Received 4 June 2024, accepted 28 July 2024, date of publication 5 August 2024, date of current version 15 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3438608

RESEARCH ARTICLE

TIHCS: Trust-Based Improved QoS for Health Care Systems in Smart Cities

HAIDER ALI[1], AHMAD NASEEM ALVI[1], MOHAMMED ALKHATHAMI[2], DEAFALLAH ALSADIE[3], (Member, IEEE), AND FATAMH ALASHAIB[2]

[1]Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), Islamabad 45550, Pakistan
[2]Information Systems Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia
[3]Department of Computer Science and Artificial Intelligence, College of Computing, Umm Al-Qura University, Makkah 21961, 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-RP23082).

ABSTRACT Healthcare management is a major application of future Internet of Things (IoT)-based smart cities. The healthcare applications rely on the use of Internet of Things (IoT) devices, which consist of sensor networks with diverse communication infrastructure. This makes it more vulnerable and increases the malicious attacks resulting in compromised Quality of Service (QoS) and anomalies in data transmission resulting in transmission delay of the legitimate nodes in the network. This may cause life threats in the healthcare system as critically ill patients' data needs to be delivered to the centralized healthcare centre of the smart cities. In this work, a Trust-based Improved QoS for Health Care System (*TIHCS*) is proposed. *TIHCS* offers a Time Division Multiple Access (TDMA) based slots allocation mechanism for legitimate nodes by introducing a malicious detection mechanism. In addition, it proposes a mechanism based on the Intelligent Reflecting Surfaces (IRS) to restrict the communication of the specific area where a malicious node is present and allow legitimate nodes of the affected area through relay node selection by proposing a Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). The simulation results show that TOPSIS-based relay selection in *TIHCS* offers a better secrecy sum rate as compared to the other three methods. Furthermore, the proposed trust-supported TDMA-based Media Access Control (MAC) protocol offers improved data transmission of the most sensitive data traffic, by allowing more highly sensitive data nodes to transmit their data as compared to the well-established standards such as First Come First Serve, Round Robin, Shortest Job First, and Longest Job First.

INDEX TERMS Trust management, smart cities, IoT, healthcare, anomaly detection.

I. INTRODUCTION

The past decade has witnessed a notable surge in the adoption of smart cities, driven by the desire for enhanced security and convenience in human lifestyles. In these smart urban environments, residents benefit from a range of intelligent services, including IoT-based healthcare, smart agriculture, live surveillance, advanced industrial processes, and intelligent transportation systems [1], [2]. The successful implementation of these applications relies on improved communication and the continuous evolution of information technologies, ensuring the secure and reliable delivery of data [3], [4], [5].

Healthcare application is one of the highest-value applications in a smart city. Small, lightweight, and wearable biomedical sensor nodes are used to monitor different health parameters of the human body such as blood pressure, sugar level, heart rate and other vital parameters to diagnose different diseases. These health parameters are forwarded to the health centre or hospitals through nearby placed fog computing nodes as shown in Figure 1.

In smart city healthcare systems, IoT applications rely on wireless sensor networks for data transmission. Nodes access medium either by contending with other nodes or by using

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

© 2024 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

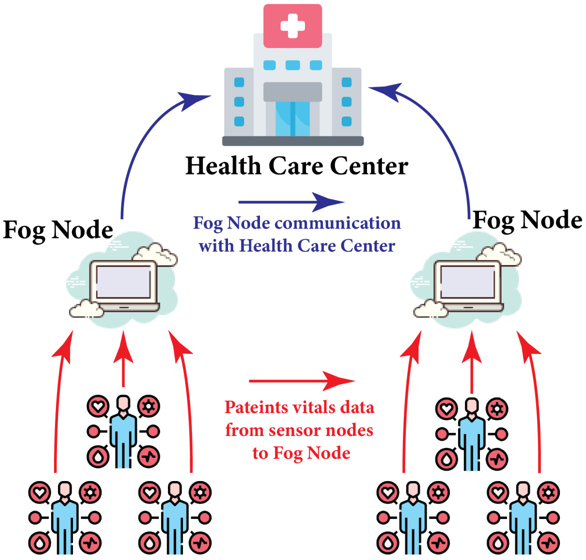
Health Care Center
Fog Node
Fog Node communication with Health Care Center
Fog Node
Pateints vitals data from sensor nodes to Fog Node

FIGURE 1. Fog enabled health care system.

dedicated slots. In contention-based medium access, nodes compete for medium access, leading to collision risks as node count increases [6], [7]. However, transferring their data through dedicated slots reduces collision risks, especially in high-node scenarios [8], [9], [10], [11]. Healthcare data demands efficient communication for real-time monitoring and healthcare applications, that's why, contention-free MAC protocols are preferred due to reliable data transmission while minimizing collision risks.

In IoT networks, wireless mediums are susceptible to interference from malicious nodes which introduce anomalies into the network, diminishing its trustworthiness and compromising the QoS [12], [13], [14], [15]. Identifying attacks during contention periods proves challenging due to collision probabilities, medium congestion, and the unfairness resulting from node occupation. As a result, the allocation of dedicated time slots for data-sending nodes to access the medium is preferred, facilitating the detection of interference from other nodes. However, malicious nodes can impersonate legitimate members by gaining guaranteed slots access resulting in reduced fruitful utilization of the medium.

In the healthcare system, sensor nodes collect and transmit data on patient vital parameters at varying time intervals, requiring adaptability. The conventional TDMA based MAC protocol offers same-size time slots to all member nodes without considering their data requirements. An adaptive data requirement-assisted TDMA-based MAC protocol is essential to address the adaptive data requirements and to improve the medium utilization. For secure and reliable data communication, an anomaly detection mechanism is required to verify the nodes' authenticity.

The focus of this paper is on specific security attacks by the malicious nodes in which they capture the time slots in an IoT network and do not transmit any data in it, thus wasting the bandwidth of the system. As compared to traditional denial of service attacks, here the malicious users save their own transmission power by only capturing the time slot without transmitting any data. Such attacks have negative impact on Quality of Service (QoS) of applications as throughput of the network is reduced and nodes with critical data may experience higher time delays.

In this work, a Trust-based Improved QoS for Health Care System in Smart Cities (*TIHCS*) is proposed for an efficient allocation of data slots. The proposed scheme allows fog computing nodes to detect malicious nodes, blocks their communications and improves the QoS of the network by allowing legitimate nodes to transfer their data through nearby legitimate nodes. The salient features of *TIHCS* are mentioned below.

1) TDMA-based MAC protocol to efficiently allocate the number of time slots to increase the data transmission in a communication session.
2) Malicious nodes detection mechanism by proposing a trust management scheme.
3) Restrict the communication region of the malicious nodes by using an IRS.
4) Improve the communication of the affected region through the relaying node mechanism.

The following sections will be covered in this paper: - Section II: Previous research related to trust management in various aspects. - Section III: A description of the system model. - Section IV: Our proposed scheme including TDMA-based communication session, anomaly detection mechanism, IRS-based restricting the communication of the specific area, and relay selection criteria for the affected nodes. - Section V: A comparative results analysis with extensive simulations. - Section VI: Conclusion of the manuscript.

II. RELATED WORK

The swift emergence of smart cities is primarily driven by the aim to enhance human lifestyles, particularly in areas like healthcare. However, the quality of the network is compromised by malicious attacks. Ensuring secure and trustworthy data delivery poses significant challenges within the healthcare system of smart cities, making it a focal point of extensive research in recent times.

In the citation labelled as [16], the Distributed Dynamic Mutual Identity Authentication (DDMIA) system is introduced to address the needs of patients referred from primary healthcare centres to specialized medical care. DDMIA employs blockchain technology to facilitate the transfer of patient data to the referred medical facility without relying on the traditional registration process. The authors in [17] highlight the significance of utilizing blockchain technology for the exchange of patient information. They propose an extensive information infrastructure that leverages smart contracts as information mediators. These smart contracts, backed by Electronic Health Records, ensure the creation of immutable, authentic, and easily accessible medical health records, promoting both privacy and expedited payment processes.

In the [18], the work by Ebrahimi et al. centres on an IoT-assisted healthcare system. They develop a decentralized trust management model within this system. The approach involves using evidence distance measurement to mitigate malicious attacks on healthcare systems. This is achieved by rewarding healthcare service providers and penalizing malicious users. In [19] a system is presented by introducing a Physical Unclonable Function (PUF)-based authentication scheme and a data-driven fault-tolerant decision-making scheme for designing an IoT-based modern healthcare system.

Authors in [20] present a context-based adaptive trust solution for smart healthcare environments using a Bayesian approach and similarity measures. They assigned adaptive weights to direct and indirect trust using entropy values to ensure the minimization of trust bias as opposed to static weighting. Context-based similarity calculations filter out recommender nodes with malicious intent using server, social contact, and service similarity. A blockchain based framework is implemented to safeguard patients' personal information and insurance policy in [21]. The authors propose a solution for the healthcare system that provides data privacy and transparency. Furthermore, in the proposed system, insurance policies are incorporated into the blockchain via the Ethereum platform and data privacy is shielded with cryptographic tools.

An integrated framework for green healthcare and the use of cutting-edge technology to make an interactive user interface was presented in [22]. They also ensured the system's scalability and performance ratio. An interface was designed and developed for patients and doctors, where patients can send their healthcare data using wearable sensors, and doctors can receive those data in real time. For data identification and analysis, a Hierarchical Clustering Algorithm was adopted to build an interactive healthcare experience. A timestamp mechanism and the Elliptic Curve Cryptography (ECC) to improve anonymous authentication protocol for a smart healthcare system is proposed in [23]. The security of this protocol is verified by Burrows-Abadi-Needham logic and Automated Validation of Internet Security Protocols and Applications (AVISPA) tools, and security features and efficiency analysis are performed with other related schemes.

A reference document related to the IoT and healthcare-monitoring systems is presented in [24]. In their work, recent research on IoT-based health-monitoring systems have been reviewed and analyzed in a systematic way. it also discuss IoT wearable things in healthcare systems and provide a classification of health-monitoring sensors, including the challenges and open issues regarding security and privacy and QoS. A cryptography algorithm embedded into the sensor device such that the packets generated with patient's health data is proposed in [25]. These encryptions are done right at the sensor device before being transmitted. The proof of concept has been verified using a lab setup with two level encryptions at the IoT sensor level and two level decryption at the receiving end at the doctor's office.

Authors in [26] and [27] focused on the challenges facing the patient-centric healthcare system are brought to attention, and a blockchain-driven remedy is suggested. The solution outlined in [26] relies on the decentralized ledger technology of blockchain to enhance patient data privacy and security. Meanwhile, in [27], the authors explore concerns related to the Internet of Medical Things (IoMT), blockchain, and cloud computing, proposing a real-time remote healthcare system structured around one-to-one care.

III. SYSTEM MODEL

IoT nodes are deployed on the human body to monitor the continuous health monitoring of patients. The vital signs of these sensor nodes are forwarded to their centralized node. All the collective data of body sensors are forwarded to the nearby fog computing nodes. From these fog computing nodes, the data is forwarded to the centralized healthcare centre for monitoring and necessary treatment of the patient as shown in figure 1.

Suppose there is N number of different types of health sensing nodes attached to a patient that are transmitting D data within each t time instance. If there are K patients in a communication area of a fog node, then the total amount of data TD that is transmitted to the fog node is calculated as:

$$TD = \sum_{i=1}^{N} \sum_{j=1}^{K} D_{i,j} \tag{1}$$

The vital signs data of the human body is divided into three levels of sensitivity, such as, high, medium, and low represented as TD_H, TD_M, and TD_L respectively. The TD is the collective sum of all three different types of data.

Each centralized node transmits the data to its fog computing node through a wireless communication channel. The received signal at the fog computing node Rx with transmission power P_f from the patient node Tx, is given as:

$$y_f = \sqrt{P_f} h_f x_0 + n_f, \tag{2}$$

where h_f denotes the channel between the Tx and Rx. n_f is the noise at the Rx, which is assumed to follow a Gaussian distribution with zero-mean and variance σ_f^2. The SNR is represented as

$$SNR = \rho_f |h_f|^2 \tag{3}$$

where, $\rho_f = P_f/\sigma_f^2$. The Channel Capacity (CC) between the patient's centralized node and the fog node is then calculated as:

$$CC = B \times log_2(1 + SNR) \tag{4}$$

where SNR is the signal-to-noise ratio of the communication channel, and B represents the channel bandwidth. The channel capacity at the malicious node

TABLE 1. Summary table of literature review.

Paper	*Scheme*	*Findings*	*Limitations*
[16]	*Distributed Dynamic Mutual Identity Authentication (DDMIA) system*	*Blockchain technology to facilitate the transfer of patient data to the referred medical facility without relying on the traditional registration process.*	*For a large number of patients running this scheme could be costly and may slow down the blockchain network..*
[17]	*Smart contracts for blockchain technology to record patient electronic health data*	*Ensure immutable, authentic and easy access to medical health records with secure payment processes*	*Authenticity within the blockchain is maintained however, during the medium access the vulnerability of data to malicious nodes is not proposed.*
[18]	*Decentralized trust management model*	*Trust management model can mitigate malicious attacks and penalise malicious users.*	*Data privacy, or real-world implementation issues that could arise when applying the decentralized trust management model.*
[19]	*Physical Unclonable Function based authentication scheme.*	*PUF scheme is fault tolerant to vulnerabilities of IoT applications.*	*Potential concerns related to the reliability, security and scalability of the authentication scheme.*
[20]	*Context-based adaptive trust solution for smart healthcare*	*Adaptive weights to direct and indirect trust using entropy values ensure the minimization of trust bias.*	*Computational overhead of implementing it in real-world smart healthcare environments.*
[21]	*Ethereum platform for data privacy*	*Block chain-based platform are beneficial for data privacy.*	*For large number of patients running this scheme could be costly and may slowdown the blockchain network.*
[22]	*A green integrated framework for interactive healthcare system*	*The advantages of cloud platform and mobile application can ensure seamless healthcare access.*	*Potential concerns such as the accuracy and reliability of data collected from wearable sensors is not addressed.*
[23]	*A timestamp mechanism and ECC for anonymous authentication protocol*	*The proposed protocol along with AVISPA can provide secure mutual authentication and resist various security attacks.*	*Computational overhead and resource requirements associated with implementing ECC in resource-constrained smart healthcare systems.*
[24]	*A review of IoT and health monitoring systems*	*The benefits of using the IoT have made it possible to automate healthcare systems in the best way.*	*Feasibility of implementing Quality of Service (QoS) measures in real-world applications is missing.*
[25]	*Encryption of Patients data at the transmission ends*	*Two level encryption and decryption can secure the patients data significantly.*	*Energy consumption in implementing cryptography algorithms and feasibility of the proposed encryption-decryption process in diverse healthcare environments.*

can also be calculated as

$$CC_m = B \times log_2(1 + \rho_m|h_m|^2) \qquad (5)$$

where, $\rho_m = P_f/\sigma_f^2$, h_m denotes the channel between the patient node and malicious node.

Suppose there are M malicious nodes present in the communication range of a fog node which access the communication medium and each of the M nodes occupies the channel by transmitting the FD amount of forged data to the fog node. If out of N number of total nodes, there are M malicious nodes transmitting their data then the total amount of data that is transmitted by legitimate nodes (TD_{Leg}) is calculated as:

$$TD_{Leg} = \sum_{i=1}^{N}\sum_{j=1}^{K} D_{i,j} - \sum_{k=1}^{M} FD_k \qquad (6)$$

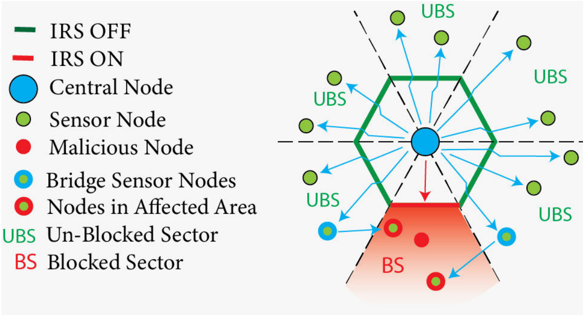

FIGURE 2. System model.

The more malicious attacks in the medium, the less amount of legitimate node data is transmitted to the fog node and the requested data slots are not allocated to legitimate nodes. Out of the total T number of Guaranteed Time Slots (GTS) requests, there are X number of GTS requests of the legitimate nodes and Y number of GTS requests of malicious nodes are assigned. If there are η GTS available in a session then the total number of GTS that were not assigned (GTS_{wasted}) to the legitimate nodes in Z number of sessions are calculated as:

$$GTS_{wasted} = \sum_{i=1}^{Z} (\eta - Y)_i \tag{7}$$

Each fog node is supposed to be surrounded by several patients which are categorized into S number of sectors. In each sector, there are varying numbers of patient nodes having different sensitivity levels of patients' data. If there are P number of patients in each sector, then the total number of patients TP available in the communication range of the fog node is the sum of all the patients available in all the sectors.

Malicious nodes present in any sector disturb the communication of all the legitimate nodes in the medium and compromise the QoS of the network. To improve the QoS, malicious node needs to be blocked. Blocking the communication of that sector where the malicious node is present, restricts the communication of the legitimate nodes present in that sector. This results in the reduced total patients' data (ζ) that is transmitted by the legitimate nodes is reduced. The system model in figure III shows the blocking sector of the malicious node's sector along with affected nodes present in the area.

If there are A number of sectors blocked and there are P number of patients available in each sector transmitting data PD, then ζ for Z number of sessions is calculated as:

$$\zeta = \sum_{j=1}^{Z} \sum_{i=1}^{S-A} DP_{i,j} \tag{8}$$

IV. PROPOSED SCHEME

Sensor nodes on the human body in health care applications of smart cities wirelessly communicate with the central node such as the fog node. Data communication in a wireless medium is vulnerable and may be under malicious attacks, resulting in a compromised QoS. The difficulty in identifying malicious attacks from nodes upon joining the network extends to the challenges of recognizing malicious access attempts during contention periods. Hence, allocating guaranteed slots to data-sending nodes is required to overcome these challenges. Furthermore, the network performance is compromised when malicious node/s transmits packets after regular intervals to affect the communication of the network with an increased collision rate. The increased collision rate compromises the QoS of the network with increases in network latency as well as a decrease in data transmission rate with reduced channel utilization. In this work, a Trust-based Improved QoS for Health Care System (TIHCS) is proposed to allocate guaranteed time slots to the legitimate nodes in transferring their data to the fog node. In addition, TIHCS identifies the malicious nodes and then nullifies their effect by restricting the communication area around it and then allowing other legitimate nodes in the affected area to communicate through the relay node. The salient features of TIHCS are mentioned below.

- The MAC protocol proposed in TIHCS adapts data slots in each session to meet the necessary data requirements of patients' sensing nodes.
- TIHCS computes the anomaly in the medium by evaluating the trust of each networking node.
- TIHCS blocks the malicious nodes by restricting the communication of the area with the help of the IRS.
- TIHCS proposes an efficient relay selection mechanism to allow the communication of the legitimate nodes present in the affected areas of malicious nodes.

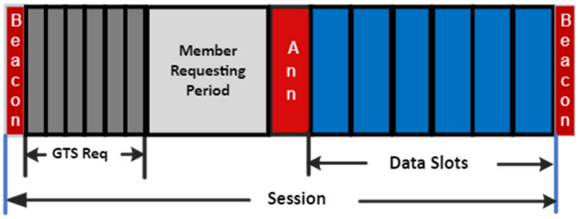

FIGURE 3. A communication session of the proposed MAC protocol.

A. PROPOSED MAC PROTOCOL

A communication session in the proposed TDMA-based protocol starts with a beacon message originating from the nearby fog node. In addition to a beacon frame, a communication session comprises of GTS requesting period, a Member Requesting period (MRP), an announcement period, and data slots. A complete communication session of the proposed scheme is shown in Figure 3.

1) BEACON FRAME (BF)

The beacon frame is transmitted by the fog node and it indicates the initiation of each session in the proposed scheme. The beacon frame contains information about the start of the member requesting period. In addition, it informs all the member nodes of a separate control slot by informing their starting slot number. The announcement period arrives (Ann_{arr}) after a fixed duration and is calculated with the help of the following formula as:

$$Ann_{arr} = 32 \times BSD$$

here, BSD is calculated by considering 250 BSD in a session and maximum duration of a session is 1 sec and the duration of each BSD is 4 msec.

The modulation scheme in the proposed MAC similar to the IEEE 802.15.4 standard offers 4 bits/symbol and offers a data rate of 250 kbps. The number of bits in a BSD (BSD_b) is calculated as:

$$BSD_b = \frac{250000 \times 4 \times CC}{1000}$$

here, CC represents the channel capacity of the communication link between a health node and the fog node as calculated in Eq. 4.

2) GTS REQUESTING PERIOD

GTS Requesting Period (GRP) comprises dedicated control slots for each member node. A dedicated control period is allocated to all member nodes in a session to send their GTS requests to the fog node. Those nodes that have data and require time slots send their GTS request along with their 2-bit data priority level mentioning High, Medium, and Low severity levels of data to the fog node during their allocated control slot. Each Control Slot Duration (CSD) and number of bits transferred in a control slot (CS_{bit}) is calculated as:

$$CSD = \frac{BSD}{8} \tag{9}$$

$$CS_{bit} = \frac{BSD_b}{8} \tag{10}$$

Each node can determine the GTS required (GTS_R) to send its data D to the fog node with the help of BSD as:

$$GTS_R = \left\lceil \frac{D_n}{BSD} \right\rceil \tag{11}$$

3) MEMBERSHIP REQUESTING PERIOD

During the Membership Requesting Period (MRP), the fog node allows a new health node to become a member of the network. This is a contention access period and the non-member health nodes send their join request messages to the fog node by applying the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithm as described in the IEEE 802.15.4 standard.

The combined duration of the GRP and MRP is fixed. When there are fewer members attached to the fog node, it allows more nodes to become members of the network by allowing more join requests resulting in an increased MRP. However, as the proposed MAC protocol accommodates a maximum of 256 nodes, the MRP reduces with the increased number of member nodes. MRP in a session is calculated as:

$$MRP = Ann_{arr} - GRP \tag{12}$$

A non-member node, that intends to become a member of this network, sends the join request message to the fog node, and the fog node after receiving this message informs the non-member node about the grant of its membership during the upcoming announcement period and assigns a unique 8-bit short address throughout its connectivity with the fog node.

4) ANNOUNCEMENT PERIOD (AP)

The fog node at the end of MRP calculates the total GTS requests received. If requested GTS are within the available slots then all the GTS requests will be fulfilled by preferring high-priority nodes first to send their data. In case, the requested GTS are more than the available limit then preference is assigned to the nodes which have a higher sensitivity level. All the successful nodes are informed about their allocated GTS by providing the information of their initial slot number along with the number of slots assigned.

5) DATA TRANSMISSION TIME SLOTS

Upon the conclusion of the announcement period, all the successful nodes become aware of their assigned GTS. Each Data Transmission Period (DTP) in a session encompasses time slots. Nodes that have been granted GTS are authorized to send their data to the fog node during their designated time slots. The duration of the Data Transmission Period varies according to the allocated GTS. If GTS requests are less than the maximum available limit in a session then the session concludes immediately. However, it may extend to its maximum limit if GTS requests exceed the DTP capacity. The available data slot capacity (DTS_{CAP} depends upon the BSD, BF, and AP in a session and it is calculated as:

$$DTS_{CAP} = [BSD \times (250 - (GRP + MRP))] - \left\lceil \frac{BF + AP}{BSD} \right\rceil \tag{13}$$

B. ANOMALY DETECTION

If the number of packets by data requesting nodes is not received by the fog node then it causes an anomaly in the network. This may be due to a noisy channel or may be due to malicious attacks in the medium. A trust mechanism is developed to detect the anomaly in the network, where the trust value of nodes is detected. The presence of malicious nodes is determined by finding out the trust value of the medium. If the trust value is greater than the certain threshold limit, then an anomaly in the network is supposed to be due to malicious attacks. However, there is no attack if it is less than a minimum threshold limit. However, if it is between the upper and lower threshold values then it is not certain that the anomaly is due to malicious nodes.

The focus of this work is to determine the anomaly due to malicious nodes. For this, the legitimacy of all the nodes present in the network is determined. Nodes' trust level is determined through interactions with their neighbours as well as with the centralized fog nodes during an exchange of control packets. This evaluation includes the packets received, correctly received packets against the originated requests and the channel capacity between the sender and receiver. For instance, if a node N_a sends K number of requested packets to its neighbouring node N_b and receives J number of response files from node N_b. Out of these J number of files, M number of packets are incorrectly received. If CC_{a-b} is the channel capacity between a and b nodes, then the trust level of node N_a for node N_b (T_b^a) is calculated as:

$$T_b^a = \frac{J - M}{K \times CC_{a-b}} \tag{14}$$

The probability of the presence of a malicious node in this work is determined by calculating the trust level a node has on the other nodes in the network.

A fog node calculates the trust value by computing each of its associated member nodes with a direct exchange of data and control frames with the trust-finding node. The fog node calculates the trust value by considering varying factors such as GTS request patterns including several requested GTS in a session, repeated and abnormal GTS requests, and regular or irregular requests arrival rate. If node 'A' exchanges m frames with the fog node, and the trust value of each of the i^{th} frames is calculated as T_i^{tf} then the fog node calculates the trust value of node 'A" (A^{tf}) as:

$$A^{tf} = \frac{\sum_{i=1}^{m} T_i^{tf}}{m} \tag{15}$$

A possible threat emanates from a malicious node with the capability to transmit a deceptive trust value. On the other hand, an authentic node would faithfully convey the true trust value of its neighbouring nodes. Completely relying on the node's self-trust value will not provide a clear picture of the trustworthiness of the node. To validate the trustworthiness of a node, trust values determine by all other nodes present in the cluster are also required to be considered. In this work, all those nodes that are in direct connection with the trust-finding nodes are also required to send their trust value to the fog computing node to get a clear picture of the trust-finding node.

Trust value of a member node T_N^{tf} is calculated by considering an input from all its available N neighbours as:

$$T_N^{tf} = \frac{\sum_{i=1}^{N} T_i^{tf}}{N} \tag{16}$$

Legitimate probability of all member nodes in a cluster is calculated by applying a weighted metric on the two different types of trust values calculated in equations 15 and 16 in such a way that the self-determining trust is assigned less weight and the trust value determined by the neighbouring nodes are highly weighted.

A trust evaluation function (δ) is formulated to ascertain the trust probability against each of the member nodes associated with the fog node, and it is computed as:

$$\delta(S_i) = \frac{1}{1 + e^{-[a(A_i^{tf}) + T_N^{tf}(T^{tf} i)]}} \tag{17}$$

Here 'a' is a weighted metric and its value is considered high as the trust value calculated by the fog node is more weighted as compared to the trust value calculated by the neighbouring node.

The higher the probability calculated, the more the node would be trustworthy and GTS requests of higher trusted over nodes with lower probabilities. However, if the trust probability falls below a critical value, its GTS request will not be entertained. Algorithm 1 outlines the complete procedure.

Algorithm 1 Trust Evaluation Criteria for Fog Node

```
Legitimate nodes determining criteria
Input:
Member nodes $N$
Trust threshold $V_{th}$
Self-trust of member nodes $T_1^{tf}, T_2^{tf}, \ldots, T_N^{tf}$
Neighboring nodes trust for node $x = T_{ndx}^{tf}$
for $i = 1$ to $N$ do
    Calculate $\delta Z_i$ for all member nodes
    if $\delta Z_i \leq V_{th}$ then
        Mark node as Malicious
    end
    else
        Mark node as Legitimate
    end
    Increment $i$
end
```

C. RESTRICTING COMMUNICATION REGION OF MALICIOUS NODES

After successfully detecting the presence of a malicious node in the network, its attacks are required to be restricted. To restrict its attack on the network, its communication channel needs to be restricted. In this work, an Intelligent Reflecting Surface (IRS) is used to restrict the communication area of the malicious node.

1) INTELLIGENT REFLECTING SURFACE

IRS is an advanced technology in wireless communication systems that leverages reconfigurable meta-surfaces to intelligently control and manipulate Radio Frequency (RF) signals. Unlike traditional static reflective surfaces, IRS can dynamically adjust its reflective properties in real time to optimize wireless communication performance. IRS finds applications in various wireless communication scenarios, including indoor and outdoor environments, smart cities, and Internet of Things deployments. It can be used to improve connectivity, data rates, and overall network performance.

Figure 4 depicts a 2-D design for a tuneable wideband absorber utilizing active elements along with its switchable transmission response. Figure 4a presents the schematic representation of this switchable surface. The unit element is

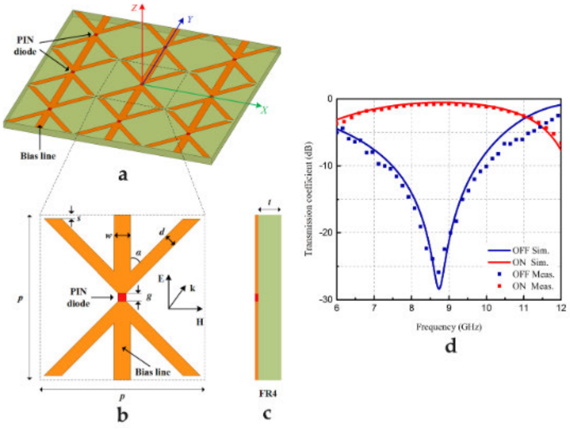

FIGURE 4. Intelligent reflecting surface.

depicted in figures 4b and 4c, showcasing both top and side views. The fundamental unit element in this design consists of a one-sided pattern on a dielectric substrate. The pattern comprises a series arrangement of two opposing anchor-shaped strips with a PIN diode placed in between. The biasing for the diodes is carried out by the straight vertical strips connecting them. This allows voltage supply to the diodes without the need for additional DC bias lines in the whole design.This design is realized on FR4 with a thickness (t) of 1 mm, having $\epsilon r = 4.4$ and a loss tangent of 0.02. The PIN diodes utilized are NXP BAP 70-03 silicon diodes, with the datasheet provided in [28]. The final design dimensions of the unit cell are shown in Table 2.

In figure 4b, as the design is vertically oriented hence it is a polarization dependent, making it responsive to plane waves with TM polarizations. Figure 4d illustrates the frequency responses of this switchable surface. Notably, the surface resonates at 8.7GHz with a transmission coefficient of -26.2dB in the OFF state. On the contrary, in the ON state, it functions as a transparent surface at 8.7GHz with a transmission coefficient of -0.7dB.

An IRS with real-time switching capabilities plays a crucial role in isolating a malicious node to enhance the efficiency of a wireless sensor network. For example, an IRS could be used to create a virtual barrier around a confidential data centre or to prevent a malicious user from eavesdropping on communications between two trusted nodes.

Figure 2 illustrates the scenario used in this work to restrict the communication area of the malicious node. In this work, we consider that IRS assisted fog node is surrounded by different healthcare sensor nodes in a hexagonal pattern, that comprises six segments, and IRS can independently switch any of the specific regions as and when required. This helps the fog node restrict the transmissions in any of the malicious node's sectors by activating the corresponding IRS section. Restricting the transmission of malicious node's sector restricts the communication of other legitimate nodes present in that area.

D. COMMUNICATION IN RESTRICTED AREA

The communication of the legitimate nodes present in the restricted area is facilitated through relay nodes present in the adjacent areas. Each legitimate node in the blocked area is allowed to transmit its data through a separate relay node as shown in figure III. The relay nodes are selected by applying TOPSIS.

TOPSIS provides a preference list by providing a multiple criteria-based TOPSIS score. It calculates the TOPSIS value to generate a preference list. The nodes with the highest TOPSIS values are selected as relay nodes. The TOPSIS value in the relay selection method is based on the following criteria parameters.

1) **Residual Energy (RE)** The residual energy is the amount of energy a wireless node holds. The nodes with higher residual energy are preferred over other nodes.
2) **Secrecy Rate (SR)** Defined as the difference of the rate at the destination and the eavesdropper i.e., $R_s = max(CC - CCm, 0)$. Where CC and CCm are defined in Eq. 4 and Eq. 5. The nodes with that provide higher secrecy rate will be preferred over the one which will give lower secrecy rate.
3) **Self-data Transmission (ST)** The node with no data to transmit in the current session should be preferred over nodes that have to transmit data in the current session.

Fog node already has the location information along with the residual energy of all the nodes present in its communication area. In addition, the fog node also has an updated trust value of all the nodes present in the network and also knows the nodes that have not requested the data slots in the upcoming session. The fog node computes the TOPSIS value of all the legitimate nodes present in the surrounding non-affected area adjacent to the affected sector. The TOPSIS value is calculated in the following steps.

1) Each selection-based parameter value is normalized to bring it to a comparable scale. It is done by dividing each criterion parameter value by the square root of the sum of the squared values for that criterion across all alternatives.
2) Multiply all the normalized values of different criterion parameters with their respective weights and add them for each alternative.
3) The maximum and minimum ideal values across all alternatives are determined to represent the best and worst possible performances for each parameter.
4) Calculate Euclidean distances for each candidate relay node to find out the difference between the weighted normalized and the ideal and negative-ideal solutions as mentioned below Eq.18.

$$S_i(Criterion) = \frac{d_i^-}{d_i^+ + d_i^-} \tag{18}$$

Here, d_i^+ and d_i^- are the distances calculated from the positive and negative ideals respectively. This step quantifies how close or far each alternative is from

TABLE 2. Dimensions of a unit cell.

Parameter	*P (mm)*	*W (mm)*	*d (mm)*	*g (mm)*	*s (mm)*	*t (mm)*	*α(degree)*
Value	*20*	*2*	*1.5*	*1*	*0.5*	*1*	*45*

the ideal and negative-ideal solutions for each criterion parameter.

5) TOPSIS score for each candidate node is calculated by combining the relative closeness values for all criteria by following the equation 19.

$$V_i = \frac{1}{3}(S_i(RE) + S_i(SR) + S_i(ST)) \tag{19}$$

The node with the highest TOPSIS value is selected as a relay node for that affected node. The selected relay node is removed from the list and again TOPSIS is calculated for the other affected nodes consequently. A complete node selection criteria along with the TOPSIS algorithm is shown in Algorithm 2.

V. SIMULATION RESULTS

In this section, the performance of our proposed scheme *TIHCS* is analyzed in different scenarios by deploying different patient nodes surrounded by the IRS-enabled fog node in the simulation environment as shown in figure 5. The simulation was carried out in Matlab. The nodes were deployed in a circular region with random phase and amplitude. The phase and amplitude were uniformly distributed in the region of $0^0 - 360^o$ and $5m - 25m$ respectively. Monte-Carlo simulation results were obtained by averaging the results over a 10000 iterations. The surrounding area of the fog node is divided into 6 equidistant sectors with a random deployment of patient nodes in each sector with legitimate and malicious nodes with varying amounts of data ranging from 50kB to 100kB. The patients' data sensitivity is divided into three different sensitivity levels. The nodes according to their data, calculate the number of GTS required and send the GTS requests to the fog node. The nodes are supposed to have their data at the start of the beacon frame. A detailed list of parameters used in this simulation is mentioned in table 3. Comparative result analysis of the proposed scheme in terms of relay selection as well as GTS allocation procedures in different prospects are compared with other schemes.

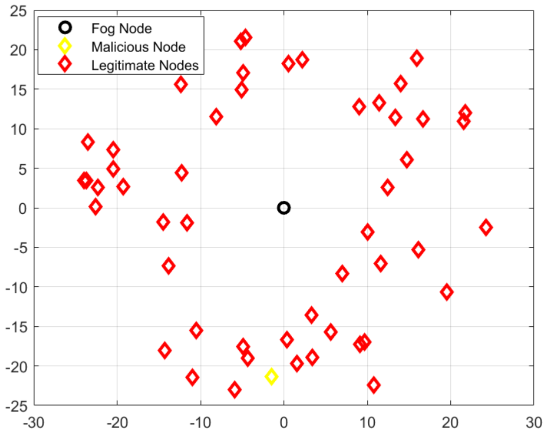

FIGURE 5. Deployment of malicious and legitimate nodes in simulation setup.

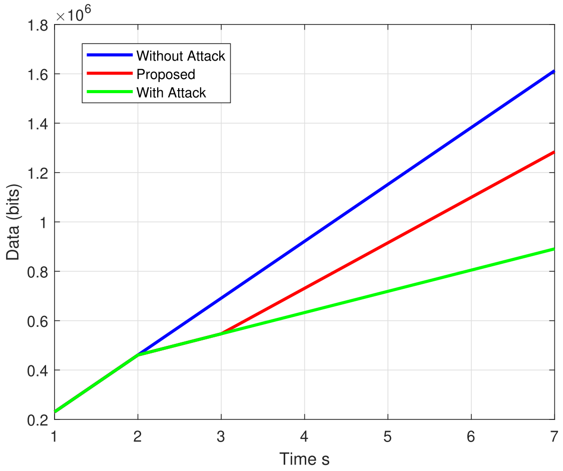

FIGURE 6. Data transmitted by legitimate nodes with and without attacks.

Results shown in figure 6 represent the effect of the proposed TIHCS scheme on data transmission in different sessions. The proposed data transmission is compared when there is no malicious node attack and when malicious nodes attack the medium to compromise the QoS. The malicious node disrupts the communication of the medium during the second session and data transmitted by the legitimate nodes is reduced as represented with green. The blue represents the normal trend of the transmitted data in case there is no attack. It is evident from the results that the data transmission in *TIHCS* is affected between 2^{nd} and 3^{rd} communication session due to a malicious node's attack. However, it detects the attack during the second session, then blocks the communication of the malicious nodes area and then data of the affected nodes are transmitted through the relay to the fog node as represented in red. The results show that the data transmission is affected during the 2^{nd} session and then it rises at the normal trend from the 3^{rd} communication session.

A. PERFORMANCE OF RELAY NODE SELECTION

This section compares the effectiveness of the relay selection scheme proposed in this work to transmit the data to the affected area nodes. The results are compared with different relay selection criteria such as, the nodes with the highest residual energy, the nodes which have better communication channels with the fog node, and the random selection of

Algorithm 2 Relay Selection Algorithm

```
Relay nodes selection for affected nodes
Input:
Member nodes $N$
Affected nodes $N_{af}$
Number of candidate relay nodes $N_r = N - N_{af}$
Residual Energy vector $R_E = [re_j]$ for $j = \{1, 2, \ldots, N_r\}$
Self data transmission vector $S_D = [sd_j]$ for $j = \{1, 2, \ldots, N_r\}$ where 2 represents absence of self data
for $i = 1$ to $N_{af}$ do
    Calculate $R_s^i = max(R_d^i - R_e, 0)$ for all possible relay nodes and arrange in a column vector $R_s^i$
    Calculate Topsis decision-Making-Matrix $W = [R_s; R_E; S_D]$ for all possible relay nodes
    TOPSIS Algorithm Steps:
    Step 1: Normalize the data for attribute $(R_s, R_E, S_D)$ between 0 and 1. The goal is to maximize all the attribute values.
        Normalized Value $= \frac{\text{Actual Value}}{\sqrt{\sum \text{Actual Value}^2}}$
    Step 2: Calculate the weighted normalized values for each relay
        WeightedValue $= (R_s \times W_{R_s}) + (R_E \times W_{R_E}) + (S_D \times W_{S_D})$
        where $W_{R_s}$, $W_{R_E}$, and $W_{S_D}$ are the assigned weights.
    Step 3: Determine the ideal and negative-ideal solutions for each attribute.
        Ideal solution: Maximum normalized value for all the parameters.
        Negative-ideal solution: Minimum normalized value for all the parameters.
    Step 4: Calculate the proximity of each task to the ideal and negative-ideal solutions using a distance measure.
        - Calculate the distance of each task from the ideal solution and the negative-ideal solution.
        $D_i^+ = \sqrt{\sum_{j=1}^{m} (\text{NormalizedValue}_{ij} - \text{IdealSolution}_j)^2}$
        $D_i^- = \sqrt{\sum_{j=1}^{m} (\text{NormalizedValue}_{ij} - \text{NegativeIdealSolution}_j)^2}$
    Step 5: Compute the TOPSIS score for candidate relay node:
        $TOPSIS_i = \frac{D_i^-}{D_i^+ + D_i^-}$
    Step 6: Rank the relays based on their TOPSIS scores.
        The relay with higher TOPSIS scores is more favourable for being selected as a relay for the $i^{th}$ affected node.
    remove the selected node from the candidate relay node and recompute all the vectors
    Increment $i$
end
```

TABLE 3. Simulation settings.

Parameter	*Value*
Deployment Area (m)	*50 X 50*
Maximum Session Duration (msec)	*1000*
Health Caring Data Nodes	*20 100*
Data Rate (bps)	*250,000*
Data Slots in a Session	*214*
Slot Capacity (bits)	*1000*
Base Slot Duration (msec)	*4*
GTS Requesting Period (msec)	*0.5*
Communication Channel Bandwidth	*2000 - 12000*
Transmission Power	*0 - 25*
Trust Level Threshold	0.35
Legitimate Nodes	$49 - 148$
Malicious Nodes in the Medium	$1 - 2$

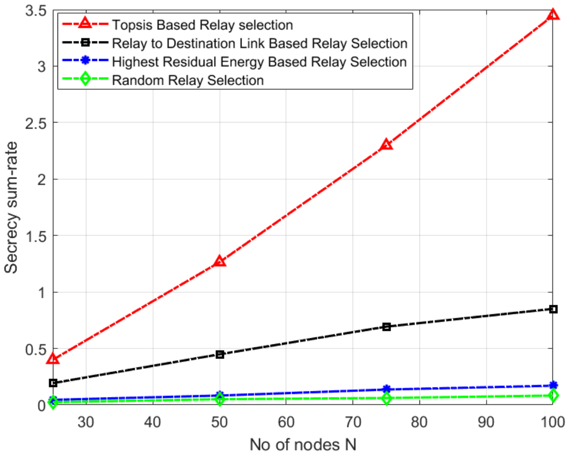

FIGURE 7. Security sum-rate of the network for varying number of nodes.

nodes from the non-affected areas. The security sum rate is calculated against different numbers of member nodes in the medium as well as for varying transmit power cab be viewer in figures 7 and 8 respectively.

Figure 7 shows the results about secrecy sum rate of the network in the proposed TOPSIS-based relay selection scheme is much higher than the other three schemes. The results further show that the secrecy sum-rate rises to 3.5 when the number of nodes reaches 100 in the network. However, the secrecy sum-rate in link-based relay selection, residual energy-based relay selection and random relay selection are 0.78, 0.12, and 0.08 respectively for 100 nodes. The results clearly shows that the TOPSIS-based relay selection in the proposed TIHCS improves the secrecy rate of the network up to 3.43 times from link-based relay selection, up to 28.16 times from the residual energy-based relay section, and 42.75 times from the random relay selection for varying number of nodes in a network.

Results in figure 8 show the comparative analysis in terms of calculating the secrecy sum rate of the network. The comparative includes the proposed TOPSIS-based relay

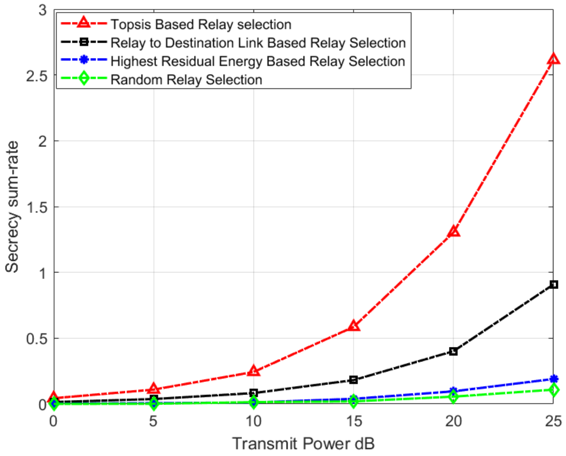

FIGURE 8. Security sum-rate of the network for varying transmission power.

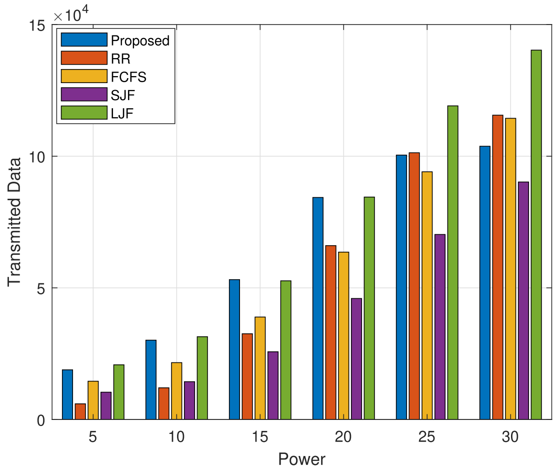

FIGURE 10. Data transmission by legitimate nodes against varying transmission power.

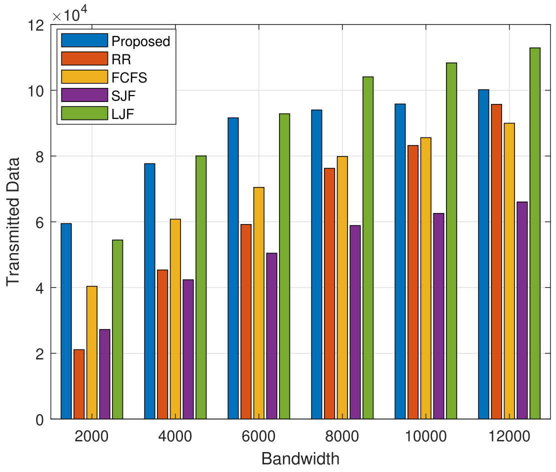

FIGURE 9. Data transmission by legitimate nodes against varying bandwidth.

selecting criteria with the other three schemes when the transmission power of the nodes is varied from 0 to 25. The results clearly show that the secrecy sum rate in the proposed relay selection scheme is much higher than the other three schemes. This is due to the reason, that the other three schemes do not consider the secrecy rate in relay selection. However, the secrecy rate is one of the weighted parameters in the TOPSIS calculation. The results show that the secrecy sum rate of the network is 205%, 1344%, and 2066% more than the link-based relay selection, Residual energy-based relay selection, and random relay selection criteria respectively for all varying transmission power of the nodes in the network.

B. TRANSMITTED DATA

The efficiency of the TDMA-based MAC protocol proposed in *TIHCS* is assessed based on several factors, including the volume of transmitted data, GTS utilization of the medium, the variety of priority levels accommodated for health nodes, and the duration required to transmit their data. This evaluation is conducted across different bandwidth and transmission power settings within the network. Comparative analysis is performed against established standards such as First Come First Serve (FCFS) [29], Shortest Job First (SJF) [5], Round-robin (RR) [30] and Longest Job First (LJF) [31].

The results in figures 9 and 10 show a comparative analysis in terms of transmitted data of our proposed scheme with the other four standards for varying bandwidth and transmission power respectively. Higher bandwidth and transmission power allow a node to transmit more data in a GTS. All the GTS requesting nodes determine their required time slots to transmit their data according to the transmission power and the channel bandwidth.

Results in figure 9 show that the amount of data transmitted in the proposed TIHCS scheme is more than the other four standards until the channel bandwidth is less than 4000. However, with the increase in bandwidth, the LJF allows more data transmission as compared to our scheme because higher bandwidth allows more data to transmit and most of the highest data nodes of the LJF transmit their data. On the other side, TIHCS scrutinize nodes by considering their priority level and some of the highest sensitive health nodes have a low amount of data and consequently, the amount of data transmitted in the proposed scheme becomes less from LJF. However, it is more than the other three schemes. SJF has the lowest data among all for all varying bandwidths except when bandwidth is 2000 where RR has less amount of data as compared to SJF. The results show that the amount of data transmitted in TICHS is up to 186% more than RR, 48% more than the FCFS, and up to 115% more than SJF.

The same trend follows for varying amount of transmitted power as shown in figure 10. The results show that the higher the transmission power of the nodes, the more the data is transmitted in a time slot. The results verify that data transmission in TIHCS is more than the other four standards until a transmission power of 20 because TIHCS allows all legal nodes to transmit their data to the fog nodes by assigning

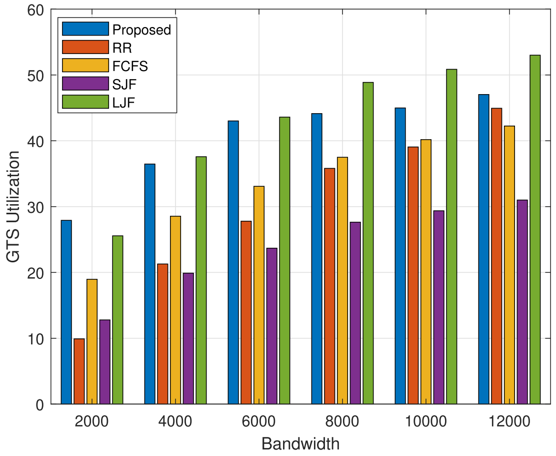

FIGURE 11. GTS utilization by legitimate nodes against varying bandwidth.

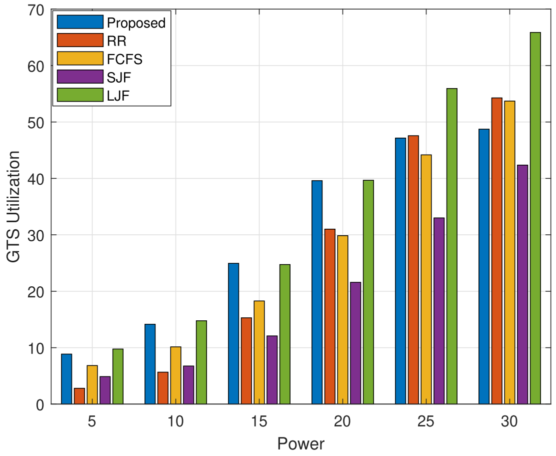

FIGURE 12. GTS utilization by legitimate nodes against varying transmission power.

GTS. whereas, the other three schemes do not apply anomaly detection mechanisms and the GTS are also allocated to the malicious nodes. The results further show that when the transmission power increases from 20, LJF allows nodes to transmit more data as compared to our proposed scheme because it selects nodes that have the highest amount of data and consequently transmitted data is increased. SJF selects nodes to transmit their data that have the shortest amount of data in allocating GTS and consequently have the least amount of data for all varying amounts of powers.

C. GTS UTILIZATION

GTS utilization in a session is calculated as the ratio between the amount of data transmitted to its maximum available capacity. Results in the figures 1112 show the GTS utilization in the percentage of all schemes against varying bandwidth and transmission power respectively.

Results in Fig.11 show that the GTS utilization increases with the increase in bandwidth because higher bandwidth allows nodes to transmit their data at a higher rate with close to its maximum capacity. The results show that the GTS allocation in the proposed scheme is the best among all the schemes when bandwidth is low. However, with the increase in bandwidth, GTS utilization in LJF rises because it allows nodes to transmit their data that have a higher amount of data and it fills most of the available GTS in a session. However, the proposed scheme allocates GTS to nodes by considering their priority and some of the higher priority data are allocated GTS though they have less amount of data. This may result in the percentage of GTS allocated to nodes being less than the LJF scheme. However, it is up to 180% more than the RR, 47% more than the FCFS, and 118% more than the SJF.

The results in Fig. 12 show the allocation of GTS for varying amount of transmission power. The results represent the same trend as the GTS utilization increases with the increase in transmission power because an increase in transmission power allows nodes' data to their maximum capacity. The results further verify that the GTS allocation in the proposed scheme is more than the SJF, FCFS, and RR for most of the varying amounts of transmission powers. However, it is almost the same as the LJF for all varying amounts of transmission power.

D. ALLOCATED NODES

The fog node after receiving the GTS requests from the nodes, allocates GTS to health nodes in transferring their data. The results in figures 13 and 14 shows a comparative analysis of successfully allocated nodes in terms of varying bandwidth and varying transmission power respectively. Each figure is a combination of three subplots showing the allocation of different sensitivity levels of nodes.

It is evident from the results shown in figure 13 that TIHCS allows most of the highest sensitive nodes to send their data in a communication session. Out of the total GTS allocated nodes, the proposed scheme allows 55% nodes of the highest priority nodes, 35% to the medium priority nodes, and only 10% least priority nodes are allocated GTS in a session. However, in all three schemes, the percentage of GTS allocating nodes in the highest priority nodes are far less than our proposed scheme. Because the other three schemes do not allocate GTS by considering their priorities and some of the GTS requests of the nodes are also not allocated due to malicious attacks. However, the percentage of GTS-allocated nodes of the least priority nodes in the proposed scheme is far less than in the other three schemes for all varying amounts of bandwidth.

The results in figure 14 show that the percentage of the highest priority GTS allocating nodes in the proposed scheme is much greater than the other three schemes for all varying levels of transmission power. The results further show that the percentage of medium-priority GTS allocating nodes is also greater than the other three schemes for varying amounts of transmission power. However, the percentage of least sensitive GTS allocating nodes is less than the other three schemes because our proposed scheme allocates GTS by considering their priority levels.

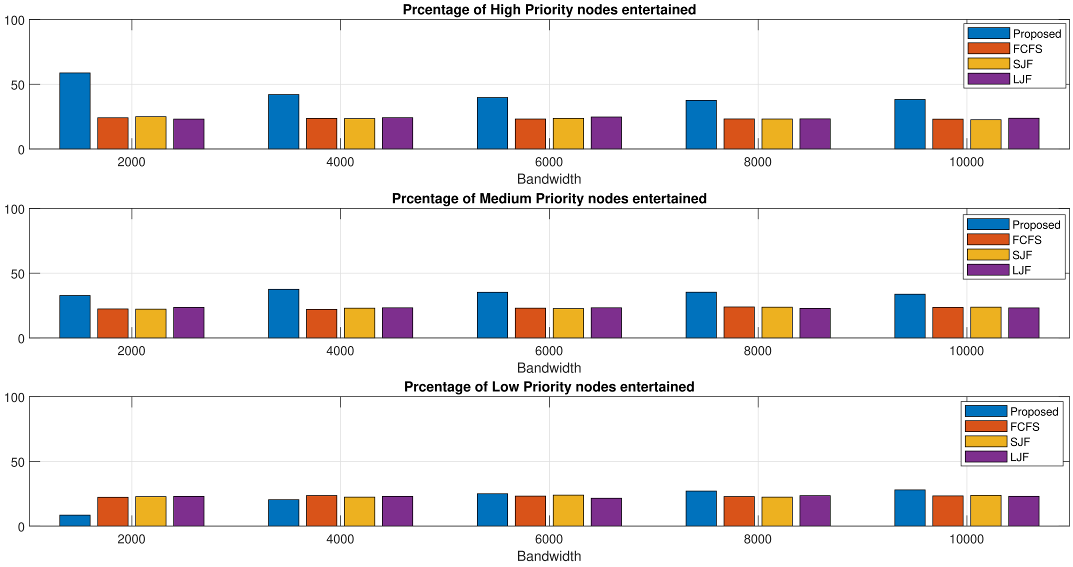

FIGURE 13. Percentage of GTS allocated nodes for varying channel bandwidth.

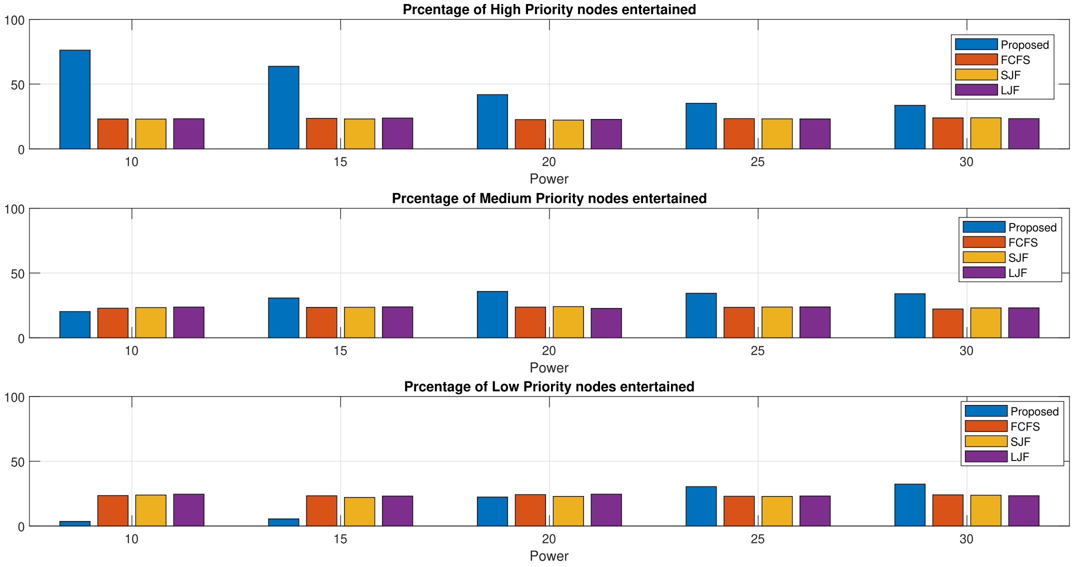

FIGURE 14. Percentage of GTS allocated nodes for varying transmission power.

E. DATA TRANSMISSION TIME

The transmission time is calculated for all successfully allocated legal GTS requesting nodes in a communication session. Figures 15 and 16 depict the data transmission time of all successfully allocated GTS nodes within a session, illustrating variations across different bandwidth and transmission power settings, respectively.

The results shown in figure 15 verify that the transmission time of the proposed scheme in transmitting legitimate nodes' data is less than the other four schemes for most of the varying bandwidth channels. This is due to the reason that other schemes also allocate GTS to the malicious nodes and overall GTS transmitting time of the legitimate nodes is increased. The results further show that the difference in transmission time increases with the increase in channel bandwidth. The same trend follows for varying amounts of transmission power as shown in figure 16.

F. DISCUSSION

The results highlight the advantages of the proposed TIHCS in terms of enhanced data transmission and secrecy sum-rate. The proposed TIHCS algorithm can work well with the present MAC algorithms. Moreover, TIHCS can perform well against specific security attacks in which malicious users do not transmit any data and only capture the time slot or channel. The considered trust mechanism in TICHS handles the above specific type of denial of service attack. However, in a real-world smart city, some malicious users may also launch jamming attacks to waste the network bandwidth. Similarly, some malicious users can transmit corrupted data

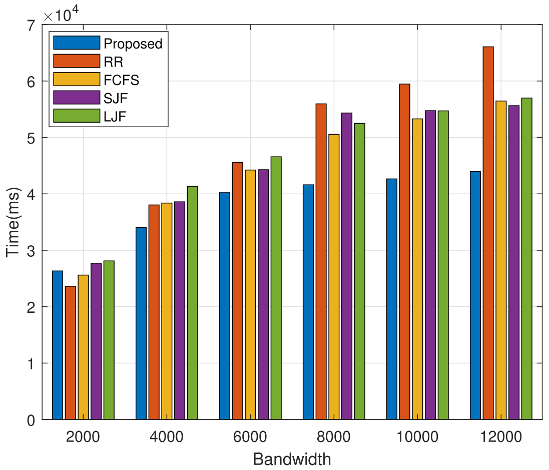

FIGURE 15. Transmission time of legitimate nodes in a communication session for varying channel bandwidth.

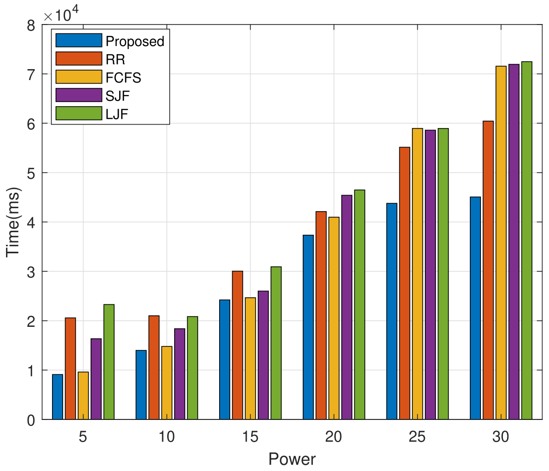

FIGURE 16. Transmission time of legitimate nodes in a communication session for varying transmission power.

information with other users, thus initiating data integrity attacks. Another important scenario in a real-world can be the case when number of malicious users are higher than the number of normal users. This specific case may require changes in the TIHCS algorithm to better evaluate the trust values and isolating any anomalies.

VI. CONCLUSION

Malicious attacks cause anomalies in data delivery that may result in human life in IoT-based health care systems. The proposed Trust-based Improved QoS for Health Care Systems (TIHCS) offers relay section criteria by applying the TOPSIS algorithm. The results show that the proposed relay selection method in TIHCS improves the secrecy sum-rate up to 205%, 1344%, and 2066% as compared to link-based relay selection, residual energy-based relay selection, and randomly selected relays respectively. In addition, the proposed MAC in TIHCS allows more highly critical legitimate data transmitting nodes to send their data in a communication session as compared to the well-known SJF, LJF, and FCFS algorithms. It is evident from he results that the proposed TIHCS prefers 100% more highly sensitive data-carrying nodes and 45% more medium-priority data nodes to send their data in a session as compared to any of the three compared standards. However, it allows 41% less amount of low-priority nodes to send their data as compared to the other three standards. The results further show that the proposed scheme allows up to 25% and 50% more data to transfer as compared to FCFS and SJF respectively. However, for increased channel bandwidth, the data transmitted by the proposed scheme is 78.5% of the LJF. The results further show that the transmitting time of all legitimate nodes in transmitting their data in a session is up to 36.11%, 37.55%, and 39.47% smaller than FCFS, SJF, and LJF respectively.

REFERENCES

[1] K. Haseeb, T. Saba, A. Rehman, Z. Ahmed, H. H. Song, and H. H. Wang, "Trust management with fault-tolerant supervised routing for smart cities using Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22608–22617, Nov. 2022.

[2] H. Bornholdt, K. Röbert, and P. Kisters, "Accessing smart city services in untrustworthy environments via decentralized privacy-preserving overlay networks," in *Proc. IEEE Int. Conf. Service-Oriented Syst. Eng. (SOSE)*, Aug. 2021, pp. 144–149.

[3] J. Yang, Y. Kwon, and D. Kim, "Regional smart city development focus: The south Korean national strategic smart city program," *IEEE Access*, vol. 9, pp. 7193–7210, 2021.

[4] Y. H. Kwak and J. Lee, "Toward sustainable smart city: Lessons from 20 years of Korean programs," *IEEE Trans. Eng. Manag.*, vol. 70, no. 2, pp. 740–754, Feb. 2023.

[5] A. N. Alvi, S. H. Bouk, S. H. Ahmed, M. A. Yaqub, N. Javaid, and D. Kim, "Enhanced TDMA based MAC protocol for adaptive data control in wireless sensor networks," *J. Commun. Netw.*, vol. 17, no. 3, pp. 247–255, Jun. 2015.

[6] C. Y. Haw, A. Awang, and F. A. Hussin, "A contention-based MAC and routing protocol for wireless sensor network," *Wireless Sensor Netw.*, vol. 15, no. 1, pp. 1–32, 2023.

[7] F. Masud, G. Abdul-Salaam, M. Anwar, A. Abdelmaboud, M. S. A. Malik, and H. B. Ab Ghani, "Contention-based traffic priority MAC protocols in wireless body area networks: A thematic review," *Egyptian Informat. J.*, vol. 24, no. 4, Dec. 2023, Art. no. 100410.

[8] A. N. Alvi, S. H. Bouk, S. H. Ahmed, M. A. Yaqub, M. Sarkar, and H. Song, "BEST-MAC: bitmap-assisted efficient and scalable TDMA-based WSN MAC protocol for smart cities," *IEEE Access*, vol. 4, pp. 312–322, 2016.

[9] W. Aman and E. Snekkenes, "Managing security trade-offs in the Internet of Things using adaptive security," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 362–368.

[10] S. Khan, A. N. Alvi, M. A. Javed, and S. H. Bouk, "An enhanced superframe structure of IEEE 802.15.4 standard for adaptive data requirement," *Comput. Commun.*, vol. 169, pp. 59–70, Mar. 2021.

[11] A. N. Alvi, S. Khan, M. A. Javed, K. Konstantin, A. O. Almagrabi, A. K. Bashir, and R. Nawaz, "OGMAD: Optimal GTS-allocation mechanism for adaptive data requirements in IEEE 802.15.4 based Internet of Things," *IEEE Access*, vol. 7, pp. 170629–170639, 2019.

[12] S. Dhelim, N. Aung, M. T. Kechadi, H. Ning, L. Chen, and A. Lakas, "Trust2 Vec: large-scale IoT trust management system based on signed network embeddings," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 553–562, Jan. 2023.

[13] C. Lewis, N. Li, and V. Varadharajan, "Targeted context based attacks on trust management systems in IoT," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12186–12203, Sep. 2023.

[14] N. Khandelwal and S. Gupta, "A review: Trust based secure IoT architecture in mobile ad-hoc network," in *Proc. Int. Conf. Appl. Artif. Intell. Comput. (ICAAIC)*, May 2022, pp. 1464–1472.

[15] J. Bai and H. Dong, "Federated learning-driven trust prediction for mobile edge computing-based IoT systems," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, 2023, pp. 131–137.

[16] M. Hegde, R. R. Rao, and B. M. Nikhil, "DDMIA: Distributed dynamic mutual identity authentication for referrals in blockchain-based health care networks," *IEEE Access*, vol. 10, pp. 78557–78575, 2022.

[17] B. Vardhini, S. N. Dass, and R. Chinnaiyan, "A blockchain based electronic medical health records framework using smart contracts," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2021, pp. 1–4.

[18] M. Ebrahimi, M. S. Haghighi, A. Jolfaei, N. Shamaeian, and M. H. Tadayon, "A secure and decentralized trust management scheme for smart health systems," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1961–1968, May 2022.

[19] P. Gope, Y. Gheraibia, S. Kabir, and B. Sikdar, "A secure IoT-based modern healthcare system with fault-tolerant decision making process," *IEEE J. Biomed. Health Informat.*, vol. 25, no. 3, pp. 862–873, Mar. 2021.

[20] A. Almas, W. Iqbal, A. Altaf, K. Saleem, S. Mussiraliyeva, and M. W. Iqbal, "Context-based adaptive fog computing trust solution for time-critical smart healthcare systems," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10575–10586, Dec. 2023.

[21] A. A. Omar, A. K. Jamil, A. Khandakar, A. R. Uzzal, R. Bosri, N. Mansoor, and M. S. Rahman, "A transparent and privacy-preserving healthcare platform with novel smart contract for smart cities," *IEEE Access*, vol. 9, pp. 90738–90749, 2021.

[22] Md. M. Islam and Z. A. Bhuiyan, "An integrated scalable framework for cloud and IoT based green healthcare system," *IEEE Access*, vol. 11, pp. 22266–22282, 2023.

[23] W. Yuanbing, L. Wanrong, and L. Bin, "An improved authentication protocol for smart healthcare system using wireless medical sensor network," *IEEE Access*, vol. 9, pp. 105101–105117, 2021.

[24] D. Kshirsagar, A. Pote, K. Paliwal, V. Hendre, P. Chippalkatti, and N. Dhabekar, "A review on IoT based health care monitoring system," in *Proc. ICCCE*, 2020, pp. 95–100.

[25] K. M. Besher, Z. Subah, and M. Z. Ali, "IoT sensor initiated healthcare data security," *IEEE Sensors J.*, vol. 21, no. 10, pp. 11977–11982, May 2021.

[26] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 8, pp. 2169–2176, Aug. 2020.

[27] J. Indumathi, A. Shankar, M. R. Ghalib, J. Gitanjali, Q. Hua, Z. Wen, and X. Qi, "Block chain based Internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (BC IoMT U6 HCS)," *IEEE Access*, vol. 8, pp. 216856–216872, 2020.

[28] *BAP70-03 General Purpose PIN Diode–Product Data Sheet*. Accessed: Dec. 7, 2017. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/BAP70-03.pdf

[29] A. N. Alvi, M. Ali, M. S. Saleh, M. Alkhathami, D. Alsadie, B. Alghamdi, and B. Alenzi, "TMPAD: Time-slot-based medium access control protocol to meet adaptive data requirements for trusted nodes in fog-enabled smart cities," *Appl. Sci.*, vol. 14, no. 3, p. 1319, 2024. [Online]. Available: https://www.mdpi.com/2076-3417/14/3/1319

[30] M. Ben Slimane, I. Ben Hafaiedh, and R. Robbana, "Formal-based design and verification of SoC arbitration protocols: A comparative analysis of TDMA and round-robin," *IEEE Design Test*, vol. 34, no. 5, pp. 54–62, Oct. 2017.

[31] A. N. Alvi, B. Ali, M. S. Saleh, M. Alkhathami, D. Alsadie, and B. Alghamdi, "Secure computing for fog-enabled industrial IoT," *Sensors*, vol. 24, no. 7, p. 2098, Mar. 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/7/2098

HAIDER ALI received the B.S. degree in electrical (telecom) engineering from COMSATS University Islamabad (CUI), in 2006, the M.S. degree in Finland, in 2009, under the faculty development program-based scholarship, and the Ph.D. degree from CUI, where his area of research was metasurfaces for wireless devices. During the M.S. degree, he was also part of the research group "Broadcasting for the 21st Century". Currently, he is an Assistant Professor with the Department of Electrical and Computer Engineering, CUI, Islamabad campus.

AHMAD NASEEM ALVI has been part of the Electrical and Computer Engineering Department, since 2010. He is currently an Associate Professor with COMSATS University Islamabad, Islamabad Campus. He held multiple senior administrative positions within and outside the department. Furthermore, he has more than ten years of professional experience in a multinational telecom industry as a Manager Technical and executed number of telecom projects. He is the author of more than 15 publications in well reputed international journals and conferences. His research interests include wireless networks, fog/edge computing, blockchain, and algorithm design.

MOHAMMED ALKHATHAMI is currently an Associate Professor with the Information Systems Department, 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.

DEAFALLAH ALSADIE (Member, IEEE) received the B.Sc. degree in computer science from Taibah University, in 2007, the M.A.Sc. degree in computer science from Latrobe University, Australia, in 2011, and the Ph.D. degree in computer science from RMIT University, Melbourne, VIC, Australia, in 2019. He is currently an Assistant Professor with the Department of Information Systems, College of Computers and Information Systems, Umm Al-Qura University, Saudi Arabia. His research interests include scheduling and resource allocation for parallel and distributed computing systems, data centers, edge computing, and the Internet of Things.

FATAMH ALASHAIB is currently with Imam Mohammad Ibn Saud Islamic University (IMSIU), Saudi Arabia. Her research interests include computer systems, wireless communications, security, and computing.

• • •