IEEE Access
Multidisciplinary ⁞ Rapid Review ⁞ Open Access Journal

Received 15 July 2024, accepted 31 July 2024, date of publication 5 August 2024, date of current version 15 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3438614

RESEARCH ARTICLE

Secure Multi-Hop Assisted IoT Communications in Smart Cities

MUHAMMAD AWAIS JAVED[1], **(Senior Member, IEEE), MOHAMMED ALKHATHAMI**[2], **ABDULAZIZ ALMOHIMEED**[3], **AND ABEER ALMUJALLI**[2]

[1]Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), Islamabad 45550, Pakistan
[2]Department of Information Systems, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia
[3]Computer Science Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia

Corresponding author: Mohammed Alkhathami (maalkhathami@imamu.edu.sa)

This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-RP23054).

ABSTRACT Security and reliability are the major requirements for the successful implementation of Internet of Things (IoT) applications in smart cities such as healthcare. IoT networks are subject to various types of network attacks that can put critical IoT data at risk. To mitigate these security issues, robust security algorithms based on Elliptic Curve Cryptography (ECC) may be utilized. However, using such cryptographic techniques requires additional delay for signing/encrypting and verification/decryption of the messages. Hence, there is a tradeoff between the security strength of the algorithm and packet delay. In this paper, we present a novel technique to adaptively select the key size of ECC-based algorithms for multi-hop IoT networks. The proposed technique uses k-means clustering to classify the secrecy rates of the potential relay nodes into k clusters. We allocate lower key sizes to the relay nodes that have the highest secrecy rates and thus have better physical layer security. The key sizes and security strengths are selected as per the recommendation of the National Institute of Standards and Technology (NIST). The second part of the work utilizes the Hungarian algorithm to select the best relay nodes for each source-destination transmission to minimize the total delay. The techniques are implemented in MATLAB and results show that the total delay of the proposed technique is improved by 57% as compared to other techniques in the literature.

INDEX TERMS IoT, security, smart cities, network delay.

I. INTRODUCTION

Internet of Things (IoT) has a wide range of applications for future smart cities including healthcare, industrial automation and intelligent transportation [1], [2], [3]. IoT uses an integrated network comprising sensors, physical devices, wireless communication modules, and computing services. IoT systems will be able to collect data using the deployment of various sensors. Using this data, many application processes can be improved [4], [5], [6], [7], [8].

Security of IoT systems especially in healthcare is a vital issue that needs to be addressed for improving the reliability of applications [9], [10], [11], [12], [13]. IoT systems are subject to several types of attacks that can compromise the privacy of the user's data. Moreover, these network attacks can also disrupt IoT applications by jamming the network and sharing wrong data information [11], [14], [15], [16], [17].

Such security attacks can be mitigated by using robust Elliptic Curve Cryptography (ECC) techniques such as Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Integrated Encryption Scheme (ECIES) [18]. In addition, these networks also rely on physical layer security techniques that can increase the signal reception at the destination and reduce the signal strength at the eavesdroppers.

A major challenge related to the security of IoT networks especially for smart city applications such as traffic management is that there exists a tradeoff between security and packet transmission delay. A robust cryptographic algorithm with a higher number of keys may be more resistant to

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

security attacks, however, this increases the packet delay as more time is needed to sign/encrypt and verify/decrypt the messages. Hence, adaptive security algorithms are needed that can manage security requirements as well as meet packet delay deadlines.

Wireless connectivity is another major challenge in IoT systems. Since IoT nodes are small and equipped with low-powered batteries and simple transceivers, the range of communication may not be high. As a result, multi-hop communications will be needed to send messages from a source IoT node to the destination IoT node. In addition, packet transmission to the IoT gateways will also require the use of relay nodes that forward the message of the source on behalf of the destination.

The selection of appropriate relay nodes is another key challenge in IoT systems. While there may be several potential relay nodes that are available for a given transmission, an intelligent algorithm is needed that can optimize the network delay. Moreover, many IoT nodes may prefer to choose a given relay node, thus causing contention.

In this paper, we provide a solution to the above challenges by proposing two algorithms, one for adaptive security and the other for relay selection. The major contributions of the work are as follows:

- We consider a system model that comprises multi-hop communications in IoT networks. Since IoT nodes have limited communication range, such a system is required to transmit long-range messages.
- We propose a novel adaptive security algorithm that manages the key sizes of ECDSA and ECIES algorithms for each IoT transmission. The major idea of the algorithm is that nodes with a better secrecy rate may operate at a lower key size and security strength to improve the network delay. Our proposal utilizes a k-means clustering scheme to classify secrecy rates into different clusters. The relay nodes in each cluster utilize a different key size that corresponds to a different security strength as per the National Institute of Standards and Technology (NIST).
- We propose a relay selection algorithm to minimize the total delay comprising of security and transmission delay. For the allocation of IoT transmissions to the relay nodes, we utilize the Hungarian algorithm to provide a matching output that minimizes the cost in terms of total delay.
- We perform detailed simulations to analyze the performance of the proposed technique and compare it with several other available techniques in the literature. Results show that the proposed technique outperforms other techniques in terms of security sign/encrypt delay, verify/decrypt delay, and total delay.

II. RELATED WORKS

In this section, we present recent work related to adaptive security, multi-hop relay selection, and the novelty of the proposed technique.

A. RECENT WORK IN ADAPTIVE SECURITY

A summary of recent work in adaptive security is shown in Table 1. The work in [19] targets defense against adaptive adversaries and reduces bandwidth consumption. For this, a linear homomorphic encryption technique is used which enables encryption of the encrypted data rather than the original data. Moreover, computing operations can be performed on the message before decryption. This enables faster processing of data and improved computational efficiency. Another important feature of the work is a low-cost key refresh scheme that reduces the amount of communications and hence reduces bandwidth consumption. Simulation results highlight the reduced communication and computation cost of the proposed technique as compared to the other schemes.

In [20], the work is focused on prioritized verification of Intelligent Transportation Systems (ITS) messages. To achieve this goal, the paper recommends the adaptive key size of the Elliptic Curve Digital Signature (ECDSA) algorithm. The idea works for multi-hop broadcast messages. A priority algorithm is proposed to verify critical messages first. A key size adaptation scheme is also proposed that changes key values based on the level of congestion. To implement this mechanism, a fuzzy logic scheme is used. The proposed technique results in improved network delay, packet success rate, and reduced broadcast retransmissions.

The work in [21] aims to improve network security by using adaptive neighborhood behavior detection. For this, the behavior is evaluated based on packet relaying performance, packet generation rate, and data integrity of the neighbor. The decision to communicate with the neighbors is selected based on their behavior profile. Simulation results highlight the reduced packet loss percentage achieved by the proposed scheme.

In [22], the goal of the technique is to improve secrecy capacity while achieving a sufficient bit error rate. The network under consideration is visible light communication. An adaptive pulse amplitude modulation scheme is introduced to meet the required goals. As modulation level increases, secrecy improves but bit error rate requirement also increases. In addition, an adaptive precoder design is also proposed by the authors. A utility function based on secrecy rate and bit error rate is defined by the work and a Q-learning scheme is proposed for adapting the modulation and precoder. Results show improved secrecy rate and bit error rate in the visible light communication network.

A trust management scheme for vehicular networks is proposed by authors in [23]. The trust evaluation is based on context information of the vehicular network. An adaptive threshold is used for malicious node detection. The proposed scheme takes into account both local and global trust evaluation. Similarly, the work also integrates direct and indirect trust in the developed mechanism. Results provide improved detection of attacks in a vehicular network setting.

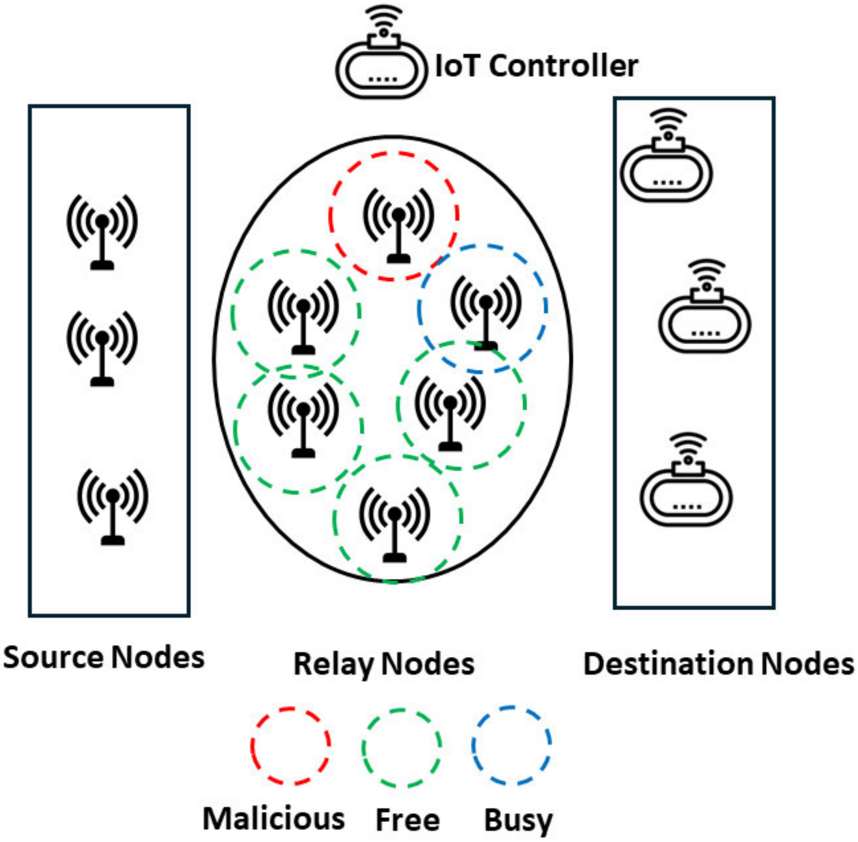

FIGURE 1. System model.

B. RECENT WORK IN MULTI-HOP RELAY SELECTION

A summary of recent work related to multi-hop relay selection is shown in Table 2. The work in [24] is focused on relay selection based on power efficiency and social awareness. A social network model is developed by the proposed scheme. The relay selection problem is formulated as a minimum power optimization problem and solved using a greedy distance-based algorithm. Simulation results show reduced power consumption by the proposed technique.

In [25], the goal of the work is to reduce Network Outage Probability (NOP). A multi-user multi-hop scenario is used by the proposed scheme. To solve the problem of relay selection, a trellis diagram-based algorithm is used. The proposed scheme solves the problem with linear time complexity. The result achieves reduced NOP in multi-hop communications.

The work in [26] develops an algorithm to improve Secrecy Connectivity Probability (SCP). The scenario considered is based on energy harvesting relays. The proposed work presents an analytical model to evaluate SCP. Moreover, the relay selection algorithm is based on maximizing SCP. Results highlight improved SCP achieved by the proposed technique.

In [27], a multi-hop technique is presented to improve network throughput. The concept of Incremental Relaying (IR) is used in the proposed work. Two types of relaying mechanisms are used by the developed technique. The first mechanism is Best-last arbitrary-rest IR in which random relays from the decoding set are used initially and the last relay selected is the one that has the best Signal to Noise Ratio (SNR) to the destination. The second mechanism used is the Maximum decoding set IR in which relay selection is such that the decoding set can be maximized in the next hop. Results show improved throughput by the proposed technique.

The work in [28] develops a reliability improvement mechanism for multi-hop networks. The scenario considered is Unmanned Aerial Vehicle (UAV) to UAV communications. A multi-hop communication algorithm is presented that uses Device to Device (D2D) users as relay nodes. The forwarding mechanism is based on channel quality and network load. Also, the relay is selected within a forwarding area. Simulation results show improved reliability and reduced delay achieved by the proposed technique.

C. NOVELTY OF THE PROPOSED TECHNIQUE

As compared to the current techniques in the literature, the proposed technique in this paper uses adaptive security to reduce the packet delay. This paper presents a novel idea of using physical layer security and cryptographic security together to improve the network delay and reduce congestion in the network. Nodes that have better physical

TABLE 1. Summary of related works in adaptive security.

Ref.	Goal	Key Idea	Results
[19]	Bandwidth consumption Handle adaptive adversaries	Utilize Linearly homomorphic encryption Efficient Key refresh scheme	Reduced communication cost Reduced computation cost
[20]	Prioritized verification Adaptive key size Broadcast multi-hop messages	Priority algorithm to verify critical messages Network congestion based key size selection Fuzzy logic	Improved network delay Improved packet success rate Reduce broadcast retransmissions
[21]	Improve security	Adaptive neighborhood behavior detection Packet relaying behavior Packet generation rate Data integrity behavior	Reduced packet loss percentage
[22]	Improved secrecy capacity Sufficient Bit error rate	Visible Light Communication Adaptive Pulse Amplitude Modulation Adaptive precoder design Utility based on secrecy rate and bit error rate Q-learning based algorithm	Improved secrecy capacity Improved bit error rate
[23]	Trust management	Vehicular network Trust evaluation based on context information Adaptive threshold for malicious node detection Local and Global trust evaluation Direct and Indirect trust evaluation	Improved attack detection

layer security (in terms of secrecy rate operate) at a lower level of cryptographic security strength (in terms of key size). The proposed technique also utilizes K-means clustering to assign adaptive levels of security to the nodes in the network. Moreover, as compared to other techniques, the proposed relay selection technique considers security sign/encrypt and verify/decrypt delays in the total network delay and reduces it using the Hungarian algorithm.

III. SYSTEM MODEL

In this paper, we consider a multi-hop communication scenario between IoT source nodes and IoT destination nodes as shown in Fig. 1. Due to the limited transmit power and communication range of IoT nodes, two hops are required to transmit the message between source and destination. The main rationale of using multi-hop communications is for radio range extension [29], [30]. We consider a central IoT controller that manages the multi-hop communication between the IoT nodes. The IoT controller node has the channel quality information of all the links in the networks. We assume perfect channel state information (CSI) to be known at IoT controller node [31]. Moreover, we assume that the controller node knows malicious nodes in the networks using trust mechanism techniques or anomaly detection algorithms [32]. This means that the controller node regularly evaluates the outlier in the data values and transmission parameters to see if a node is sending wrong information or trying to jam the network with too many transmissions. Based on the anomaly detection technique, a trust or reputation mechanism is established which helps in identifying potential eavesdropper nodes.

All IoT nodes in the network are marked as source, destination, free relay nodes, and busy relay nodes by the controller node. Here, the free relay nodes are the potential nodes that are neither the source nor the destination and are also available for forwarding the message from a source towards the destination. On the other hand, busy relay nodes are the ones that are assigned relaying service by the

TABLE 2. Summary of related works in multi-hop relaying.

Reference	Goal	Key Idea	Results
[24]	Power efficiency Social awareness	Develop Social network model Minimize power optimization problem Greedy distance based algorithm	Reduced power consumption
[25]	Reduce NOP	Multi-hop multi-user scenario Trellis diagram based algorithm Linear time complexity	Reduced NOP
[26]	Improve SCP	Energy harvesting relay Analytical model of SCP Relay selection for maximum SCP	Improved SCP
[27]	Improve throughput	Incremental relaying Best-last arbitrary-rest IR Maximum decoding set IR	Improved throughput
[28]	Reliability improvement	UAV-UAV communications Multi-hop using D2D enabled users Channel and load based forwarding Relay selection within a forwarding area	Improved reliability Reduced delay

TABLE 3. Security strength of ECDSA at different key sizes.

Security Strength	ECC p-value	Key Size
80-bit	P-160	160 bits
112-bit	P-224	224 bits
128-bit	P-256	256 bits
192-bit	P-384	384 bits
256-bit	P-521	521 bits

controller node. Once the busy relay node completes the message forwarding, its status is changed to free.

IV. PROPOSED TECHNIQUE

The goal of the proposed technique is twofold. The first goal is adaptive key size selection of the security algorithm to improve the time required for encryption and decryption of the packet. The second goal is to select the appropriate relay node so that the total packet delay is reduced. In the following, we explain how these two goals are achieved.

A. K-MEANS BASED ADAPTIVE SECURITY

The first part of the proposed algorithm is adaptive security selection in which the cryptographic key sizes of each transmission are selected. As per the National Institute of Standards and Technology (NIST), the ECDSA and ECIES algorithm provides different levels of security strength at different key sizes [33]. Here security strength is defined as the number of operations that are needed to compromise a security algorithm. Table 3 presents the security strength of the ECDSA and ECIES algorithms at different key sizes.

Moreover, Table 4 shows the delay required to encrypt/sign, and decrypt/verify ECDSA and ECIES messages at different key sizes [18]. It can be seen that that higher key sizes require significantly longer delays for encryption/signing and decryption/verification. Thus, there is a tradeoff between robust security and delay. While security strength value can be increased to improve data privacy, it can increase the total delay of the message.

We propose a novel adaptive security mechanism in which IoT nodes select the level of cryptographic security based on

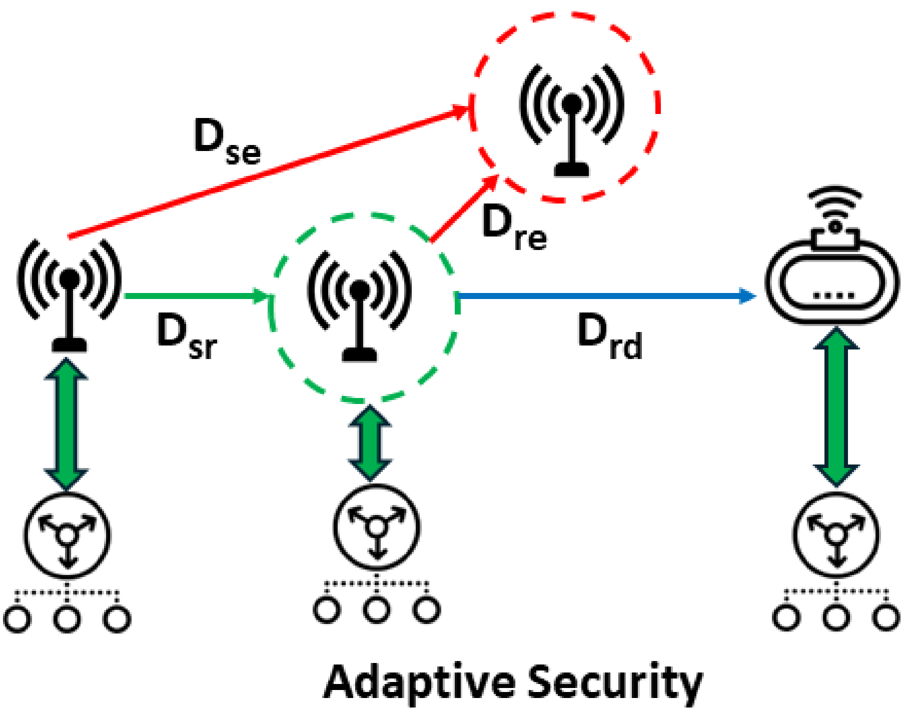

FIGURE 2. Adaptive security based on secrecy rate.

TABLE 4. Time required for signature/encryption and verification/decryption using ECDSA and ECIES at different key sizes.

ECC variant	Signature Delay (ms)	Verification Delay (ms)
P-160	8.01	14.25
P-224	10.54	18.92
P-256	13.43	21.2
P-384	49.29	87.78
P-521	58.2	104.5

the secrecy rate as shown in Fig. 2. Nodes with higher secrecy rates are those that have better data rates at the destination as compared to the eavesdropper. The key idea is that those nodes that have a higher secrecy rate can operate at a lower level of security. Hence, nodes with better physical layer security can use a lower level of cryptographic security.

The IoT controller has channel quality information of all links in the network. As shown in Fig. 2, the secrecy rate of each link is calculated by the IoT controller. The secrecy rate R_{sr} of the link (s, r) where s is the source transmitting node and r is the relay receiving node can be given as follows:

$$R_{sr} = D_{sr} - D_{se} \tag{1}$$

where D_{sr} is the data rate of link (s, r) and D_{se} is the data rate of the link (s, e). Here e is the maximum rate of any eavesdropper [34].

Once the secrecy rates are obtained, we utilize K-means clustering to divide the relay nodes into k different secrecy rate levels $SRL = \{SRL_1, SRL_2, \ldots, SRL_k\}$ as shown in Algo. 1. The relay nodes with the highest secrecy rate are placed in SRL_1 and so on. The nodes with the least value of secrecy rate are placed in the last group SRL_k. The goal of k-means clustering is to minimize the square of the sum of errors (i.e., the difference between secrecy rate levels and the centroid of a cluster). This is calculated from the following equation:

$$\underset{SRL}{arg\ min} \sum_{l=1}^{k} \sum_{R_{sr} \in SRL_l} ||R_{sr} - \mu_l||^2 \tag{2}$$

where μ_l is the centroid of a cluster l and is given as follows:

$$\mu_l = \frac{1}{|SRL_l|} \sum_{R_{rs} \in SRL_l} R_{rs} \tag{3}$$

where $|SRL_l|$ is the number of items in the cluster SRL_l. The algorithm for k-means clustering is shown in Algo. 1. The algorithm takes as input the secrecy rate of all links $R_{s,r}$ and several desired clusters k. Initially, the centroid value of each cluster is selected randomly. In Step 2, each link secrecy rate is assigned to a centroid based on the nearest distance value. In step 3, the centroids are updated as the average of all secrecy rate values in the cluster. Steps 2 and 3 are

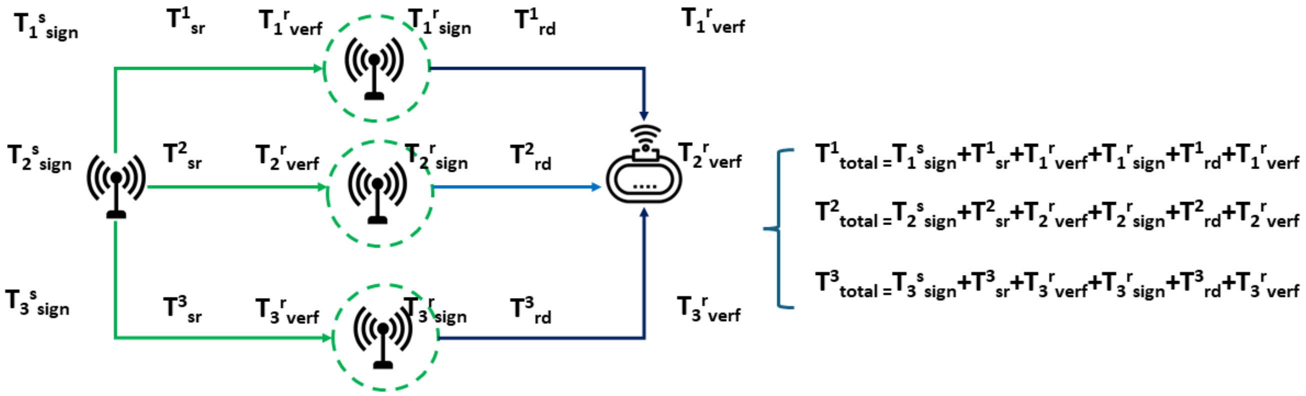
$T_1{}^s{}_{sign}$
$T^1{}_{sr}$
$T_1{}^r{}_{verf}$
$T_1{}^r{}_{sign}$
$T^1{}_{rd}$
$T_1{}^r{}_{verf}$
$T_2{}^s{}_{sign}$
$T^2{}_{sr}$
$T_2{}^r{}_{verf}$
$T_2{}^r{}_{sign}$
$T^2{}_{rd}$
$T_2{}^r{}_{verf}$
$T_3{}^s{}_{sign}$
$T^3{}_{sr}$
$T_3{}^r{}_{verf}$
$T_3{}^r{}_{sign}$
$T^3{}_{rd}$
$T_3{}^r{}_{verf}$
$T^1{}_{total} = T_1{}^s{}_{sign} + T^1{}_{sr} + T_1{}^r{}_{verf} + T_1{}^r{}_{sign} + T^1{}_{rd} + T_1{}^r{}_{verf}$
$T^2{}_{total} = T_2{}^s{}_{sign} + T^2{}_{sr} + T_2{}^r{}_{verf} + T_2{}^r{}_{sign} + T^2{}_{rd} + T_2{}^r{}_{verf}$
$T^3{}_{total} = T_3{}^s{}_{sign} + T^3{}_{sr} + T_3{}^r{}_{verf} + T_3{}^r{}_{sign} + T^3{}_{rd} + T_3{}^r{}_{verf}$

FIGURE 3. Total delay of packet from source to the destination.

repeated unless the link secrecy rate does not converge, i.e., the assignment of the link secrecy rate to the centroid is not changed anymore.

Algorithm 1 Secrecy Rate-Based Clustering of Communication Links Using K-Means Clustering

```
Input: Secrecy rate of all links $R_{s,r}$, Number of clusters $k$
Step1: Initialize the secrecy rate of all $k$ centroids randomly
Step2: Assign each link secrecy rate to a centroid based on the nearest distance value as follows
$SRL_l = \{(s,r) : ||R_{sr} - \mu_l||^2 \leq ||R_{s,r} - \mu_i||^2 \forall i, 1 \leq i \leq k\}$
Step3: Update the centroid values of each secrecy rate level as follows
$\mu_l = \frac{1}{|SRL_l|} \sum_{R_{sr} \in SRL_l} R_{sr}, \forall l$
Repeat Step 2 and Step 3 unless the assignment of the link secrecy rate to the centroid is not changed anymore
```

B. RELAY SELECTION TECHNIQUE

The goal of the relay selection technique is to use relay nodes that can minimize the overall delay. For each source-destination transmission, the IoT controller node selects the appropriate relay. The total delay T_{sd} from the source to destination as shown in Fig. 3 can be given as follows:

$$T_{sd} = T^s_{sign} + T_{sr} + T^r_{verf} + T^r_{sign} + T_{rd} + T^d_{verf} \tag{4}$$

Here T^s_{sign} is the signature and encryption time taken by the packet at the source node. This time depends on the current key size the source-relay link is operating at. T_{sr} is the transmission delay of the packet from the source node to the relay node and is given as follows:

$$T_{sr} = \frac{P_s}{D_{sr}} \tag{5}$$

T^r_{verf} is the signature verification and decryption delay taken by the packet at the relay node. This time also depends on the current key size of the source-relay link.

Similarly, T^r_{sign} is the signature and encryption time taken by the packet at the relay node. T_{rd} is the transmission delay of a packet from the relay node to the destination node. Finally, T^d_{verf} is the verification and decryption delay at the destination node.

To solve the problem of the assignment of relay nodes to the source-destination transmission, we utilize the Hungarian algorithm. Here relay nodes are the machines, and packets to be transmitted are the jobs. The cost for each relay node and source destination transmission pair can be given using equation 4. As an example, Fig. 3 shows the cost of a single source destination transmission for all of its potential relay nodes.

Similarly, the cost function matrix for three transmissions and three potential relays is shown in Table 5. Here row 2 and column 2 of the table show that the first source-destination transmission pair has a cost (i.e., total delay) of $T^1_{(s1d1)}$ when using relay 1 for data transmission.

The formulated problem for relay selection is depicted below:

$$\min \quad T_{sd} = \sum_{i=1}^{N} \sum_{j=1}^{N} c_{ij} x_{ij}$$

$$x_{ij} = \begin{cases} 1, & \text{if relay is assigned to the source-destination} \\ & \quad \text{transmission pair} \\ 0, & \text{otherwise} \end{cases}$$

TABLE 5. Hungarian algorithm Table for the given problem.

	Relay1	Relay2	Relay3
Transmission Source1-Destination1	$T^1_{(s1d1)}$	$T^2_{(s1d1)}$	$T^3_{(s1d1)}$
Transmission Source2-Destination2	$T^1_{(s2d2)}$	$T^2_{(s2d2)}$	$T^3_{(s2d2)}$
Transmission Source3-Destination3	$T^1_{(s3d3)}$	$T^2_{(s3d3)}$	$T^3_{(s3d3)}$

$$C1 \quad \sum_{j=1}^{N} x_{ij} = 1 \text{ for i =1...N} \tag{6}$$

$$C2 \quad \sum_{i=1}^{N} x_{ij} = 1 \text{ for j =1...N} \tag{7}$$

The goal of the relay selection problem is to minimize the delay from source to destination T_{sd} for all source-destination pairs. Here c_{ij} represents the cost of each element in the cost matrix C. x_{ij} represents the assignment of transmissions to the relays, a value of 1 refers to assignment, and a value of 0 refers to no assignment. There are two constraints in this problem as shown in equations 6 and 7. Constraint 1 requires that all the relays must be assigned. Constrain 2 requires that all source-destination transmissions must be executed.

Algorithm 2 Relay Selection Using Hungarian Algorithm

```
Input: Cost matrix in the form $T_{sd}$ for all $N$ source-destination and relay pairs
Step1: Row Subtraction: Subtract the smallest cost in each row of the cost matrix from the complete row
Step2: Column Subtraction: Subtract the smallest cost in each column of the cost matrix from the complete column
Step3: Use the minimum number of lines to cover all zero entries of the rows and columns
Step4: If minimum number of lines are less than $N$, than assignment is not completed. Find the minimum cost that is still not covered by any line. Subtract this number from each uncovered item. Add this number to each item that is covered twice. Go to Step 3
Step5: If minimum number of lines are $N$, then assignment is completed
Return Assignment matrix $X_{ij}$
```

TABLE 6. Simulation parameters.

Parameters	Values
Number of IoT Nodes	50-300
Number of Source Nodes	5-30
Number of Eavesdroppers	2-12
Packet Size	100-500 kbytes
Maximum Data rate	10-50 Mbps
Security Strength	160-521 bits

Relay selection based on the Hungarian algorithm is shown in Algo. 2. The algorithm takes as input the cost matrix in the form of T_{sd}. The first step is row subtraction where the smallest cost in each row is subtracted from the complete row. The second step is column subtraction in which the smallest cost in each column is subtracted from the complete column. In step 3, the minimum number of lines is used to cover all zero entries of the rows and columns. Step 4 evaluates if the minimum number of lines is less than N, this means that the assignment is not complete. To move forward, the algorithm finds the minimum number that is still not covered by any line. This number is then subtracted from each uncovered item. Also, this number is added to each item that has been covered twice (by horizontal as well as vertical line). The algorithm moves to Step 3 again. Finally, the algorithm terminates when the number of lines is N. The final assignment matrix X_{ij} is returned.

V. PERFORMANCE EVALUATION

A. SIMULATION SCENARIO

The proposed algorithm is implemented in MATLAB software. The number of IoT nodes is varied from 50-300. Out of all the nodes, 10% nodes are assumed to be source nodes that are transmitting a message to some destination nodes. Thus, the number of source nodes is varied from 5-30. The number of malicious eavesdropper nodes is taken as 2-12. The remaining nodes in the network are potential relay nodes. The packet size is varied from 100-500 kbytes. The maximum

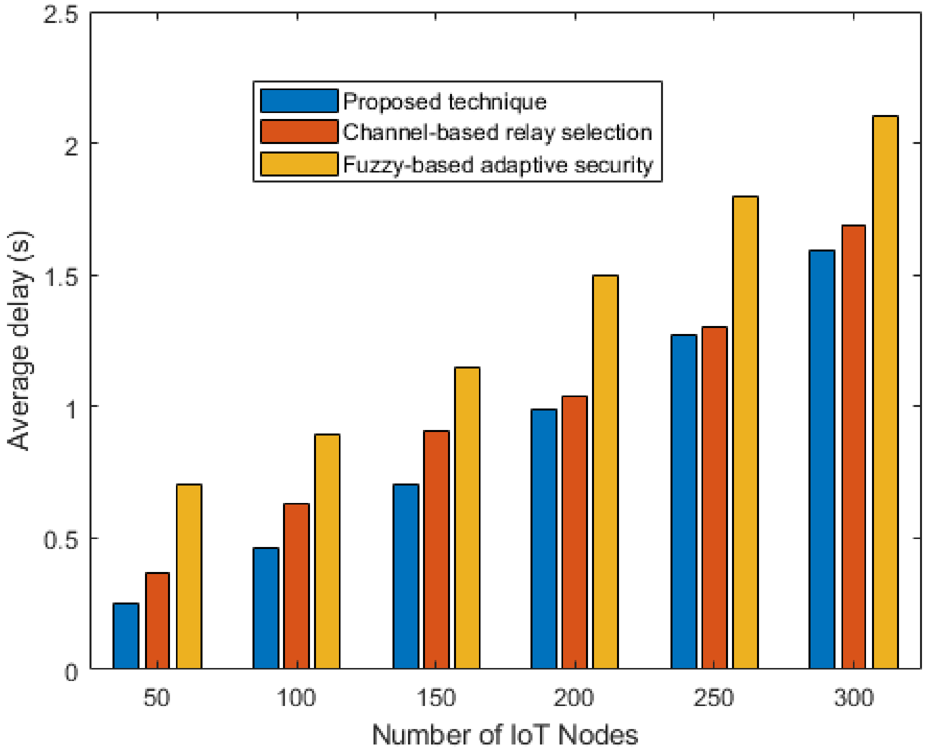

FIGURE 4. Average Delay vs Number of IoT Nodes.

data rate of the network is varied between 10-50 Mbps. The security strength varies between 160-521 bits as per Table 3. The simulation parameters are listed in Table 6

B. TECHNIQUES USED FOR COMPARISON

The performance of the proposed technique is compared with two other related techniques, one which focuses on relay selection and the other one which is based on adaptive security. The first technique is an intelligent relaying technique that uses channel quality and network load to select relay nodes [28]. Since this technique does not have an adaptive security feature, we consider that all nodes operate at a medium-level security strength of 256 bits. The second technique uses fuzzy-logic-based adaptive key size selection and reduces the security strength as network congestion is increased [20].

C. METRICS USED FOR COMPARISON

For comparison, we use delay from source to destination as per equation 4. We also evaluate two different components of the delay. The first is the security delay (including signature, encryption, verification, and decryption delay) at the relay and destination. The second component of delay is the transmission delay from the source to the relay node, and then to the destination node. The performance metrics also include the average security strength at which adaptive algorithms operate. This gives an idea of the level of cryptographic security in the network. Moreover, we also present the percentage of non-secure nodes which is defined as the percentage of nodes that operate below the mean security strength of the network and also have a secrecy rate of less than the mean secrecy rate. The rationale for using this metric is to identify the percentage of nodes that lack both cryptographic as well as physical layer security.

D. RESULTS

The plot in Fig. 4 shows the value of average delay against the number of IoT nodes. The average delay of the proposed technique remains below 1.5s even at the high density of IoT nodes. In comparison, the channel-based relay selection technique results in a 5-30% higher delay than the proposed technique at different numbers of IoT nodes. The fuzzy-based adaptive security exhibits the largest delay, particularly at a higher number of IoT nodes reaching up to 2.1s. The improvement in delay by the proposed technique is due to considering both channel quality and security adaptation in the relay selection.

In Fig. 5, the average delay is plotted against maximum data rate values. Note that the data rate experienced by each user depends on the number of transmitting nodes and the maximum data rate is divided among the users. It can be seen that the proposed technique has the best performance at different data rates. At 30 Mbps, the delay by the proposed technique, channel-based relay technique, and fuzzy-based adaptive security technique are 1.19s, 1.27s, and 1.58s respectively.

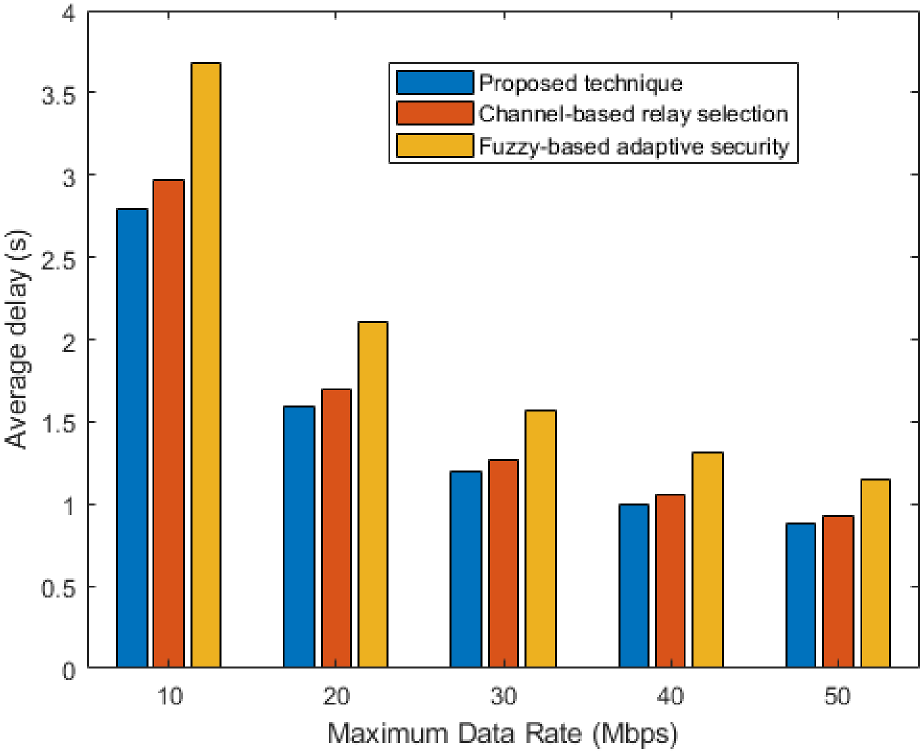

FIGURE 5. Average Delay vs Maximum Data Rate.

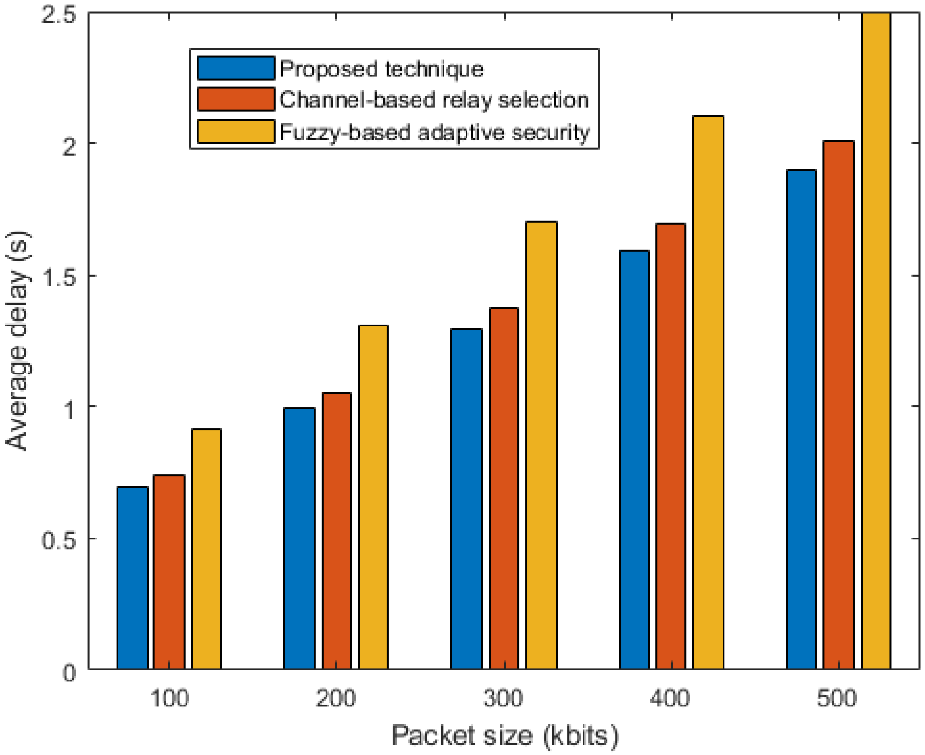

FIGURE 6. Average Delay vs Packet Size.

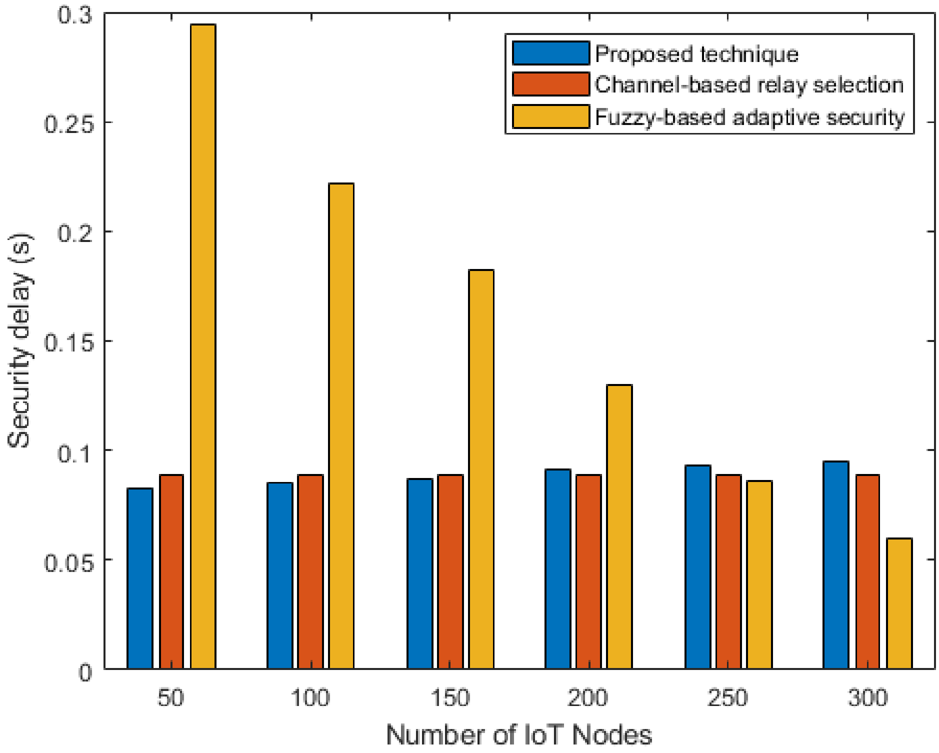

FIGURE 7. Security Delay vs Number of IoT Nodes.

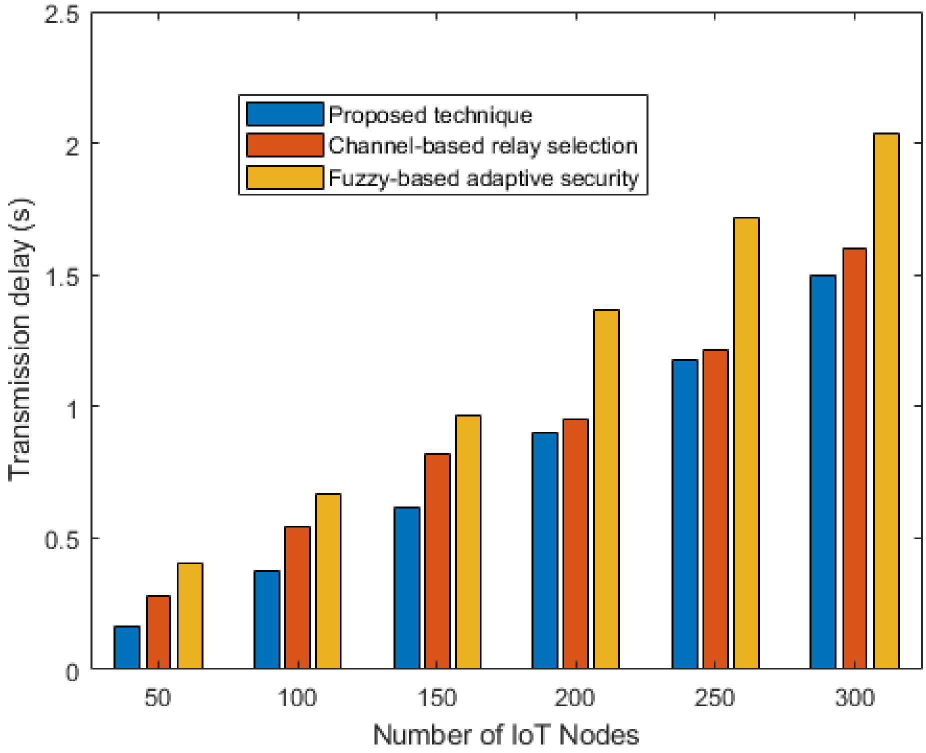

FIGURE 8. Transmission Delay vs Number of IoT Nodes.

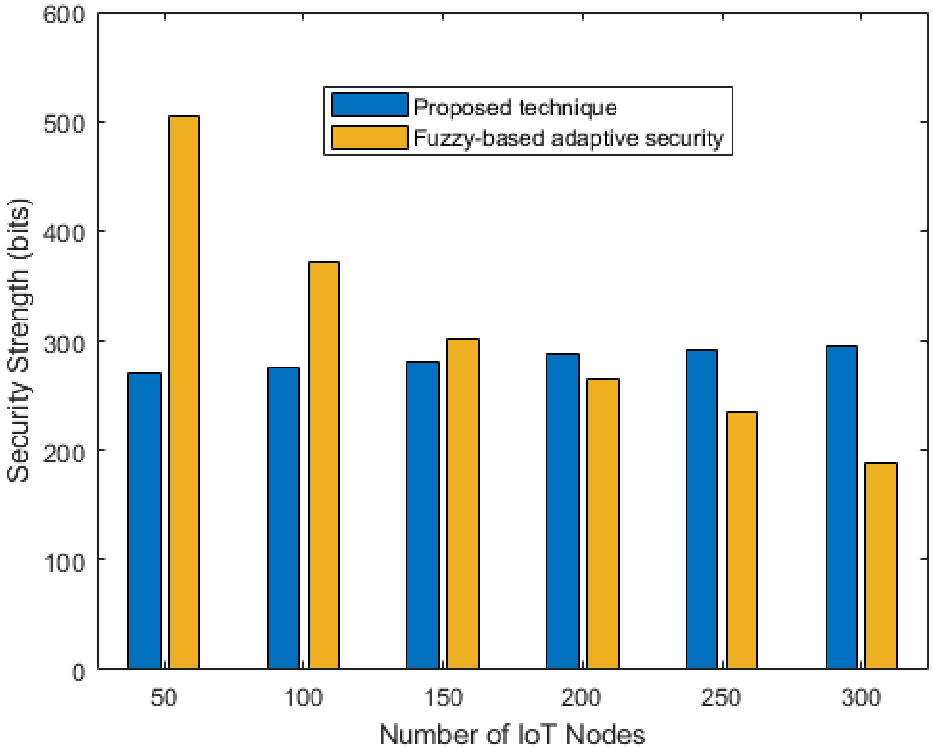

FIGURE 9. Security Strength vs Number of IoT Nodes.

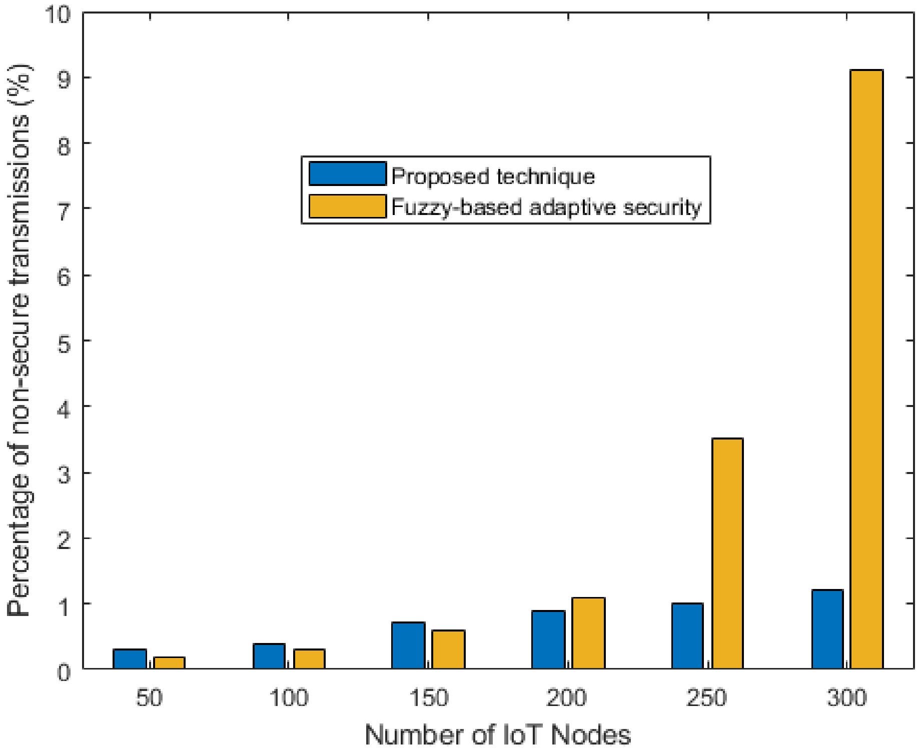

FIGURE 10. Percentage of non-secure transmissions vs Number of IoT Nodes.

The delay performance of the three techniques is also evaluated at different packet size values. As the packet size is increased, the average delay of all the techniques is increased. However, the proposed technique shows the best performance at all packet sizes. The reason for this improved performance is utilizing physical layer security to the benefit and adapting the security strength of the users accordingly. Moreover, the Hungarian-based relay selection selects optimal relaying to reduce delay.

The results in Fig. 7 show the security delay of all three protocols. It can be seen that the proposed technique maintains a security delay of around 0.9ms. This is because the algorithm uses k-means clustering to provide different levels of security strengths to different clusters. As a result, there exist nodes with all levels of security strength and hence, average security delay remains around the same value. For the channel-based relaying that does not use adaptive security, we consider a medium-level security, and hence its security delay remains the same at all network densities. Lastly, the fuzzy-based adaptive security technique reduces security strength with an increase in network density. Hence, its security delay decreases as the number of IoT nodes increases.

Fig. 8 shows transmission delay vs the number of IoT nodes in the network. It is evident from the results that the proposed technique has the best relay selection policy that results in the lowest delay. Channel-based relay selection exhibits up to 0.2s higher delay as compared to the proposed technique. On the other hand, the fuzzy-based adaptive technique shows up to 0.53s higher delay as compared to the proposed technique.

We also plot the security strength of the two adaptive security algorithms in Fig. 9. It can be seen that the proposed technique provides on average same level of security to the nodes. In comparison, the fuzzy-based adaptive technique has a high level of security strength at a lower number of nodes and vice versa. Thus, when the network density is high, the fuzzy-based adaptive technique reduces the security strength without considering secrecy rates.

In Fig. 10, we plot the percentage of non-secure transmissions against the number of IoT nodes. It can be seen that at a low number of nodes, most of the nodes operate at a reasonable level of security strength. However, at a higher number of IoT nodes, the level of security in the network is considerably reduced when using a fuzzy-based adaptive security algorithm. Up to 9% nodes operate at less than the mean level of security strength and secrecy rates. This issue is addressed by the proposed technique as it considers both adaptive security and secrecy rates in the algorithm and thus the percentage of non-secure nodes remains around 1%.

VI. CONCLUSION

The work in this paper considers a multi-hop IoT network that uses an Elliptic Curve Cryptography-based signature and encryption algorithm. The goal of the proposed work is to improve the delay of messages in IoT networks. To achieve this task, the proposed technique relies on two major parts. The first part provides an adaptive security technique to dynamically select the key sizes. The k-means clustering technique is used to categorize potential relay nodes in terms of their secrecy rate. Higher key sizes are allocated to the relay nodes with low secrecy rates. The second part of the proposed technique uses a Hungarian algorithm to select relay nodes that minimize the total delay. Simulation results highlight the improvement of the proposed technique in terms of total packet delay. In the future, we will consider the working of the proposed technique in scenarios where CSI information is not perfectly available.

REFERENCES

[1] I. Chakour, C. Daoui, M. Baslam, B. Sainz-De-Abajo, and B. Garcia-Zapirain, "Strategic bandwidth allocation for QoS in IoT gateway: Predicting future needs based on IoT device habits," *IEEE Access*, vol. 12, pp. 6590–6603, 2024.

[2] S. Baker and W. Xiang, "Artificial intelligence of things for smarter healthcare: A survey of advancements, challenges, and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1261–1293, 2nd Quart., 2023, doi: 10.1109/COMST.2023.3256323.

[3] J. Li, W. Liang, W. Xu, Z. Xu, Y. Li, and X. Jia, "Service home identification of multiple-source IoT applications in edge computing," *IEEE Trans. Services Comput.*, vol. 16, no. 2, pp. 1417–1430, Mar. 2023.

[4] Z. Zeng, C. Xie, W. Tao, Y. Zhu, and H. Cai, "Knowledge-graph-based IoTs entity discovery middleware for nonsmart sensor," *IEEE Trans. Ind. Informat.*, vol. 20, no. 2, pp. 2551–2563, Feb. 2024.

[5] G. Mao, Y. Liu, W. Dai, G. Li, Z. Zhang, A. H. F. Lam, and R. C. C. Cheung, "REALISE-IoT: RISC-V-based efficient and lightweight public-key system for IoT applications," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 3044–3055, Jan. 2024.

[6] Y. Madhwal, Y. Yanovich, S. Balachander, K. H. Poojaa, R. Saranya, and B. Subashini, "Enhancing supply chain efficiency and security: A proof of concept for IoT device integration with blockchain," *IEEE Access*, vol. 11, pp. 121173–121189, 2023.

[7] A. Rehman, K. Haseeb, T. Saba, J. Lloret, and U. Tariq, "Secured big data analytics for decision-oriented medical system using Internet of Things," *Electronics*, vol. 10, no. 11, p. 1273, May 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/11/1273

[8] M. Bahutair, A. Bouguettaya, and A. G. Neiat, "Multi-use trust in crowdsourced IoT services," *IEEE Trans. Services Comput.*, vol. 16, no. 2, pp. 1268–1281, Mar. 2023.

[9] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 53–87, 1st Quart., 2022.

[10] H. Cao, J. Du, H. Zhao, D. X. Luo, N. Kumar, L. Yang, and F. R. Yu, "Toward tailored resource allocation of slices in 6G networks with softwarization and virtualization," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6623–6637, May 2022.

[11] D. Marabissi, L. Mucchi, and A. Stomaci, "IoT nodes authentication and ID spoofing detection based on joint use of physical layer security and machine learning," *Future Internet*, vol. 14, no. 2, p. 61, Feb. 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/2/61

[12] K. Haseeb, Z. Jan, F. A. Alzahrani, and G. Jeon, "A secure mobile wireless sensor networks based protocol for smart data gathering with cloud," *Comput. Electr. Eng.*, vol. 97, Jan. 2022, Art. no. 107584. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790621005206

[13] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, and J. Zhang, "A semi-centralized trust management model based on blockchain for data exchange in IoT system," *IEEE Trans. Services Comput.*, vol. 16, no. 2, pp. 858–871, Mar. 2023.

[14] P. Vijayakumar, M. Azees, S. A. Kozlov, and J. J. P. C. Rodrigues, "An anonymous batch authentication and key exchange protocols for 6G enabled VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1630–1638, Feb. 2022.

[15] A. Rehman, T. Saba, K. Haseeb, R. Singh, and G. Jeon, "Smart health analysis system using regression analysis with iterative hashing for IoT communication networks," *Comput. Electr. Eng.*, vol. 104, Dec. 2022, Art. no. 108456. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790622006711

[16] S. A. Soleymani, S. Goudarzi, M. H. Anisi, Z. Movahedi, A. Jindal, and N. Kama, "PACMAN: Privacy-preserving authentication scheme for managing cybertwin-based 6G networking," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4902–4911, Jul. 2022.

[17] S. Dhelim, N. Aung, M. T. Kechadi, H. Ning, L. Chen, and A. Lakas, "Trust2Vec: Large-scale IoT trust management system based on signed network embeddings," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 553–562, Jan. 2023.

[18] E. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, Jul. 2015.

[19] G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta, and I. Tucker, "Bandwidth-efficient threshold EC-DSA revisited: Online/offline extensions, identifiable aborts proactive and adaptive security," *Theor. Comput. Sci.*, vol. 939, pp. 78–104, Jan. 2023. [Online]. Available: https://www.-sciencedirect.com/science/article/pii/S0304397522006004

[20] M. A. Javed, S. Zeadally, M. Usman, and G. A. S. Sidhu, "FASPM: Fuzzy logic-based adaptive security protocol for multihop data dissemination in intelligent transport systems," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 11, Nov. 2017, Art. no. e3190.

[21] T. Ovasapyan and D. Moskvin, "Security provision in WSN on the basis of the adaptive behavior of nodes," in *Proc. 4th World Conf. Smart Trends Syst., Secur. Sustainability (WorldS4)*, Jul. 2020, pp. 81–85.

[22] D. M. T. Hoang, T. V. Pham, A. T. Pham, and C. T. Nguyen, "Q-learning-based joint design of adaptive modulation and precoding for physical layer security in visible light communications," in *Proc. IEEE 97th Veh. Technol. Conf. (VTC-Spring)*, Jun. 2023, pp. 1–5.

[23] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "Trust in vehicles: Toward context-aware trust and attack resistance for the Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 9546–9560, Apr. 2023.

[24] B. Ying and A. Nayak, "A power-efficient and social-aware relay selection method for multi-hop D2D communications," *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1450–1453, Jul. 2018.

[25] S. Dayarathna, R. Senanayake, and J. Evans, "Optimal routing for multi-user multi-hop relay networks via dynamic programming," *IEEE Wireless Commun. Lett.*, vol. 11, no. 8, pp. 1713–1717, Aug. 2022.

[26] G. Si, Z. Dou, Y. Lin, L. Qi, and M. Wang, "Relay selection and secure connectivity analysis in energy harvesting multi-hop D2D networks," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1245–1248, Jun. 2022.

[27] H. Sun, M. Naraghi-Pour, W. Sheng, and Y. Han, "Performance analysis of incremental relaying in multi-hop relay networks," *IEEE Access*, vol. 8, pp. 68747–68761, 2020.

[28] M. Z. Khan, M. Rahim, M. A. Javed, F. Ghabban, O. Ameerbakhsh, and I. Alfadli, "A D2D assisted multi-hop data dissemination protocol for inter-UAV communication," *Int. J. Commun. Syst.*, vol. 34, no. 11, Jul. 2021, Art. no. e4857. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4857

[29] M. E. Morocho-Cayamcela, H. Lee, and W. Lim, "Machine learning to improve multi-hop searching and extended wireless reachability in V2X," *IEEE Commun. Lett.*, vol. 24, no. 7, pp. 1477–1481, Jul. 2020.

[30] M. O. Farooq, "Multi-hop communication protocol for LoRa with software-defined networking extension," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100379. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660521000238

[31] G. Chen, J. Tang, and J. P. Coon, "Optimal routing for multihop social-based D2D communications in the Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1880–1889, Jun. 2018.

[32] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, "Secure relaying in non-orthogonal multiple access: Trusted and untrusted scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 210–222, 2020.

[33] *Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters*, Standard NIST SP 800-186, Nat. Inst. Standards Technol., Feb. 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/186/final

[34] M. K. Pedhadiya, R. K. Jha, and H. G. Bhatt, "Device to device communication: A survey," *J. Netw. Comput. Appl.*, vol. 129, pp. 71–89, Mar. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804518303345

MUHAMMAD AWAIS JAVED (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Engineering and Technology, Lahore, Pakistan, in August 2008, and the Ph.D. degree in electrical engineering from The University of Newcastle, Australia, February, in 2015. From July 2015 to June 2016, he worked as a Postdoctoral Research Scientist at Qatar Mobility Innovations Center (QMIC) on the SafeITS Project. He is currently working as an Associate Professor with COMSATS University Islamabad, Pakistan. His research interests include intelligent transport systems, vehicular networks, protocol design for emerging wireless technologies, and the Internet of Things.

MOHAMMED ALKHATHAMI is currently working as an Associate Professor with the Department of Information Systems, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia. His research interests include communication systems, networks, security, and computing.

ABDULAZIZ ALMOHIMEED received the master's degree from Monash University, Australia, and the Ph.D. degree from the University of Southampton, U.K. He is currently an Assistant Professor with the College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia. His research interests include natural language processing, artificial intelligence, data science, the Internet of Things, and network security. He is passionate about leveraging technology to create innovative solutions.

ABEER ALMUJALLI received the master's degree from the College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia. Her research interests include communication networks, security, and smart cities.