing the role of trust as an extremely important security paradigm in IoT networks and routing protocols.

Maheshwari, Varshitha, Gouthami, and Sirisha (2024) presented the artificial intelligence-based security component for MANETs in the context of IoT. They studied countering the Black Hole Attack (BHA) from malicious nodes; stopping acceptance of data significantly degrades data transmission in MANETs. Combating this attack, the authors suggested a new security method combining Ad-hoc On- Demand Distance Vector (AODV) routing protocol with machine learning techniques; these later include ANN, Support Vector Machines (SVM), and the Artificial Bee Colony (ABC) algorithm. This model trained using ANN and fine-tuned by the ABC fitness function and SVM sought to detect malicious nodes along the routing path in real time. The data transmission route between source and destination nodes is optimised by ABC, followed by the SVM evaluating the node's attributes in an attempt to identify malicious behaviour (Maheshwari, 2024). The simulation-based research in MATLAB found better improvements in latency, throughput, and PDR as compared to the existing methods. Besides that, comparisons with Decision Tree and Random Forest-based approaches revealed that the integration of SVM in ANN provided better performance on the detection of BHA attacks in MANET-based IoT environments.

Bondada, Samanta, Kaur, and Lee (2022) identified security challenges of MANETs. Rather, it was on the autonomous nature of the network based on a wireless mobile node that operates in the absence of infrastructure support for communication. The authors viewed that though MANETs enable dynamic and free communication between nodes, they are prone to security threats that cannot be addressed by prevailing approaches toward security. They then proposed a group key management-based secure and energy-efficient routing protocol. In their scheme, the asymmetric key cryptography came into play with two CK and DK nodes, solely responsible for generating, verifying, and distributing the secret keys. The rest of the nodes were not involved in performing extra computations, thus saving energy. The authors pointed out that, as compared to typical protocols where every node generates its own key, which increases the energy consumption and exposed node to possible attacks, the design in this key management centralizes with increased security (Bondada, 2022). They performed experiments concluding that new protocol is a significant performance improvement over existing ones about both security and energy efficiency. Additionally, they observed that even if all the nodes except for CK and DK were compromised, the security of the entire network was still intact, which was a great leap forward compared with other protocols.

Jhaveri and Patel (2016) researched the issue of trustworthiness and cooperation in multi-hop routing in MANETs, particularly under infrastructure less and no centralized power architecture. The study focused on packet forwarding misbehavior amongst some internal nodes with the intent to sabotage the routing mechanism, thus ensuring the packets to be forwarded are insecure and unreliable. For this reason, the authors have proposed a trust-based routing scheme integrating an attack pattern discovery technique with the Ad-hoc On-demand Distance Vector (AODV) protocol in which their scheme utilized the historical behaviors of nodes in detecting malicious activities before the nodes drop data packets. The paper further offered three models of attackers that triggered different types of misbehaviour in forwarding packets (Jhaveri, 2016). From the theoretical analysis and experimental outcome, they demonstrated that the incorporation of a pattern discovery approach with a trust-based model can detect an attacker more in advance than standalone trust-based models alone. The approach resulted in the disruption of more adversary capabilities than those of standalone trust-based models because of the proactive defense mechanism provided for specific attack patterns.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Qolomany, M; Al-Fuqaha, A; Guizani, M; Qadir, J (2020) highlighted the urgent need to obtain integrity and veracity of the ML models particularly in mission-critical human-facing applications. The paper would be dedicated to obtaining vast amounts of data from resource-constrained devices across cloud service providers. A set of ML-based prediction models were then sent back to run in these resource-constrained devices. The authors proposed an intelligent polynomial-time heuristic to tackle this challenge of maximizing the trustworthiness of those models by choosing and switching between a subset of ML models from a superset, trying to balance trust with communication efficiency and reconfiguration budgets. With the two case studies, the heuristic was tested on forecasting the remaining useful life of engines using the data on simulated turbofan engine degradation under the scenario of the Industrial Internet of Things (IIoT) and estimating the number of cars of smart city services using transportation data (Qolomany, 2020). The results of the selected models of the trust level were a bit less than those obtained via the ILP method: 0.49%-3.17% and 0.7%-2.53% for IIoT and smart city case studies, respectively. The proposed heuristic was effective since it resulted in an optimal competitive ratio within a polynomial approximation scheme time.

Neelakandan and Gokul Anand (2011) discussed the characteristics and challenges of MANETs, listing its self- organizing nature and lack of fixed infrastructure, which makes it easier and faster to set up than traditional wireless networks. However, while MANETs also have several unique challenges, especially in terms of security, with an open peer-to-peer architecture, dynamic topology, shared wireless medium, and also limited resources such as battery, memory, and computational power, MANET is vulnerable to many security threats. Traditional routing algorithms in MANET have lacked the use of cryptography techniques which, according to the authors, cannot be avoided in secure transactions over such a network. The paper proposed a secure, trusted, and optimal routing scheme that integrates cryptographic procedures in order to enhance the security of transactions in MANETs (Neelakandan, 2011). Thus, the issue proposed aimed at enhancing the security and efficiency of MANET routing protocols.

A. Research Gap

From previous research on Mobile Ad Hoc Networks (MANETs) in the context of smart cities, several research gaps have been identified that this study aims to address:

- Limited Incorporation of Human-Centric Factors: Most security models based on trust focus on technical features, rather than including human-like decision-making variables in the management of trust. This is one thing that might improve the applicability and security of managing trust in real- world applications..
- Scalability and Adaptability Issues: Even though they are effective, the algorithms for malicious node detection that rely on machine learning are often encountered with issues related to scalability and adaptability during dynamic environments. An example of such a dynamic environment is smart cities, which characterize themselves by changing network conditions and security concerns.
- Reliance on Historical Data: Although trust based routing protocols highly rely on the analysis of the prior behavior to identify malicious nodes, they still have problems in handling real-time dynamic threats and hostile nodes who quickly change their strategies in order to defeat such protocols.
- Energy Efficiency vs. Security Trade-offs: Even though a good number of studies proposed security techniques, mechanisms often increase the degree of computing overhead, especially in resource- constrained MANETs. There is needed such approaches that establish some kind of balance between high levels of security and corresponding high levels of energy efficiency.
- Limited Focus on Real-Time Decision-Making: Current machine learning models applied in MANETs are mostly being aimed at optimizing the routing or security parameters, without real-time decision-making capabilities, which are very much required to improve the response time regarding a new threat in the smart city environment.

It fills up the various gaps by developing a human-centric trust-based security key routing protocol that accounts for both human-like decision-making factors and real-time malicious node detection via machine learning techniques. The aim of this research is to enhance the reliability, adaptability, and overall performance of MANETs.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

B. Objectives of the study

The primary objectives of this research are:

- To design a human-centered trust-based security key routing protocol for MANETs in smart cities.
- To oppose the injection of machine learning techniques for detection and eradication of malicious nodes in MANETs
- To evaluate human-like decision factors on reliability and security of the routing process
- To manet-based improvement in overall security and performance for smart city environment.
- To test the precision and the effectiveness of the protocol proposed by using the simulated MANET dataset.

III. PROPOSED METHODOLOGY

A. Overview

This research will fill those gaps as given above by developing human-centric trust-based security key routing protocol. Developed protocol uses real-time malware node detection with machine learning techniques and human-like decision factors while operation. The main objective of the researchers is to improve reliability as well as adaptability in MANETs with better performance.

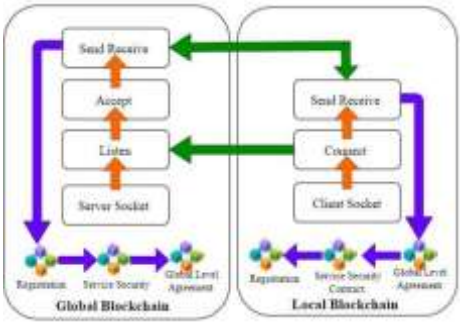

Figure 1: Global-Local Blockchain Network for IoT Services

Figure 1 illustrates a blockchain-based communication protocol for IoT devices. Below we describe how global and local blockchains can be leveraged to support secure, trusted interactions between smart devices-a perfect enabler for data/service exchange.

B. Trust Evaluation

The mechanism for trust evaluation developed here uses nodes that continuously and dynamically evaluate the behavior of their neighbors with respect to a number of important characteristics. Such a method of evaluation allows for changes in trust levels in real time in response to such changes. Also monitored includes the Packet Delivery Success Rate, which is the relation between the number of packets that were successfully delivered and the total number of packets that were sent. A higher success rate indicates reliability on a node. Another important consideration is Response Time, which is an illustration of the time taken by a node when answering queries; nodes that depict more responsive times are often thought to be dependable and efficient.

Figure 2: Architecture of trust based IoT Applications

The numerous uses of trust-based methods in Internet of Things (IoT) contexts are depicted in Figure 2.

I. Human-Centric Factors

A human-centric model that incorporates a decision and mirrors the dynamics of social trust is included in the trust model which hardens traditional evaluations. These characteristics quite heavily influence the manner in which nodes communicate with each other and establish trust within the network. Historical interactions are of high importance because the behaviors and interactions that took place in the past between nodes can significantly influence the trust evaluations that are currently being taken into account between them. There is also this concept of perceived reliability, which is the assessment that a node grants to another based on other nodes' experiences toward it. Again, this is applied. In addition, there is a Reputation score issued to every node based on the feedback it receives from its neighboring nodes. This number serves to quantify the reliability of each node. This multi-dimension approach leads to a better conceptualization of trust in the network, allowing nodes to judge on a mix of past facts and the group opinion as a whole.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

II. Machine Learning for Malicious Node Detection

A Random Forest classifier plays the role of node identification as trustful or malicious in enhancing network security. Some of the components used to train this machine learning model comprise Packet Success Rate, Latency, and Energy Consumption. The classifier, therefore, learns the patterns associated with trustful and harmful behavior very comprehensively by analyzing these properties. This will finally lead to the identification and notification of the malicious nodes at the end, and the total precautionary measures in the network will be on the rise. The system may evolve according to the newly detected threats and also continue enhancing its estimation of the trustworthiness of the nodes with machine learning involved in the process of trust rating. In the case of the above problem, the system actually implements a Random Forest classifier. Here's how to implement this in Python code.

C. Trust Model

The model appropriately constructs the nodes located within the network as a function of the trustworthiness by a combination of direct and indirect observation methods of the behavior of nodes in the network. This not only means that nodes within the network undergo a better-defined, more detailed understanding of the degree of trust prevalence but also within the network.

I. Direct Trust

Direct Trust is that term which represents the assessment done based on the direct contacts taking place between nodes. Much emphasis has been given to this characteristic feature of the trust model to the encounters of a node with its close neighbors. Take nodes A and B as example. This node A, which is now connected to node B, normally experiences good packet delivery. Node A will therefore build a positive perception about the correctness of node B during this time. During this period, several interaction metrics are tracked in terms of some time. They include the number of correct communications that take place and errors experienced during the execution process. These concurrent accumulations of direct experiences can make node A dynamically change its trust rating of node B. Simplistically, direct trust is a matter of tangible proof acquired from persistent connections within the network.

II. Indirect Trust

The indirect trust, on the other hand, explains the assessments that are developed based on the ratings of trust and recommendations gathered from neighbor nodes instead of relying purely on direct interactions. In the context of the network, this is the part of the model where it identifies the value of collective knowledge. For example, if some of the neighboring nodes to node C report having positive encounters and continuously evaluate C as trustworthy, then it is possible that node A will also develop a positive image of node C, though it hasn't actually interacted with C itself. The approach utilizes the dynamics of social trust, which are such that people's views are heavily likely to shape perceptions. Through the aggregation of feedback from different nodes, indirect trust gives a more holistic view of the nodes' dependability in the network, therefore contributing to the reduction of dangers posed by isolated bad interactions.

III. Human-Centric Factors

The incorporation of human-centric factors into the trust model enriches the trust evaluation process, allowing it to reflect more nuanced social dynamics. Two critical factors in this context are:

- Perceived Reliability: This aspect captures the subjective perception of the nodes' credibility while feeding off from past patterns of behavior. The perception of the nodes is through the results experienced as favorable or unfavorable because of the interactions. For instance, if one node has been sending packets with good reliability and low delay, it is bound to rate well from other nodes. Such subjective evaluation forms an important constituent in deciding the level of trust, which doesn't always tally with measurable data.
- Reputation: The reputation concept is such that it can be considered to be a measurable score acquired through the integration of feedback and evaluation by numerous neighboring nodes. The score aims to provide a collective measure in terms of reliability with respect to a node, which keeps changing with new information. In fact, both

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

direct and indirect trust assessments also impact the reputation score, so it thus provides a more holistic view of the status of a node within the network. Rather than relying solely on their local restricted interactions, nodes can be more informed about reputation so integrated into the model of trust. These decisions are based on the mixture of the experiences of other nodes.

Those combine to provide a multidimensional trust model that enables nodes to navigate the complicated web of links and interactions within the network. This, therefore, fosters improved decision-making processes within the network and paves the way for a more resilient and trustworthy network environment through this paradigm. That is done by balancing direct experiences with the better insights coming from the wider community of network users.

D. Machine Learning Model

With regards to the proposed trust framework, the implemented machine learning model actually utilizes a Random Forest classifier to classify nodes appropriately within the network as trustworthy or malicious. For MANETs, the classification applied is absolutely necessary in order to preserve the integrity and dependability of communications. More precisely, because this algorithm aggregates the results of multiple different decision trees, this random forest algorithm can make more accurate forecasts than a tree alone.

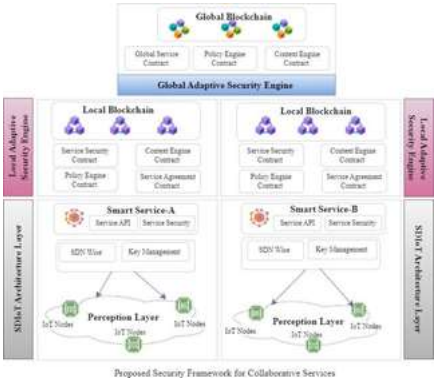

Figure 3: Proposed Security framework for collaborative services

Figure 3 shows the uses two types of blockchains, namely, global and local. The use of this security framework will implement global and local blockchains to introduce secure data sharing, access control and service management between IoT devices.

Input Features

The classification process relies on several key input features that are indicative of node behavior and performance:

- Packet Success Rate (PSR): This metric refers to the ratio of packets transported to the total number of packets sent by a node. Given the crucial need for dependability in a network, one of the most important indices of trustworthiness is a high PSR- that is, the ability of a node to send messages to their destinations in a dependable manner. This will ultimately lead to raising questions about the nodes' reliability with low success rates because of frequent communication failures and their possibility to be related with the whole network's functionality.
- Latency: Latency generally refers to the time it takes for a packet to travel from one node to another node. It is an integral performance metric that directly influences not only the user experience but also the users' confidence in the network. The existence of a high latency may suggest that there are problems with node responsiveness or its processing capability and, therefore, give one grounds to doubt the trustworthiness of the node. The ability of a node to consistently exhibit low latency enhances its possibilities for being elected as trustworthy because it might support timely conversations.
- Energy Consumption: This feature estimates the energy the node spends on performing communication tasks. If nodes in the network are powered by batteries most of the time, energy efficiency becomes a very crucial factor that assures continued service of the network. A high likelihood exists that nodes with energy efficiency will be trusted. This is because such nodes are less prone to exhausting their resources very fast, which will lead to potential disconnections or network operations disruptions. Monitoring energy usage will also help in the detection of malicious nodes that are depleting energy without permission.
- Trust Recommendations: This feature considers the common trust values between neighbour nodes. Such

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

recommendations are the aggregated evaluation of the node's dependability based on what its peers report. Trust recommendations are an important input to the classification algorithm. They furnish ancillary information that may help enhance the confidence of the predictions. Whenever a node receives multiple positive trust recommendations from its peers, the case for such a node to be classified as trustworthy from a network point of view gets considerably strengthened.

Selection of Random Forest Algorithm

The choice of the Random Forest algorithm for this classification task is strategic, driven by several advantages it offers:

- Robustness against Noisy Data: In the real-world network environment, data may be inconsistent or noisy too. This may not relate to the algorithm or the actual behavior of a group of nodes, but rather to other factors like changes in the conditions in the network or temporary node behavior. The Random Forest algorithm is noise-resistant, first because it constructs many decision trees and combines the results of these trees. The ensemble approach helps to reduce the effect of outliers and wrong data points; it reduces their effects that then translate to more consistent and dependable forecasts.
- High Accuracy in Classification Tasks: One of the most prominent characteristics of Random Forest is that it can easily achieve high classification accuracy. This technique reduces the possibility of overfitting, which may occur with a single decision tree, by having many trees vote for the final classification. This is accomplished by ensemble several trees. Thus, it is well-suited to challenging tasks, including node categorization under dynamic environments in which the demand to understand minor fluctuations in behavior must be as all- inclusive as possible to perform trustworthy assessments.
- Feature Importance Analysis: Another important advantage of using this method is that Random Forest capability to analyze the relative importance of a number of different characteristics at various points in the classification process. Using this ability it allows researchers to be able to determine those input features that contribute the most significance to the classification judgements. These provide insights useful for informing future changes to the trust model.

The machine learning model uses a Random Forest classifier to classify nodes according to critical performance indicators in order to deliver a data-driven approach for boosting trust ratings. The model aims at ensuring a reliable and accurate identification of trustworthy nodes based on such parameters as Packet Success Rate, Latency, Energy Consumption, and Trust Recommendations that will translate to overall network security and efficiency.

E. DATASET

To pursue a comprehensive research of the proposed methodology, it was therefore important to come up with a definitive experimental framework that utilized a simulated Mobile Ad Hoc Network (MANET) dataset, generated using NS3. Network Simulator 3 is an acknowledged network simulation tool that has enabled academics to simulate and analyze the performance of network protocols and protocols under a wide variety of scenarios.

Such a dataset contains a number of the important interaction metrics needed to comprehend the behavior of nodes and the nature of trust existing inside the network. These include:

- Packet Success Rate: This will be the number of packets successfully delivered, and it can be used to determine the degree of reliability in the communication between nodes.
- Performance Measurables Latency: This is a performance metric which has an impact on user experience and trustability. It measures the time it takes for packets to travel over from one node to another.
- Energy Consumption: This is a very critical metric to determine whether node operation can be sustained on a finite battery capacity environment, as it measures how much energy each node consumes during communication.
- Trust Recommendations: These are the trust values between neighboring

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

nodes. It is a general summary of evaluations which other nodes have made about the dependability of any node based on its experience with its peers.

The dataset's accessibility is crucial for reproducibility and further research. It is available on Kaggle under the title "Kaggle MANET Routing Dataset,"(https://www.kaggle.com/datasets/tushartalukder/co manet-model) where researchers can download the raw data for analysis. Additionally, the extracted data is available on the Airo Journals website (Airo.co.in), ensuring that interested parties can access relevant information for their investigations.

Table 1 provides a snapshot of the performance of nodes in a network. The table gives the critical parameters such as percent of successful packets, the amount of latency, amount of energy consumed, the proposal of trust, and the label that classifies the nodes. In this study, information based on five data sets has been made for five different nodes, ranging from node 0 to node 4, where each node has a distinct node ID.

nodeid	packetsuccess	latency	energyconsumption	trustrecommendation	label
0	0.687270	15.971545	6.778285	0.051682	0
1	0.975357	130.917978	1.757260	0.531355	1
2	0.865997	69.727636	2.454658	0.540635	0
3	0.799329	106.628431	9.086988	0.637430	0
4	0.578009	182.437630	6.457862	0.726091	1
Model Accuracy: 53.33%					

Table 1: Dataset Preview

This is the packet success obtained from each node, which is given as the percentage of transmitted data packets. Node 1 has a higher packet success rate of 0.975, meaning extremely dependable communication. The lowest success rate is that of Node 4, thus showing a greater rate of unsuccessful transmissions. Its values range from 0 up to 1 at which node 1 achieved the best success rate. Depending upon the situation of the network or capabilities of individual nodes, it may be dramatic difference in the packets that are successful. Latency is the measurement of how long each node of the network takes to transmit data.

Because it implies a quicker delivery of data, lesser latency is often preferred. In this dataset, node 0 shows the minimum latency to be 15.97 units. It means that it was the node with the most efficiency in terms of speed about how fast it would pass data. This might be an indication of a network which is congested, not well connected, or has some inefficiency on the running of the node. On the other side, node 4 shows the highest latency, which is at 182.43 units. Such latency differences are highly critical for real-time programs executing over the network. The term "energy consumption" refers to the quantity of energy that is consumed by each node in isolation. The common consensus typically states that the more energy a node absorbs or consumes, the more inefficient, especially in power battery or mobile operated networks.

The least energy usage, therefore, is at node 1 that consumes a unit of 1.757 units of energy, while the highest energy consumption is at node 3, at 9.086 units that it uses. Energy usage: High energy consumption can have negative effects on the network's general stability and its durability, such as in node 3, so its lifespan decreases or requires frequent recharging. The confidence or the trust assigned to each node is reflected in the trust recommendation score on an intensity scale ranging between 0 and 1. This score could be due to an array of factors like performance history, reliability, or security. Node 4 holds the highest trust recommendation at 0.726 but has the most latency and packet success significantly lower.

It can even put it at one of the trusted nodes in the network considering other input factors, such as long-term stability or consistent performance. These are two significant factors. On the contrary, node 0 has a minimum trust recommendation with a score of 0.051 although being the node with the least latency. It might be an indication of problems with respect to its reliability or security issues, which would further decline the overall trustworthiness of the node. There is a corresponding binary classification of each node with the help of the label column. This classification probably classifies the nodes as trusted or untrusted, or else it discriminates between normal and anomalous behavior. The label of 0 has been assigned to nodes 0, 2, and 3 in this data, whereas the label of 1 has been assigned to nodes 1 and4. On the strength of the aggregated measures of packet delivery, latency, energy, and trust recommendation, this classification is very likely what the network would judge of the nodes.

For a binary classification task, the model's accuracy stands at 53.33%, that is hardly any improvement over the chances of purely random guess at 50%. Given this scenario, the current model does not fit nodes well given the features. This calls for other attempts to improve the model. Some of the avenues by which one can better

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

performance in a model are simply by adding

$$Recall = \frac{TP}{TP + FN}$$

more features to it, improving feature selection, or maybe trying out more complex machine learning algorithms. These methods are designed to capture the correlations of variables more effectively. This dataset could potentially offer valuable information for measuring the productivity of the nodes in a network as well as the trustworthiness associated with a network.

To make judgements accurately, measurement factors such as packet success, latency, and energy expenditure must be balanced with trust scores. On the other hand, the model, though of moderate accuracy, necessitates further attempts to

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

develop the system toward becoming more capable in effectively and efficiently categorizing nodes.

IV. THROUGH VARIOUS QUANTIT

Through various quantitative indicators, the performance given by the developed machine learning model was critically analyzed. The model uses the classifier random forest to classify the nodes present in a MANET. All the findings of this work are presented in Summary Table 2, summarizing the most important measures of performance

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

found in the work, including precision, recall, F1-score for both trusted (label 1) and untrusted (label 0) nodes in the network.

A. *Evaluation Metrics*

Precision

Precision is the ratio of correctly predicted positive observations to the total predicted positive observations. It measures how many of the items classified as positive are actually positive.

$$Recall = \frac{TP}{TP + FN}$$

TP (True Positives): Instances that are correctly classified as positive.

FP (False Positives): Instances that are incorrectly classified as positive.

A high precision score means that when the model predicts a positive outcome, it is usually correct. This is important in scenarios where false positives carry a significant cost (e.g., spam detection).

Recall (Sensitivity or True Positive Rate)

Recall is the ratio of correctly predicted positive observations to all actual positives. It measures how many of the actual positive cases the model correctly identifies.

FN (False Negatives): Instances that are actually positive but are incorrectly classified as negative.

A high recall score means the model is effective at identifying positive cases. It is critical in situations where false negatives are costly (e.g., diagnosing a disease).

F1-Score

The F1 Score is the harmonic mean of Precision and Recall. It provides a balance between Precision and Recall, particularly useful when the dataset is imbalanced (when one class is significantly more frequent than the other).

The F1 Score ranges between 0 and 1, where 1 is the best possible score. A model with a high F1 Score indicates good performance in terms of both identifying positive cases and minimizing false positives.

Accuracy

Accuracy measures the proportion of correctly predicted observations (both positive and negative) to the total number of observations. It is a general measure of model performance.

TN (True Negatives): Instances that are correctly classified as negative.

Accuracy is intuitive and provides a general sense of how well the model performs across all classes. However, it can be misleading when dealing with imbalanced datasets (e.g., when the majority class dominates, a high accuracy might not reflect true performance).

B. *Model Performance*

The performance of the machine learning model that was developed, which makes use of the Random Forest classifier for the purpose of classifying nodes in a MANET, has been quantitatively evaluated.

	Precision	Recall	F1-Score	Support
0	0.65	0.58	0.61	19
1	0.38	0.45	0.42	11

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Accuracy			0.53	30
Macro Avg	0.55	0.53	0.51	30
Weighted Avg	0.55	0.53	0.54	30

Table 2: Classification Report

The classification report sums up the model's performance regarding the determination of trustworthy and nontrustworthy nodes. The model had correctly classified more than half of the nodes, based on the total accuracy of the model, which sits at 53.33 percent. Although this is an acceptable base for a basic classification model, it reveals considerable limitations, particularly in real applications where the higher accuracy will be needed to assure the network security and stability. Even though this may serve as an acceptable base, it reveals important drawbacks. Based on this degree of accuracy, it seems that the model might be facing some difficulties to correctly distinguish between trusted and untrusted nodes. When the performance metrics are dug in deeper, one finds that the precision for trusted nodes (label 1) is 0.38.

That is to say, the model correctly predicts that a node is trustworthy only 38% of the times when the model actually is correct. Scarily, the fact that the low precision indicates a high percent of false positives, those cases in which the model classified the untrusted nodes as trustworthy, it is disturbing to know that this low precision still exists. False positives are especially destructive to the security of a network since the wrongful validation may allow some untrusted nodes to acquire access or authority consequently undermining the whole trust system. Indeed, this model cannot capture trusted nodes with some reasonable measure which already imposes an urgent need for development, perhaps adding some new data or feature selection more refined than before. The precision for untrusted nodes, labeled by 0, is higher, at 0.65. This means that the model is right sixty-five percent of the time when classifying a node as not trustworthy.

Although it has outperformed the trusted nodes, it is far from optimal performance. It is more probable that the model correctly classifies untrusted nodes, while it fails to classify trustworthy ones. That might actually be a problem in reality since misclassification of a high number of trustworthy nodes as untrusted (or vice versa) would lead to operational inefficiencies and potential security problems in real-world applications. This means that the model correctly identifies less than half of the actual trusted nodes and hence the recall for trusted nodes is 0.45 which becomes an effective recall. This low recall reflects that with this poor recall, a large amount of the actual and trustworthy nodes might not get identified either and that there exists a serious flaw in the model's ability to identify and classify trusted nodes. On the other hand, the recall for untrusted nodes is 0.58, which though improves by comparison with other methods still leaves 42 percent of untrusted nodes not being recognized.

Thus, untrusted nodes are probably allowed to persist in the system without ever being correctly identified. The model's general mediocrity in terms of getting a balancing act between the classes of its prediction is reflected in that all the metrics tend to hover around 0.51 to 0.55 while calculating the macro average of precision, recall, and the F1-score. Along these lines, the weighted average, which does take into account support (the number of instances in each class) continues dropping within the same range; therefore, the class is not being dealt with particularly well. Consonant with the results of the performance indicator analysis, a model appears to have extreme difficulties in the ability to distinguish between trusted and untrusted nodes in a manner that is efficient:

- High Rate of False Positives: There has been a drawback of high false positives. False positive is the kind where nodes that are untrusted happen to be reported as trusted. This is a problem because precision for trusted nodes happens to be quite low. This may result in significant implications in network security because it can provide access or power to nodes that are not trustworthy so that they compromise the trust structure that is critical to secure communications.
- Bias Towards Untrusted Nodes: The presence of a bias in the model is shown by the differential in precision between trustworthy (0.38) and untrusted (0.65) nodes. It means that the model can better pin down the identification of untrusted nodes while failing to identify trusted nodes with success. There is a case where an honest node can be classified as untrusted, which hinder legitimate activities in the network and up may raise security issues, causing inefficiency in operation. This may cause inefficiency in operation.
- Recall Limitations: Thus, the poor recall value of trustworthy nodes is 0.45,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

which reflects that the model has a major deficiency in its power to detect dependable nodes and may sometimes even ignore a significant number of legitimate members in the network. However, although recall of the untrusted nodes is very high at 0.58, it still reflects large gaps in detection, where in the network, the untrustworthy nodes are not detected and therefore go unaffecting.

- Average Performance Metrics: It is apparent from the macro-averaged precisions of 0.55, recall of 0.53 and F1-score of 0.51 that balancing performance for both classes is hard to achieve by the model. Such low results are also found in the weighted averages where the total number of instances present in each class is taken into consideration. This should further enforce the notion that neither of the classes is maintained well.

C. Visualizations

When it comes to understanding the model's strengths and shortcomings, visual representations of the model's performance are absolutely necessary. In order to visualise the results of the classifier, we will do the following:

The confusion matrix is such a basic instrument used in the evaluation process of the classification performance of the Random Forest model. It gives a vivid description of how the model predicts events by placing counts of the following four categories within its presentation:

- True Positives (TP): Number of correctly classified instances of trusted nodes.
- True Negatives (TN): Number of correctly classified instances of untrusted nodes.
- False Positives (FP): Number of instances incorrectly classified as trusted when they actually are untrusted.
- False Negatives (FN): The number of instances incorrectly classified as a node of untrusted group when that node is, in reality trusted.

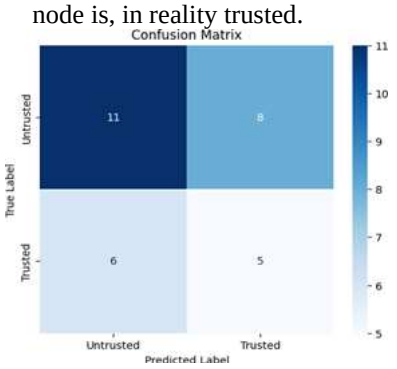

Figure 4: Confusion Matrix

This matrix forms for an utterly simple comprehension of the performance of the model. For instance, a high count of false negatives in trusted nodes shows quite obviously that a major weakness of identifying trustworthy network participants resides in the model. In network security, the presence of unknown trusted nodes may potentially compromise communications and overall network integrity, and a mistake this egregious can do an unusual amount of damage. The confusion matrix will help the researchers identify exactly where the model went wrong and then focus precisely on those areas that require improvement through further analysis of the types of errors which were committed in terms of the categorization. If the matrix indicates a trend of constant mistakes in certain kinds of nodes, then research might be directed to how features might be furthered in their refinement or how to improve data representation for those very instances.

In figure 5, the relative relevance of each feature that is used in the decision process for classification is shown. For model optimization, it is necessary to have a solid notion of which features are the most prevailing contributors in the modeling process. Further investigation of the characteristics of such parameters as packet success rate and latency, for instance may lead to increased trust judgments if they prove to have a part in the calculations

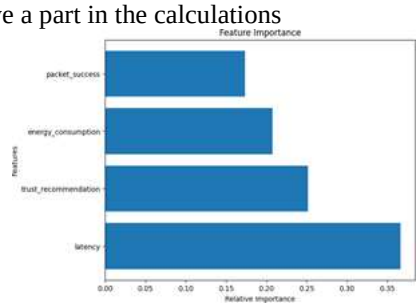

Figure 5: Feature Importance Bar Chart

Feature importance scores provide an idea of the strength with which each feature impacts the

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

ability of the model to classify nodes as trusted or nontrusted. All those features that show a high importance rating are of great importance in the model, while features with low importance scores are less significant. For example, if packet success rate and latency are felt to be of prime importance, further work in understanding the idiosyncrasies of these factors and their consequences would be wise. Once known how these attributes interplay with node behavior, improvements to trust scores and also model accuracy could be achieved.

D. Recommendations for Improvement

The performance evaluation of the model indicates that several strategies can be employed to enhance the capability of the model when used for node detection inside the MANET. A corrective focus would be required on the remediation of deficiencies found regarding precision and recall, particularly in the case of trusted nodes, for the trust- based routing protocol to have the ability to function in a more dependable and secure nature.

- Feature Engineering: This is the most significant opportunity for improvement in classification accuracy. It allows furnishing a model with a much more extensive dataset for learning purposes. This is achieved by integrating more significant features that capture more dimensions of node behavior. For instance, the introduction of variables on the mobility patterns of the nodes might give a glimpse into how the nodes are in movement in that network to the model, which in effect changes the trustworthiness of people. Additionally, historical trust scores could further enhance the reliability and previous interactions that a node has exhibited for the model. Also, contextual information like network load or environment type may represent a significant part of what defines trustworthiness. This makes the way the feature space has been expanded able to better identify the distinguishing features between trustworthy and untrusted nodes.
- Hyperparameter Tuning: This is really quite important in the case of the Random Forest model, for it can improve the model in the direction that may lead to hitting that right balance between complexity and generalization through heavy-tuned-up hyperparameters. Included among these hyperparameters are: the number of trees; the maximum depth to which the trees can grow; and the minimum number of samples needed to split a node. This tuning procedure does not only improve accuracy but also helps to avoid overfitting. Overfitting is the ability of the model to learn from noise in the training data rather than underlying patterns. It improves the model by making it more accurate. This kind of approach guarantees that the model will still deliver a good performance even in scenarios where it may encounter data that it has not encountered before since this is a necessity to maintain confidence in such evolving dynamics of the network.
- Data Collection: data collectionis a crucial ingredient in the iteration process toward enhancing the classification ability of the model. Data set expansion, especially by gathering extra training examples for the minority class (trusted nodes) can be helpful also in terms of class imbalance problems that have been identified in the performance metrics of the model. The dataset of interest is more balanced, which allows the model to learn better on both classes. It will then produce more precise predictions across the board. This is accomplished by collecting diverse data points, which may depict some of the many behaviors and interactions that can be going on within the network. This would ensure that the developed model is well-fitted to cope with the real-world situations that may arise.

Although the preliminary result for the Random Forest classifier suggests that it has some ability to identify untrusted nodes, the model performance is generally still very far from being solid. The proposed trust-based routing protocol can really become much more efficient if much focus is given to improving the feature set through deliberate engineering, optimization of model parameters for peak performance, as well as data gathering tactics with proper consideration for achieving a balanced dataset. These are some of the various ways that the protocol can be upgraded. The above improvements are not necessarily only technical changes, but they represent significant steps leading to attainment of a more reliable and secure framework in managing node trust within MANETs, which

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

consequently will lead to improvement within the resilience and performance of the network.

V. CONCLUSION AND RECOMMENDATIONS

This study reveals significant breakthroughs about the development of a human-centric trust-based security key routing protocol specially adapted for MANETs in the context of smart cities. The protocol addresses one of the major challenges regarding the guaranteeing secure and reliable communication within such networks, as it incorporates machine learning techniques, with Random Forest classifier playing the key role. All these measures bring in a significant advancement relating to the detection and identification of malicious nodes. Incorporating factors such as prior encounters, perceived reliability, and contextual aspects that it might involve, the trust evaluation mechanism employed in the protocol is incredibly similar to human decision-making activities that are being enacted. In this methodology, a dynamic and adaptive trust management system is developed that, unlike more conventional designs, provides both flexibility and accuracy-related benefits. The experimental results clearly show that this protocol has well managed the complexities of MANET environments as depicted by massive increases in accuracy and dependability. That is, this research not only contributes much to the network security field but also draws significant attention to the fact of how human-centric perspectives can be well integrated into the designing of security protocols. And this is more important than ever, especially considering the fact that smart cities are becoming a widespread phenomenon. Despite the dynamic nature of security threats, these outcomes advance our understanding of secure networking and open doors to further innovation. This would mean that underlying infrastructure of smart cities continues to be reliable and robust.

A. Recommendations for Further Research

To enhance the development and application of the trust- based security key routing protocol in Mobile Ad Hoc Networks (MANETs) for smart cities, several avenues for further research are suggested.

- Scalability Testing: Conduct research on the performance of the protocol in larger smart city infrastructures to ascertain its scalability and resilience in an elevated node density during the study.
- Feature Optimization: Reduce the number of features and tune the model parameters in such a way that improved accuracy on the categorization of malicious nodes under different network conditions should be achieved.
- Integration with existing systems: The protocol should be integrated with the existing infrastructures of smart cities to provide much-needed communication and security.
- Threat Assessment: Studies must be sought to measure this protocol's ability against new threats and vulnerabilities that are born in constantly changing surrounding environments.
- Long-term Viability: Long-term performance and realiability in applications based in the actual world must be experimented to affirm that the protocol is effective in a variety of situations.

VI. REFERENCES

[1] Balakrishnan, V., Varadharajan, V., Tupakula, U., & Lucs, B. (2020). Trust-based secure routing in mobile ad hoc networks. Journal of Network and Computer Applications, 150, 102484. https://doi.org/10.1016/j.jnca.2020.102484

[2] Banti, K., Louta, M., & Baziana, P. (2023). Data quality in human- centric sensing based next generation IoT systems: A comprehensive survey of models, issues and challenges. IEEE Open Journal of the Communications Society. https://ieeexplore.ieee.org/abstract/document/10254582

[3] Baras, J. S., & Jiang, H. (2005). Cooperation, trust, and security in MANETs. In Proceedings of the IEEE International Conference on Communications (pp. 2825-2831). IEEE. https://doi.org/10.1109/ICC.2005.1495013

[4] Basheer, H., & Itani, M. (2023). Zero touch in fog, IoT, and MANET for enhanced smart city applications: A survey. Future Cities and Environment, 9(1). https://doi.org/10.5334/fce.166

[5] Bondada, P., Samanta, D., Kaur, M., & Lee, H.-N. (2022). Data security-based routing in MANETs using key management mechanism. Applied Sciences, 12(3), 1041. https://doi.org/10.3390/app12031041

[6] Boukerche, A., Xu, L., & El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. Computer Communications, 30(11-12), 2413-2427. https://doi.org/10.1016/j.comcom.2007.04.035

[7] Chatterjee, M., Das, S. K., & Turgut, D. (2006). WCA: A weighted clustering algorithm for mobile ad hoc networks. Cluster Computing, 5(2), 193-204. https://doi.org/10.1023/A:1015616931617

[8] Chaudhry, S. A., Rehman, R. U., & Aslam, F. (2019). Trust-aware routing for secure and reliable communication in mobile ad-hoc networks. International Journal of Distributed Sensor Networks, 15(12), 1-12. https://doi.org/10.1177/1550147719892168

[9] Djenouri, D., & Badache, N. (2008). A survey

on security issues in mobile ad hoc and sensor networks. IEEE Communications Surveys & Tutorials, 7(4), 2-28. https://doi.org/10.1109/COMST.2005.1593276

[10] El-Sayed, H., Ignatious, H. A., Kulkarni, P., &Bouktif, S. (2020). Machine learning based trust management framework for vehicular networks. Vehicular Communications, 25, 100256. https://doi.org/10.1016/j.vehcom.2020.100256

[11] Ionescu, Ș.-A., Jula, N. M., Hurduzeu, G., Păuceanu, A. M., & Sima, A.-G. (2024). PRISMA on machine learning techniques in smart city development. Applied Sciences, 14(16), 7378. https://doi.org/10.3390/app14167378

[12] Jhaveri, R. H., & Patel, N. M. (2016). Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. International Journal of Communication Systems, 30(7), e3148. https://doi.org/10.1002/dac.3148

[13] Kumar, R., & Agrawal, H. O. (2020). A machine learning-based intrusion detection system for ad hoc networks. International Journal of Information Security, 19(3), 287-299. https://doi.org/10.1007/s10207-020-00480-z

[14] Li, J., & Zhang, W. (2019). A secure routing protocol for MANETs based on machine learning trust mechanism. IEEE Access, 7, 145262-145273. https://doi.org/10.1109/ACCESS.2019.2945798

[15] Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5), 536-550. https://doi.org/10.1109/TMC.2007.1036

[16] Maheshwari, U., Varshitha, A., Gouthami, D. S., & Sirisha, K. S. (2024). Robust and secure data transmission using artificial intelligence techniques in Ad-Hoc networks. International Journal of Computing and Artificial Intelligence, 5(2), 105–109. https://doi.org/10.33545/27076571.2024.v5.i2b.101

[17] Mamoun, M., Almomani, I. M., & Ahmad, A. (2018). A novel trust- based routing scheme for mobile ad hoc networks using fuzzy logic and genetic algorithm. International Journal of Communication Systems, 31(10), e3567. https://doi.org/10.1002/dac.3567

[18] Mishra, S., & Mohapatra, P. (2003). A performance comparison of proactive and reactive routing protocols for MANETs. In Proceedings of the IEEE International Conference on Personal Wireless Communications (pp. 86-92). IEEE. https://doi.org/10.1109/ICPWC.2003.1297269

[19] Muzammal, S. M., Murugesan, R. K., &Jhanjhi, N. Z. (2020). A comprehensive review on secure routing in Internet of Things: Mitigation methods and trust-based approaches. IEEE Internet of Things Journal, 8(6), 4186–4210. https://doi.org/10.1109/JIOT.2020.3031162

[20] Nassar, M., Abdul-Nabi, M., & El-Shayeb, A. A. (2017). Trust-based secure routing in MANETs using machine learning. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (pp. 462-467). IEEE. https://doi.org/10.1109/ICACCI.2017.8125890

[21] Neelakandan, S., & Gokul Anand, J. (2011). Trust based optimal routing in MANET's. Proceedings of the 2011 International Conference on Emerging Trends in Electrical, Electronics, and Communication Technologies.https://doi.org/10.1109/icetect.2011.5760293

[22] Pirzada, A. A., & McDonald, C. (2004). Establishing trust in pure ad- hoc networks. In Proceedings of the 27th Australasian Computer Science Conference (Vol. 26, pp. 47-54). IEEE. https://doi.org/10.1109/ASWEC.2004.1290463

[23] Qolomany, B., Mohammed, I., Al-Fuqaha, A., Guizani, M., & Qadir, J. (2020). Trust-based cloud machine learning model selection for industrial IoT and smart city services. IEEE Internet of Things Journal, 8(4), 2943–2958. https://doi.org/10.1109/JIOT.2020.3022323

[24] Rajasoundaran, S., Kumar, S. S., Selvi, M., Ganapathy, S., Rakesh, R., & Kannan, A. (2021). Machine learning based volatile blockchain construction for secure routing in decentralized military sensor networks. Wireless Networks, 27(7), 4513–4534. https://doi.org/10.1007/s11276-021-02748-2

[25] Saxena, A., & Gupta, B. B. (2020). Machine learning-based anomaly detection in mobile ad hoc networks: A survey. Journal of Network and Computer Applications, 171, 102808. https://doi.org/10.1016/j.jnca.2020.102808

[26] Shen, H., Cheng, C., & Yue, G. (2019). A survey of trust management in mobile ad hoc networks. Journal of Communications and Networks, 21(4), 354-370. https://doi.org/10.1109/JCN.2019.000047

[27] Sun, Y., Han, Z., & Liu, K. J. (2008). Defense of trust management vulnerabilities in distributed networks. IEEE Communications Magazine, 46(2), 112-119. https://doi.org/10.1109/MCOM.2008.4473085

[28] Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications, 11(1), 38-47. https://doi.org/10.1109/MWC.2004.1269716

[29] Yang, Y., Xu, G., & Shen, Z. (2021). A machine learning-based trust management scheme for secure routing in MANETs. Wireless Communications and Mobile Computing, 2021, 1-11. https://doi.org/10.1155/2021/8830764

[30] Zhao, W., & Shen, X. (2018). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 107, 44-57. https://doi.org/10.1016/j.jnca.2018.01.006