International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Machine-to-Machine Communication in Telerobotic Systems for Robotics Science

G. Sathish Kumar[1], T. Padmapriya[2], Basant Sah[3], Muruganantham Ponnusamy[4], Anandan[5]

Submitted: 14/09/2023 **Revised:** 30/10/2023 **Accepted:** 14/11/2023

Abstract: Machine-to-machine communication devices interact and share data independently to carry out required activities. The device uses a wireless network to connect to another device. The Internet of Things (IoT) is predicted to flourish when mechanical things can interact on their own. This paradigm is used in security, transportation, business, and healthcare every day. Security experts claim that there are several flaws associated with IoT devices. To perform surgery, treatment, and diagnostics over short or long distances while utilizing wireless communication networks, telerobotic systems are created. For the telerobotics community and data security, the systems additionally offer a minimal delay and a secure communication mechanism. The system can carry out duties intelligently and independently, easing the stress on medical staff and enhancing the standard and efficiency of patient care. Surgeons and patients in the medical industry are dispersed across different locations but connected via open networks. Therefore, with or without the attack, performance is ensured by the design of a medical sensor node network using the LEACH protocol for secure and dependable communication. Lastly, low delay and dependable, secure network transfer are demonstrated by the simulation results.

Keywords: Internet of Things (IoT); LEACH; Machine-to-machine communication (M2M); Telerobotic

1. Introduction

M2M communications are one of the most exciting uses of the top technical advancements in the world. M2M communications are used more frequently because of how widely they are used in many industries. To create Internet of Things generation networks, numerous intelligent devices are connected via wired or wireless connections in M2M communication. These technologies communicate with one another without the direct involvement of a human [1]. The Internet of Things effort may lead to the creation of new job possibilities in fields like environmental surveillance, energy management, medical care, intelligent transportation systems, architectural automation, and smart homes. The security of those data sets that contain private data is a serious concern because M2M communication takes place over an open channel. M2M communication is very vulnerable to attackers for several reasons. In the beginning, its constituent sections frequently expend a larger portion of their energy unattended, which also, makes it simple to physically attack them. Second, the majority of communications take place online, which makes listening in on downlink transmissions fairly easy.

A master robot is shown in a schematic illustration of teleoperation systems in Figure 1.1. In the absence of M2M device identities, the approach has established mutual authorization for inter- and intra-domain communications. The proposed approach can secure text-based tiny data but is unsuitable for large-scale data encryption. Work on corporate disarray with privacy has recently been done. Mathematics' study of chaos examines the behavior of dynamic frameworks that are highly susceptible to starting conditions, unpredictability, and volatility. The authors proposed a nonlinear dynamical system-based private nonorthogonal multiple-access visible-light system for encryption. All authorized users are guaranteed privacy during communication against attackers thanks to the encryption technique. A two-level encryption system has recently been used in a scheme to encrypt data for several users using various keys.

[1]*Assistant Professor, ECE, P.T.Lee Chengalvaraya Naicker College of Engineering and Technology, Oovery, Kanchipuram-631 502, Tamilnadu, India*
Email: sathish14@gmail.com
[2]*Melange Publications, Puducherry, India*
Email: padmapriyaa85@pec.edu
[3]*Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.*
Email: basantbitmtech2008@gmail.com
[4]*Deputy Registrar, Indian Institute of Information Technology Kalyani, Nadia - 741235, West Bengal,*
Email: mp@iiitkalyani.ac.in
[5]*Associate Professor, Department of Mechanical Engineering Vinayaka Mission's Kirupa Nanda Variyar Engineering College Salem.*
Email: anandan@vmkv.edu.in

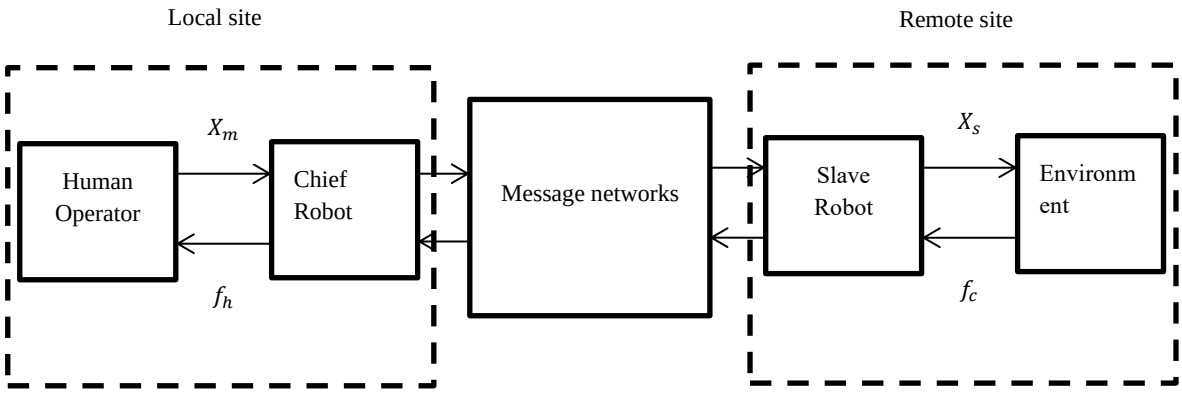

Fig 1.1. A master robot is shown in a schematic illustration of Teleoperation Systems

To provide a more effective, accurate, and affordable alternative to traditional medical procedures, a secured telerobotic surgery has been proposed, compared to current technologies, and operations. Secured Performance criteria are used to evaluate surgical environments, which pose technological hurdles and limits, Energy-saving procedure LACHE is a network parameter that was examined in the medical sensor node of the network. Performance characteristics are measured using an energy-efficient technique based on fuzzy inference systems, both with and without an attack [2]. For secure telerobotic operation, the Efficient Device type Detection and Classification protocol is proposed and created for device recognition and categorization in messaging between machines. Not to mention, employing three features of each sensor nodes, the trust score computation technique is used to construct the periodic trust rating of each node n.

Numerous changes in numerous facets of the human standard of living have been brought about by robotic systems. Several manufacturing sectors use robotics to complete a variety of difficult, sophisticated [3], and demanding jobs like the welding process, assembling goods, evaluation, wrapping, inspection, and many more. Preprogrammed robotics, with its 100% accuracy and round-the-clock functionality, has revolutionized the industrial landscape. Robotics activities were expanded into more ad hoc contexts as network technologies were combined with robotics as it developed.

The committee has identified two classes of networked robots:

- Robots that are tele-operated are ones that people use commands to control from a distance. Most applications for teleoperated robotics are in research, teaching, and general public use.
- Autonomous: Network-operating, information-exchanging robots equipped with sophisticated sensors.
- Robots can now communicate over greater distances and conduct some activities in a highly coordinated manner thanks to sensor technologies.

Here is the remainder of this essay. The Literature review is shown in section 2. Results of the simulation are covered in Sections 3 and the study of M2M communications security requirements is given. Potential challenges to M2M security are discussed in Section 4, along with countermeasures. Section 5 serves as the paper's conclusion.

2. Literature Review

Stojmenovic, I. et.al [4] The definition of M2M and IoT is a goal of several European Union projects. The M2M and IoT-A standards and architectures were suggested by the European Telecom Standards Institute (ETSI). The "local cloud" of gateways, BETaaS (www.betaas.eu) suggested that the internet-connected smart items (such as cellphones, home routers, and roadside units) take the place of the cloud as the location for M2M applications. This makes it possible for apps that operate in a time- and space-constrained environment, demand straightforward and regular user interactions, and react consistently.

Zhang, H., Fu, L., et.al [5] Teleoperation systems are frequently used in challenging industrial settings, like deep sea, space, and nuclear radiation environments, due to their superior qualities. They are crucial in these technical uses as well. In a typical teleoperation setup, the operator moves the master robot while the slave robot is controlled to mimic the master robot's position-tracking motions. Two controls are normally put at the master end and the slave summary, accordingly, to achieve position-tracking management. The term "bilateral control" is also used to describe this control system. Based on bilateral control, the operator can detect the state of the robot's interaction with the task environment.

Bao, J., Fu, L., et.al [6] In a typical telerobotic structure, the slave machine, the communication canal, the human operator, and the job environment are all present. The bilateral control scheme is typically the control architecture of the teleoperation system. The human operator moves the master robot, and a communication link is used to send location information from the masters' robot to the slave sides. The slave robot may complete the task by tracking the master robot's position using the slave controller. Additionally, positional signals or force indications that respond to the environment around the master robot can be sent, and the master robots and operator will be affected by these signals when the master controller acts on them.

Mehrdad, S., et.al [7] A few years later, in the late 1980s and early 1990s, the first surgical robots were introduced, largely to assist surgeons in inserting needles while the patient was within a imaging device for an upcoming in-depth historical review. The first widely acknowledged medical requirement for medical robots, however, was for teleoperated robots in laparoscopic surgery to control an endoscope. It is vital to differentiate

between autonomous robots, guide robots, remote rehabilitation, and robotic simulations to educate hospital staff in order to comprehend this frenzy.

Valner, R., et.al [8] several uses of telerobotics have successfully demonstrated their value, enabling controllers to carry out operations from a secure distance. But despite the risks and the expenses of safety equipment, training, and extra waste disposal, many operations are still carried out by human operators. Workers still outperform distant technologies in terms of efficiency and cognition, including work rate, flexibility, dexterity, and minimum latency and delay during task preparation and execution. These benefits make this option appropriate in all but the most hazardous of circumstances.

Rostami, S., et.al [9] Currently, there are around 4 billion M2M devices in use worldwide; by 2022, that number is expected to reach 50 billion. According to Cisco, a single M2M device may currently generate as much traffic as three feature-rich, entry-level mobile phones. In addition, new M2M network apps and services are predicted to raise the average monthly traffic per device increased from 70 MB in 2014 to 366 MB in 2018. Future M2M networks will encounter numerous obstacles due to the rapid increase in device numbers and high demand for data traffic, particularly about the alleged spectrum constraint issue.

Stojmenovic, I. et.al [10] Cyber-physical systems combine and coordinate the computational and physical components of the system closely. They also incorporate designed and physical systems that are heavily reliant on computers and communication. The Internet of Things is a significant class of CPS. It is an infrastructure that connects common physical things with discusses, based on conventional information carriers like the Internet and telephony networks. Recently, the idea of the Sensor Web has gained attention. It aims to combine distributed data collection with the web's ubiquity and availability, enabling close contact between the digital and physical worlds.

Lokhande, M. P., et.al [11] IoT challenges including data interchange safety, confidentiality, device heterogeneity sensors confidentiality, assistance with decisions, etc. are brought on by the interconnected things that make up IoT. According to an IoT analysis by Ericsson, there will be close to 50 billion linked devices by 2020. Due to major issues with data security and privacy, messaging between machines is affected. Because they are heavily focused on human intervention to shorten their communication time, decision-support mechanisms are still the fundamental issue with the inter-machine network, also known as the IoT.

3. Methods and Materials

M2M Communication Proposed Protocol for Secure Telerobotic Surgery

M2M is a system where many intelligent gadgets collaborate, share, and produce information without the aid of people. Despite having many uses and advantages, the M2M network's design has several technical issues. Security is one of the main concerns that underpin economic progress. However, it is crucial to give the end user accurate and secure data. So, for secure telerobotics having surgery, the author suggests the Efficient Device type Detection and Classification protocol for device recognition and categorization in M2M communication in Figure 3.1. The network is introduced to N number of medical devices, each with a size of X to Y. The following factors were taken into account when formulating the suggested protocol for EDDC:

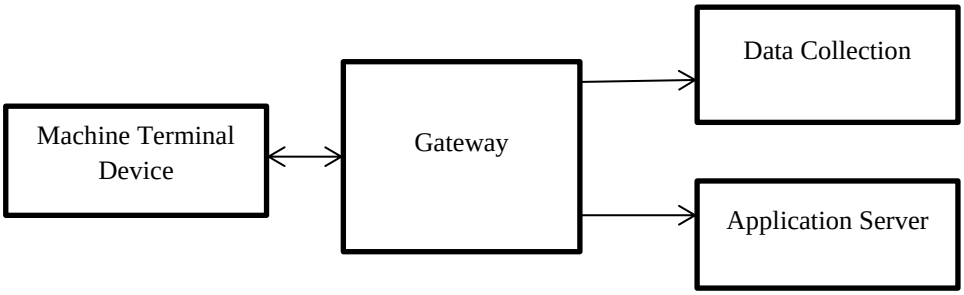

Fig 3.1. M2M connectivity decentralized from a central system

- The Base station (BS) refers to a medical gadget that can sense medical data and transmit it to one medical station.
- Medical services in various locations deploy medical equipment at random.
- Every medical gadget is static and functions uniformly throughout the network.
- The received signal strength indicator (RSSI) is used to determine each device's position.
- Using traditional K-means, all nodes are organised into clusters.
- Data is transferred using a multipass approach from the CMs to the CHs they are assigned.
- Outside of the network part, BS nodes are not limited.
- All medical sensor protuberances have battery and computing power limitations.
- The ability of nodes to do data receiving, data transmission, and data transferring is assumed in M2M.

Understanding a specific kind of gadget

When constructing the trust-score computation methodology for estimating the regular trust score of every node m [12], the (stage analyzes whether the device type is an authorized sensor gadget or a hostile sensor device. To try to recognize a node as an enforceable medical device, initially determine its trust score (TS). If the node's TS value rises over the global trust threshold rating, the node is acknowledged as an attached medical device.

SPD Trust: Exchange HELLO packets with adjacent nodes in the beginning, then realize each device's SPD trust score. This is vital since the perpetrator node makes use of the network to maintain fraudulent obligations, and the SPD does not thrive well on the

network. The preceding algorithm is intended to assess the SPD of node m for the actual time period u-1 to u:

$$SPD^m = \frac{m^{a(u-1,u)}}{m^{b(u-1,u)}} \quad (1)$$

In the above equation, $m^{a(u-1,u)}$ denotes the total number of packets received in the particular time interval $u-1$ to u. While $m^{b(u-1,u)}$ illustrates the total number of packets generated in the particular time interval $u-1$ to u. Greater SPD values maximize the possibility that nodes will eventually be deemed to be legitimate medical instruments.

EL Trust: Malicious nodes consist of those that utilize this energy more quickly although continuing to market themselves as potential partners in data transfer or CH filtering procedures. Therefore, it makes sense to figure out the trust through how much energy every gadget currently has left in it:

$$EL^m = \frac{F_c(m^u)}{F_j(m)} \quad (2)$$

where $F_j(m)$ signifies the initial energy level and $F_c(m^u)$ signifies the energy that remains available at time u. High EL scores improve the possibility that a node will eventually be recognized as a true medical product.

Trust ND: This research investigation figures out ND as the third consistency assess to evaluate the trustworthiness of healthcare devices during the grouping and data transit phase. False accusations generated by an attacker, can serve as a source of data, enabling neighbors to communicate info across a short distance to its intended audience. Using RSSI, the total number of neighbors NC of node m at time u is determined as follows:

$$NC = count\left[\frac{M}{dist(M,Q)} < rssi\right] \quad (3)$$

Where $m \neq qj$, distance (m, qi), requires m's RSSI to compute the distance between m and $qi^{th} \in M$. The trust score was estimated employing the following equation:

$$ND^m = 1 - \left(\frac{1}{NC}\right) \quad (4)$$

The number of one-hop or nearest nodes to the presently under investigation node m is derived in the formula mentioned above. Assessing the RSSI limits includes making confident that the distance between the current node (m) and its nearest node (qi) is lower than the studied node's RSSI value. The value of the count element represents the total number of nodes NC that meet the RSSI standards and will be counted as the closest nodes to the node m that is currently under investigation. A weighted method is used to calculate the node m's ultimate trust score:

$$TS = (x^1 \times SPD^m) + (x^2 \times EL^m) + (x^3 \times ND^m) \quad (5)$$

Here, x^1, x^2, and x^3 have been configured at 0.5, 0.3, and 0.6 sequentially so that the total of them is 1. The trust score TS presently fluctuates between 0 and 1 for node m. Any node with an elevated confidence value is taken into consideration to be reliable medical equipment.

The telerobotic system's layout utilizes force steering

The schematic representation of the telerobotic technology with force guidance according to perception is shown in Fig. 3.2. A bilateral master and slave are employed in the system. The operator manages the master, which generally includes two separate force feedback joysticks as well as a Computer graphics (CG) display. Microsoft SiderWinder2 force-sensitive joysticks are alternatives for force feedback joysticks adopted, with 16 programmable buttons [13]. This includes the eight-action buttons along with eight-direction cap and the potential to convey approximately 100 different forces. The "Bumblebee" stereo vision sensor and an engineering robot constitute the slave. The building of the machinery has four hydraulically powered actuators that can be controlled by four servo valves via a control computer (PC1), and the "Bumblebee", a calibrated camera method made by Point Grey Research Inc., is placed on top of the machine alongside its optical axis parallel to the ground's surface. For applications like tracking, creating virtual reality models, creating human machine interfaces, and mobile robotics, this camera enables real-time stereo picture recording. At a pace of as many as twenty images per second, it can quickly figure out precisely the distance between the robot and the item in its range of view.

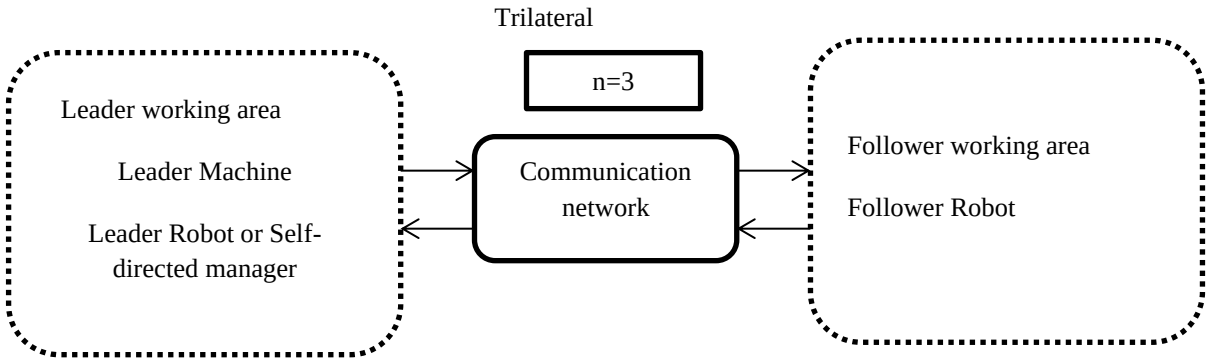

Fig 3.2. Telerobotic Technologies with Force Guidance

With the aid of the 3-D virtual environment in front of him, the operator manages the construction robot via remote joysticks. Then, PC1, which evaluates the operational data from the joysticks as well, develops the functional signals for the robot's servo actuators. On-site deflection sensors mounted to the hydraulic pumps of the building robot evaluate the rotations of the hydraulic cylinders, transmit the data to PC2, and cause the visual representation of the robot to rotate in the virtual space in accordance. The virtual powers, which include the magnetizing force from the task object and the repelling force that emanates from the obstacles or ground surface, are computed in PC2 and submitted back to the controller using data about the mutual posture among the robot and environment. Under the assistance of these powers, the person in charge is able to guide the robot in

the direction of its objective fast while intelligently eliminating obstructions.

Telerobotics Architecture

The HRI testbed that was provided by the researchers was used as a starting point for the invention of the mobile telerobotics system. The telerobotics technology can be broken down into three major parts (Fig. 3.3). These are the mobile robot, the connectivity link, and a person's control interface. In today's execution, the portable robot's features include not solely those needed for online operation, especially path planning, directions, adaptation, etc., as well as those essential to benefit individuals by tracking their control actions.

The primary goal of the robot-assisted navigation scheme is to allow the robot to perform a navigation operation beneath semi-autonomous control while offering adequate assistance (for example, remaining on the way) and avoiding hazards.

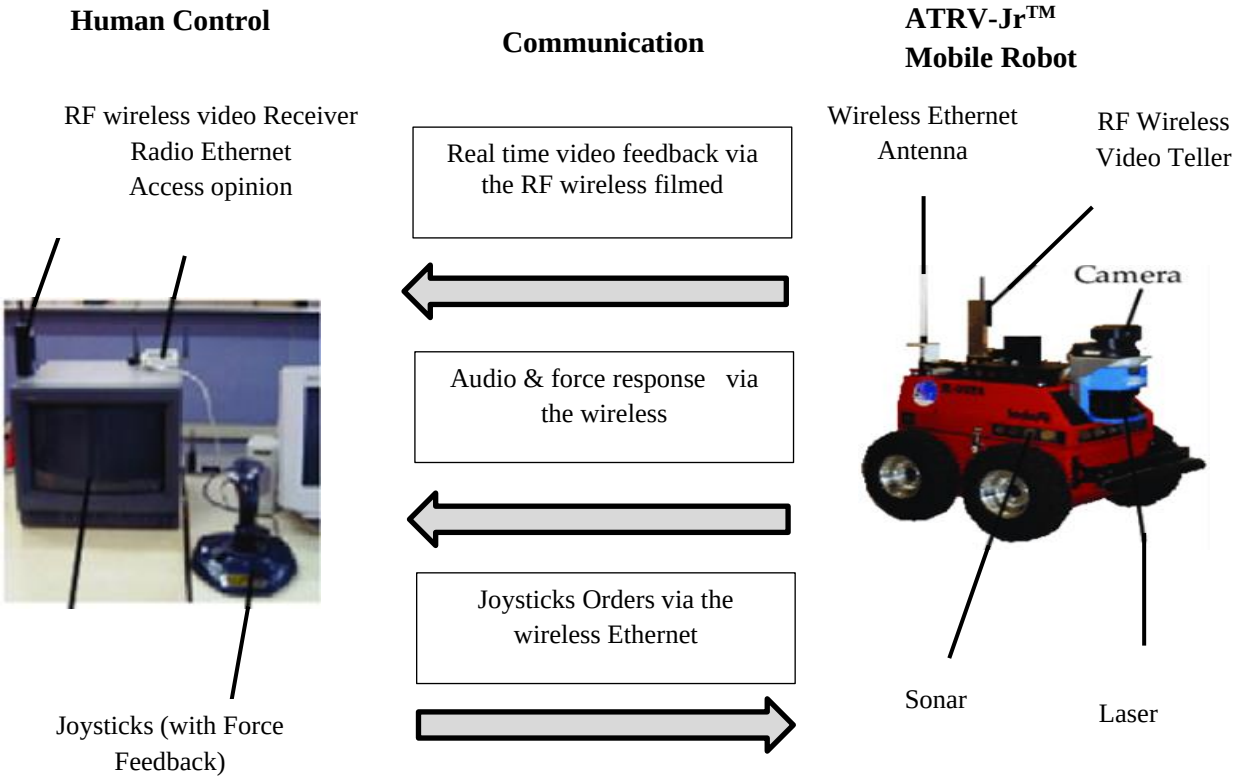

Fig 3.3. Breaking down telerobotics technology into three main components

A hybrid approach made up of arbitrating using priorities and superposition-based commands has been utilized for efficiently organizing both human and robot activity. The individual determines the control methodology via priority-based judgment.

It implies that individuals will adopt the level of communication mode that works appropriately for accomplishing the particular assignment. The supervisor will take advantage of this to decide on the correct robot behaviors to put in effect. As a consequence, fewer calculations are required to coordinate all the diverse robot activities during the execution of the task [14, 15]. This happens due to non-used behaviors being allocated to a lower ranking (or turned off) according to their method's identity. As a consequence, by giving the user as much power as is practical, a superposition-based command merging is used to provide semi-autonomous supervision of the robotic. By that approach, human instruction gets incorporated into the overall personality of a machine as any other cognitive unit inside the robot's framework. Ultimately, the machine holds a temporary record of its forward awareness (possessing 6m x 3m grids) of its surroundings relying on the sonar and laser sensors to guarantee a secure path and proactively coping with human intervention.

The proposed system's algorithm

Restricted processing capacity and battery power are limitations when using medical sensor nodes.

Three metrics are employed by the periodical credibility score of every node to assess the probability that a particular node is an attacker. All three of these metrics were picked for evaluating the illegal activities of network offenders. The parameters being measured are the quantity of successfully delivered packets, energy available, and node degree. In Algorithm 1, GT represents the global confidence rating and TS for the specific gadget trust value.

Utilizing these three characteristics, Total Trust Score calculates the trust scores:

1) Successful Packet Delivery Ratio:

The intruder's node makes use of the internet for malicious objectives, which results in an undesirable SPD. For the present-day time range from j-1 to j, the SPD of node m is calculated as:

$$SPD^m = \frac{m^{s(k-1,k)}}{m^{h(k-1,k)}} \quad (6)$$

Where $m^{s(k-1,k)}$ indicates that the total number of packets received while $m^{h(k-1,k)}$ indicates the total number of packets

generated. Genuine medical devices had been observed in some nodes that have elevated SPD values.

2) Energy available (EA):

During transmission of data or choosing procedures, an individual node that drains energy faster while promoting to the cluster head (CH) is considered as the violent node. Every appliance defines the current residual energy supply in conjunction with:

$$EA^m = \frac{F_s(MU)}{F_j(m)} \quad (7)$$

$F_j(m)$ is the initial energy level and $F_s(MU)$ illustrates the remaining energy at time u. An increased EA score enhances the probability that a node will recognize itself as genuine medical equipment.

3) Degree of Node (DN):

In the current investigation, DN is the third probability measure that has been focused on. It establishes the healthcare equipment's reliability throughout the grouping and transmission of data stages. Sources of information become operational as an outcome of intrusions like DDoS and eavesdropping. Gadgets operate on inaccurate declarations thinking individuals have sufficient nearby neighbors to send data along only a few kilometers to their focus on position. Using RSSI, the total amount of neighbors C^m of node m at time u is evaluated as follows:

$$C^m = count\left[\frac{M}{dist(M,Q)} < RSSI\right] \quad (8)$$

Where $M \neq Q$, dist (M, Q), requires m's RSSI to compute the distance between M and $Q^{th} \in M$. The trust score was estimated employing the following C^m:

$$DN^m = 1 - \left(\frac{1}{C^m}\right) \quad (9)$$

A balanced approach is utilized to figure out node n's ultimate trust score:

$$TS = x^1 \times SPD^m + x^2 \times FM^m + x^3 \times ME^m \left(\frac{1}{C^m}\right) \quad (10)$$

In the above equation they are pickingx^1, x^2, and x^3 values have been picked. Therefore the addition of these values will give the output 1. The range of the node n's trust score, TS, remained 0–1. Legitimate medical equipment is a product which has a high trust score rating.

4. Implementation and Experimental Results

Outcome of the simulation and discussion

From the initial position for this investigation, 100 medical sensor nodes are installed in the wireless sensor networks to generate a square of 1000×1000 m. The source code operates in the NS-2 simulator, and the initial site settings are picked without prearrangement. Each node is supplied with a starting point energy value in Joules units to symbolize the network, and following the simulation, the total amount of energy consumed is evaluated. Develop a LEACH protocol at the start after which enforceable traffic will start to flow [16]. After that, a DoS or Man-in-the-Middle attack is launched to examine its impact on the network's efficiency.

Subsequently evaluate metrics for performance like throughput, packet delivery rate, latency, overhead, and node energy consumption. Implementing the proposed approach, studies demonstrate that the operational lifespan of the network can be lengthened by roughly 21–26%. A probability function has been employed to create CH in standard methods, in each round, CHs are chosen [17]. All nodes can record the amount of energy they use thanks to the perpetual simulation method. In Tab. 1, you may view the simulation's chosen variables.

Table 1. Features Involving Simulation

Parameter	**Values**
Quantity of IoT	200, 300, 500, 600, 700, 800
No. of Muggers	11% of bulges
Pattern of transportation	CBR
Influences number	11
Basin	Base station
Part	1000×1000 (extended distance communications)
MAC	803.11
Topology	Accidental deployment
Direction-finding protocol	LEACH
Initial vigor	1.5 J
Transmitter energy ingesting	17.7 nJ
Receiver energy ingesting	37.1 nJ
Imitation time	300 instants

In Fig. 4.1, the data transfer rate of the complete network is shown in kbps, and the X-axis represents the medical nodes that gather data, such as cameras, medical screening devices, desktop computers, printers, etc., while the Y-axis represents node performance metrics. It displays the effectiveness of the system and shows the LEACH procedure both with and without an assault. The LEACH protocol with the attack has been designated by LEACH-A. The method of computation of information that is transmitted effectively over an allocated amount of time from the sending node towards the receiving node is known as performance. The final result reveals that LEACH-A with attacks possesses lesser throughput figures than LEACH-A without attacks. LEACH-A with an attack has an average efficiency of 59.56 kbps, while LEACH-A without an attack is 64.88 kbps.

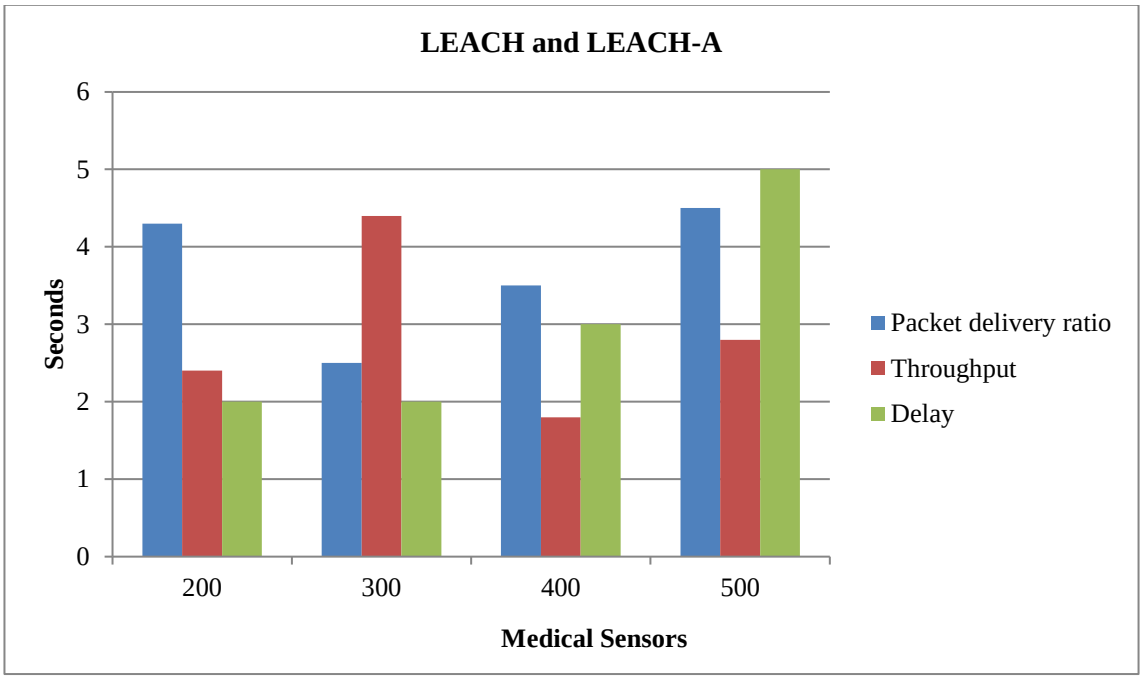

Fig 4.1. Throughput, packet delivery ratio, and delay in LEACH and LEACH-A

The network's packet delivery ratio (PDR) is highlighted in percentage, featuring the medical sensor nodes and the Y-axis represents the packet delivery ratio. Calculating PDR is the ratio of receiving to sending packets. When utilizing the LEACH protocol without an assault, the PDR is higher than when using LEACH-A with a malicious attempt. LEACH-A with a criminal offense has a PDR of 70.98%, while LEACH-A without an assault is 90.25%.

The network delay can be observed having the locations of sensor nodes on the X-axis and the whole system's delay in seconds on the Y-axis. Whenever a packet of information can be transmitted via a link by the source's physical layer, typically is latency. The LEACH protocol exhibits a thinner delay than LEACH-A offers while beneath attack. LEACH and LEACH-A have different delays in seconds of 0.3327 and 0.3845, accordingly, with a variance of +0.0618. The medical sensor nodes, which consist of surveillance systems, health checkup devices, personal computers, printers, etc., are portrayed by the X-axis in Fig. 4.2, which also depicts Y-axis the entire system's communication bandwidth in a millisecond.

Transmission overhead is the proportion of computed communication time to actual communication time. The assault and the LEACH-A protocol has an additional bandwidth requirement than the LEACH protocol without the assault. LEACH-A with a malicious attack has a communication overhead of 8.51 milliseconds (ms) in contrast to 6.28 ms for LEACH-A without a strike, which is a difference of +3.23 ms.

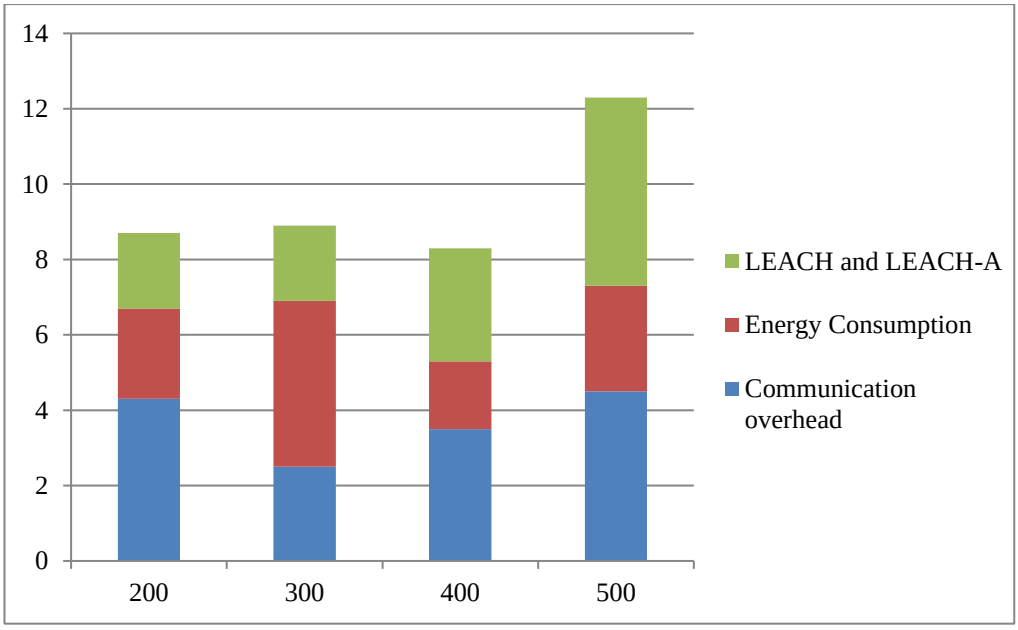

Fig 4.2. Energy consumption and communication overhead

Although energy is the biggest problem in WSN, employing virtual nodes to raise throughput is a must for better energy efficiency. Figure 4.2 portrayed the node's consumption of energy. Based on the research results, the LEACHA with attack 0.05294 (J) burns more energy than the LEACH without assault 0.041 (J). The difference between the energy expenditure of the LEACH protocol without an attack and the LEACH-A protocol with an attack is +0.02194 (J).

5. Conclusion

A new type of active implanted medical technology has now become possible because to machine-to-machine (M2M) connectivity. The implantable device not only monitors, but it also has the ability to intervene when necessary. Medical device producers now have more opportunities to seize the market and expand aftermarket services thanks to M2M connectivity.

The major objective of this paper's proposed M2M communication system in Tele-Robotics aims to reduce the workload on the medical staff by automatically creating numerous jobs without human involvement. In this investigation, we first discuss common network security vulnerabilities in M2M systems and possible countermeasures to lessen or eliminate them. Then, we look into the problems and unresolved research questions in M2M security. The identification and implementation of sufficient safety precautions must be taken into account at the start of the design and development phases, as stated in the article. M2M designers can guarantee complete safety in M2M implementations by taking into account an overall holistic safety approach.

Securing a network from threats is crucial for the security of crucial healthcare procedures. Energy-wise, a sensor network's resources are limited, the medical sector, the most significant performance indicators are delay, throughput, PDR, and communication overhead. Here, performance metrics for the LEACH and LEACH-A protocols are measured.

According to the results of the simulation, LEACH performs better than LEACH-A in terms of energy conservation and minimal delay.

References

[1] Rahman, S. U., Sultan, A., Alroobaea, R., Talha, M., Hussain, S. B., & Raza, M. A. (2021). Secure OFDM-Based NOMA for Machine-to-Machine Communication. Wireless Communications and Mobile Computing, 2021, 1-8.

[2] Lokhande, M. P., Patil, D. D., Patil, L. V., & Shabaz, M. (2021). Machine-to-machine communication for device identification and classification in secure telerobotics surgery. Security and communication networks, 2021, 1-16.

[3] Batth, R. S., Nayyar, A., & Nagpal, A. (2018, August). Internet of robotic things: driving intelligent robotics of future-concept, architecture, applications and technologies. In 2018 4th international conference on computing sciences (ICCS) (pp. 151-160). IEEE.

[4] Stojmenovic, I. (2014). Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems. IEEE Internet of Things Journal, 1(2), 122-128.

[5] Zhang, H., Fu, L., & Zhang, A. (2023). A Novel Adaptive Finite-Time Position Tracking Control Strategy for Teleoperation System with Varying Communication Delays. Mathematics, 11(6), 1486.

[6] Bao, J., Fu, L., Zhang, H., Zhang, A., Guo, W., & Chen, T. (2022). An Adaptive Proportional Plus Damping Control for Teleoperation Systems with Asymmetric Time-Varying Communication Delays. Mathematics, 10(24), 4675.

[7] Mehrdad, S., Liu, F., Pham, M. T., Lelevé, A., & Atashzar, S. F. (2020). Review of advanced medical telerobots. Applied Sciences, 11(1), 209.

[8] Valner, R., Kruusamäe, K., & Pryor, M. (2018). TeMoto: Intuitive multi-range telerobotic system with natural gestural and verbal instruction interface. Robotics, 7(1), 9.

[9] Rostami, S., Alabadi, S., Noori, S., Shihab, H. A., Arshad, K., & Rapajic, P. (2016). Spectrum Assignment Algorithm for Cognitive Machine-to-Machine Networks. Mobile Information Systems, 2016.

[10] Stojmenovic, I. (2013, June). Large scale cyber-physical systems: Distributed actuation, in-network processing and machine-to-machine communications. In 2013 2nd Mediterranean Conference on Embedded Computing (MECO) (pp. 21-24). IEEE.

[11] Lokhande, M. P., & Patil, D. D. DEVICE CLASSIFICATION FOR MACHINE TO MACHINE COMMUNICATION IN INTERNET OF THINGS FOR TELE-ROBOTIC SURGERY: A REVIEW.

[12] Manikanthan, S. V., Padmapriya. T. (2021). Implementation and design of wireless IoT network using deep learning. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(3), 563-572.

[13] Lokhande, Meghana P., et al. "Machine-to-machine communication for device identification and classification in secure telerobotics surgery." Security and communication networks 2021 (2021): 1-16.

[14] Lokhande, M. P., & Patil, D. D. (2021). Network performance measurement through machine to machine communication in tele-robotics system. Tehnički glasnik, 15(1), 98-104.

[15] Mehrdad, S., Liu, F., Pham, M. T., Lelevé, A., & Atashzar, S. F. (2020). Review of advanced medical telerobots. Applied Sciences, 11(1), 209.

[16] Sharifi, M., Behzadipour, S., & Salarieh, H. (2016). Nonlinear bilateral adaptive impedance control with applications in telesurgery and telerehabilitation. Journal of Dynamic Systems, Measurement, and Control, 138(11), 111010.

[17] Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T., & Chizeck, H. J. (2015). To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. arXiv preprint arXiv:1504.04339.