IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 17 June 2024, accepted 4 July 2024, date of publication 8 July 2024, date of current version 19 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3425153

RESEARCH ARTICLE

Blockchain-Based Trust and Authentication Model for Detecting and Isolating Malicious Nodes in Flying Ad Hoc Networks

KASHIF NASEER QURESHI[1], HANAA NAFEA[2], IBRAHIM TARIQ JAVED[3], AND KAYHAN ZRAR GHAFOOR[4,5]

[1]Department of Electronic and Computer Engineering, University of Limerick, Limerick, V94 T9PX Ireland
[2]Department of Computer Science, College of Computer Science and Engineering, Taibah University, Madinah 42353, Saudi Arabia
[3]Blockchain@UBC, University of British Columbia, Vancouver, BC V6T 1Z4, Canada
[4]Department of Computer Science, Knowledge University, Erbil 44001, Iraq
[5]Department of Information and Communication Technology Engineering, Erbil Polytechnic University, Erbil, Kurdistan 44001, Iraq

Corresponding author: Kashif Naseer Qureshi (kashifnaseer.qureshi@ul.ie)

This work was supported by the University of Limerick.

ABSTRACT Flying Ad Hoc Networks (FANET) is an emerging area of research due to its low cost, high coverage and fast transmission features. In these networks, the flying nodes are connected with ground stations and communicate wirelessly, especially when the networks are congested and complex. Due to mobility, and lack of predefined infrastructure, these networks have suffered from various security and trust issues. The traditional trust and security solutions are designed for ground networks and are not feasible for these networks. This paper proposes a trust and authentication model including Trust Establishment Mechanism for FANET (TEM-FANET) and authentication system by using Block-chain method. The trust is calculated to evaluate the node's trust status and ensure the existence of the trustworthy nodes by using direct, indirect, and cumulative trust values. Whereas the authentication system is utilizing blockchain technology for nodes authentication and evaluate its feasibility. The proposed model is lightweight and able to monitor the node's behavior and compute the trusted quality and broadcast the node status with neighbor nodes. The proposed model is also integrated with ground stations for record keeping and decision-making processes. The proposed model is evaluated in simulation with state-of-the-art trust solutions where the results show the better performance in terms of overhead, data delivery, node detection rate, and computational time.

INDEX TERMS Trust, evaluation, FANET, security, malicious, attacks, blockchain.

I. INTRODUCTION

Flying Ad Hoc Networks (FANET) have evolved from a single node operation to a group of nodes to accomplish a specific task. Drones or Unmanned Aerial Vehicles (UAVs) are used in these networks to monitor the networks by using sensing and communication technologies such as for traffic management, fire and disaster management, agriculture and remote sensing, monitoring, civil security, and other fields of life like military surveillance and civil areas monitoring [1], [2]. Over the past few years, these networks have gained popularity due to their flexible, cost-effective, and versatile features. In these networks, multiple nodes are wirelessly interconnected autonomously and expand operational scalability. Multi-drones are used to perform the monitoring by using the small radar cross-section compared to the large radar cross-section. These networks also provide a systematic distribution of nodes, large coverage, low-cost transmission services, and able to communicate with the Base Station (BS) on the ground [3], [4]. Furthermore, the nodes in these networks cover specific geographical areas and are more feasible for an emergency where normal network deployment is impossible. These networks improved the traditional field operations and processes such as defense monitoring, forming, firefighting, and transportation with help of an ad hoc network [5]. However, with various

The associate editor coordinating the review of this manuscript and approving it for publication was Arun Prakash.

benefits, these networks have suffered from security, trust, and privacy issues that can affect and degrade network performance [6]. Although FANET is similar to other ad hoc networks, few features make it different from other types of networks, like higher mobility of nodes, ample freedom of movement, three-dimensional (3D) rotation, dynamic topology, and moving in open space to locate easily. Short and long-range wireless technologies incorporate the FANET, including IEEE 802.15.1, IEEE 802.15.4, and IEEE 802.11 [7], [8].

Security is one of the requirements of these networks due to the open broadcast nature of nodes where the wireless channels make data transmission vulnerable and susceptible to various malicious attacks and activities [9], [10]. The active and passive attacks are performed for traffic monitoring and analysis, such as jamming, interference, and hybrid attacks. Furthermore, passive eavesdropping attacks are performed in multihop communication to overhear the broadcasted information. In addition, other common threats for FANET networks are spoofing, Denial of Services (DoS), Black-hole, Sybil, and hello flood attacks [11]. These attacks disturb, fabricate, and manipulate the data process in the network [12], [13]. As per the trust aspect, the node's behavior analysis is significant in identifying any malicious or selfish node. Therefore, trust management methods have been adopted to evaluate the trust of nodes by using the trustworthiness of nodes and detecting malicious nodes.

However, the existing trust evaluation solutions use any single or two factors, like direct or indirect trust to evaluate the node's trustworthiness. Most solutions have been developed for ground networks or fixed devices like cloud or edge servers [14], [15], [16]. This paper proposed a Trust Establishment Mechanism for FANET (TEM-FANET) to tackle internal and external attacks, monitor or judge the nodes, prevent the network from malicious nodes, and eliminate such nodes from the network. The proposed solution provides the best and most secure path to the drones for data combination. The detailed contributions of this paper are as follows:

- To calculate the trust values of the nodes and isolate the malicious nodes from the network
- To broadcast the node's status about malicious nodes in FANET and ground networks.
- To keep a record of malicious and untrustworthy nodes for future reference
- To authenticate the FANET nodes by using Blockchain technology
- The proposed TEM-FANET model is evaluated in terms of false positive rate, malicious nodes detection rate, data throughput, data delay and blocktime.

The rest of the paper is organized as follows: Section II presents the detailed literature review. Section III presents the proposed solution and its design and development phases. Section IV and V discuss the simulation results and discussion. The last section concludes the paper with possible future directions.

II. RELATED WORK

Authors in [6], proposed a Fuzzy-based novel trust model to handle the node's behavior and then classified the nodes using multicriteria fuzzy classification. The usage of Artificial Intelligence (AI) is also discussed to tackle security attacks and monitor the country's borders. The proposed solution also manages and predicts the disaster performed rescue operation to save lives and property and carry transportation. The proposed model is designed for FANET with two main features, including collaboration and cooperation, that help to perform their function in a different environment. The behavior of these two functions depends on the trust value of the nodes. Different trust-based proposed models have been designed based on different parameters to calculate the trust rate or value, especially for portable and mobile networks. The FANET network has different unique features compared to traditional ad hoc networks, such as the high velocity of the working node, which causes disconnection or link losses. These challenges also make these networks vulnerable and open to various security attacks. The proposed fuzzy novel-based technique handles these networks' unexpected outcomes by applying multicriteria fuzzy features in a complex network. However, fuzzy methods are difficult and more feasible for fixing device networks with more resources and processing capabilities.

In [17], the authors proposed a novel trust model by using a genetic algorithm for trust evaluation. To provide secure data communication and trust evaluation, the authors designed the trust model by using a genetic algorithm and minimized the weight of different values-based parameters to check the direct trust values of nodes for secure data communication. Direct trust is aggregated with the recommendation to evaluate the final trust values of nodes. After this, all nodes that produced the trusted values come under one group or class, and the others that produced the variant values come in the risky class and assessment based on risk assessment class. If a malicious node is found, it can easily separate from regular nodes by using this direct trust list. However, more than the direct trust evaluation is needed to calculate the trust of nodes because indirect and cumulative trust is important, especially in FANET networks.

In another study [18], the authors proposed a trust evaluation model for FANET networks. The proposed model is designed by using the lightweight and efficient trust mechanism for secure data communication. The nodes formed a secure self-organized network and facilitated the users with different applications. Security and trust are the major challenges due to the open nature of these networks. These networks need more resources for processing power, battery, and coverage. The attackers easily enter the network and make a node untrustworthy to imitate the attacks in the network. Different types of trust and security solutions have been designed to address security and trust matters. However, the traditional solutions are different from FANET's special requirements. The proposed solution is designed to consider all special characteristics of FANET nodes by using trust and

stable values of nodes. The proposed solution is evaluated in terms of data delivery ratio and node detection. However, with many benefits, these types of mechanisms have limited features and can only handle part of the network due to the distance between nodes and the dynamic and unpredictable topologies of the networks.

Authors in [19], designed a Trust Based Clustering Scheme (TBCS) by using the clustering technique for secure data communication. The coordination and cooperation among nodes are considered an evaluation criterion by adopting the trust concept. The trust is evaluated based on internode organization and collaboration for balance and better data flow. The interaction between nodes is based on the trust evaluation results of nodes. The proposed solution distinguishes the node's incompatibility and interruptions to improve the data reliability. The proposed scheme builds the node group or clusters with faith. The proposed scheme uses various methods of sorting in a vague and complex environment. The rewards and discipline help change the node's structured trust and distinguish malicious and intrusion nodes in FANET. In addition, a safety team leader is selected based on the trust value and is responsible for the trust evaluation of control units, data communications, and groups. The simulation results indicated better performance of the proposed scheme. However, the proposed process is complex due to cluster head election, selection, and then trust calculation among nodes.

Authors in [20], proposed a unique Cumulative Trust analysis-based economical Technique (CTBET) by focusing on various viewpoints on the implementation and governance of safety in edge-based IoT networks. The projected CTBET is designed based on the cumulative trust concept and direct and indirect trust values among the available paths between the sender and the recipient nodes. The proposed technique focused on the packet transfer rate and drop rate among transmission nodes and then calculated the direct and indirect trust among corresponding nodes. The proposed solution implemented trust and ensured network security. The most common attacks considered by the proposed scheme are on-off, Denial of Service (DoS), and Bad-Mouth attacks. However, the proposed scheme can isolate malicious nodes from the network. However, this technique is designed for IoT networks, whereas the FANET networks are different compared to IoT networks.

Authors in [21], adopted a blockchain-based method to ensure network security. The blockchain is a decentralized mechanism to secure the network from any kind of malicious nodes. This method protects the network and ensures data security from unauthorized and malicious node activities. The blockchain decentralized method ensures the security of the network and protects the network from security breaches. The proposed solution is also able to handle the ground stations when notified by the network with any node tempering detection. The simulation results indicated that the proposed solution performance is better due to its smart contract deployment strategy in the Ethereum network. The proposed solution can tackle different security attacks, including gray hole attack, data interception, and black hole attack. The proposed solution is also detecting false information broadcasting. These attacks degraded the network performance and injected false information. The simulation results indicated the better performance of the proposed solution in the UAV network. Although the proposed solution handles different attacks, a different response system is needed for each type of attack in the network.

Authors in [22], proposed a Drone Assisted Internet of Vehicles (TPDA-IoV) for data routing, drone nodes, and trust evaluation. The proposed solution is based on three modules: drone communication, drone-to-vehicle communication, and trust evaluation. The proposed solution is to work with flying and ground zones and ensure nodes' trust by using a route discovery strategy. The trustworthiness is evaluated by using the packet evaluation metrics. Based on the drone's behavior, the trust value is calculated by the increment and decrement of trust values. Each drone node is responsible for calculating the trust value of neighbor nodes. The proposed solution uses request packets for trust evaluation. The experiment results indicated the proposed solution's better performance than existing solutions. However, this work needs to include the most important results regarding malicious node detection and false positive rate. Table 1 shows the discussed solutions key features and limitations.

After a detailed discussion in the literature, it is concluded that the existing trust evaluation solutions are based on direct or indirect trust factors to evaluate the node's trustworthiness. It is also noticed that several existing solutions are designed for IoT backbone networks or edge and cloud networks. FANET is a demanding area of research due to its flexible features and coverage, especially in congested networks. Security is always a top priority due to the FANET node's movement and flying strategies. The drone-to-middle method has been observed in these networks where one malicious node disseminates fake information or engages the network using malicious activities. Therefore, there is a need to design a trust-based solution to handle internal and external attacks to evaluate and protect the network.

III. TRUST AND AUTHENTICATION MODEL FOR FANET

In this section, the proposed trust evaluation model design and development phases discuss in the detailed process. The proposed model calculates the trust value of drone nodes and finds the more trustworthy routes for data forwarding. The trust model identifies the malicious or selfish node status in the network and updates the status in the network. The proposed trust model contains four main phases including the attack model, trust analysis model, and trust decision model. The first attack model is used to initiate the internal attacks to identify the selfish and malicious nodes. The trust decision model is used to analyze the node's behavior and store all the data for further analysis. All the recorded data is further forwarded towards the trust decision model to rectify and identify the malicious and selfish nodes in the network. This model is also useful to decide the trustworthy path for

TABLE 1. Existing solutions key features and limitations.

Approach/Model	Key Features	Limitations/Challenges
Fuzzy-based trust model [6]	Multicriteria fuzzy classification Incorporation of AI for security Disaster prediction and rescue operations	- Fuzzy methods may be resource-intensive - Challenges with high velocity nodes in FANET networks
Genetic algorithm-based trust model [18]	Genetic algorithm for trust evaluation Direct trust aggregation Differentiation of nodes based on trust	- Limited evaluation of indirect and cumulative trust - Complexity in calculating trust for FANETs
Lightweight trust evaluation model [19]	Efficient trust mechanism Consideration of FANET characteristics Evaluation based on data delivery ratio	- Limited coverage due to dynamic topologies - Challenges with resource constraints in FANETs
Trust-Based Clustering Scheme (TBCS) [20]	Clustering for secure communication Trust-based node organization Rewards and discipline mechanism	- Complexity in cluster management - Challenges with trust calculation among nodes
Cumulative Trust analysis-based Technique (CTBET) [21]	Cumulative trust concept - Focus on packet transfer rate and drop rate Isolation of malicious nodes	- Designed for IoT networks, not specifically FANETs - Limited discussion on performance metrics
Blockchain-based security method [22]	Decentralized security using blockchain Detection and handling of various security attacks Smart contract deployment	- Need for specific response systems for different attacks - Potential complexity in implementation
Drone Assisted Internet of Vehicles (TPDA-IoV) [23]	Utilization of drones for data routing and trust evaluation Incremental trust calculation based on behavior Better performance in experiments	- Need for further evaluation on malicious node detection - Lack of discussion on false positive rates

data communication in the presence of an attack model. After completing the process from three models, the next and last process is broadcasting the malicious nodes updates in the network. All the information is stored in routing tables for reliable and feasible data communication. Figure 1 shows the proposed trust model's four modules.

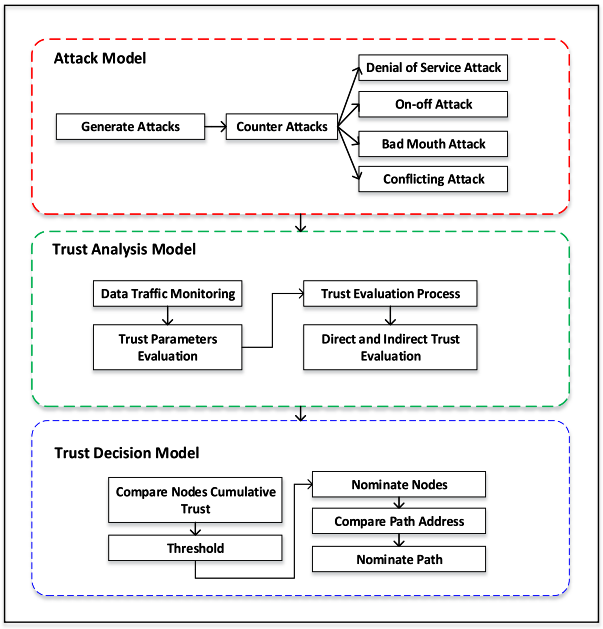

FIGURE 1. Trust model for FANET.

A. ATTACK MODEL

For the attack model, three well-known attacks are considered, including bad mouth, Denial of Service (DoS), and on-off attacks. The malicious nodes generated a volume of data to engage the network and create overhead and burden. These attacks are developed and keep all records and track the data forwarded or received [23]. The bad-mouth attack generates incorrect values and information related to the neighbor nodes. This attack records the track of packet dropping, delay processes, and other communication parameters [24]. The on-off attack checks the node's behavior and then forwards the incorrect information to the network. The selfish nodes are behaving well or sometimes badly. These attacks are handled using the trustworthiness, network lifetime span, packet drop, and packet rate parameters [25], [26].

If the network is under attack, the flying nodes are modified and generated, falsifying the incorrect data. This process degrades the network performance, causing a packet drop, energy depletion, and overhead. These attacks are generated in this module to check the proposed model processes and performance [27]. This attack model is assessed and evaluated by the network nodes. This model also refutes the data transmission towards the network with multiple and continuous packet generation. Three states are considered to check the node behavior if the node rate is less than 0.5, so it considers the malicious node. The second state is node dropping rate analysis with 0.5 greater value or equal to 0, which is considered a selfish node. Another state is a node good or bad behavior measurement with a value greater than 0.5 and considered a malicious node. In Equation 1, the Flying Node (FN) behavior denotes FN(n) as a random variable. Therefore, the node misbehaves transmission in the

attack model presented in Equation 1.

$$FN(n) = \begin{cases} 1, & if\ n\ relays\ packet \\ 0, & if\ n\ drops\ packet \\ -1 & if\ n\ compromise\ packet \end{cases} \quad \text{where } n \in N \tag{1}$$

The attack model generates false information from flying nodes and makes them malicious to evaluate the trust values among nodes.

B. TRUST ANALYSIS MODEL

This model evaluates the nodes by monitoring the node's records and behavior. A packet profiler is maintained at every node to check the node behavior by evaluating the packet traffic. The data traffic is evaluated based on data received and drop rate, direct and indirect trust evaluation. This model provides a detailed evaluation of selfish and malicious node traffic and helps to select the trustworthy path for data communication. The first phase is flying nodes trust evaluation of adjacent nodes by adopting the direct and indirect trust calculation. The result of this calculation is in the form of cumulative trust of nodes where all records are stored at each flying node. The direct trust evaluation is calculated by using different parameters such as packet receiving and transmission probability. The threshold values are calculated based on Packet Sent Time (PST) and Packet Received Time (PRT). If the node fulfilled the criteria and successfully transmits the packets and received the packets, then it considers trustworthy. If the Packet Send Ratio (PSR) is greater than or equal to its mean the node is trustworthy. Direct trust is also considered based on local knowledge evaluation. Indirect trust evaluation is calculated based on recommendation information coming from other trusted flying nodes. The indirect trust is set up between two nodes that have less associated such as lack of information about neighbor flying nodes and direct trust score.

After positive verification, both the direct and indirect trust, both values are considered for the cumulative trust value of flying nodes as shown in Equation 2. For the cumulative trust value, the direct and indirect trust values are combined.

$$Direct\&Indirect\ Trust = \frac{Direct\ TrustFN + Indirect\ TrustFN}{2} \tag{2}$$

Figure 2 shows the direct and indirect trust calculation process among UAV nodes. The calculated value is stored in new packet format to avoid any extra overhead and computational complexities. The existing solution has been suggested the cluster or aggregation-based methods. But these methods consume extra energy and cause overhead in the network. These methods generally require partitioning the nodes in the network into clusters whereby each cluster has a designated cluster head (CH) who is responsible for the collection of data and forwarding of information to other clusters or a central controller. Though the applications of

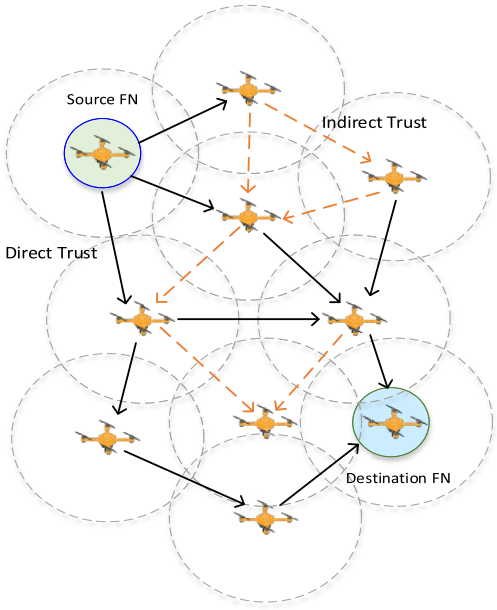

FIGURE 2. Direct and indirect calculation among FN nodes.

these strategies include such advantages like scalability, load balancing, and decrease of data duplicating, they have their drawbacks. Interestingly, the CHs always work more and therefore, consume more energy than the other nodes in the network; the formation of clusters and maintaining the clusters also involve some extra communication load and computational cost. Furthermore, if the CH role is not being rotated effectively, then some nodes energy will be expended more as compared to the others leading to the formation of imbalances in the network. While using aggregation-based methods helps to decrease the amount of data transmitted as well as optimize bandwidth usage, it increases the overall energy requirements for the data processing, and could lead to the problem of latency. Additionally, nodes that engage in the aggregation process may become overloaded and, therefore, create points of failure.

C. TRUST DECISION MODEL

In this model, the trust evaluation decision is initiated by broadcasting the cumulative trust message in the network. The cumulative trust value is updated by using the data message with two new fields including the neighbor FN identity and the opinion of the sender about the neighbor as indirect trust. The cumulative value is updated if any FN observed that the neighbor FN is an untrusted node then it will set that node value <0.5 for untrusted FN and >0.5 for trusted FN value. The cumulative trust value message format shows in Figure 3.

When all FN nodes transmitted the data with a trust score. When the network is updated with trust values of FN then the packet transmissions started by using the best data route. As shown in Figure 4, where the Source-FN and Destination-FN forward the data in the presence of malicious and selfish nodes and are successfully eliminated from routing tables.

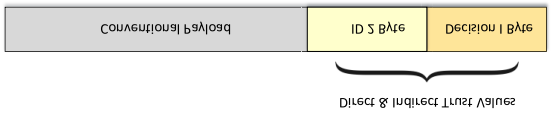

FIGURE 3. Recommendation packet format.

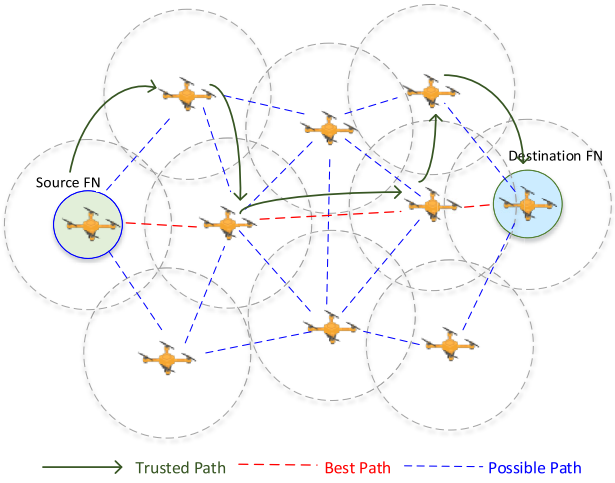

FIGURE 4. Illustration of trusted path selection and data transmission.

FIGURE 5. Flow chart of TEM-FANET.

The routing table is updated with all node's statuses. Figure 4 shows the trusted path calculation for data transmission.

The proposed solution caters to the false positive ratio or incorrect recommendation information and calculates the trust values by using direct and indirect trust. The trust evaluation value is based on different communication parameters including packet drop rate, packet received rate, and time analysis. The flow chart of the proposed TEM-FANET shows in Figure 5.

In the flow chart, the routing process is initiated where the nodes check the best and preferable path for data routing from source FN to destination FN. After selecting the node, the next step is trust calculation where the direct and indirect trust is evaluated for cumulative trust value. After this process, the threshold process initiates and if FN is under threshold, then the node is marked as normal otherwise considered malicious. All steps are repeated until all paths are calculated in terms of the trust. In last, the most trustworthy path considers based on cumulative trust and updates with source and destination FN. The malicious nodes are eliminated from the network and updated the network about the status of the node.

D. BLOCKCHAIN-BASED FANET AUTHENTICATION SYSTEM

In this section, we propose a blockchain-based authentication system for FANET networks. Authentication and verification of FANET nodes are crucial for the network's security and trust. Traditional identity management systems often face challenges in the dynamic and open network of FANETS. We propose the integration of blockchain technology into FANET for robust identity management. The proposed system leverages the immutability and decentralization features of blockchain technology to establish and manage node identities securely.

We choose to implement the FANET authentication system using a consortium blockchain. The consortium blockchain offers advantages in terms of privacy, performance, and scalability when compared to the public blockchain. Consortium blockchain provides a trusted environment with regulated access protecting sensitive authentication data. It further provides faster, more efficient transaction processing to enable reliable access within FANETS networks. We choose Ethereum to deploy a consortium blockchain over other alternatives like Hyperledger, Quorum and Corda. Our selection of the Ethereum network is based on two factors. Firstmost, Ethereum supports solidity-based smart contracts that empower us to create highly customizable and programmable authentication processes while using well-established authentication token standards. Furthermore, Ethereum offers interoperability with the public Ethereum blockchain that allows secure data sharing and asset transfers to other applications running over the public blockchain. We chose the Proof of Authority (PoA) consensus mechanism, also known as Clique for the FANET authentication system. PoA offers efficiency low latency, and controlled governance, making it well-suited for implementing authentication systems in FANETs. PoA strikes a balance between efficiency and security by relying on trusted identities for network validation, ensuring enhanced security in FANET environments. Its low-latency transaction processing is crucial for real-time communication needs in FANETs, while its minimal resource requirements make it energy-efficient

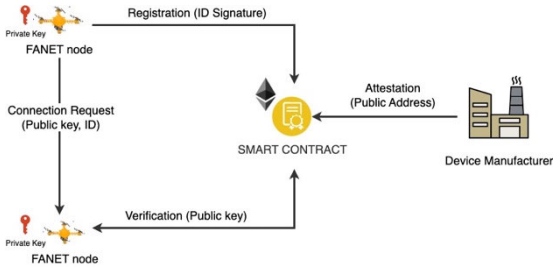

FIGURE 6. System overview: blockchain based FANET authentication system.

for resource-constrained networks. The system overview of the FANET authentication system is presented in Figure 6.

The smart contract is deployed over the Ethereum PoA private blockchain and comprises four essential functions:

a. **Registration:** The registration function is used to register the identities of new FANET nodes.
b. **Verification:** The verification function is used to verify the authenticity of the identity of the FANET nodes.
c. **Attestation:** The attestation function is used by the manufacturer to provide attestation of their FANET nodes.

In the FANET network, new nodes register themself using the registration smart contract. Before registration, each FANET node is assigned a public-private key pair. The public key is used to generate a public address which identifies the node over the blockchain. The private key is used to sign transactions. The FANET node initiates the registration process by calling the registration function and uploads the signature of the device identifier along with the required identity information. The signature contains the encrypted hash of the identity information using the node's private key. After registering the FANET node can send connection requests to the network. This request includes the user's public key and identity information. The received FANET node verifies the identity by calling the verification function. It downloads the signature and validates that it belongs to the sending FANET node. By using the verification function the receiver also receives the attestation from the manufacturer.

IV. EXPERIMENT RESULTS

This section discusses the simulation and experiment setup to test and evaluate the proposed scheme TEM-FANET in terms of trustworthiness with time, malicious nodes detection, detection accuracy, packet delivery, packet delay ratio, and network lifetime. The proposed scheme is evaluated in a well-known OMNET++ open-source simulator [28], [29]. This simulator is one object-oriented integrated discrete event simulator with a graphical user interface. The simulator is specially designed for traffic modeling and protocol testing. The simulation is also suitable for trust evaluation due to its diverse descriptive features and support for various kinds of security attacks. The FN are randomly deployed in the network, whereas the total area of the network is around 15 X 150 meters. The FN communication range is around 20 to 30 meters. The malicious nodes are created in the network by using the network attack model. The simulation parameters are presented in Table 2.

TABLE 2. Simulation parameters.

S#	Parameters	Values
1	Network Size	150m x 150m
2	Time	100 to 1000 second
3	Node Deployment	Random
4	Data packet Size	50 bytes
5	Data Traffic Load	CBR
6	Traffic Type	CBR
7	Agent Type	UDP
8	Routing Protocol	AODV
9	Physical Standard	IEEE 802.15.4
10	No of Nodes	20, 40, 60, 80, 100
11	Initial Power	100 J
12	Queue Type	Drop Tail

A. ADVERSARY MODEL

An adversary model is used for security analysis and evaluating the overall system security. This model is utilized for this research to access the potential threats and identifying the vulnerabilities in the system. We used SEA++ (Environment, and Adversary) framework with OMNET++ to evaluate the security attacks. The SEA++ framework extend the OMNET++ framework to check the security attacks in the network. For the adversary part, three well-known attacks are considered, including bad mouth, Denial of Service (DoS), and on-off attacks. The malicious nodes generated a volume of data to engage the network and create overhead and burden. To assess the attacks impact, the attack model already discussed in proposed model section. The SEA++ uses the high-level description for attacks evaluation by using attack specification language and generate the single *adl* file. The attacks description results in this file are further store in database and interoperate by using Python script and then run the simulation.

To evaluate the proposed scheme, the different performance evaluation parameters are level of trustworthiness, detection rate, detection accuracy, false positive rate, network lifetime, average throughput, and delay analysis. The level of trustworthiness refers to the accurate identification percentage of malicious nodes in the network. The false reporting is analyzed for the proposed scheme in the presence of selfish nodes. The detection rate analysis parameter is used to analyze the malicious nodes detection ratio. The accurate detection of malicious nodes is also analyzed whereas the false positive rate on different attacks is evaluated. Data throughput and delay are checked during data transmission to evaluate the proposed scheme's performance in the network.

B. TRUSTWORTHINESS ANALYSIS

In this section, the trustworthiness of FNs is analyzed based on the trust threshold. The threshold values are between 0 and 5. Several experiments are conducted to check the proposed scheme performance and trustworthiness of FNs in the presence of malicious nodes in the network. The proposed

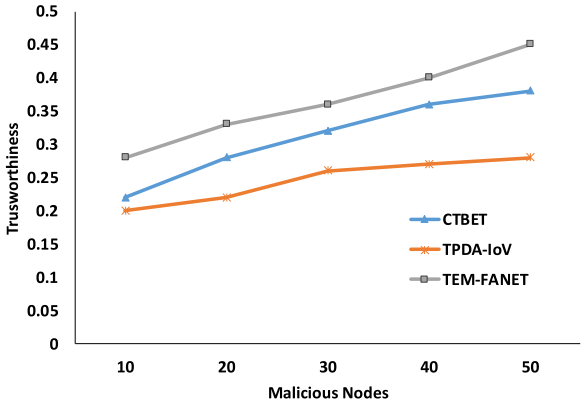

FIGURE 7. Trustworthiness analysis with no of flying nodes and time.

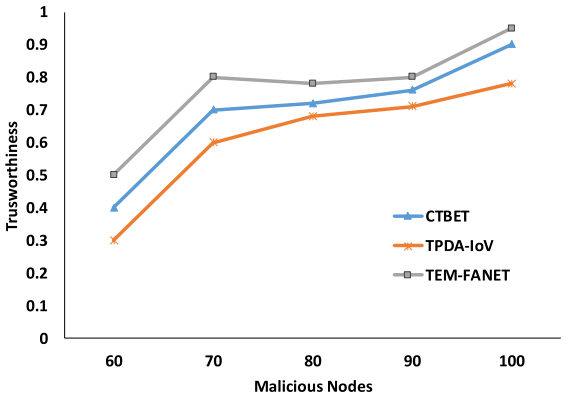

FIGURE 8. Trustworthiness analysis with no of flying nodes and time.

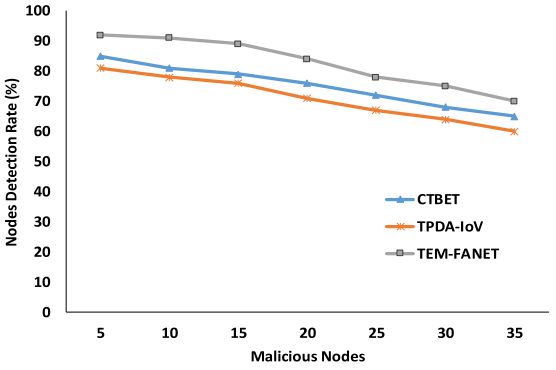

FIGURE 9. Rate of detecting malicious nodes against internal attacks.

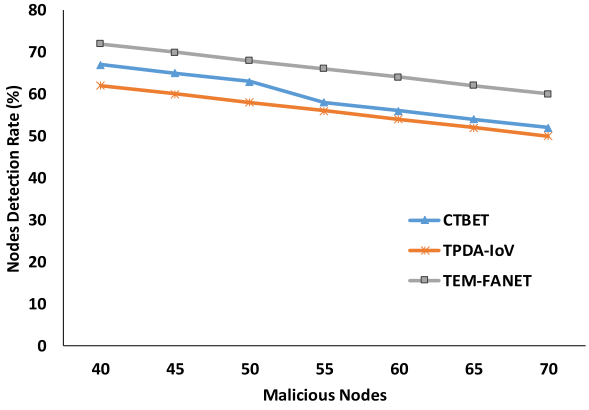

FIGURE 10. Rate of detecting malicious nodes against internal attacks.

TEM-FANET scheme is compared with two state-of-the-art existing schemes including CTBET, and TPDA-IoV. The CTBET is designed for smart cities and IoT networks whereas the TPDA-IoV is designed for the internet of vehicles and drones. Figure 7 and 8 show trustworthiness analysis with no of flying nodes with time. The results showed the better performance of TEM-FANET as compared to the other three existing trust evaluation schemes due to its simple and three-way trust evaluation process.

C. MALICIOUS NODES DETECTION ANALYSIS

In this experiment, the malicious nodes ratio is analyzed in the presence of different malicious nodes in the network. The malicious nodes are generated by using bad-mouth, on-off and DoS attacks behavior to check the proposed scheme detection ratio. Figure 9 shows the detection of malicious nodes against internal attacks where it is observed the better and high performance of the proposed scheme TEM-FANET as compared to CTBET and TPDA-IoV schemes. It is also observed that the CTBET performance is better due to the operation of its non-mobility devices for smart city networks. The TPDA-IoV scheme is designed for the drone's network but due to its complex functions and evaluation as compared to TEM-FANET degraded its overall performance in the network.

In the second experiment (Figure 10), we increased the number of malicious nodes in the network to check the proposed scheme's performance. Overall, the performance of TEM-FANET is better than CTBET and TPDA-IoV.

D. FALSE POSITIVE RATE ANALYSIS

This section discusses the experiments conducted for false positive rate analysis. The false positive rate is analyzed in the presence of different internal attacks. The best false positive rate is 0 whereas the worst is 1. The False Positive Rate (FPR) in detecting malicious nodes measures the proportion of benign nodes incorrectly flagged as malicious. High FPR can lead to resource wastage, operational disruption, and erosion of user trust, necessitating a balance with other performance metrics like True Positive Rate (TPR). The three main attacks are considered for these experiments including DoS, On-Off, and Bad-Mouthing attacks. The lesser values indicated the trustworthiness of nodes whereas the malicious nodes have higher values as shown. Figures 11 shows the FPR in the presence of malicious nodes.

For the second experiment, we increased the number of malicious nodes to check the proposed TEM-FANET performance. It is observed in Figure 12, the results are smooth as compared to previous experiment due to settlement of network and nodes in the network.

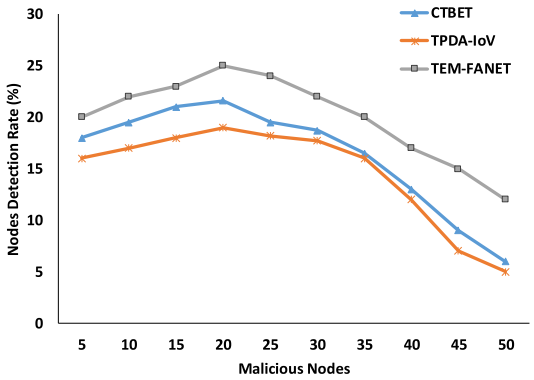

FIGURE 11. False positive rate with number of FN.

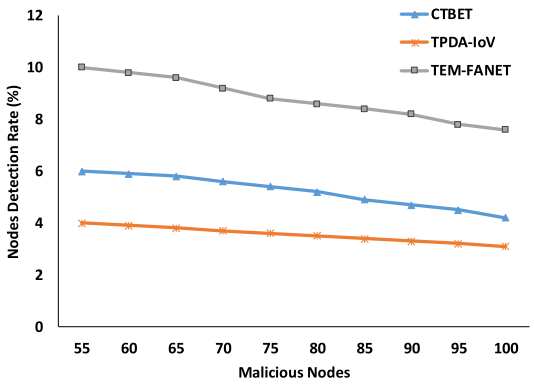

FIGURE 12. False positive rate with number of FN.

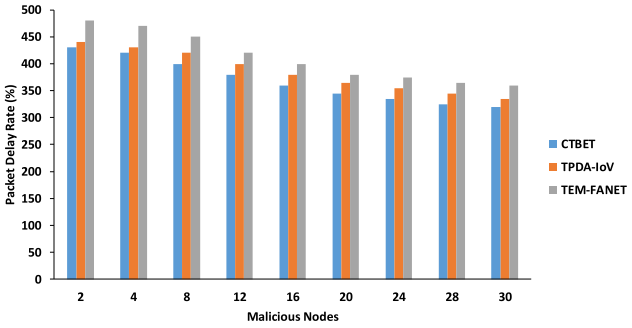

FIGURE 13. Network lifetime (seconds).

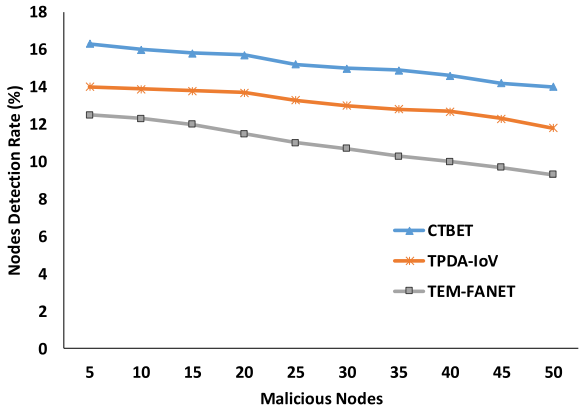

FIGURE 14. Average packet delay ratio in the presence of malicious FN.

E. NETWORK LIFE TIME ANALYSIS

This section presents the network lifetime analysis with time analysis to check the overall network lifetime. This analysis is useful to count the time of sensor-based network FN operated or alive in the network. This parameter is used to check the time of any FN energy level. Energy is one of the significant requirements of the network, especially for FANET nodes. Whenever any malicious node exists in the network it creates an impact on the network where nodes are depleted earlier and not able to perform better services in the network. This experiment analyzed the presence of a malicious node in the network. It is observed that the proposed scheme TEM-FANET network lifetime is better compared to CTBET and TPDA-IoV. The result of TPDA-IoV is better than CTBET because of its node's mobility consideration whereas the CTBET is designed for static devices for smart cities and IoT networks. When the network has less infected with fewer malicious nodes then the network lifetime is more. Figure 13 shows the network lifetime by calculating the packet delay rate in the presence of malicious nodes.

F. AVERAGE PACKET DELAY ANALYSIS

The packet average delay is analyzed in the presence of malicious nodes in the network. The packet delay occurs when there is any unusual activity during data transmission. The experiments and results indicated the better performance of the proposed TEM-FANET scheme as compared to the existing CTBET and TPDA-IoV. The performance of the proposed TEM-FANET scheme in terms of delay average rate is higher when there are more malicious nodes due to trust evaluation in the network. Figure 14 shows the packet delay rate in the presence of malicious nodes.

G. AVERAGE DATA THROUGHPUT

The data throughput is analyzed in the presence of malicious nodes in the network. The data throughput is evaluated by using the total payload over the entire session divided by the total time. A higher data rate is required for a stable network. The proposed TEM-FANET data throughput rate is better than TPDA-IoV and CTBET. As compared to CTBET, the TPDA-IoV data throughput result is better and higher due to its design strategy for flying nodes. Figure 15 shows the average data throughput result.

After conducting different experiments in terms of trustworthiness, malicious node detection, data throughput, data delay, and node detection rate, it is observed that the proposed scheme TEM-FANET performance is better as compared to existing CTBET and TPDA-IoV solutions. The better results are due to lightweight and direct, indirect, and cumulative trust calculation strategy and scheme suitability for flying nodes. Whereas the CTBET is designed to fix devices where the energy is not an issue. On the other hand, the TPDA-IoV also achieved better results as compared to CTBET.

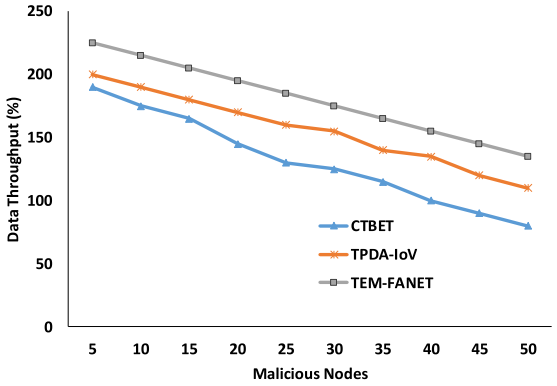

FIGURE 15. Average data throughput in the presence of malicious nodes.

H. DISCUSSION ON TEM-FANET

After detail results experiments, this section summarizes the performance indicators of the discussed solutions in the literature and their comparison with the proposed solutions. It is noticed that the proposed solution TEM-FANET is evaluated with more parameters especially with false positive rate and average delay throughput compared to other solutions. Many existing solutions also missed the packet nodes trustworthiness analysis, which is one of the significant requirements for data communication. It is also observed that the existing solutions are evaluated with three or four parameters, whereas the TEM-FANET is tested with six parameters. Table 3 shows the performance parameters of the existing and proposed solutions.

I. PERFORMANCE EVALUATION OF FANET AUTHENTICATION SYSTEM

We deployed a blockchain consortium of five nodes using a Go Ethereum client (Geth) and connected each node using their eNode addresses. Each node was housed on Amazon Web Services (AWS) EC2 virtual computers. The virtual machine has 1 GB of RAM, and 20 GB of storage, and was configured to run the Linux Ubuntu operating system. The configuration of critical parameters in the JSON genesis file including, 'chainID', 'gasLimit', 'alloc', 'extraData', and 'Epoch' were defined to establish a clique PoA consensus network. The 'chainID' parameter was used to assign a unique identifier for the network.

The 'gas limit' parameter was initialized to 20000000 to define the maximum limit of gas that can be used per block. This limits the number of transactions within each block. Account addresses for FANET nodes were defined at the genesis block where each account was pre-allocated with 2 ETH using the 'alloc' parameter. The nodes that can validate transactions were set as Sealers using the 'extraData' parameter. The 'Epoch' parameter was varied to explore block time intervals with values of 1, 2, 3, 5, 10, and 15 seconds. Table 4 shows the transaction gas cost.

We computed three performance metrics including Transaction Gas Cost, Transaction Per Second and Propagation Delay to evaluate the performance of the blockchain. The

TABLE 3. Tested performance parameters comparison analysis.

Existing Solutions	Trustworthiness Level	Energy Consumption	Transmission Delay	Packet Drop Ratio	Packet delivery Ratio	Network Lifetime	Malicious Node Detection Analysis	False Positive Rate Analysis	Average Data Throughput
Fuzzy based Model [1]	✓	✓	✓	✓	×	×	×	×	×
Trust Model for UAVs [2]	✓	×	✓	✓	×	×	×	×	×
FNDN [3]	✓	✓	✓	×	×	×	✓	×	×
TBCS [4]	×	×	✓	✓	✓	×	×	×	×
CTBET [5]	✓	×	✓	×	×	✓	×	×	×
Blockchain Method [6]	×	×	✓	×	×	×	×	✓	×
TPDA-IoV [7]	×	×	✓	×	✓	✓	×	×	×
TEM-FANET	✓	×	✓	×	×	✓	✓	✓	✓

TABLE 4. Transaction gas cost.

Smart contract	Transaction Gas Cost
Deployment	774405
Registration	50534
Verification	10572
Attestation	24500

Transaction Gas Cost is used to compute the complexity of the smart contract. To make the smart contract efficient and less complex it is crucial to monitor and optimize the gas cost. Table 4 shows the list of all smart contract functionalities and their associated Transaction Gas Costs. The Smart Contract Deployment takes a significant gas cost of 774,405, however, this expense would only be once as after deployment only the functions of the smart contract will be accessed. Registration of new FANET nodes comes at a cost of 50,534 gas. Each node will register only once. On the other hand, Verification which is an essential step in confirming the authenticity of FANET identity has a relatively lower cost of 10,572 gas. The attestation of FANET by manufacturers also consumes less cost of 24,500 gas. Table 5 shows the transaction per second.

The Transaction Per Second is an important metric for measuring blockchain performance. It quantifies the number of transactions that a blockchain can process within a second. A higher Transaction Per Second indicates that the blockchain network can handle a larger volume of transactions and is more scalable. Table 4 presents a detailed representation of Transaction Per Second in relation to the block time parameter. It can be observed that when the block time is increased the Transaction Per Second reduces significantly. This trend shows that to achieve a higher TPS in the clique network a lower block time should be selected.

TABLE 5. Transaction per second.

Block time (seconds)	Transaction Per Second
1	991.24
2	470.29
3	314.45
5	183.11
10	84.67
15	56.65

TABLE 6. Propagation delay.

Sealer	Propagation Delay (µs)
1	387.565
2	579.853
3	729.425
4	789.652
5	982.721

However, we have also observed that when the block time, for instance, is set very low, such as 1 second, the number of lost blocks tends to be higher. This is because the sealers do not have sufficient time to validate the transactions before the next block appears. Therefore, a block time between 1 and 2 is suggested. Table 6 shows the propagation delay.

We further conducted an assessment of the Propagation Delay in the network. Propagation Delay measures the time it takes for a transaction to be broadcast across the network and received by all participating nodes. In a clique network ''sealers'' are the validator nodes responsible for creating new blocks and confirming transactions. Our evaluation of Propagation Delay revealed a noteworthy correlation with the number of sealers in the network as shown in Table 5. It can be seen that an increase in the number of sealers would lead to increased propagation delay in the network. This means that the FANET nodes would face higher delays in the authentication process. Therefore, it can be concluded that to achieve optimal performance, a lower block time and reduced number of sealers should be used. This will result in higher throughput and reduced delays in the network which would lead to a faster authentication process for the FANETs.

V. CONCLUSION

This paper proposed a Trust Establishment Mechanism for FANET (TEM-FANET) networks to evaluate the node's trust status and ensure the existence of the trustworthy node and identified the malicious nodes in the network. The FN is evaluating trust by using direct and indirect trust values and then determined the cumulative trust based on threshold values. The proposed mechanism is specially designed for drone nodes by using lightweight metrics. The proposed solution can ensure the trust scenario in the network and identify the malicious nodes by updating the existence of the malicious node in the network. When there are any malicious nodes identified in the network and not qualified for the trust merit, it is eliminated from the network and their details are broadcasted. The proposed model is evaluated with existing solutions in terms of false positive rate, malicious nodes detection rate, data throughput, and data delay. The experiment results showed the better performance of the proposed trust-based solution as compared to the state-of-the-art trust solutions. We also proposed an FANET node authentication system using blockchain technology and evaluate its performance. The experiments show that by setting a blocktime between 1-2 we can achieve a TPS of above 500. In the future, we will integrate the edge network with FANET and implement the proposed model to check its performance. Moreover, we are going to implement it in agriculture precision environments.

ACKNOWLEDGMENT

The authors would like to express our gratitude to the Department of Electronic and Computer Science at the University of Limerick for their invaluable support and resources.

REFERENCES

[1] K. Kumar, S. Kumar, O. Kaiwartya, P. K. Kashyap, J. Lloret, and H. Song, ''Drone assisted flying ad-hoc networks: Mobility and service oriented modeling using neuro-fuzzy,'' *Ad Hoc Netw.*, vol. 106, Sep. 2020, Art. no. 102242.

[2] G. Abbas, A. Mehmood, M. Carsten, G. Epiphaniou, and J. Lloret, ''Safety, security and privacy in machine learning based Internet of Things,'' *J. Sensor Actuator Netw.*, vol. 11, no. 3, p. 38, Jul. 2022.

[3] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, ''Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends,'' *Intell. Service Robot.*, vol. 16, no. 1, pp. 109–137, Mar. 2023.

[4] A. Vinci, R. Brigante, C. Traini, and D. Farinelli, ''Geometrical characterization of hazelnut trees in an intensive orchard by an unmanned aerial vehicle (UAV) for precision agriculture applications,'' *Remote Sens.*, vol. 15, no. 2, p. 541, Jan. 2023.

[5] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret, ''Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain,'' *Ad Hoc Netw.*, vol. 86, pp. 72–82, Apr. 2019.

[6] K. Singh and A. K. Verma, ''A fuzzy-based trust model for flying ad hoc networks (FANETs),'' *Int. J. Commun. Syst.*, vol. 31, no. 6, p. e3517, Apr. 2018.

[7] M. M. Alam and S. Moh, ''Survey on Q-learning-based position-aware routing protocols in flying ad hoc networks,'' *Electronics*, vol. 11, no. 7, p. 1099, Mar. 2022.

[8] M. Gupta and S. Varma, ''Optimal placement of UAVs forming aerial mesh networks to handle network issues,'' *Adhoc Sensor Wireless Netw.*, vol. 48, 2020.

[9] A. Malhotra and S. Kaur, ''A comprehensive review on recent advancements in routing protocols for flying ad hoc networks,'' *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3688, Mar. 2022.

[10] X. Bai, S. Chen, Y. Shi, C. Liang, and X. Lv, ''Blockchain-based authentication and proof-of-reputation mechanism for trust data sharing in Internet of Vehicles,'' *Adhoc Sensor Wireless Netw.*, vol. 53, 2022.

[11] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, ''Security in vehicular ad hoc networks: Challenges and countermeasures,'' *Secur. Commun. Netw.*, vol. 2021, pp. 1–20, Jun. 2021.

[12] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C.-H. Hsu, ''Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4757–4769, Jul. 2021.

[13] S. Swain, B. R. Senapati, and P. M. Khilar, ''Evolution of vehicular ad hoc network and flying ad hoc network for real-life applications: Role of VANET and FANET,'' in *Modelling and Simulation of Fast-Moving Ad-Hoc Networks (FANETs and VANETs)*. Hershey, PA, USA: IGI Global, 2023, pp. 43–73.

[14] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *Proc. 25th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Apr. 2006, pp. 1–13.
[15] S. Theodorou and N. Sklavos, "Blockchain-based security and privacy in smart cities," in *Smart Cities Cybersecurity and Privacy*. Amsterdam, The Netherlands: Elsevier, 2019, pp. 21–37.
[16] A. M. Hilal, A. A. Albraikan, S. Dhahbi, S. S. Alotaibi, R. Alabdan, M. A. Duhayyim, A. Motwakel, and I. Yaseen, "Trust aware oppositional sine cosine based multihop routing protocol for improving survivability of wireless sensor network," *Comput. Netw.*, vol. 213, Aug. 2022, Art. no. 109119.
[17] K. Singh and A. K. Verma, "A trust model for effective cooperation in flying ad hoc networks using genetic algorithm," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2018, pp. 0491–0495.
[18] E. Barka, C. A. Kerrache, R. Hussain, N. Lagraa, A. Lakas, and S. H. Bouk, "A trusted lightweight communication strategy for flying named data networking," *Sensors*, vol. 18, no. 8, p. 2683, Aug. 2018.
[19] K. Singh and A. K. Verma, "TBCS: A trust based clustering scheme for secure communication in flying ad-hoc networks," *Wireless Pers. Commun.*, vol. 114, no. 4, pp. 3173–3196, Oct. 2020.
[20] K. N. Qureshi, A. Iftikhar, S. N. Bhatti, F. Piccialli, F. Giampaolo, and G. Jeon, "Trust management and evaluation for edge intelligence in the Internet of Things," *Eng. Appl. Artif. Intell.*, vol. 94, Sep. 2020, Art. no. 103756.
[21] H. Sachdeva, S. Gupta, A. Misra, K. Chauhan, and M. Dave, "Improving privacy and security in unmanned aerial vehicles network using blockchain," 2022, *arXiv:2201.06100*.
[22] K. N. Qureshi, A. Alhudhaif, A. A. Shah, S. Majeed, and G. Jeon, "Trust and priority-based drone assisted routing and mobility and service-oriented solution for the Internet of Vehicles networks," *J. Inf. Secur. Appl.*, vol. 59, Jun. 2021, Art. no. 102864.
[23] H. Wang, L. Xu, and G. Gu, "FloodGuard: A DoS attack prevention extension in software-defined networks," in *Proc. 45th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, Jun. 2015, pp. 239–250.
[24] N. Karthik and V. S. Ananthanarayana, "A hybrid trust management scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 97, no. 4, pp. 5137–5170, Dec. 2017.
[25] E. K. Wang, Y. Li, Y. Ye, S. M. Yiu, and L. C. K. Hui, "A dynamic trust framework for opportunistic mobile social networks," *IEEE Trans. Netw. Service Manage.*, vol. 15, no. 1, pp. 319–329, Mar. 2018.
[26] K. R. Liu and B. Wang, *Cognitive Radio Networking and Security: A Game-Theoretic View*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[27] S. A. Jeba and B. Paramasivan, "False data injection attack and its countermeasures in wireless sensor networks," *Eur. J. Sci. Res.*, vol. 82, no. 2, pp. 248–257, 2012.
[28] A. Varga, "OMNeT++," in *Modeling and Tools for Network Simulation*. Springer, 2010, pp. 35–59.
[29] A. Varga, "A practical introduction to the OMNeT++ simulation framework," in *Recent Advances in Network Simulation: The OMNeT++ Environment and Its Ecosystem*. Cham, Switzerland: Springer, May 2019, pp. 3–51.

KASHIF NASEER QURESHI received the master's degrees in computer science (MCS) and information technologies (MSIT) from renowned universities, and the Ph.D. degree from University Teknologi Malaysia (UTM), in 2016, with a specialization in wireless communication. He is currently an Associate Professor with the Department of Electronic and Computer Engineering, University of Limerick, Ireland. His dedication to academia is mirrored in his role as a principal investigator for a government-funded cybersecurity projects. His name stands proudly within the top 2% of scientists globally and he garnered consecutive best researcher awards for his outstanding and impactful work. With a wealth of expertise spanning 14 years, his career is distinguished by his dual proficiency in teaching and research with the prestigious academic institutions. His qualifications extend beyond the theoretical, as he is a certified network and security professional by both Cisco and Microsoft. His collaborative efforts have traversed the globe, encompassing ventures in several developed courtiers. These cooperative projects have been instrumental in the realms of cyber security, wireless communication, smart cities, the IoT, artificial intelligence, intelligent transportation systems, ad hoc networks, and cyber-physical systems. His intellectual prowess is evidenced by the publication in esteemed international journals. In recent times, his scholarly pursuits have focused on critical domains, such as cybersecurity, trust-oriented edge and cloud solutions, secure internet connectivity for vehicles, drone-enabled networking security, electric vehicle charging management, and safeguarded healthcare systems. Beyond his research contributions, he has taken on additional roles as an associate editor and a guest editor in distinguished SCI journals and special issues for esteemed platforms. His multifaceted engagements underscore his commitment to advancing knowledge and fostering innovation within his fields of expertise.

HANAA NAFEA received the master's degree in computer science from Nottingham Trent University, Nottingham, U.K., in 2012. She is currently pursuing the Ph.D. degree with Liverpool John Moores University (LJMU), U.K. She is also a Lecturer with the Department of Computer Science, Taibah University, Madinah, Saudi Arabia. Her current research interests include network security, the security of complex systems, intrusion detection, secure service composition, privacy-preserving data aggregation, cryptography computer science, and cloud security.

IBRAHIM TARIQ JAVED received the Ph.D. degree in computer science from Institut Mines-Telecom, Telecom SudParis. He is a Research Fellow with Blockhain@UBC. Before taking this role, he was an Associate Professor with Bahria University. He received a Postdoctoral Fellowship co-sponsored by the European Commission under the Marie Skłodowska-Curie Program and Science Foundation Ireland through Lero–the Irish Software Research Centre. He has been able to publish his research in top-tier journals and conferences. His research interests include blockchain technology, Web3.0, decentralized applications, privacy, identity, and trust management.

KAYHAN ZRAR GHAFOOR received the B.Sc. degree in electrical engineering from Salahaddin University, in 2003, the M.Sc. degree in remote weather monitoring from Koya University, in 2006, and the Ph.D. degree in wireless networks from University Technology Malaysia, in 2011. He is with the Department of Computer Science, Knowledge University, Erbil, Iraq. His current research interests include vehicular communication Internet of Things, big data in VANET, and software defined networks. He is a member of the IEEE Vehicular Technology Society, the IEEE Communications Society, the Internet Technical Committee (ITC), and the International Association of Engineers (IAENG).