Hindawi
Security and Communication Networks
Volume 2023, Article ID 9854329, 1 page
https://doi.org/10.1155/2023/9854329

Retraction

Retracted: Machine-to-Machine Communication for Device Identification and Classification in Secure Telerobotics Surgery

Security and Communication Networks

Received 5 December 2023; Accepted 5 December 2023; Published 6 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] M. P. Lokhande, D. D. Patil, L. V. Patil, and M. Shabaz, "Machine-to-Machine Communication for Device Identification and Classification in Secure Telerobotics Surgery," *Security and Communication Networks*, vol. 2021, Article ID 5287514, 16 pages, 2021.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 5287514, 16 pages
https://doi.org/10.1155/2021/5287514

Research Article

Machine-to-Machine Communication for Device Identification and Classification in Secure Telerobotics Surgery

Meghana P. Lokhande,[1,2] **Dipti Durgesh Patil**,[3] **Lalit V. Patil**,[4] **and Mohammad Shabaz**[5,6]

[1]*Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India*
[2]*Research Scholar, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, India*
[3]*Department of Information Technology, MKSSS's Cummins College of Engineering for Women, Pune, India*
[4]*Department of Information Technology, Smt. Kashibai Navale College of Engineering, Pune, India*
[5]*Arba Minch University, Arban Minch, Ethiopia*
[6]*Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India*

Correspondence should be addressed to Mohammad Shabaz; mohammad.shabaz@amu.edu.et

Received 21 July 2021; Revised 19 August 2021; Accepted 20 August 2021; Published 28 August 2021

Academic Editor: Chinmay Chakraborty

The capacity of machine objects to communicate autonomously is seen as the future of the Internet of Things (IoT), but machine-to-machine communication (M2M) is also gaining traction. In everyday life, security, transportation, industry, and healthcare all employ this paradigm. Smart devices have the ability to detect, handle, store, and analyze data, resulting in major network issues such as security and reliability. There are numerous vulnerabilities linked with IoT devices, according to security experts. Prior to performing any activities, it is necessary to identify and classify the device. Device identification and classification in M2M for secure telerobotic surgery are presented in this study. Telerobotics is an important aspect of the telemedicine industry. The major purpose is to provide remote medical care, which eliminates the requirement for both doctors and patients to be in the same location. This paper aims to propose a security and energy-efficient protocol for telerobotic surgeries, which is the primary concern at present. For secure telerobotic surgery, the author presents an Efficient Device type Detection and Classification (EDDC) protocol for device identification and classification in M2M communication. The periodic trust score is calculated using three factors from each sensor node. It demonstrates that the EDDC protocol is more effective and secure in detecting and categorizing rogue devices.

1. Introduction

Currently, wireless and wired systems interacting with other devices having similar functionality have become one of the fastest-growing areas of research. Machine-to-machine communication (M2M) is a new technology that allows machines to communicate without human intervention [1]. Intelligent software applications are the process that collects data and provides the end user with a set of intelligent services and practical interfaces [2]. The idea of implementing telematics and telemetry is known, but in connection with the proliferation of the Internet and the ubiquitous trend to connect, especially through a wireless communication system, the M2M system has attracted the attention of both academia and industry [3].

In the medical device industry, M2M communication is one of the fastest-growing sectors. According to Global Info Research, the connected medical device market is projected to expand from $939 million in 2018 to $2.7 billion by 2023, with the largest growth forecast for the United States [4]. M2M communication faces various security challenges. Most of the vulnerability issues arise from a lack of a central authority and a wireless medium of transmission. Route creation and data transmission are two important functions of the routing algorithm. These two stages must be protected from attackers. The routing protocol must be strong enough

to withstand various attacks. Thus, reliable communication needs a secure routing algorithm. Proper identification and classification of devices before any operation is required.

Machine-to-machine (M2M) communication system is an emerging technology for next-generation communication networks. M2M system facilitates ubiquitous communication among smart devices with minimum human intervention. The key characteristic of M2M is decreasing the cost of human resources and providing great research in the medical and industrial fields. The telerobotic system operates at different levels of topologies. It starts from direct control to command tracking telerobots. The major challenges are communication delay, access control, and stability [5]. M2M communication works for long-distance communication and can be easily incorporated for telerobotic surgeries. The existing telerobotic challenges are solved with M2M security measures. In M2M, malicious nodes are identified and provide a reliable route for data transmission in robotic surgery. Thus, it reduces communication delay and synchronization problems.

Remote healthcare is an evolving area of research as the world moves from remote surveillance to real-time and rapid detection of diseases. Robotic surgery gives birth to telerobotic surgery [6]. In robotics, surgeons perform operations while sitting near a patient's console. Instead, telerobotic surgery allows surgeons to remotely control patients using surgical robots and a communication network between them. In telerobotic systems, the surgeons control the slave which is at a different location. Telerobotic surgery offers several products and benefits, including high-quality assistance for people in developing countries and providing the surgical needs for soldiers [7]. Similarly, it can overcome the limits and inconsistency of the systems of public health in developing countries and developed countries and regions. These types of procedures are a major barrier to patient safety, data security, and privacy concerns. The main challenge is reliability in performing telerobotic surgery due to the unavailability of a secure mechanism for device identification and classification in M2M communication.

Wireless communication in M2M makes the attacker easily monitor the network traffic and discovers vulnerable machine-type devices even though network is secured through encryption [8]. Instead of passively monitoring the traffic and identifying vulnerable devices, the malicious devices can be identified based on their network behaviour. In this context, the medical devices perform unexpected activities by monitoring surgical environment and create denial of service attack. To improve security, it is important to know the type of devices connected to the network. Medical tools or equipment used during surgeries need to be identified. It helps the system to specify filtering rules or block the access for particular devices from which unexpected or irrelevant data is transmitted. The devices that make the network vulnerable need to be identified and classified to make secured surgical environment. As network traffic from medical field will have high priority than other industry or enterprise data, for medical device configuration, administrator has to configure different filtering and access rules depending on type of device. This manual configuration is time-consuming for unscalable IoT network. To ensure security and quality of services, the access rules are defined based on device type and its priorities. However, device classification is nontrivial task as IoT consists of heterogeneous devices with dynamic nature of network traffic.

In M2M communication, devices interact with each other and exchange information autonomously to perform the necessary tasks. During surgery, it is important to protect the network against various types of attacks. A small communication delay can create a threat to patient life. It may also slow down the entire system in the operating room. To make telerobotic surgery efficient and reliable, the proposed system is designed. The main objective is to design the system to incorporate machine-to-machine communication in a telerobotic surgical environment to meet security requirements. To make the network secure and reduce energy consumption, nonmalicious devices are identified and classified.

The proposed secured telerobotic surgery is based on robust and beneficiary control techniques for providing a more efficient, precise, and cheaper alternative for medical surgeries as compared to existing technologies. Secured surgical environments are tested through performance parameters which create technical limitations and challenges in surgeries. Standard energy-efficient protocol LEACH is analyzed for network parameters in the medical sensor node network. Fuzzy inference system-based energy-efficient protocol is adapted to measures performance parameters with and without attack. Efficient Device type Detection and Classification (EDDC) protocol is proposed and designed for device identification and classification in M2M communication for secure telerobotic surgery. This protocol identifies the node as legitimate or attacker. Finally, the trust score computation technique using three parameters of each sensor node to compute the periodic trust score of each node n is designed. The parameters are Successful Packet Delivery (SPD), Energy Level (EL), and Node Degree (ND) selected to correctly estimate the malicious behaviours of attackers in the network.

One of the motivations in healthcare is the need for long-distance medical surgeries. Under resourced locations such as semiurban and areas near the border, there is often a lack of medical equipment and expert surgeons. It provides a technological and clinical solution in the robot-assisted surgical techniques to improve the quality and results of surgical intervention. Providing this technology to surgeons has led to the development of new surgical techniques that would otherwise be impossible.

The traditional surgical techniques are being enriched by robot-assisted surgery especially in long-distance surgeries. Unsecured network affects the functionality of telesurgery. The proposed research work shows novel research for making the telerobotic system robust, reliable, and attack-resistant.

(a) The system identifies the legitimate device and attacking device based on trust parameters by using the device identification algorithm.

(b) The available energy of each legitimate device is checked periodically and based on energy available, the devices will be provided with access to the available resources in the operating room. Here, end-to-end security of devices is ensured.

(c) The legitimate and attacker nodes are identified at each interval and accordingly it will be involved in the routing mechanism.

(d) Thus, only the legitimate and authorized device can only access the resources. This makes the system robust for attack and improves the quality of service parameters in terms of packet loss and delay as well.

The main objective of the work is to propose an energy-efficient protocol to meet the security requirement in medical practice. Though several researchers worked with available energy-efficient protocols, this idea is being introduced in the telerobotic surgery with the objective of providing a secured and reliable environment during surgeries. A robust and reliable network is possible by minimizing the energy utilization of medical nodes and involving the communication of trusted nodes in data delivery.

The reason behind choosing the medical application is twofold. First of all, the authors would like to provide an excellent medical facility to underresource locations. Secondly, the proposed model makes the existing healthcare system robust and attack-resistant. It also improves quality services to medical staff and patients. However, it can be extended for military application and industrial automation.

This paper addresses the concern of ensuring secure network communication with low energy consumption. Data and device protection is the primary function of this concept, which has not been fully explored by researchers. The simulation study shows the optimum use of EDDC protocol in achieving secured and reliable communication which allows the surgeon to perform the surgery without any threat to patient life.

The rest of the paper is organized as follows. Section 2 reviews related work and Section 3 covers the proposed M2M protocol. In Section 4, experimental results are discussed and presented. In Section 5, the performance metric of the proposed protocol is discussed. Finally, Section 6 summarizes points in conclusion.

2. Related Work

This section summarizes the existing work on M2M communication and telerobotic surgery and communication networks, the device identification and classification, and their secure communication. Regardless of the clear growth rate, researchers need to work to develop an innovative solution and come out with different device characteristics and requirements. The second problem arises that the technical solutions for the entire functioning of M2M system are quite diverse [9]. Perhaps the use of M2M or a wired application may be related to research on equipment technology for wireless connectivity, or short distances, communication, or special standards or specialized communication technologies [10].

Smart healthcare M2M is a new emerging paradigm that offers promising solutions [11]. Various types of smart applications use the M2M data communication approach [12]. An M2M-based healthcare system is proposed in [13]. It illustrates the monitoring of patient health but has less focus on security requirements. The main problem and aspect is security, where M2M communications must be standardized and widely considered before they can be fully involved in practical life [14]. M2M communication model without centralized management is shown in Figure 1. This model facilitates discussion of specific wireless communications and security approaches for M2M applications [15]. Its design specifically covers two separate communication areas that support M2M wireless communications for the Internet. Its integration with remote sensing devices and the other connection supports the rest of Internet communications. Gateway technology is a way to connect end devices to back-end platforms. Communication between the two domains can be mediated by a security gateway that implements a filtering policy for communication according to the requirements of each application. This device can also have other control and safety functions. It serves as an internal system or control unit for M2M remote sensing applications.

Wireless communication between devices in the M2M domain can take place in an unsupervised manner, raising important security concerns such as authentication and trust between devices without knowing each other beforehand. Many applications also require communication with a back-end or gateway device. The gateway unit communication model can actually support the role of personal or industrial control devices or electrical devices, according to the requirements of a specific M2M wireless remote sensing application; it also supports communication between M2M remote sensing devices and the Internet.

Since applications for M2M include devices with low size, independent power supply, and energy restriction, the security solution must take into account the size of the key, the complexity of encryption algorithms, and the key algorithms used for authentication [15]. Also, M2M applications should deal with security threats [16] and other attacks that can negatively affect functionality.

(a) Incorrect network attack: when the M2M device is disabled, an attacker can pass the identification (impersonation) of the M2M device to other network components and obtain confidential information.

(b) False network response: since some M2M devices (such as the Mote sensor) operate with a low-power battery and turn off the radio to save power, an attacker can continuously put the device to sleep by sending a fake network trigger to waste power.

(c) Tamper attack: the triggered indicator may contain the IP address of the application server to which the

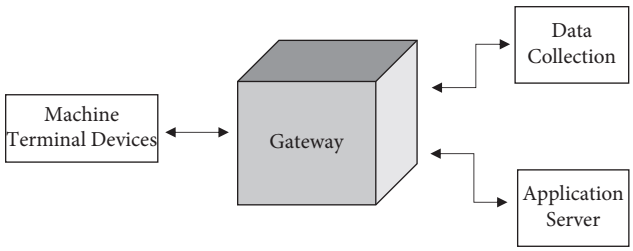


Figure 1: M2M communication without a centralized system.

M2M device should connect. If the IP address is amplified by an attacker, the M2M device may establish a connection to the wrong server, thereby failing to communicate with the correct server and wasting energy and losing the data.

M2M applications for connecting mobile users and home networks are designed in [17]. The authentication and key-based algorithm are used to ensure secure communication between network nodes. However, the proposed security scheme is not suitable for more complex scenarios and has dynamic connections between users and M2M devices. Privacy and information functions [18] are used to preserve hash integrity.

IoT device classification [19] for network security makes the device turned on a white list of permitted devices while connecting to the network. The device classification method is developed to identify and examine their network traffic using IoT devices [20]. The classification of graph-based method proposes [21] correlation graphs of objects by a random walk. It proposes a probabilistic multifunctional model for classifying heterogeneous objects according to a classification scheme with multiple labels. The researchers also worked on detecting device types for security in the IoT [22]. The new devices are designed to find things that have the appearance of the Internet when they are added to the network, so they can easily customize the way the device is detected. The neural network is introduced in [23] to recognize and control the user's intentions of the robot. In both cases, devices are classified under deep neural networks, especially repetitive neural networks.

Despite advances in robotic surgery, safety for telerobotic surgery is challenging. Complete security system, particularly the design and development of the telerobotic surgery security aspects is yet to be designed. It is important to find out not only legal and technical requirements for telerobotic surgery but also security [24]. A security requirement for telerobotic surgery is not yet proposed [25]. Secure ITP uses open source software and Federal Information Processing Standards (FIPS) to develop prototypes that meet strict security requirements in telerobotic surgery. While securing ITP is of reasonable construction, it cannot solve such critical problems as steal personal information from a patient or other administrative and legal issues [26].

Safety issues of telerobotic surgery are identified and divided into telerobotic surgical procedures [27]. Researchers [28] point to the security; availability, price, and legal liability of surgeons are major obstacles to the success of remote robotic surgery. Mechanisms were demonstrated in [29], when the remotely handled software proved the possibility of surgical telerobotic. The author proposed a new way of integrating light privacy and reliability with uniform protocol and compliance performance of cryptographic AES systems [30]. Security attacks with advanced remote-controlled robotic surgical systems are analyzed and investigated [31]. Reference [32] presented a two-way generalized predictive controller associated with QoS-friendly IP security protocol for telerobotic systems. An approach for using incorrect commands in surgery using an ML algorithm is proposed [33].

In addition, it is proposed to ensure the public safety of several patients in a network with data from remote health monitoring systems. The author proposed a multimedical framework [34]. Data is analyzed using remote sensing sensors during patient anonymity and monitoring. The framework does not ensure the security policy. Data security algorithms for the sensors in the body, which are necessary for intelligent systems in healthcare, are developed [35]. The system does not guarantee security policy and is not error-tolerant. Reference [36] proposed an easy authentication method for IoT-enabled medical environments. The system ignores anonymity and does not apply a security policy.

The current standard [37] allows handling or ensuring a reliable connection to a healthcare environment. These standardized protocols and security mechanisms may be used for scenarios of M2M communication but may be modified according to application requirements. Therefore, a new mechanism is required to ensure the security and confidential information via M2M communication. On the contrary, many common security protocols and access control approaches can be adapted to meet the requirements of security [38]. The author proposes real-time data mining for body area network in the wireless network [39, 40]. Several researchers offer device classification and security protocols for efficient route discovery. The authors exclusively focused on resource allocation for a limited number of devices. In most of the research, there are lack of centralized administrative control, low mobility of nodes, and failure to integrate and manage information in the IoT environment. The authors provided security solutions but there in need to provide efficient solutions that will help to enhance security in medical field.

The various researchers propose techniques for telerobotic surgery using mobile edge computing and machine-to-machine network. So, the author proposes the best security protocol called Efficient Device type Detection and Classification (EDDC) protocol and the practical design principle provides a complete safety guide. Protocol-based authentication ensures confidentiality, integrity, anonymity, and responsibilities. The 5 G network for robotic surgery is discussed in [41]. The M2M network performance in presence of malicious nodes is presented for the telerobotic surgery [42].

2.1. Attacks in IoT and Telerobotic Surgery. Telerobotic surgery is subject to various types of active and passive attacks [43]. These attacks and investigation scenarios are shown in Table 1.

Table 1: Attacks in IoT and telerobotic surgery.

Type of attacks	Investigation scenarios
Replay attack	The enemy will play a legitimate message/command illegally later
Eavesdropping	Attackers passively enter conversations and disclose personal information about patients without permission
Masquerading attack	Authorized authentication mechanisms and methods will try to break by bypassing users
Session hijacking	An attacker could gain control of consoles or settings for a session
Brute force attack	To recover the private key with all possible keys in the keyspace
Data removal	Enemies remove the data
Forgery attack	The enemy will play the command illegally and try to play it illegally
Viruses/worms	Virus, worm, crash the operating system
Data theft	Static and dynamic data

2.2. Challenges in Telerobotic Surgery. Several IoT devices are deployed in an open field where security and privacy are of most important concerns [44]. Security leaks in remote control systems pose an existential threat to the area of surgical robots in general, as mounted attacks can break the robot or damage other nearby devices in the operating room. Even if the attack is minor, the damage caused by the surgical robots can weaken the public's trust.

It has attacks as follows:

(a) Node hardening: an attacker replaces nodes on the entire device and either connects it directly or changes access to confidential information, and so on [45].

(b) Fake node: attackers adjust the fake node and access the information [46].

(c) Physical damage: enemies can physically damage your device with Internet of Things that cannot be serviced. The device's Internet stuff can be deployed in both open and closed places, which makes them vulnerable to physical harm from attackers.

(d) Malicious code injection: an attacker physically invades a node by inserting malicious code into the node, which gives unauthorized access to the system.

(e) Sensor data protection: data privacy requirements for sensors are low because an adversary can place a sensor near an IoT system sensor and feel the same value.

(f) Authentication of node: many medical sensors in IoT systems face authentication problems [44]. Thus, a huge amount of network communication affects performance.

(g) Congestion in node: big sensor data communicating with many device authentications can cause network congestion.

(h) RFID interference: the RF signal used by RFID is distorted by the noise signal, which causes a denial of service.

3. Proposed Protocol in M2M Communication for Secure Telerobotic Surgery

3.1. System Architecture. As represented in Figure 2, clustering is carried out autonomously for identifying the node as cluster head (CH) and cluster member (CM). Further to improve the clustering process, nodes are identified as legitimate or attacking devices based on trust score parameters. The weighting parameters are used to get the trust score value between 0 and 1.

Based on the trust-score value, nodes are identified as legitimate and attacking devices. The cluster head list is updated with legitimate devices and the cluster member list with attacking devices. At the periodic interval, the trust-score value of each node in the cluster head list is calculated to decide the cluster head for that interval. The selected cluster head advertises and announces the time slot for data transmission. At each interval, the remaining energy for the cluster head is checked, and accordingly, the cluster cycle is updated.

3.2. Proposed Protocol. M2M is a network where a large number of intelligent devices create, share, and collaborate information without humans. Having a variety of applications and many benefits, the design of the M2M network faces several technical problems. One of the key issues underlying economic growth is its security. However, it is very important to provide correct and secure information to the end user. So, the author proposes an Efficient Device type Detection and Classification (EDDC) protocol for device identification and classification in M2M communication for secure telerobotic surgery. N number of medical devices are introduced in the network their size $X * Y$. Considerations for developing the proposed protocol EDDC are given as follows:

(a) A medical device capable of sensing medical data and transmitting them to a single medical station is called a base station (BS)

(b) Medical devices are randomly deployed in medical services in different locations

(c) Every medical device is static and works evenly in the network

(d) The position of each device is calculated using the received signal strength indicator (RSSI)

(e) All nodes are grouped into clusters using conventional K-means

(f) Data transfer from the CMs to their assigned CHs is carried out in a multipass method

(g) BS nodes that are outside the network area are not restricted

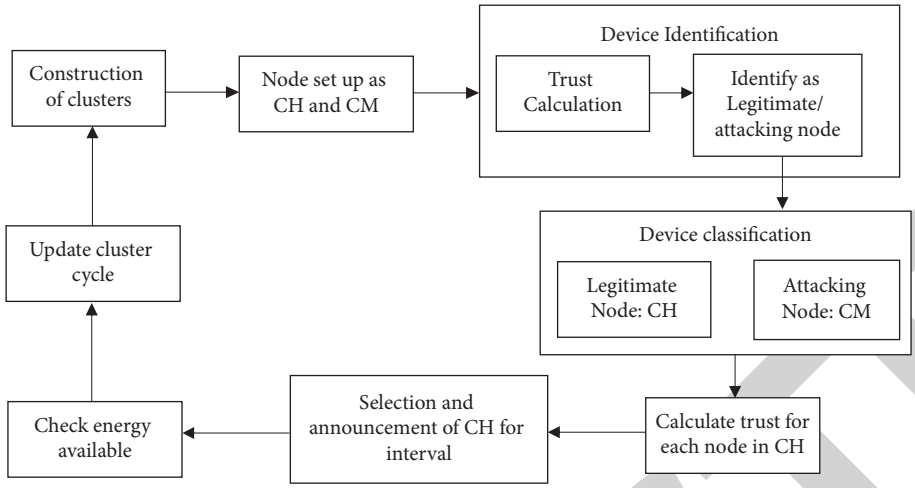


Figure 2: System architecture for Efficient Device type Detection and Classification (EDDC).

(h) All medical sensor nodes are limited by limited computing power and battery

(i) In M2M, it is assumed that nodes can perform data receiving, data forwarding, and data forwarding

3.3. Device Type Identification. This stage identifies that the device type is a legitimate sensor device or an attacker sensor device, which designs the trust-score computation technique to compute the periodic trust score of each node n. First, calculate the trust score (TS); if TS value of a node is larger than the global trust threshold value, then the node is identified as a legitimate medical device; otherwise, the node is identified as an attacked medical device.

To identify nodes s legitimate or attacking, the author has developed a method for calculating the confidence score using three parameters for each sensor node to calculate the periodic trust score for each node. The parameters like Successful Packet Delivery (SPD), Energy Level (EL), and Node Degree (ND) were selected to correctly estimate the malicious behaviours of attackers in the network. In Algorithm 1, the TS^n = get Trust Score (n) computes the trust scores using these three parameters.

3.3.1. SPD Trust. Since the attacking node performs a malicious task on the network and the SPD does not work well on the network, first exchange HELLO packets with neighbouring nodes and calculate the SPD trust score for each device. The SPD of node n on the current time interval $t-1$ to t is calculated as follows:

$$SPD^n = \frac{n^{rcv(t-1,t)}}{n^{ge(t-1,t)}}, \tag{1}$$

where $n^{rcv(t-1,t)}$ and $n^{ge(t-1,t)}$ are the total number of packets received and generated in time interval $t-1$ to t. Nodes with higher SPD values are more likely to be identified as legitimate medical devices.

3.3.2. EL Trust. Nodes that drain this energy faster and still advertise themselves as candidates for data transfer or CH selection processes are also considered malicious nodes. Therefore, it is very important to calculate the trust according to the current level of remaining energy of each device:

$$EL = \frac{E_{\text{rem}}\left(n^t\right)}{E_i\left(n\right)}, \tag{2}$$

where $E_{\text{rem}}(n^t)$ indicates the remaining energy at time t and $E_i(n)$ indicates the initial level of energy. Node with high EL values is more likely to be identified as legitimate medical devices.

3.3.3. ND Trust. ND is the third reliability parameter calculated in this study to determine the reliability of medical devices in the clustering and data transfer phase. An attacker, such as DDoS or eavesdropping, can attract a source of information with false claims enough for neighbours to send information over a small geographical distance to their intended destination. The number of neighbours NC of node n at time t is calculated as using RSSI:

$$NC = \text{count}\left[\frac{n}{\text{distance}\left(n, pi\right)} < rssi\right], \tag{3}$$

where $n \neq pi$ and distance (n, pi) calculates location distance of n and $pi^{th} \in N$ using RSSI of n. The NC is used to calculate the trust score value as

$$ND^n = 1 - \left(\frac{1}{NC}\right). \tag{4}$$

In the above equation, the number of nearest or one-hop nodes of the currently investigated node n is computed. This is done by checking the RSSI limits (i.e., the distance between current node n to its nearer node pi) should be below the RSSI value of the investigated node.

GT: global trust threshold value
TS^n: trust-score value of n^t sensor device
TS^n: trust-score value of n^t sensor device
Inputs
N: number of medical devices
$TS^n = 0.35$: threshold value of trust score
S: simulation time
Output
LS D: node identified as legitimate
AS D: node identified as legitimate
(1) While (*k*)
(2) At each periodic interval $pi \in S$ Deploy
(3) *N* number of medical devices
(4) For each node $n \in N$
(5) TS^n = get Trust Score (*n*)
(6) If ($TS^n > GT$)
(7) "node identified as legitimate medical device"
(8) *LS D*←*n*
(9) Else
(10) "node identified as attacked medical device"
(11)*AS D*←*n*
(12) End If
(13) End For
(14) *pi* + +
(15) End While
(16) Stop

Algorithm 1: Device type identification.

The count parameter represents the total number of nodes NC that satisfy the criteria of RSSI counted as the nearest nodes of the currently investigated node *n*.

The final trust score of node *n* is calculated using a weighted approach:

$$TS = \left(w^1 \times SPD^n\right) + \left(w^2 \times EL^n\right) + \left(w^3 \times ND^n\right). \quad (5)$$

Here, the values for w^1, w^2, and w^3 are chosen as 0.4, 0.3, and 0.3 so that the sum is 1. The trust score *TS* for node *n* now ranges from 0 to 1. The node with a high trust score value is considered as a legitimate medical device.

3.4. Device Classification. In this stage, the output of the device identification stage is the input of the device in the classification stage; we perform the next steps in Algorithm 2, using a periodically calculated trust score.

Each sensor node is identified and labelled under legitimate nodes and attacking nodes. Initially, the network is classified into clusters consisting of cluster head and cluster members. For each node in the network, the trust-score value is calculated based on the packet delivery ratio, energy available, and number of neighbours. The final trust-score value decides device type as legitimate or attacking nodes. The legitimate nodes considered for further cluster head selection and attacking nodes act as member in the cluster. For each node in the cluster head list, the trust score is calculated, and based on the trust-score value, the cluster head for the current interval is selected and announced in the network. All the cluster members transmit data to the announced cluster head in their time slots. A periodical trust score is calculated at each interval to find the behaviour of nodes in the network. Identified legitimate nodes are classified for cluster head and candidate for cluster head. As the cluster head needs to be active all the time during data transmission, it consumes maximum energy. Periodically, trust scores are calculated and cluster heads are chosen. Due to some network circumstances, the energy of the cluster head starts draining, and the candidate for the cluster head list is considered to further decide the cluster head for that period. The new cluster head advertises and the cluster member node joins the cluster. Thus, the nodes in the candidate cluster head list further take the responsibilities if cluster head energy is minimum and not able to aggregate data.

3.5. Data Transmission. The proposed model is applied to the CMS system, where sensory medical data are periodically classified based on their similarity. The samples described will be trained and tested using the artificial neural network (ANN) machine learning classifier to build a machine learning model. As a result, the classification model can recognize new samples and classify them accordingly. CH, where all the heterogeneous data readings are transmitted, consumes the minimum energy for each set of redundant data to be discarded. Thus, the sensed readings redirected to the CH from the CMs are restricted thereby saving energy of individual sensor nodes.

CC: current cluster
$\in\in NC$CM: cluster member of CC
CH: cluster head of CC
Inputs
LS D: node identified as legitimate
AS D: node identified as the attacker
S: simulation time
NC: number of clusters
Output
CH: list of selected *CH* nodes at interval*S*
(1) While (*S*)
(2) At each periodic interval $pi \in S$
(3) For each cluster $CC \in NC$
(4) For each node $l \in CC$
(5) If ($l \neq AS\ D$)
(6) 'classify into CCH'
(7) $CCH \leftarrow l$
(8) Else
(9) 'classify into CM'
(10) $CM \leftarrow l$
(11) End If
(12) For each node $i \in CCH$
(13) R^i = Fetchscore (i)
(14) val (i)$\leftarrow R^i$
(15) End For
(16) index = max (val)
(17) $CH \leftarrow$index
(18) Announce *CH* Selection
(19) End For
(20) $pi++$
(21) End While
(22) Stop

Algorithm 2: Device classification.

4. Result and Discussion

This section defines the results obtained after running the performance metrics. The system is build using the NS-2 parameter. A 1000×1000 m square area is created with 100 nodes. Nodes are considered as medical devices used in the medical operating room. The study involves the simulation of nodes such as cameras, health checkup machines, and other medical sensors. The authors use sensory channels like haptic input, visual information, and auditory information. Compare the proposed EDDC protocol, LEACH, and ECFU protocol under various attacks like DDoS attack, replay attack, and eavesdrop attack using performance parameters such as throughput, packet delivery speed (PDR), delay, overhead, and energy consumption. Experiments have made it possible to increase the service life of the network by about 20–25% using the proposed method. High-density sensor network consists of a huge number of small and power constrained nodes. The proposed model can be enhanced for large number of power constrained nodes. The model uses IEEE 802.11 medium access control protocol for communication. The model works on cluster based approach. It coordinates communication among nodes and determines cluster head and members based on available energy. Even though model is introduced in high-density network, it handles communication among heterogeneous nodes and classifies the nodes into different clusters. The cluster based approach simplifies network monitoring and determines residual energy of nodes. The initial experimentation is done for 100 to 600 medical sensor nodes. The quality of service parameters is measured in presence of various attacks. In traditional protocols, CH is created on the probability function, and CHs are selected in each round. The continuous simulation process provided that all nodes are consumed with energy values. Simulation is performed from 100 to 600 nodes (Table 2).

Telerobotic surgeries in a machine-to-machine (M2M) communication network carry data over long distances. The signal needs to travel for longer distances with sensor and control nodes that are distinctly located. To accommodate M2M aspect in telerobotic surgery, the author proposed using IEEE 802.11ah standard. It is a wireless standard designed to be utilized in the Internet of things (IoT) network.

LEACH is a routing protocol that organizes a cluster in such a way that energy is evenly distributed across all sensor nodes in the network. The LEACH protocol creates multiple clusters of sensor nodes and one node at the head of a particular cluster and acts as a routing node for all other nodes in the cluster. Before the communication has been started, select the cluster head (CH). The CH is responsible

Table 2: Simulation factors.

Parameter	Values
Number of IoT/machines/sensor nodes	100, 200, 300, 400, 500, 600.
Number of attackers	10% of nodes
Traffic pattern	CBR
Number of connections	10
Sink	Base station (BS)
Area	1000×1000 (long-distance communications)
MAC	802.11
Topology	Random deployment
Routing protocol	EDDC, ECFU, LEACH
Initial energy	0.5 J
Transmitter energy consumption	16.7 nJ
Receiver energy consumption	36.1 nJ
Simulation time	200 seconds

for routing the entire cluster. The LEACH protocol for randomization and cluster heads is chosen from a group of nodes, but this selection of CH from multiple nodes is more likely to result in longer latency. CH is responsible for collecting the data and transmitting them to the BS. In process of data transmission, more energy is consumed [46]. If the threshold value is less, the node fits as CH. The threshold $T(n)$ is [44]

$$T(n) = \begin{cases} \dfrac{1}{1 - p(r \bmod (1/p))}, & \forall n \in G, \\ 0, & \text{otherwise}, \end{cases} \quad (6)$$

where p is the percentage of sensor nodes, r shows a circle, and G is a group of nodes in $1/p$ round. ECFU clustering technology, together with machine learning technology, made it possible to achieve efficient network operation using fuzzy updating. The author used performance parameters such as throughput, packet delivery speed (PDR), delay, communication overhead, and energy consumption.

The authors considered 200 seconds to represent simulation. However, we verified the quality of service parameters for different time frames. The authors incorporated various attacks and measured network performance during these 200 seconds. The literature indicates that the performance of the system can be measured at a smaller time scale. It is observed that analysis of the network with respect to packet loss can be possible in the mentioned time frame.

5. Performance Metrics

The wireless sensor network (WSN) is becoming increasingly used in the medical field. As WSN continues to expand, it provides many opportunities but also creates security challenges. The sensor network is vulnerable to various attacks. One of the most common types of attacks carried out recently is distributed denial of service (DoS) attack, replay attack, and eavesdropping.

In Figure 3(a), the number of packets with different packet sizes is sent to the network and their response time is recorded. Delay is one of the parameters responsible for reducing network performance. The response time in the presence of a DoS attack in the same network is measured and shown in Figure 3(b) which shows delay due to misbehaved nodes present in the network.

5.1. Influence of Attack on Network Lifetime. Security in sensor networks is an issue that has been raised over a period of time. As WSN continues to grow, it opens the door to vulnerability. The most common and threatening type of attack carried out is distributed denial of service (DDoS) and replay attack. The attacks occur from multiple end of the sensor network and compromise legitimate nodes. These attacks make network resources unavailable to legitimate devices. These attacks affect the network performance and eventually lead to complete network failure.

An energy-efficient protocol is required in a medical sensor network that can increase network lifetime. The proposed EDDC protocol improves energy consumption and provides nodes for secured data transmission. The protocol extends network lifetime using a cluster based approach.

The network performance of the proposed algorithm is measured for 100 to 600 nodes. The malicious nodes are introduced and service parameters are measured. The author considered legitimate and attacking nodes in the medical sensor network. The effect of malicious nodes with respect to packet size and response time is measured and shown in Figure 3. The algorithmic performance is verified with 10% malicious nodes. The performance is measured based on node malicious nodes behaviour. The effect of malicious nodes on network performance for DDoS, replay, and eavesdrop attack is shown in Figures 4–6. The key service parameters such as delay, energy consumed, communication overhead, and packet delivery ratio are measured which are challenging to achieve in a telerobotic environment.

Experimental results are enhanced by introducing the impact of attacks on packet response time. For variable packet size, the response time of packets with and without attack is shown in Figure 3. Energy consumption is the key parameter that decides the network lifetime.

The performance metrics such as throughput, packet delivery ratio, delay, communication overhead, and energy consumption are considered for analysis and the efficiency

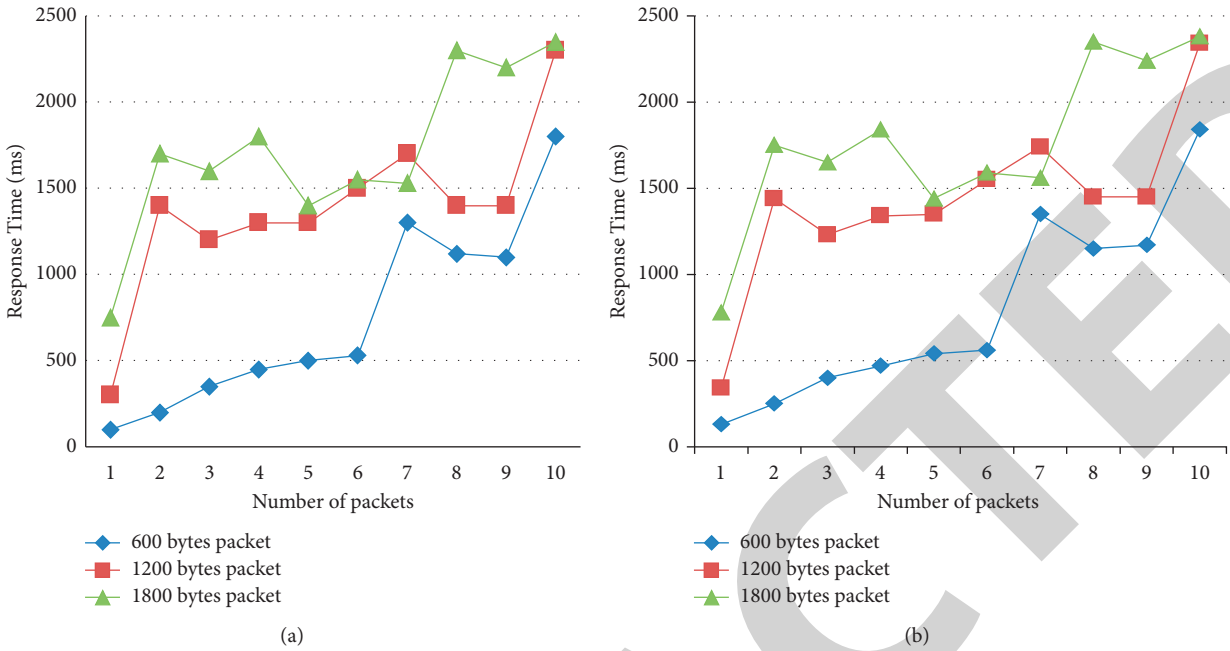


Figure 3: Node response time with respect to packet size. (a) Without attack. (b) With attack.

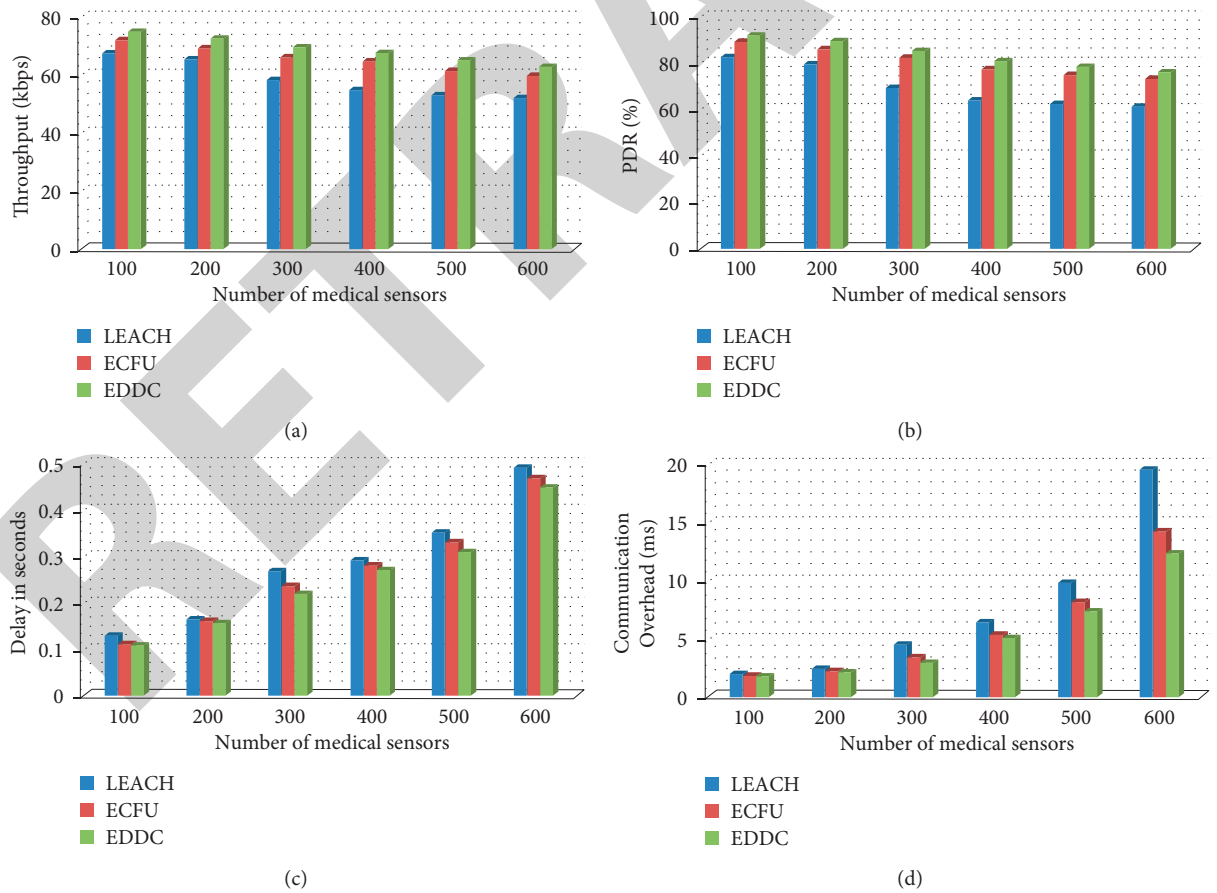
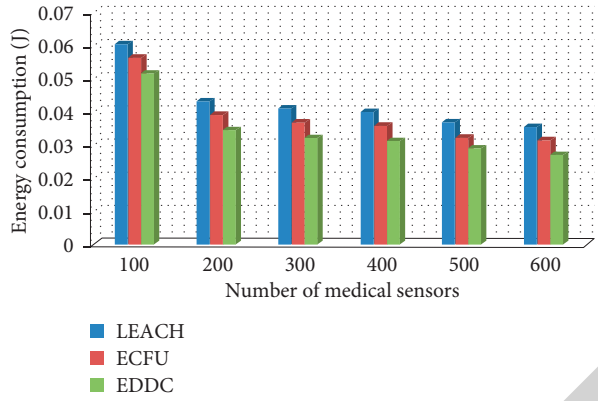


Figure 4: Continued.



(e)

Figure 4: Performance measurement under DDoS attack. (a) Throughput. (b) PDR. (c) Delay. (d) Communication overhead. (e) Energy consumption.

of the proposed EDDC system was compared with existing energy-efficient systems. The graphs are plotted for LEACH, ECFU, and EDDC for 100 to 600 medical sensor nodes network.

Throughput is the difference between send and receive data at the base station. The higher the ratio, the better the performance. The throughput of the system under DDoS attack is shown in Figure 4(a), the throughput of the system under replay attack is shown in Figure 5(a), and the throughput of the system under eavesdrop attack is shown in Figure 6(a). The number of medical sensors is defined on the x-axis representing the medical sensor nodes such as cameras, health checkups machines, computers, and printers, and throughput values are defined on the y-axis measured by EDDC protocol, LEACH, and ECFU protocol. Figures 4–6 show that the throughput value of the LEACH is less than the ECFU protocol and the throughput value of the proposed EDDC protocol is higher than LEACH and ECFU protocol. It is cleared from the graph that the proposed EDDC protocol outperforms better in increased sensor nodes and under DDoS, replay, and eavesdrop attacks. Throughput (T) is calculated by [47]

$$T = \frac{\sum_{I=1}^{\text{node}} \left(P_{\text{Suceessful delivered}}\right) \times \left(P_{\text{Average Size}}\right)}{P_{\text{sent time}}}, \tag{7}$$

where $(P_{\text{Suceessful delivered}})$ is a packet sent successfully, $(P_{\text{Average Size}})$ = average packet size, and $P_{\text{sent time}}$ is the total time to the sent packets.

PDR calculation is the percentage of the receiving to sent packets. The PDR of the system under DDoS attack is shown in Figure 4(b), PDR of the system under replay attack is shown in Figure 5(b), and the PDR of the system under eavesdrop attack is shown in Figure 6(b). The number of medical sensors is defined on the x-axis; it represents the medical sensor nodes such as cameras, health checkups machines, computers, printers; and PDR values are defined on the y-axis measured by EDDC protocol, LEACH, and ECFU protocol. The figures show that the PDR value of the LEACH is less than the ECFU protocol and the PDR value of the proposed EDDC protocol is higher than LEACH and ECFU protocol. It is clear from the graph that the proposed EDDC protocol delivers more packets under DDoS, replay, and eavesdrop attacks. The PDR is calculated by [47]

$$P\ DR = \frac{\sum_{I=1}^{\text{node}} \left(P_{\text{delivered}}\right)}{P_{\text{sent}}}. \tag{8}$$

The delay value suggests that the simulator has all kinds of time spent sending packets from the data source of the node to the destination node of the cluster. The system delay under DDoS attack is shown in Figure 4(c), delay of the system under replay attack is shown in Figure 5(c), and the delay of the system under eavesdrop attack is shown in Figure 6(c). The number of medical sensors is defined on the x-axis; it represents the medical sensor nodes such as cameras, health checkups machines, computers, printers; and delay values are defined on the y-axis measured by EDDC protocol, LEACH, and ECFU protocol. The figures show that the delay value of the LEACH is more than the ECFU protocol and the delay value of the proposed EDDC protocol is less than LEACH and ECFU protocol under DDoS, replay, and eavesdrop attacks. So, the delivery of packets is fast by EDDC protocol. The delay (D) is calculated by [47]

$$D = \sum_{I=0}^{\text{node}} T_{\text{time}} + R_{\text{time}} + W_{\text{time}}, \tag{9}$$

where T_{time} = transmission time of packets, R_{time} = receiving time of packets, and W_{time} = waiting time of packets. Communication overhead is the ratio of actual communication time and computed communication time for real communication. The communication overhead of the system under DDoS attack is shown in Figure 4(d), the communication overhead of the system under replay attack is shown in Figure 5(d), and the communication overhead of the system under eavesdrop attack is shown in Figure 6(d). The number of medical sensors is defined on the x-axis; it represents the medical sensor nodes such as cameras, health

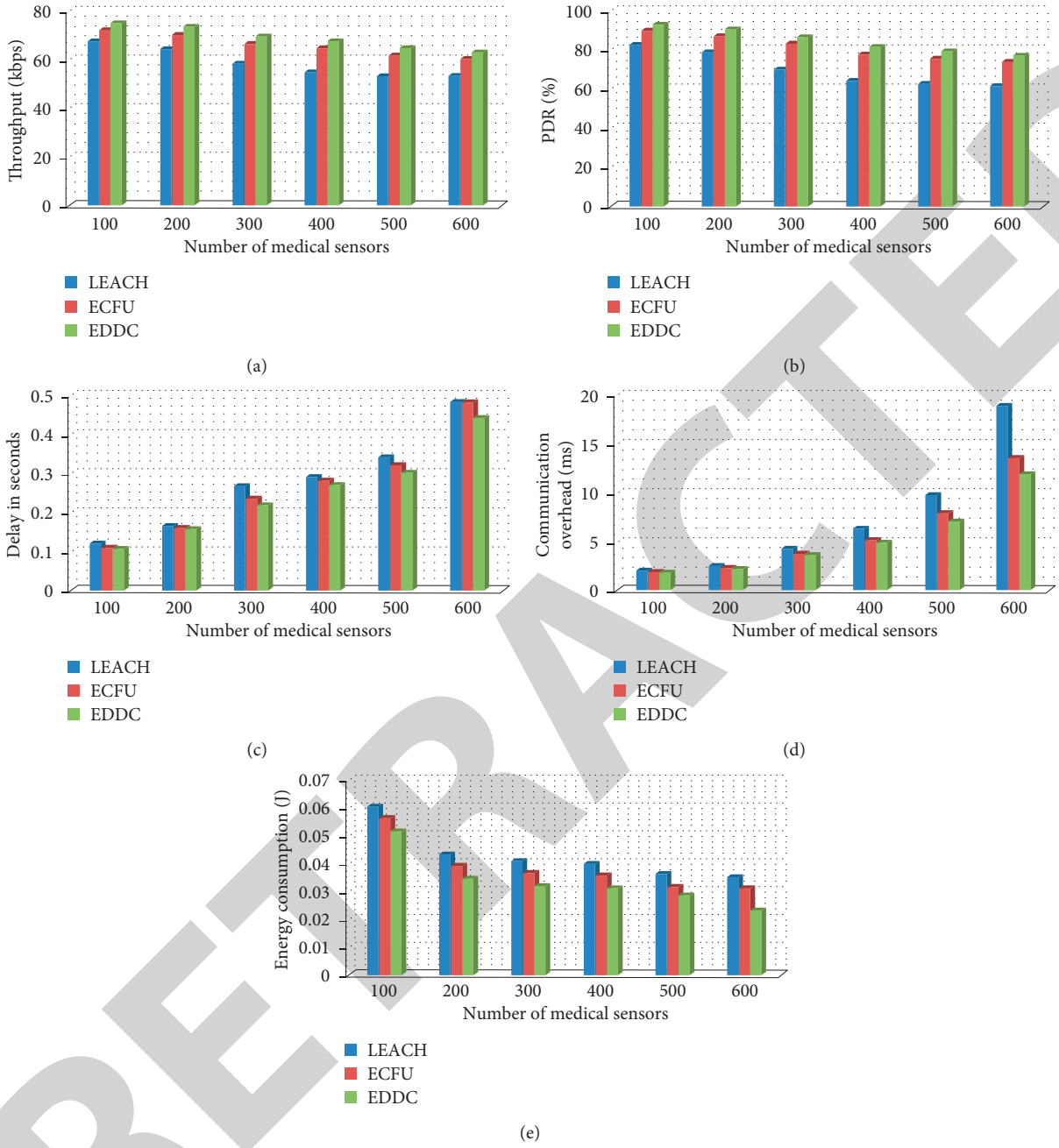


Figure 5: Performance measurement under replay attack. (a) Throughput. (b) PDR. (c) Delay. (d) Communication overhead. (e) Energy consumption.

checkups machines, computers, printers; and communication overhead values are defined on the y-axis measured by EDDC protocol, LEACH, and ECFU protocol. The figures show that the communication overhead time of the LEACH is more than the ECFU protocol and the communication overhead time of the proposed EDDC protocol is less than LEACH and ECFU protocol under DDoS, replay, and eavesdrop attacks. The communication overhead (CO) is calculated by [47]

$$\mathrm{CO} = \frac{\left(\text{Communication time}_A - \text{Communication time}_b\right)}{\text{Communication time}_A}. \tag{10}$$

The energy consumption of the system under DDoS attack is shown in Figure 4(e), the energy consumption of the system under replay attack is shown in Figure 5(e), and the energy consumption of the system under eavesdrop attack is shown in Figure 6(e). The number of medical

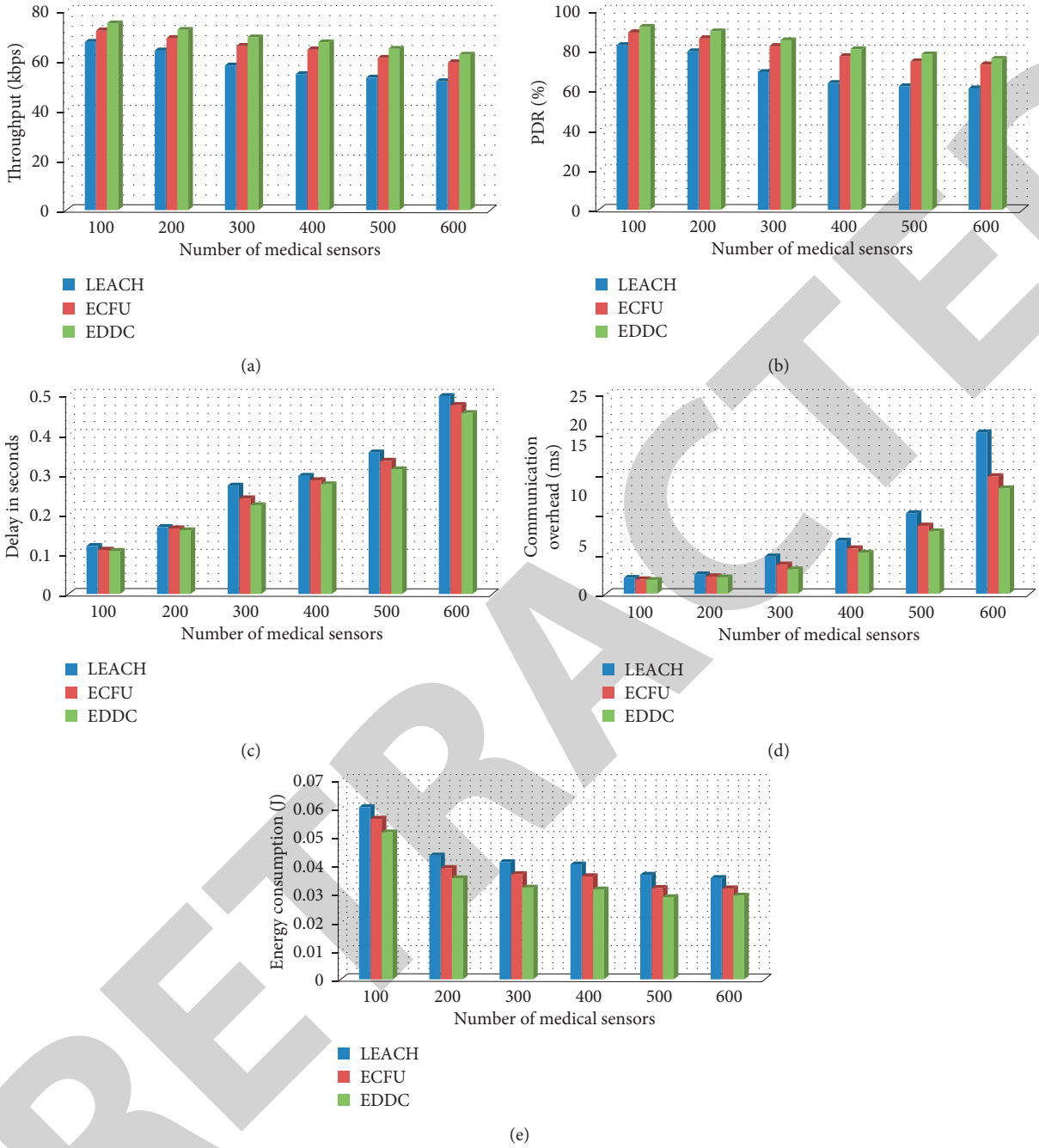


Figure 6: Performance measurement under eavesdrop attack. (a) Throughput. (b) PDR. (c) Delay. (d) Communication overhead. (e) Energy consumption.

sensors is defined on the x-axis; it represents the medical sensor nodes such as cameras, health checkups machines, computers, printers; and energy consumption values are defined on the y-axis measured by EDDC protocol, LEACH, and ECFU protocol. The figures show that the energy consumption of the LEACH is more than the ECFU protocol and the energy consumption of the proposed EDDC protocol is less than LEACH and ECFU protocol under DDoS, replay, and eavesdrop attacks. The energy consumption is calculated by [47]

$$P_{\text{con}} = \sum_{i=1}^{\text{node}} T_e + R_e + W, \tag{11}$$

where T_e = energy consumption while packet is sent, R_e = energy consumption while receiving packets, and W_e = energy consumption while waiting for packets.

The performance measurements for ECFU and EDDC for DDoS, replay, and eavesdrop attacks are analyzed separately and shown in Figures 7 and 8. To increase network

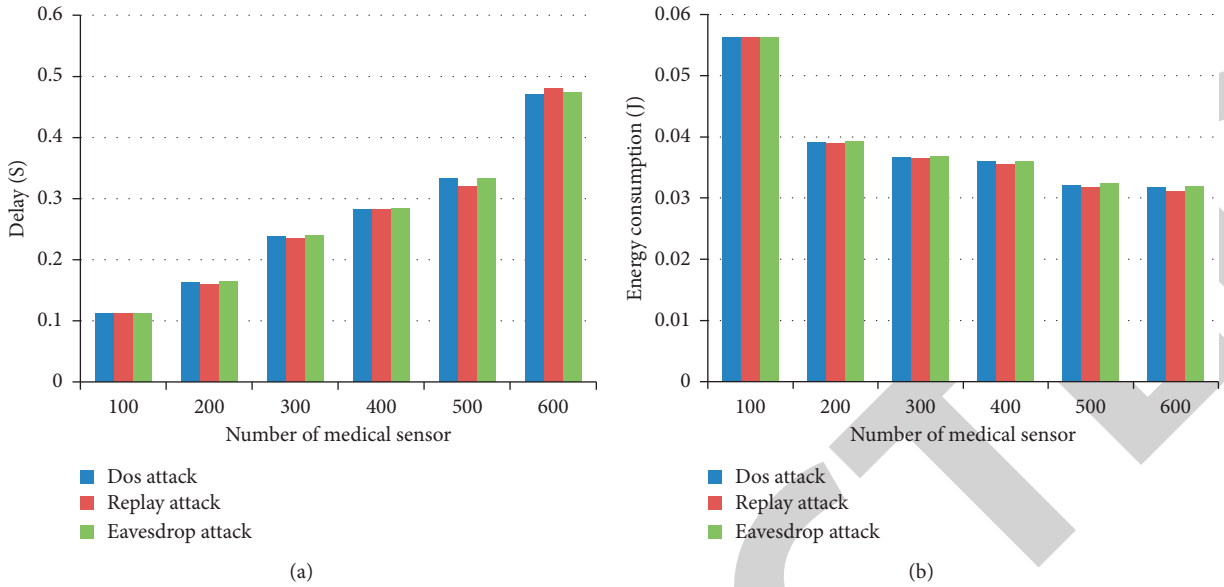


Figure 7: Performance measurement under DDoS, replay, and eavesdrop attack using ECFU algorithm. (a) Delay. (b) Energy consumption.

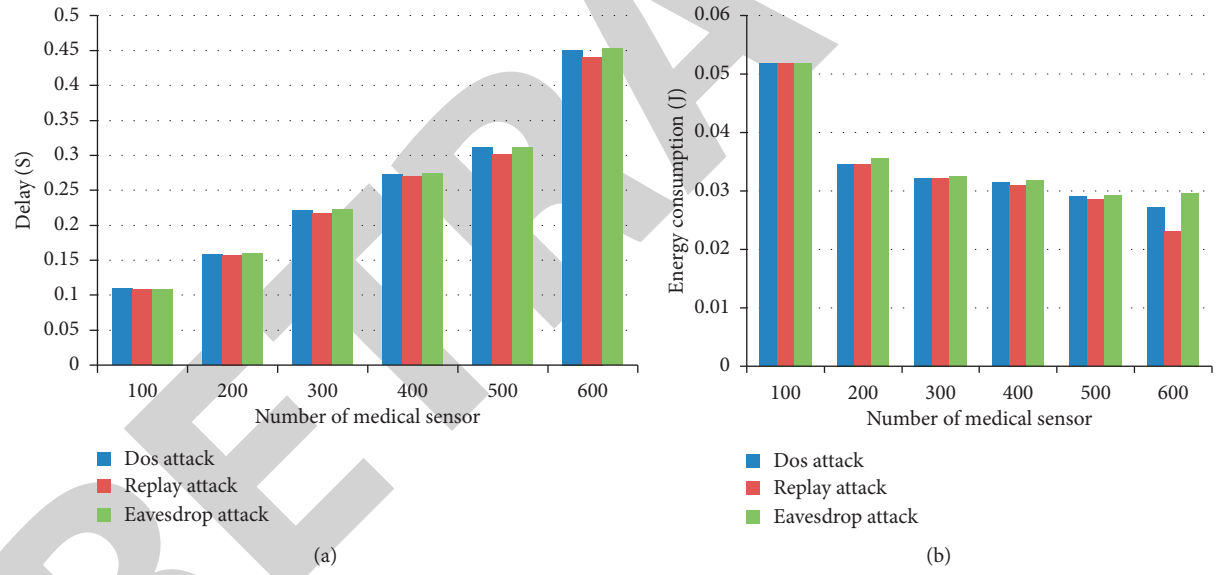


Figure 8: Performance measurement under DDoS, replay, and eavesdrop attack using EDDC algorithm. (a) Delay. (b) Energy consumption.

lifetime and reduce transmission delay, the performance of the network for delay and energy consumption in presence of attacking nodes are discussed and analyzed. The comparative results indicate proposed system shows improved performance metrics in presence of attacks.

6. Conclusion

The proposed Efficient Device type Detection and Classification (EDDC) protocol is designed for device identification and classification in M2M communication for secure telerobotic surgery. The designed protocol meets the strict security requirement of the telerobotic surgical system. The contribution of this article is multifaceted. This study shows accurately detection of malicious devices in M2M communication. To identify the node as legitimate or attacker, design the trust-score computation technique to compute the periodic trust score of each node. Then, perform classification on identified devices at periodic intervals based on their similarities. The machine learning classifier artificial neural network (ANN) is built for efficient data transmission. The article presents the effectiveness of this method with operational parameters. It shows the proposed EDDC protocol performs better than LEACH and ECFU protocol

under DDoS, replay, and eavesdrop attacks. The proposed algorithm for device identification and classification is energy-efficient and scalable. We conducted a simulation as a proof of the concept where we showed the quality of service parameters is influenced by changing the number of nodes, packet size, and simulation time. Malicious and nonmalicious nodes classification for secure telerobotic surgery further contributes to efficient and secure communication. Future plan is to calculate the trust score of each device for designing access control to telerobotic devices for high-density networks.

Data Availability

Data are available on request.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Z. Meng, Z. Wu, C. Muvianto, and J. Gray, "A data-oriented M2M messaging mechanism for industrial IoT applications," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 236–246, 2017.

[2] M. Kaur and S. Kadam, "Discovery of resources over Cloud using MADM approaches," *International Journal for Engineering Modelling*, vol. 32, pp. 83–92, 2019.

[3] K. Jairath, N. Singh, V. Jagota, and M. Shabaz, "Compact ultrawide band metamaterial-inspired split ring resonator structure loaded band notched antenna," *Mathematical Problems in Engineering*, vol. 2021, Article ID 5174455, 12 pages, 2021.

[4] A. Kishor, C. Chakraborty, and W. Jeberson, "Reinforcement learning for medical information processing over heterogeneous networks," *Multimedia Tools and Applications*, vol. 80, no. 16, pp. 23983–24004, 2021.

[5] M. Kaur and S. Kadam, "A novel multi-objective bacteria foraging optimization algorithm (MOBFOA) for multi-objective scheduling," *Applied Soft Computing*, vol. 66, pp. 183–195, 2018.

[6] M. Islam, D. A. Atputharuban, R. Ramesh, and H. Ren, "Real-time instrument segmentation in robotic surgery using auxiliary supervised deep adversarial learning," *IEEE Robotics and Automation Letters*, vol. 4, no. 2, pp. 2188–2195, 2019.

[7] A. A. Shvets, A. Rakhlin, A. A. Kalinin, and V. I. Iglovikov, "Automatic instrument segmentation in robot-assisted surgery using deep learning," in *Proceedings of IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 624–628, IEEE, Orlando, FL, USA, December 2018.

[8] M. Kaur, "Elitist multi-objective bacterial foraging evolutionary algorithm for multi-criteria based grid scheduling problem," in *Prpoceedings of the 2016 International Conference on Internet of Things and Applications (IOTA)*, pp. 431–436, Pune, India, January 2016.

[9] OECD Report, "machine-to-machine communications: connecting billions of devices," *OECD Digital Economy Papers*, vol. 192, 2012.

[10] T. Kaur and D. Kumar, "Computational intelligence-based energy efficient routing protocols with QoS assurance for wireless sensor networks: a survey," *International Journal of Wireless and Mobile Computing*, vol. 16, no. 2, pp. 172–193, 2019.

[11] M. Chen, J. Wan, and F. Li, "Machine-to-Machine communications: architectures, standards and applications," *KSII Transactions on Internet & Information Systems*, vol. 6, pp. 480–497, 2012.

[12] Z. Yan Zhang, Y. Rong Yu, X. Shengli Xie, Y. Wenqing Yao, X. Yang Xiao, and M. Guizani, "Home M2M networks: architectures, standards, and QoS improvement," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 44–52, 2011.

[13] S.-J. Jung, R. Myllyla, and W.-Y. Chung, "Wireless machine-to-machine healthcare solution using android mobile devices in global networks," *IEEE Sensors Journal*, vol. 13, no. 5, pp. 1419–1424, 2013.

[14] J. Granjal, E. Monteiro, and J. S. Silva, "Security issues and approaches on wireless M2M systems," in *Wireless Networks and Security*, S. Khan and A.-S. Khan Pathan, Eds., Springer, Berlin Germany, pp. 133–164, 2013.

[15] C. Lai, L. Hui, Z. Yueyu, and C. Jin, "Security issues on machine to machine communications," *KSII Transactions on Internet & Information Systems*, vol. 6, pp. 498–514, 2012.

[16] M. P. Lokhande and D. D. Patil, "Security threats in M2M framework of IoT," *International Journal of Advanced Science and Technology*, vol. 29, no. 8, pp. 1809–1823, 2020.

[17] X. Sun, S. Men, C. Zhao, and Z. Zhou, "A Security authentication scheme in machine-to-machine home network service," *Security and Communication Networks*, vol. 8, pp. 2678–2686, 2012.

[18] W. Ren, L. Yu, L. Ma, and Y. Ren, "RISE: a RelIable and SEcure scheme for wireless Machine to Machine communications," *Tsinghua Science and Technology*, vol. 18, no. 1, pp. 100–117, 2013.

[19] M. Yair, M. Bohadana, A. Shabtai, M. Ochoa et al., "Detection of unauthorized IoT devices using machine learning techniques," 2017, https://arxiv.org/abs/1709.04647.

[20] A. Sivanathan, D. Sherratt, H. Hassan Gharakheili, R. Adam, C. Wijenayake, and A. Vishwa, "Characterizing and classifying IoT traffic in smart cities and campuses," in *Proceedings f the IEEE INFOCOM Workshop Smart Cities Urban Computing*, pp. 1–6, Atlanta, GA, USA, May 2017.

[21] V. Bhatia, S. Kaur, K. Sharma, P. Rattan, V. Jagota, and M. A. Kemal, "Design and simulation of capacitive MEMS switch for ka band Application," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 2021513, 8 pages, 2021.

[22] M. Miettinen, S. Marchal, I. Hafeez, A.-R. Sadeghi et al., "Iot SENTINEL: automated device-type identification for security enforcement in IoT," in *Proceedings of the IEEE 37th International Conference on Distributed Computing Systems*, pp. 2177–2184, Atlanta, GA, USA, June 2017.

[23] X. Zhang, L. Yao, C. Huang, Q. Z. Sheng, and X. Wang, "Intent recognition in smart living through deep recurrent neural networks," in *Proceedings of the International Conference on Neural Information Processing (ICONIP)*, pp. 748–758, Guangzhou, China, November 2017.

[24] B. M. Dickens and R. J. Cook, "Legal and ethical issues in telemedicine and robotics," *International Journal of Gynecology & Obstetrics*, vol. 94, no. 1, pp. 73–78, 2006.

[25] H. H. King, K. Tadano, R. Donlin et al., "Preliminary protocol for interoperable telesurgery," in *Proceedings of the international conference on advanced robotics*, pp. 1–6, Munich, Germany, June 2009.

[26] G. S. Lee and B. Thurai singham, "Cyberphysical systems security applied to telesurgical robotics," *Computer Standards & Interfaces*, vol. 34, no. 1, pp. 225–229, 2012.

[27] N. Dowler and C. J. Hall, "Safety issues in telesurgery: summary," in *Proceedings of the IEEE Colloquium on towards Telesurgery*, pp. 6/1–6/3, London, UK, June 1995.

[28] B. Challacombe, L. Kavoussi, A. Patriciu et al., "Technology insight: telementoring and telesurgery in urology," *Nature Clinical Practice Urology*, vol. 3, no. 11, pp. 611–617, 2006.

[29] K. Coble, W. Wang, B. Chu, and Z. Li, "Secure software attestation for military telesurgical robot systems," in *Proceedings of the Military Communications Conference*, pp. 965–970, San Jose, CA, USA, November 2010.

[30] M. E. Tozal, Y. Wang, E. Al-Shaer et al., "On secure and resilient telesurgery communications over unreliable networks," in *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 714–719, IEEE, Shanghai, China, April 2011.

[31] Y. Dong, N. Gupta, and N. Chopra, "On content modification attacks in bilateral teleoperation systems," in *Proceedings of the American Control Conference (ACC)*, pp. 316–321, IEEE, Boston, MA, USA, July 2016.

[32] A. A. El Kalam, A. Ferreira, and F. Kratz, "Bilateral teleoperation system using QoS and secure communication networks for telemedicine applications," *IEEE Syst J*, vol. 10, no. 2, pp. 709–720, 2016.

[33] P. Fekri, P. Setoodeh, F. Khosravian et al., "Towards deep secure tele-surgery," in *Proceedings of the International Conference on Scientific Computing (CSC)*, pp. 81–86, Wuxi, China, June 2018.

[34] R. Amin, S. H. Islam, P. Gope, K.-K. Raymond Choo, and N. Tapas, "Anonymity preserving and lightweight multi-medical server authentication protocol for telecare medical information system," *IEEE J Biomed Health Inf*, vol. 23, no. 4, pp. 1749–1759, 2019.

[35] V. Sureshkumar, R. Amin, V. R. Vijaykumar, and S. Raja Seker, "Robust secure communication protocol for smart healthcare system with FPGA implementation," *Future GenerComputSyst*, vol. 100, pp. 938–951, 2019.

[36] S. D. Suganthi, R. Anitha, V. Sureshkumar, S. Harish, and S. Agalya, "End to end light weight mutual authentication scheme in IoT based healthcare environment," *J ReliabIntell Environ*, vol. 2019, pp. 1–11, 2019.

[37] A. Hommersom, P. J. F. Lucas, M. Velikova et al., "MoSHCA - my mobile and smart health care assistant," in *Proceedings of the E-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on*, pp. 188–192, Lisbon, Portugal, October 2013.

[38] M. Shabaz and A. Kumar, "SA sorting: a novel sorting technique for large-scale data," *Journal of Computer Networks and Communications*, vol. 2019, Article ID 3027578, 7 pages, 2019.

[39] P. Dipti Durgesh and M. W. Vijay, "Adaptive real time data mining methodology for wireless body area network based healthcare applications" advanced computing," *International Journal*, vol. 3, no. 4, 2012.

[40] C. Chakraborty, "Chronic wound image analysis by particle swarm optimization technique for tele-wound network," *Wireless Personal Communications*, vol. 96, pp. 3655–3671, 2017.

[41] D. Meshram and D. P. Dipti, "5G enabled tactile internet for tele-robotic surgery" , third international conference on computing and network communications," *Procedia Computer Science*, vol. 171, pp. 2618–2625, 2020.

[42] M. P. Lokhande and D. D. Patil, "Network performance measurement through machine to machine communication in tele-robotics system," *Tehnički Glasnik*, vol. 15, no. 1, pp. 98–104, 2021.

[43] J. Bhola and S. Soni, "Information theory-based defense mechanism against DDOS attacks for WSAN," in *Advances in VLSI, Communication, and Signal Processing*, D. Harvey, H. Kar, S. Verma, and V. Bhadauria, Eds., Springer, Singapore, 2021.

[44] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives," *Journal of Food Quality*, vol. 2021, Article ID 7608296, 20 pages, 2021.

[45] A. Kishor and C. Chakraborty, "Artificial intelligence and internet of things based healthcare 4.0 monitoring system," *Wireless Pers Commun*, vol. 120, 2021.

[46] T. M. Behera, U. C. Samal, and S. K. Mohapatra, "Energy-efficient modified LEACH protocol for IoT application," *IET Wireless Sensor Systems*, vol. 8, no. 5, pp. 223–228, 2018.

[47] J. Bhola, S. Soni, and G. K. Cheema, "Genetic algorithm based optimized leach protocol for energy efficient wireless sensor networks," *J Ambient Intell. Human Comput.*vol. 11, pp. 1281–1288, 2020.