

A Mobility-aware Human-centric Cyber-physical System for Efficient and Secure Smart Healthcare

Abdul Razaque, *Fathi Amsaad , Musbah Abdulgader, Bandar Alotaibi, and Fawaz Alsolami, *Member, IEEE*; Duisen Gulsezimhas, *Student Member, IEEE*; Saraju Mohanty and Salim Hariri, *Senior Member, IEEE*

Abstract—Cyber-physical systems (CPS) have developed rapidly in recent years, contributing to an efficient integration between the cyber and physical worlds in intelligent and connected city environments. However, efficient mobility in a CPS is not well solved. Here, we present a prototype for a privacy-aware secure human-centric mobility-aware (SHM) model proposed and tested to analyze physical and human domains in IoT-based wireless sensor networks (WSNs). The proposed SHM model involves five modules: sensor advertisements, mobile sensor recruitment, load balancing, transmission guarantee, and privacy with data-sharing phases. The proposed model is also validated using an accurate testing method that involves software and hardware tools and mathematical modeling to confirm secure communication. The model provides a trade-off between energy efficiency and quality-of-service (QoS) requirements and compares the performance with other known models/protocols. Our testing process continued for four days, demonstrating that the SHM model provides compelling features of a secure cyber-physical system based on actual testing results. In practice, our model can be used in hospitals, as evident from validation in a real-life environment following the protocols.

Index Terms—Mobility-aware human-centric cyber-physical system, secure IoT-based human-centric mode, secure smart healthcare mobility, wireless brain sensor network.

I. INTRODUCTION

CYBER-PHYSICAL system devices, i.e., sensors, actuators, microprocessors, etc., are gaining importance in IoT applications [1]. CPS systems combine efficient and real-time applications while focusing on security, energy, mobility,

Abdul Razaque is with Arizona University. He is now with the Department of Computer Engineering & Cyber Security USA, International Information Technology University, Kazakhstan, (e-mail: a.razaque@edu.iitu.kz).

*Fathi Amsaad (**Corresponding author**) is an Assistant Professor with the School of Information Security and Applied Computing, Eastern Michigan University (EMU), Ypsilanti, MI, USA 48197 (e-mail: fathi.amsaad@email.edu).

Musbah Abdulgader, Bandar Alotaibi, and Fawaz Alsolami, is with the Computer Science Department, Norfolk State University (NSU), VA, USA, (e-mail: mmabdulgader@nsu.edu).

Bandar Alotaibi is with the Information Technology Department and Sensor Networks and Cellular Systems Research Center, University of Tabuk, Tabuk, Saudi Arabia, (e-mail: b-alotaibi@ut.edu.sa).

Fawaz Alsolami is an Assistant Professor with the Computer Science Department, King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: fal-solami@kau.edu.sa).

Duisen Gulsezim is a student with the Department of Computer Engineering & Cyber Security USA, International Information Technology University, Kazakhstan, (e-mail: Gulsezimduisen@iitu.kz).

Saraju Mohanty is a Professor with the Computer Science and Engineering Department, University of North Texas, Denton, Texas, USA 76203, (e-mail: saraju.mohanty@unt.edu).

Salim Hariri is a Professor with the Electrical and Computer Engineering Department, University of Arizona, Tucson, AZ, USA 85721, (e-mail: hariri@ece.arizona.edu).

Manuscript received December 1, 2020; revised November 10, 2021.

health, and industry [2]. Although CPS is useful in health and real-time system applications, its adoption has been delayed because of the mismatch between the abstraction and properties of physical processes [3].

Using massive networks of sensors and actuators, large environmental areas of CPS can be accessed and revolutionized in real time [3]. Mobility is introduced in many systems, including the Industrial Internet of Things (IIoT), automotive human mobility systems, and robotic and distributed systems that perform automated tasks [4, 5]. As an application of CPS, the interconnection between power control systems and edge/fog IoT-based systems can be efficiently analyzed [6].

Fig. 1 shows an overview of the cyber-physical system domain. CPS mobile nodes can detect information over a large wireless area and send it back to the base station for analysis. Additionally, CPS nodes can solve the resource limitation problem in the static model and improve its efficiency. CPS wireless communication development includes interconnected robots, autonomous vehicles, vehicular ad-hoc networks (VANETs), smart grids, etc., and creates ideal mobile nodes in the CPS environment [7, 8, 9]. Furthermore, embedded CPS computing systems have gradually become the core development direction for many applications, including IoT and mobility, due to their excellent market demand and promising prospects [10].

The paper is organized as follows. Section III presents the paper's related work. Section II specifies the research problem addressed and the main contentions of the current paper. Section V introduces the problem formulation. Section IV specifies the proposed model. Section VI explains the development phases of the proposed model. Section VII discusses the experimental results and shows an analytical comparison between the proposed model and the competing models. Section VIII concludes the paper and outlines future work.

II. RESEARCH PROBLEM AND CONTRIBUTIONS

Despite the aforementioned benefits of the cyber-physical systems, many challenges still arise in CPSs. For example, current mobility systems require CPS sensors during their communications to efficiently communicate sensitive information related to humans, machines, sensors, etc. [11]. For a balanced throughout and efficient human-centric transmission process, the quality-of-service (QoS) and performance issues, including reliability, ensuring the minimum loss rate, enhanced link quality, advertising each sensor's lifetime, etc., require

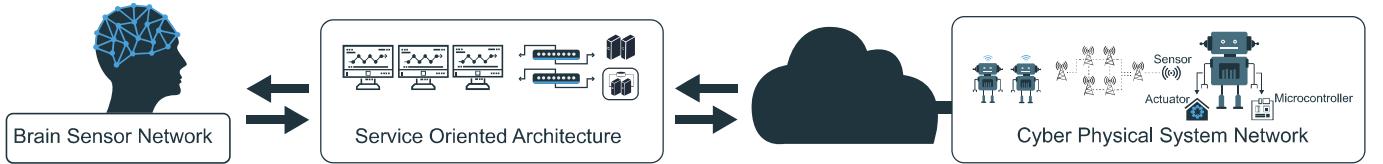


Fig. 1: Overview of the cyber-physical system domain.

well-resolved approaches. Also, many of the existing CPS models lack information about the implementation of CPS mobility models on real hardware devices, the integration process between CPS hardware devices, particularly handling static sensors and mobile robot sensors, and the software tools used, which is needed for an efficient mobility-aware system model. Further, CPS mobile nodes are increasingly deployed in a nonsecure physical environment; thus, they are vulnerable to new cyberattacks that need to be addressed before they are widely deployed [12]. If a CPS mobile node fails to function due to a CPS attack, the whole system becomes comprised and untrusted [13]. The challenge here lies in integrating new techniques, as part of the system prototype, to ensure secure and private data sharing and transmission, i.e., the sensor's core buffer and data-forwarding path.

The main contributions of this work are as follows.

- ▷ An efficient and privacy-aware secure human-centric mobility-aware CPS model is proposed that covers both stationary and mobile sensors. Static sensors are fixed to monitor sleeping patients, whereas mobile sensors monitor moving patients to gather data and store it on cloud servers.
- ▷ A mobile sensor recruitment phase is employed to enhance the throughput and reduce latency by incorporating a mobility-aware component. As a result, the load of the entire network is balanced throughout the data transmission process.
- ▷ A sensor-based advertisement process that focuses on the loss rate and link quality before advertising the lifetime of each sensor for improved QoS requirements is proposed.
- ▷ A human-centric mobility-aware model makes full use of the core buffer and data-forwarding path and ensures private and secure data-sharing transmission.

III. RELATED WORK

Table I summarizes the contemporary related work for handling the security in CPS. As seen in the table, Robust control for mobility based on cyber-physical systems is introduced in [14]. This concept is used to implement a system architecture that provides end-to-end connectivity for a team of robots that performs tasks assigned by human operators. In this research, the authors adopted a stochastic model to address the wireless routing problem. However, this model is used for either local control or global planning, but it fails for continuous communication. A design space exploration (DSE) architecture is proposed to handle detailed CPS parameters such as bus width, voltage levels and cache size [15]. The proposed architecture is applied with the inverted-pendulum application. The proposed architecture was capable of detecting and managing these

trade-offs. However, the proposed architecture failed to reduce energy consumption. Optimal tracking control is proposed to support the CPS when the cyber domain is attacked by a denial-of-service attack (DoS) [16].

The Riccati equation is used for an amplified system. The probability of determining a successful DoS attack is analyzed. Finally, the effectiveness of the proposed method is detected using an F-16 aircraft and DC motor. However, the proposed method experiences the problem of potential attacks encountered by the CPS. Blockchain-enabled technology is introduced for the SDN cyber-physical system to reduce the system latency [17]. The proposed SDN-CPS consists of the resource management process for providing cooperation flexibility. Joint computation, communication, and consensus problems are formulated to balance resource allocation and ensure data security. To introduce stability and safety features in cyber-physical systems, [18] adopted a unified invariants approach in which cyber and physical component requirements were addressed. However, this approach is limited to some extent when a system is unresponsive and when there are analytic requirements and a failure to define errors. A method to detect a potential attack in a cyber-physical system was introduced in [19]. Based on existing CPSs and attack scenarios, it illustrated a unified modeling framework for cyber-physical systems. However, it did not explain how to address attacks that are identified as "undetectable." The IIoT with a self-adaptive collaborative control (SCC) model that leverages leveraging of cyber-physical systems mobility is proposed to enhance the resilience and flexibility of manufacturing discrete systems [20].

Cyber-physical system mobility puts the human-in-the-loop presence in the CPS given in [21], in which the system processes the signals from the mind and body and then converts those signals into robot signals. These signals interact with the physical environment. However, the authors failed to define and implement this idea properly. Healthcare systems based on cyber-physical systems were also introduced in [22]. The author proposed a novel false alarm detection method for healthcare applications. Despite the threshold alarm method, it is combined with multiple classifiers. Additionally, different sensors are considered in CPS to ensure that heterogeneous sensors' coexistence is reliable. This model improved the accuracy and efficiency of the false alarm detection system. However, a complete CPS architecture is not addressed.

IV. COMPONENTS OF THE PROPOSED MODEL FOR CPS

Mobile wireless sensor networks (MWSNs) are effective mechanisms in the growing CPS. The increasing pervasiveness and generality of MWSNs in several IoT application domains

TABLE I: Contemporary works for handling the security in CPS.

Works	Security protocols for CPS	Features	Vulnerabilities/Shortcomings
Fink et al. 2012 [14]	The mobility-based protocol for the CPS	Provides end-to-end connectivity for the robots that perform the task assigned by human operators. In addition, adopted a stochastic model to address the wireless routing problems.	Failed to provide continuous communication and has no secure communication.
Maral and Givargis 2020 [15]	Design space exploration architecture for the CPS parameters.	Uses DSE to enhance the performance of the CPS parameters for improvement in the CPU speeds, cache configuration, and sampling.	Failed to automate the search for large scale CPS configurations.
Paul et al. 2014 [18]	Common semantics for CPS.	Provides unified invariants that guarantee the correctness of the individual subsystem in CPS.	Reduces the accuracy due to the use of the logical truth. It also lacks security of the CPS.
Pasqualetti et al. 2018 [19]	Mathematical framework for CPS.	Designed distributed and centralized model to monitor and detect the attacks in CPS.	Neither testing nor validation is provided for the proposed model.
Guo et al. 2021 [20]	Self-adaptive collaborative control (SACC) for a smart protection login system.	Enables the manufacturers to deploy the IoT in CPS to make intelligent, resilient, and flexible production logistics systems.	Suffers due to security threats and additional latency.
Schirner et al. 2013 [21]	Platform for human-in-the-loop application	Designed prototype to support the wide-ranging class of systems that extend human communication with the CPS.	Produced abstract idea without any validation and testing.
Li et al. 2018 [22]	Medical fuzzy alarm filter for healthcare environments.	Attempts to reduce the false alarms for maintaining the system effectiveness generated by the sensors.	Specified for the healthcare environment, but failed to provide an acceptable accuracy rate.
Wu et al. 2021 [16]	Optimal tracking control for CPS.	Attempts to design an optimal tracking control method for preventing the control signal transmission caused by DoS attacks.	Limited to only DoS attacks and vulnerable to other potential attacks on CPS.
Wang et al. 2021 [17]	Blockchain technology for SD-CPS.	Minimization in system latency and provision of flexibility of cooperation.	Blockchain-enabled features are not properly employed to handle security threats.
This work	Privacy-aware SHM model for CPS.	Provides hardware testing of mobility-aware IoT devices and maintains security and privacy in the CPS.	No known potential security and privacy threats

make actuators, mobile sensors, and embedded devices significant CPS design components. An MWSN can be a network with hundreds of mobile sensors interrelating to resolve/handle complex tasks or events. They are predominantly arrayed as interfaces through which data are assembled from/about the physical environment and then transported to the cyber domain. There is an urgent need for a system model to migrate multifaceted processing tasks outside an MWSN network while integrating missing intelligence, autonomy, and context-awareness features. Such an MWSN system model is needed to address several challenges, including the amalgamation of appliances with sensor node mobility, different communication protocols, and sensor data distribution to the CPS on time.

As part of the system model, a distributed CPS mobility system is needed to detect information about static and moving objects (humans), allowing the system to use a sensor-based process that focuses on the loss rate and link quality to advertise each sensor's lifetime for improved QoS requirements. This system should also include a mobile sensor recruitment phase to enhance the throughput and reduce latency by incorporating a mobility-aware component. As a result, the load of the entire network is balanced throughout the data transmission

process. This paper proposes a novel human-centric mobility-aware system model that can be used for several applications, such as diagnosing patients and storing the information of the patient in a distributed environment, a grid monitoring system (static and mobile robot sensors), vehicle monitoring processes (to avoid accidents and reduce crime rates), and airport surveillance systems (monitoring passengers and their activities). The model involves data acquisition, data management, and IoT features. Vindicating the limitations of MWSNs, the system model comprises four parts: a brain sensor network (BSN), data processor, secure service-oriented architecture (SSOA), and data management domain, as shown in Fig. 2. These four parts work collectively through message exchange and information retrieval, as delivered through solid and dotted lines in the proposed architecture (see Fig. 2).

Our IoT-based CPS mobility model is human-centric and covers two types of sensors: mobile and stationary sensors. The proposed sensor mobility system makes full use of the core buffer and data-forwarding paths and ensures private and secure data-sharing transmission. The stationary sensors are fixed to monitor sleeping patients, whereas mobile sensors monitor moving patients to gather data and store it on cloud

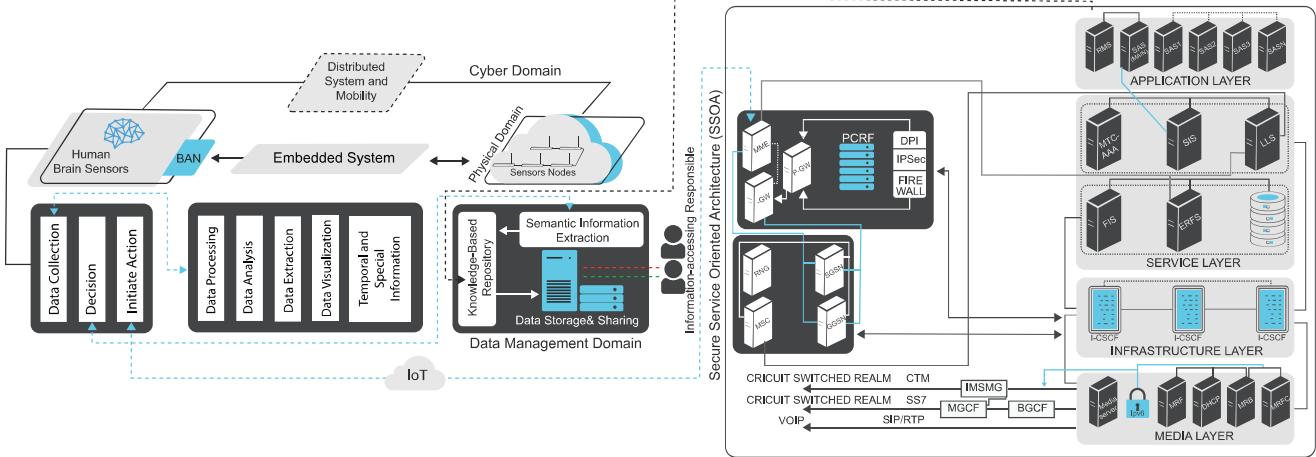


Fig. 2: Framework of the proposed human-centric mobility-aware (SHM) cyber physical system model.

servers. The model uses BSN, a Brain Sensor Network (BSN), to collect data from the brain with the help of the sensor, the actuator, and the controller. The BSN consists of embedded system devices of a physical domain. The brain signals are sent to a mobile robot by the BSN, where the human-to-machine interaction is realized. These signals are monitored and analyzed by secure service-oriented architecture (SSOA). The SSOA results are reported to the base station for the determination of proper action. Eventually, data are transmitted to a knowledge-based repository, which stores data and provides information access so that responsible entities (such as doctors) can check them from remote places.

As seen in Fig. 2, the brain sensors are attached to the head of the patient. BSN is a wireless sensor network that obtains physical and physiological constraints from brain sensors. A BSN can also be beneficial for transferring information on several diseases, including diabetes (e.g., measuring insulin levels in the blood), glaucoma, heart disease, and hypertension. The benefit of attaching the brain sensor is to monitor the neurological variations and help to recover cognitive functionalities. The physical domain of the system also includes actuators, sensors, and controllers. These sensors also report data to the chosen base station (BS) to play the head node's role. The BS transports it to the actuator or controller. Finally, the robot decides which action should be performed. The brain signal is converted into a robot signal through this process, which can be easily stored and analyzed later. After the human signal has been converted, the data processor works to evaluate these data. This process is further divided into three parts: data collection, decision, and action initiation. In the data collection, data processing, data analysis, data extraction, data visualization, and temporal processing with unique information are conducted. Based on the obtained results, a decision is made to store the information on cloud servers using semantic information extraction. Additionally, the initial action is performed by the SSOA model through the IoT, as shown in Fig. 2.

The SSOA model has four layers: the application layer, the service layer, the infrastructure layer, and the media layer.

There are two types of servers in the **application layer**: a secure authentication server and the role-based management server. A secure authentication server is a unique authentication process that can protect the user's authentication. For instance, if the whole system has only one authentication server, others will easily access the data. A secure authentication server can divide users' data into different servers, strengthening the entire system's security. A role-based management server also helps to keep the system safe and stable. It can produce a public key to reduce malicious damage. Role assignment and management can help distribute secret keys to users. These two servers complement each other to ensure the security of the SOA.

In the **service layer**, six types of servers are included, as shown in the bottom part of Fig. 2. The names of these servers are: MTC-AAA (machine type communication-authentication, authorization, and accounting) server, SIS (subscriber information server), LLS (location locator server), FIS (feature integrating server), ERFS (efficient route-finding server), and MPS (mobile profile server) that holds the registered profiles. The international mobile subscriber identity (IMSI) with the external identifier of equipment identifiers (UE) is mapped by the MTC-AAA server, which also helps with subscriber information retrieval (SIR) and sends it to the SIS. After receiving the request from the MTC-AAA, the SIS checks the valid subscription for legitimate mobile cloud users. If the user's identity is confirmed (already stored in SIS), the SIS sends an affirmative response to the MTC-AAA and the LLS; otherwise, the SIS refuses the request and sends a negative message to the MTC-AAA. In the former circumstance, the LLS is responsible for determining the location of the mobile cloud user. The ERFS receives an updated location from the LLS to perform proper routing. Additionally, the MPS owns the profile of the registered users, which provides the authentication process at the service layer and stores the QoS information on specific services and subscribers.

The **infrastructure layer** consists of a call session control function (CSCF), which works to generate the boundary between a mobile cloud user's IP address and its public identity.

A CSCF is made up of three components: a proxy-CSCF (PCSCF), serving-CSCF (S-CSCF), and an interrogating CSCF (I-CSCF). This layer supports various services, such as web, video conference, email, and telephone services. The **media layer** includes a media resource broker (MRB) and a media resource function controller (MRFC), which combine to bring the best multimedia experience. Additionally, it can make the whole process smoother. A fast, seamless handoff mobile IPv6 (FSHIPv6) is proposed to solve the handoff packet loss and latency. The MRB and MRFC are both connected to IPv6 to ensure that the handoff process is successful. Additionally, the MRF and DHCP are connected to the MRB. The data management domain consists of semantic information extraction, a knowledge-based repository, and cloud servers.

The **semantic information extraction system (SIES)** is used to search, analyze, and conclude automatically. In the proposed CPS system model, after the robot makes decisions, based on the sensors' information, these decisions are transmitted to the semantic information extraction system. The SIES then analyzes the decisions to determine these decisions and whether they need to be stored in the knowledge-based repository. For instance, the robot makes decisions according to the patient's activity. Then, semantic information extraction analyzes the concluded decision so that the doctor can quickly provide his/her feedback. The proposed model offers a visual method for users to obtain vital information efficiently and rapidly. The decision information (extracted by the semantic information extraction process) and initial action (from SSOA) are stored in the knowledge-based repository, whose structure makes the system more intelligent. Data in the knowledge-based repository are hierarchical. Data at the lowest level are "facts", in the middle grade are "rules, processes" (action), and at the highest level are "strategies" (decisions).

Cloud-based servers are adopted as part of our proposed system model due to their ability to provide fast and uninterrupted communication in addition to their cost-effectiveness since enterprises only need to pay for what they use, avoiding extra expenses to hold and manage IT infrastructure. A cloud server is used on a physical or virtual infrastructure that ensures legitimate remote access control of system model information. They basically guarantee that only the authorized user, such as doctors, will gain remote access to sensitive data, i.e., patient data, and can audit them by means of the Internet or cloud services. The system's original data are either structured or unstructured, which are modular by the knowledge-based repository. All data in different layers are marked with credibility, which means uncertain data do not exist. As part of this process, the knowledge-based repository uploads the credibility data to the cloud servers.

V. PROBLEM FORMULATION

We assume that the SHM model for the CSP is denoted by the interrelated components and composition rules ΔR that are picked from the library (collection) $\forall \gamma$. Each component involves the set of attributes that capture both functional, extrafunctional and nonfunctional properties, for example, energy efficiency, load balancing, QoS, reliability and end-to-end delay. Each component consists of a set of terminals

specified with terminal variables T_v . The components can perform different functions and play different roles. We focus on embedded systems, WSNs and service-oriented architectures that exchange quantities via different flows. Input and output terminals are used to receive and send the signals. On the other hand, the composition rules specify the connections that will be permitted and how terminal variables should be assigned. To achieve the objectives, each component is characterized with a specific type τ and terminal variables including its functionality (tasks or roles). Thus, the overall performance of the SHM model for the CSP S_C can be computed as

$$S_C = \forall \gamma = \sum_{i=1}^{C_t} \{(C)_i T_v \tau\} + (\Delta R)^+ \quad (1)$$

where $(\Delta R)^+$ is the total number of applied rules from obtaining the data from the sources to data storage at the cloud servers, and C_t is the total number of the components of the system.

Definition V.1 A CPS involves a finite set of components and their interrelated connections and can be specified as a directed Graph $G = (C, I)$, where each component $c_x \in C$ and each interrelated connection $i_{xy} \in I$ from c_x to $c_y \{x, y \in (1, \dots, |C|), |C|\}$ are of cardinality C .

A. Energy constraints

Each component and interrelated connection is associated with energy. Therefore, the energy function can be expressed as the sum of all instantiated components and connections of the CSP given by

$$\sum_{x=1}^{|C|} (C)_i E_x + \sum_{x=1}^{|C|} \sum_{y=1}^{|C|} E_{xy}^{\sim} i_{xy} \quad (2)$$

where E_x is the energy of the component $(C)_i$, and E_{xy}^{\sim} is the consumed energy of the connection for forwarding the signals (or data).

B. Flow constraints

Let us assume that flow originates from the source (human) and is transferred to cloud servers through intermediate components and connections. If a component has a specific role C_i^{sr} in the functional flow that is neither a source nor destination component, then, input flow rate F_{in} at C_i^{sr} can be expressed as

$$F_{in} = \sum_{x=1}^{|C|} F_r C_i^{sr} \quad (3)$$

The output flow rate F_{ou} for all of the connections $i C_i^{sr} \forall c$ for all of the components can be computed as

$$F_{ou} = \sum_{x=1}^{|C|} (F_r C_i^{sr}) (i_x C_i^{sr}) = \sum_{x=1}^{|C|} (F_r C_i^{sr} \forall c) (i C_i^{sr} \forall c) \quad (4)$$

where F_r is the flow rate through the connection.

C. Workload constraints

Each component in C is labeled with a ∂ . If this component denotes the medical equipment, then the incoming workload can be bound to avoid overloading. Thus, the workload for the component c_i can be determined as:

$$c_i = \sum_{x=1}^{|C|} (F_r c_y) \leq \partial_y \quad (5)$$

D. Timing Constraints

It refers to the time needed to collect the signal from the source (human) and send it to cloud servers. Let us assume that each component is characterized by propagation delay d_{pr} and consider the CSP model, where the delay for the overflowed components is equal to the amount of delay of each component. Let $\Delta\varepsilon$ be the set of routes from the source q' to cloud servers C_{so} ; then, the time t_c for each route \mathbb{T} in $\Delta\varepsilon$ should not exceed the entire time of the CPS system T^* given by:

$$t_c = \sum_{x=1}^{|C|} d_{cB_v^{\mathbb{T}}} \leq T^* \forall \mathbb{T} \in \Delta\varepsilon \quad (6)$$

where d_c is the delay of the component, and $B_v^{\mathbb{T}}$ is a binary variable that assumes a value of 1 if $c_x \in \mathbb{T}$; otherwise, it is 0. Thus, the binary variable can be computed as

$$B_v^{\mathbb{T}} = \text{1iff} \sum_{y=1}^I (P_{xy}^{\mathbb{T}}) \vee (P_{yx}^{\mathbb{T}}) \quad (7)$$

where $P_{xy}^{\mathbb{T}}$ is the all possible connections from the source to the destination, and $P_{yx}^{\mathbb{T}}$ is the all possible connections from cloud servers to the source (human).

E. Privacy-preservation constraints

A typical privacy constraint describes the violation of cloud servers, i.e., the information flow from the source (human) to cloud servers could be tempered. Thus, we must compute the privacy violation of the CPS. Let the privacy violation of the cloud servers be a P_v , in which the signal/data temptation occurs; then, the acquired information at the cloud servers is not fully confidential. We assume that if any component is exposed, then it cannot be reliable to maintain privacy, and adjacent components cannot be trusted. Furthermore, the privacy violation in different components is self-governing. Let T_i be threat that affects the component c_x that leads to compromised information. Then, privacy preservation no longer remains for the component. Thus, the privacy violation in the cloud servers can recursively be determined as

$$P_{vx} = T_i \bigcup_{1 \leq y \leq |C|, eyx \neq 0} \bigcap P_{vy} \quad (8)$$

where eyx is the y^{th} row and x^{th} column element of the adjacency matrix e of the CPS model. In other words, component c_x is attacked when either an attack is generated by an outsider adversary or induced through a malicious insider.

F. QoS Constraints

According to the data storage process in SHM-CPS, the medical sensing data go through three stages:

- ▷ Obtaining signals/data from the source (human) through BAN and WSNs.
- ▷ The initial action is performed by SSOA to process data through four layers.
- ▷ SIES searches, analyzes and concludes data automatically for making decisions.

Let us consider end-to-end delay that is mostly calculated by the attainable data rate $(DR)_{xy}$ for a given CPS. The data rate obtained through MWSN W_{sn} from P_n patient is associated with the number of allotted components involved in the data process given by

$$(DR)_{xy} = \sum_{c_i \in C_t} (Co_{xy}^{c_i}) F_r, \forall x \in X, y \in Y \quad (9)$$

where $Co_{xy}^{c_i}$ is associated connection between two components.

We observe that the more components are assigned to the source, the higher the data rate that can be attained. Thus, the delay for the $W_{sn}(d)$ can be calculated as

$$W_{sn}(d) = \frac{D_s}{(DR)_{xy}} \quad (10)$$

We assume that the data received through the BAN from the source (human) are distributed with the associated WSN with fixed probability. Therefore, the data influx rate in WSN is flowing successfully.

VI. DEVELOPMENT PHASES OF THE PROPOSED MODEL

The proposed cyber-physical system mobility model is developed to serve human demands. The model is tested to analyze the physical domain and the human domain. In this model, the data are stored and shared to be accessed by relevant persons in the data management domain. The distributed system and mobility component are installed. The SHM model covers two types of sensors: mobile and stationary sensors. The stationary sensors are fixed to monitor and control the static objects, whereas mobile sensors monitor moving objects to determine their activities and report them to the base station. The model scales the heterogeneous network in the physical domain and involves the star topology and the flat topology. This model consists of the following phases:

- ▷ Sensor Advertisements Phase
- ▷ Mobile Sensor Recruitment and Selection Phase
- ▷ Load-balancing Phase
- ▷ Transmission Guaranteed Phase
- ▷ Privacy and Data-sharing Phase

A. Sensor Advertisement Phase

This module works differently than an IP network because an IP network is used to create an agent discovery phase for a foreign agent and the home agent. Mobile sensors use advertisements to confirm whether they are coupled to their respective home networks or foreign networks. This

advertisement process helps sensors advertise their lifetime within the network. The lifetime of the sensors in WSNs is associated with time constraints, so it is more important to determine the remaining lifetime of the sensors (RLS). Let us assume that the sensors are homogeneous and possess the same physical capability as communication and sensing power.

The location of the sensor is stationary or mobile. The stationary location of sensors and actuators is only used for monitoring static objects (patients). Mobile sensors and mobile actuators are installed for monitoring the movable objects (moving patients) whose performance is reported to the base station. The mobility of mobile sensors is controllable. The sensors can communicate within the communication range using a multihop process. The remaining energy of the sensors (RES) defines the RLS. Moreover, each sensor's remaining lifetime is advertised when competing for particular cycles to receive and send messages. The packets are retransmitted if the WSN is unstable. Thus, it focuses on the loss rate and link quality before advertising each sensor's lifetime. Therefore, the proposed model can define the RLSs after determining the consumed energy for message transmission. Thus, the RLS ratio of the remaining energy to each set of initial sensor powers can be calculated as follows:

$$R_l = 1 - \frac{\sum_{i=0}^{T_C} i(E_p) \times N(E_p) \times \beta(E_p) \times E_{\Delta_s} \times \varpi \times \mathfrak{R}}{E_i} \quad (11)$$

where R_l is the remaining lifetime of the k sensor, E_i is the initial energy of the sensor, T_C is the transmission cycle for monitoring the events, E_p is the amount of consumed energy of each sensor device once it receives each packet, $N(E_p)$ is the number of packets each sensor device receives during communication, $\beta(E_p)$ is the number of retransmitted packets, E_{Δ_s} is the amount of energy consumed by each sensor device for a single received packet, ϖ is the number of reply messages sent to each sensor device, and \mathfrak{R} is the number of retransmissions experienced by each sensor device.

B. Mobile Sensor Recruitment and Selection Phase

The goal of recruiting the sensor device and selecting the proper actuator is to improve throughput and reduce latency. The recruitment process is applied once the actuator (cluster head sensor) does not find enough sensors in its cluster domain. As a result, the actuator initiates the recruitment request from another actuator. First, the actuator checks its zone areas by sending the recruitment request. If the actuator does not find the required sensors in its neighborhood, it broadcasts the multicasting message for recruitment inquiry. When the actuator reaches the sensor devices from its nonadjacent cluster, the pipelining-based (it allows different practical units of a system to work synchronously) approach reduces the latency that a long distance could cause.

Furthermore, the recruiting actuator first recruits the sensors from its neighbor and then recruits them from nonadjacent domains. The model determines the recruitment processes as follows. Let us assume that the actuator recruits sensor z from other cluster domains. The actuator is a static sensor that is part of the monitoring building where data about the person are gathered; thus, every monitoring point M_p (an area close to

the persons being monitored) requires sensors via recruitment. The probability P_r of a sensing requirement by the recruited sensor is given by

$$\int_{N_r}^n f_x(z \times N_{rec}, C_{adj}) \partial N \quad (12)$$

where N_r is the recruited sensor, N_{rec} is the number of recruited sensors, and C_{adj} is the adjacent cluster domain or nonadjacent cluster domain. The probability of a monitoring point that can be determined when an action is performed at another monitoring point M_{p1} is $\partial_{p1,p}$. Thus, the probability of having to monitor point p so that the data can be sensed using the recruited sensor N_r is determined as

$$N_{r(d)} = 1 - \sum_p^{p=\infty} p \left(1 - \left(\partial_{p1,p} \int_{N_r}^n f_x(N \times N_{rec}, C_{adj}) \partial z (1 - \sum_{t=0}^n t(1 - \partial_{p0,p1})) \right) \right) \quad (13)$$

where $\partial_{p1,p}$ is the distance of the recruited sensor from its domain to the recruiting sensor's domain and $\partial_{p0,p1}$ is the distance of the recruited sensor from the recruitment sensor's domain to its domain. Once the recruited sensor starts to sense the data, if the amount of data is more than the sensing capability of the deployed and recruited sensors, then the recruiting actuator A_{rec} initiates the additional sensor recruitment process from the adjacent and nonadjacent cluster domains given by

$$A_{rec} = 1 - \prod_{N_r \in R} N \times 1 - \sum_p^{p=\infty} p \left(1 - \left(\partial_{p1,p} \int_{N_r}^n f_x(N \times N_{rec}, C_{adj}) \partial N (1 - \sum_{t=0}^n t(1 - \partial_{p0,p1})) \right) \right) \quad (14)$$

Following the additional sensor recruitment process, we obtain a new vector P'_r that demonstrates the probability that monitoring point M_p requires being covered by recruiting the additional sensor devices.

$$P'_r = \begin{cases} \frac{P_r - A_{rec}}{1 - A_{rec}}, & \text{if } A_{rec} \leq P_r \\ 0, & \text{otherwise.} \end{cases} \quad (15)$$

where A_{rec} is the recruiting actuator.

The placement of the actuators is important and could affect the performance and coverage. Thus, the actors should cover all the deployed sensors. As a result, a midpoint algorithm is applied to balance the proper placement of the sensors. Therefore, the optimal number of actuators A_{opt} is given by

$$A_{opt} \left\{ \sqrt{\frac{K_n}{2\pi}} \times \sqrt{\frac{FS_e}{MP_e}} \times \sqrt{\frac{A_{net}}{D_{avg}}} \right\} \quad (16)$$

where K_n is the number of sensors; FS_e is the amplifier energy of free space; MP_e is the multipath energy; A_{net} is the network area; and D_{avg} is the mean distance from the actor to the base station. Algorithm 1 separates the optimal number of actuators concerning the clusters. An actuator heads each cluster. The actuator broadcasts the packet to the sensors to form the cluster. The packet comprises the actuator's location and identity. On receipt of the packet, the sensor device acknowledges its identity and residual energy. When a sensor

Algorithm 1 Determine the optimal actuator average midpoint

Input: r in
Output: r_{in} out

- 1: **Initialization:** γ_o : Origin; γ_e : Each point; r : Distance; r_{in} : Initial centroid distance; r_s : Sorting distance
- 2: **Determine** r between γ_o & γ_e
- 3: **Repeat** step 2 for all γ_e
- 4: **Set** r into r_s
- 5: **if** $r_s \cong r_{in}$ **then**
- 6: **Set** r_{in}
- 7: **else if** $r_s \neq r_{in}$ **then**
- 8: **Go** to step 4
- 9: **end if**

device receives a cluster formation message from more than one actuator, the sensor node must join the nearest actuator. However, this cluster formation association can increase the path length because it could be possible that the actuator is located far from the base station (BS). Thus, to avoid back transmissions, an average midpoint of the actuator should be determined. Thus, algorithm 1 is employed to determine the actuator that should be closer to the base station (BS) to avoid data loss.

Moreover, the sensor device collects information from an event that should not be lost and needs to be forwarded to the correct actuator (optimized actuator). In step 1, the variables are initialized. The input and output are described at the beginning of the algorithm. In step 2, the distance is measured from the original point to each point. Step 3 continues the process until the distance is measured to all of the points. Steps 4-6 explain the sorting distance in ascending order and check if a sorting distance is equal to the initial centroid distance. Then, the initial centroid distance is set as a final distance that is near the closest actuator. Steps 7-8 demonstrate that if a sorting distance is not the initial centroid distance, then the distance sorting process is reperformed, as given in step 4. Algorithm 1 leverages the linear features so that the time complexity of the algorithm in the best case is $O(1)$ and worst case is $O(\log n)$.

In existing approaches, a sensor device receives a cluster formation message from more than one actor. Only the nearest actuator is chosen to join based on the location inserted in the packet. However, this cluster formation association increases the path length because the actuator might be located far from the base station. Thus, to avoid back transmissions, an average midpoint of the optimal actuator algorithm is useful. Suppose the sensors obtain a higher received signal strength indicator (RSSI) from the base station rather than from the actuator. In that case, the sensor device should send data to the base station rather than the actuator.

Similarly, the sensor can calculate the distance between itself and the base station, and determine its midpoint. Based on the midpoint, the sensor decides to send the data either to the actuator or the base station, as represented in Fig. 3. The figure shows that the sensor relates to Actuator-1 due to receiving a higher signal strength, but Actuator-1 is far from the base station compared to Actuator-2. As a result, additional energy is consumed, and the delay is extended. Thus, the

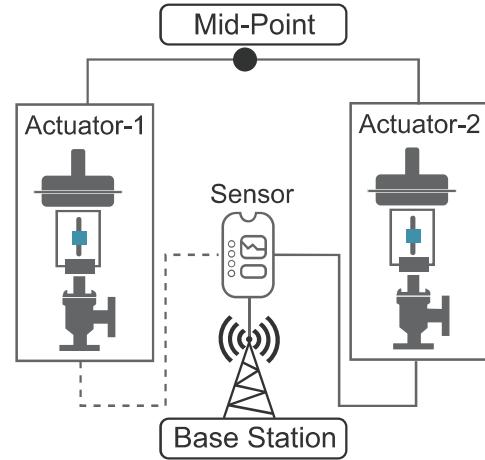


Fig. 3: Average midpoint of the optimal actuator.

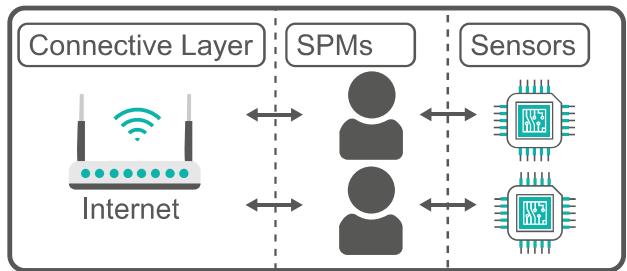


Fig. 4: Three layers of the SPM model.

proposed algorithm is applied to determine the midpoint to reduce the delay and improve energy efficiency. The SPM (sensor pervasive mobility) model adding a layer of mobile sensors (patients) between the accessing points and the sensor layers is shown in Fig. 4.

- ▷ **Sensor Layer:** offers communication and can transmit data within a short range. Among the three layers, the sensor layer has the most limited resources. Thus, the work of the sensors is minimized.
- ▷ **SPM Layers:** mobile entities (such as patients) can communicate with sensors and access points and transfer data between them. SPMs do not communicate with each other.
- ▷ **Connective Layer:** servers with access to the Internet with strengthened power, storage, and processing capabilities.

This framework can be placed on one device depending on the scenarios, which can improve its applicability. The layers work as receivers for the data collected by the SPM and stored in cloud servers.

For instance, a sensor can be attached to a patient where the sensor and SPM layers are mapped to the same device. Similarly, if SPMs can be connected to the Internet, they can also function as access points with the combination between the SPM and the access point layers. Then, we introduce the mobility of the base station. First, we place the base station at a location with the maximum energy efficiency, and then we can prove that the lifetime of the network is minimal when a

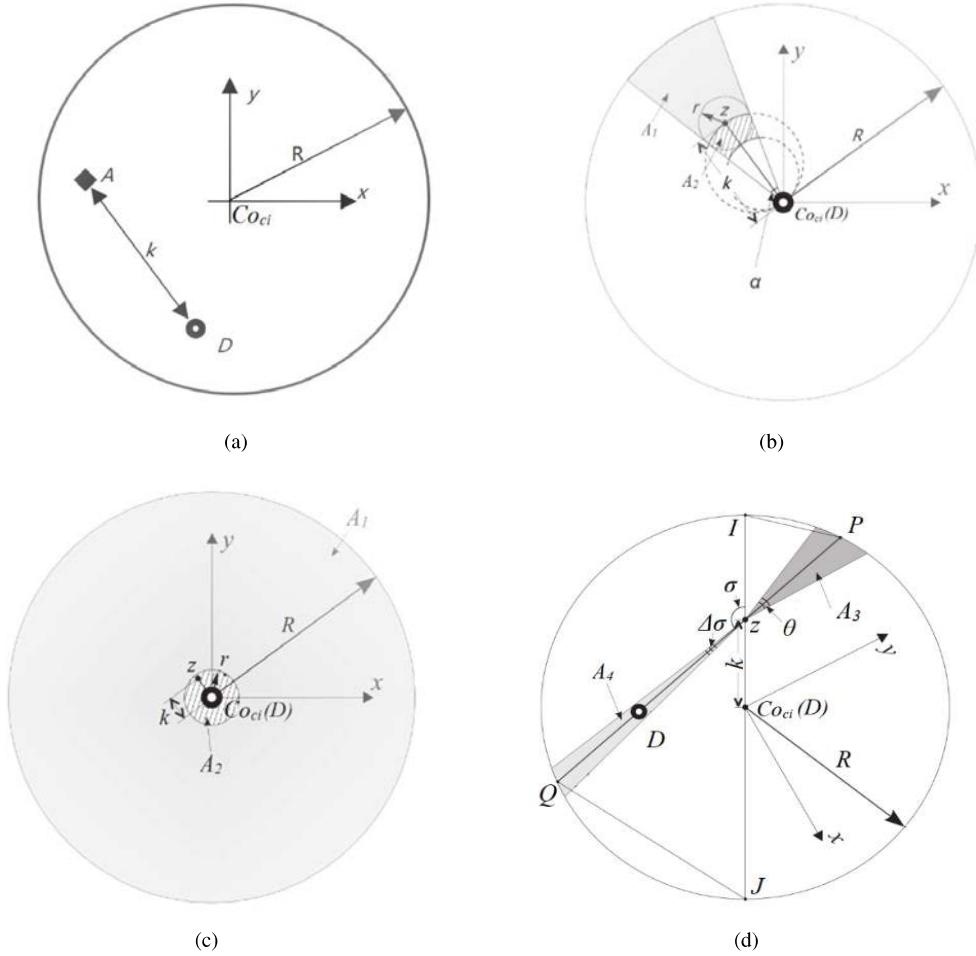


Fig. 5: The network lifetime load distribution of the BS position. (a) Optimal BS position proof. (b) Calculation of the load distribution while $k \geq r$. (c) Calculation of the load distribution while $k \leq r$. (d) Closed expression model $k \leq r$.

BS is at this location.

Claim 1 In terms of energy savings for data collection, the center of the circle Co_{ci} is the best base station.

Proof 1 Place the base station at $D(x_D, y_D)$, and then select a minimum area A at the center of (x, y) when measuring $dx \times dy$, as shown in Fig. 5(a).

The Euclidean distance E_d is given by

$$E_d = \sqrt{(x - x_D)^2 + (y - y_D)^2} \quad (17)$$

Because of the assumption of the short-path routing protocol given in [11], the length from A to D is approximately equal to E_d . Thus, the energy consumption E_c by transmitting data from A to D can be calculated as

$$E_c = zd\phi \times t\omega \times E_d \quad (18)$$

where $t\omega$ is the amount of data produced at time t , and $zd\phi$ is the energy used by sensor z to forward the data from A to D per unit. The total energy consumption E_t that transmits A to D is given by

$$E_t = \iint ((zd\phi \times t\omega) \times E_d) dx dy \quad (19)$$

Hence, the minimized total consumed energy E_t^- can be calculated as

$$E_t^- = \int_{-R}^{+R} \int_{-(R-y)}^{+(R-y)} ((zd\phi \times t\omega) \times E_d) dx dy$$

where $-R$ and $+R$ are the minimum to maximum region, respectively. By substituting the value of E_d we will have

$$E_t^- = \int_{-R}^{+R} \int_{-(R-y)}^{+(R-y)} zd\phi \times t\omega \times \sqrt{(x - x_D)^2 + (y - y_D)^2} \times dx dy$$

By simplification and derivation, we obtain

$$E_t = \left[(zd\phi \times t\omega) \times \frac{1}{2}\pi R^2 (2x_D^2 + 2y_D^2 + R^2) \right] \quad (20)$$

when $x_D = y_D = 0$; thus, we can determine the minimum value at which the BS stays at the center of circle Co_{ci} . We demonstrate that even at this best location, the attribution between the load sensors is still lacking. Given a sensor z at a distance k from the base station D (also Co_{ci}), as shown in Fig. 5(b), this sensor's average geographical load is proportional to $\frac{(A_1 + A_2)}{A_2}$.

All branches from A_1 and A_2 must pass the sensors in A_2 , forming pressure on these sensors. Therefore, the geographical average power of the sensor data flow in A_2 can

be transformed to the intensity of pressure Iz of the sensor, where $\omega\mu\phi$ is the amount of data. The average load is inversely proportional to the distance between the sensors to the selected BS, which means that when the distance becomes shorter, the load increases dramatically. In other words, the sensors around the BS consume more energy than other sensors because they must send a large amount of data flow to maintain balance, even when the number is limited. Therefore, the lifetime of the network depends on the lifetime of the sensors. Additionally, the BS cannot continue collecting data when these sensors run out of power, although most sensors are still alive. Last, according to Fig. 5(c), the load remains the same while the location of the BS changes. In conclusion, the center of the circle is the best location in terms of energy efficacy.

Intuitively, a mobile BS can assign the role of "hot spots" (the sensors around the base station) over time so that the load is averaged. We prove that this hypothesis is correct in this section. As the data collection process continues anywhere in the BS, (1) the worst-case latency increases whenever the BS leaves the center (compared to a central static BS, its top doubles), and (2) the moving speed is not necessary for the movement strategy.

Assuming that the BS's movement always maintains the same frequency, if we continue using the model above, it results in an extremely complicated integral that can only be calculated numerically and cannot provide adequate system performance. To achieve a closed expression, we simplify the model. Let us consider the power consumption of any sensor z , which is at a distance k from the center, and the BS's position is D . The forwarding load from a small sector A_3 is in charge of sensor z (geographical average) when the BS is at D on the segment of zQ , as Fig. 5(d) shows. The line zD intersects the circle at P and Q , and A_3 is centered around line nA with an angle of θ . To facilitate calculation, we consider that D stays in another sector A_4 , centered around line zQ with an angle of $\Delta\sigma$. When $\Delta\sigma \rightarrow 0$, D is on the line zQ .

Since D can be everywhere within the circle, we divide D into a disjoint sector (A_4^σ) that should be written as $U_\sigma A_4^\sigma = D$. Then, the average load of the sensor L_z is given by

$$\begin{aligned} L_z &= \sum_{\sigma=0}^{2\pi} L_z|_{\{D \in A_4^\sigma\}} \times J_r\{D \in A_4^\sigma\} \\ L_z &= \sum_{\sigma=0}^{2\pi} L_z A_3^\sigma t\omega \times \frac{A_4^\sigma}{\pi R^2} \\ &\approx \sum_{\sigma=0}^{2\pi} \frac{1}{2} |zP|^2 \bar{\theta} t\omega \times \frac{\frac{1}{2} |zQ|^2 \Delta\sigma}{\pi R^2} \end{aligned}$$

where $\Delta\sigma$ takes a discrete value of n . Thus, $n \in \mathbb{Z}_+$. $J_r(A_4^\sigma)$ that calculates the occupying frequency depends on the assumption that the BS is moving at the same frequency. Because ΔzPI and ΔzJQ are similar, $|zP| \times |zQ|^2 = (R^2 - k^2)^2$. Let $\Delta\sigma \rightarrow 0$, and the formula becomes an integral over $[0, 2\pi]$:

$$L_z = \int_{\sigma=0}^{2\pi} \frac{(R^2 - K^2)^2 \bar{\theta} t\omega}{4\pi R^2} d\sigma$$

The result shows that in the case of a mobile BS, the maximum average load is much lower, which prolongs the network lifetime.

C. Load-Balancing Phase

Once the actuator completes the sensors' borrowing process, then the base station initiates its execution process. The base station sends the query to the exciting area using the shortest path described in [23]. The sensor first receives the query request that sets its priority $= \phi$ and then forwards the query process inside the region to let other sensors know that the base station is ready to communicate. The query-forwarding sensor becomes a sensing sensor, and the query-receiving sensors forward the data to it. This process helps to share the actuator's load; otherwise, the actuator can reduce its energy after some specific time. Initially, a small tree is constructed between the query-forwarding sensor and the other queried region sensors. Thus, the data sensed by the three sensor members are forwarded to the query-forwarding sensor device. Finally, the query-forwarding sensor device delivers the collected data to the actuator or BS depending on the distance. Let us assume that inside the region, a total number of K sensors exist that can be explained as follows.

$$K = (k_1, k_2, k_3, \dots, k_n) \quad (21)$$

The set of K sensors has the coordinates (a_j, b_j) , where $1 \leq j \leq K$. We assume that the query-forwarding sensor sends the query along the y-axis. Assume that the forwarded query is broadcast in the order of $q_1, q_2, q_3, \dots, q_n$, where we have $y_j < y_{j+1}$. Thus, the forwarded query can be explained as

$$|q_j - q_j + 1| = \frac{1}{\sqrt{(a_j - a_{j+1})^2 + (b_j - b_{j+1})^2}} \quad (22)$$

where (a_j, b_j) are the coordinates of each sensor device inside the region, ϕ is the sensor that sets the priority because it receives a query from the actuator, $K = k_1, k_2, k_3, \dots, k_n$ is a set of sensors that receives a query message. We also assume that the queries start at $q_s(a_s, b_s)$ and end at $q_e(a_e, b_e)$ as $q_1, q_2, q_3, \dots, q_n$ is the set of queries, where q_e is the end of the query and q_s is the start of the query.

D. Transmission Guaranteed Phase

This phase is more critical because it includes two types of sensors: static and mobile sensors. The goal of this phase is to ensure contention-free transmission. The heterogeneous infrastructure used for static objects (humans who are not moving) is reliable and supports the improved throughput even during the mobility of sensors. Our model implements error-free communication by handling the problem of RSSI. The RSSI faces abnormal fluctuation and introduces large errors in a multifaceted and variable indoor environment. As a result, it causes a large error in the adaptation that leads to weak communication.

To handle this problem, a nonmetric multidimensional scaling (NMS) function is employed. The NMS helps to map the accurate relative locations of the objects. The dissimilarity matrix has also been created, and associated coordinates of

the IoT devices in the low-dimensional spaces are acquired. Thus, the distribution of RSSI at diverse transmission levels can efficiently be handled and can be adapted according to environmental changes. Furthermore, multidimensional scaling possesses strong fault tolerance, so the technology can easily be incorporated into indoor RSSI positioning, which not only provides error-free communication but also increases the anti-jamming capability of the positioning and obtains a better positioning impact. Furthermore, an optimized midpoint is used that provides a closer receiving point to the transmission point, which leads to stronger signals that have a positive impact on the communication. This phase involves the RSSI and samples the pairs of transmission power levels using a curve-fitting approach [24]. To obtain these samples, each sensor device transmits a group of beacon messages at different power intensities. Furthermore, the neighbor of each sensor listens to the RSSI vectors and returns that value. Let us assume that matrix Z involves a set of RSSI vectors Z_j . Each neighbor hears the RSSI vectors that can be explained as follows:

$$\{Z_1, Z_2, Z_3, \dots, Z_n\}^n \quad (23)$$

It can be simplified as:

$$Z_j = \{z_j^1, z_j^2, z_j^3, \dots, z_j^n\} \quad (24)$$

Equation 25 shows the RSSI vector for the neighbor sensors j , in which Z_j^k is the RSSI value that is measured at sensor j conforming to the beacon transmitted by power level (Δp_k). We apply a linear function to describe the correlation between RSSI and the transmission power on a pairwise basis. The reason for using linear function is to deploy the constant connection between components of the CPS and limit data transmission only to permitted connections. The linear functions help to reduce approximation error and computational complexity. Furthermore, linear functions provide constancy between RSSI and transmission power because the proposed CPS does not require rapid inconsistent change.

$$z_j(\Delta p_k) = x_j \times \Delta p_k + y_j \quad (25)$$

We further apply the least square approximation formulation, which requires little computational overhead that can easily be adjusted in the sensor device. Based on the sample vectors, the coefficients x_j and y_j can be determined to minimize P^2 .

$$P^2 = \sum_j^{\infty} z_j(\Delta p_k) - (Z_j^k)^2 \quad (26)$$

The features of the ranking model have been used for determining the coefficients x_j and y_j , which detect the errors in RSSI. The value of the RSSI determines whether the nature of the signal is poor or strong. Thus, the ranking model retrieves strong signals from the RSSI and drops the weak signals. Therefore, strong signals are used to send the data successfully. In contrast, the poor signals of the RSSI that cause the error can be avoided in this way. The ranking model

sets the threshold values for the coefficients x_j and y_j to select the signal with a higher strength.

$$\begin{bmatrix} x_j \\ y_j \end{bmatrix} = \frac{1}{N \sum_{k=0}^N (\Delta p_k)^2 - \sum_{k=0}^N (\Delta p_k)^2} \times \left[\sum_{k=0}^N Z_j^k \sum_{k=0}^N (\Delta p_k)^2 - \sum_{k=0}^N (\Delta p_k) \cdot \sum_{k=0}^N (\Delta p_k) \right. \\ \left. - Z_j^k N \sum_{k=0}^N (\Delta p_k) \cdot Z_j^k \sum_{k=0}^N (\Delta p_k) \sum_{k=0}^N Z_j^k \right] \quad (27)$$

where j is the neighbor sensor, P^2 is the vector sample, Δp_k is the power level, Z_j^k is the RSSI value measured at sensor j and Z_j is the RSSI vector heard by the neighbor sensors. Equation 28 creates an initial model that is used to handle the RSSI. Furthermore, continuous updating is required when changing the environment.

E. Privacy and Data-sharing Phase

This phase provides a secure method for sharing the data and delivery process among the sensors. Let us assume the sensor shares $\Delta \varrho$ out of the forwarded data, such that Δd are required blocks to regenerate the data. Thus, each sensor is loaded with the same $\Delta \varrho \times \Delta d$ matrix $V = [x_i, q]$, where V should be selected in such a way that each combination of Δd columns should make an invertible $\Delta \varrho \times \Delta d$ matrix. Note that our scheme does not depend on V 's privacy. Hence, the sensors may insert it, regardless of exposing compromises. When a sensing event is triggered, sensor k collects its readings in a core buffer of length Δd . Thus, the block reading can be expressed as follows:

$$B_r = [b_{k,1}, b_{k,2}, b_{k,3}, \dots, b_{k,\Delta d}] \quad (28)$$

When the sensor's buffer is full, then the sensor computes $\Delta \varrho$ diverse shares of unitary length that are forwarded along the paths. These shares consist of different elements that can be expressed as follows:

$$S = [b_{k,1}, b_{k,2}, b_{k,3}, \dots, b_{k,\Delta d}] \times [x_i, q] \quad (29)$$

When the actuator receives $\Delta \varrho$ shares, it is in the position of regenerating the data. Let us assume it receives $S_k = [s_{k,q1}, s_{k,q2}, s_{k,q3}, \dots, s_{k,q\Delta d}]$ Thus, the reading can be obtained by resolving Equation 30.

$$S_k = \begin{cases} b_k, 1x_1, q_1 + b_k, 2x_2, q_2 + b_k, 3x_3, q_3 + \dots \\ \quad + b_k, \Delta dx_{\Delta d}, q_1 = s_{k,q1} \\ b_k, 1x_1, q_2 + b_k, 2x_2, q_2 + b_k, 3x_3, q_3 + \dots \\ \quad + b_k, \Delta dx_{\Delta d}, q_2 = s_{k,q2} \\ b_k, 1x_1, q_3 + b_k, 2x_2, q_2 + b_k, 3x_3, q_3 + \dots \\ \quad + b_k, \Delta dx_{\Delta d}, q_3 = s_{k,q3} \\ \vdots \quad \vdots \quad \vdots \\ b_k, 1x_1, q\Delta d + b_k, 2x_2, q\Delta d + b_k, 3x_3, q\Delta d + \dots \\ \quad + b_k, \Delta dx_{\Delta d}, q\Delta d = s_{k,q\Delta d} \end{cases} \quad (30)$$

If matrix V is chosen, then no known method exists to regenerate the parts of the original data from the $t-1$ samples, as this privacy-aware sharing also helps for data aggregation. Given messages $\Delta m_{k1}, q$ and $\Delta m_{k2}, q$ on path q , then the

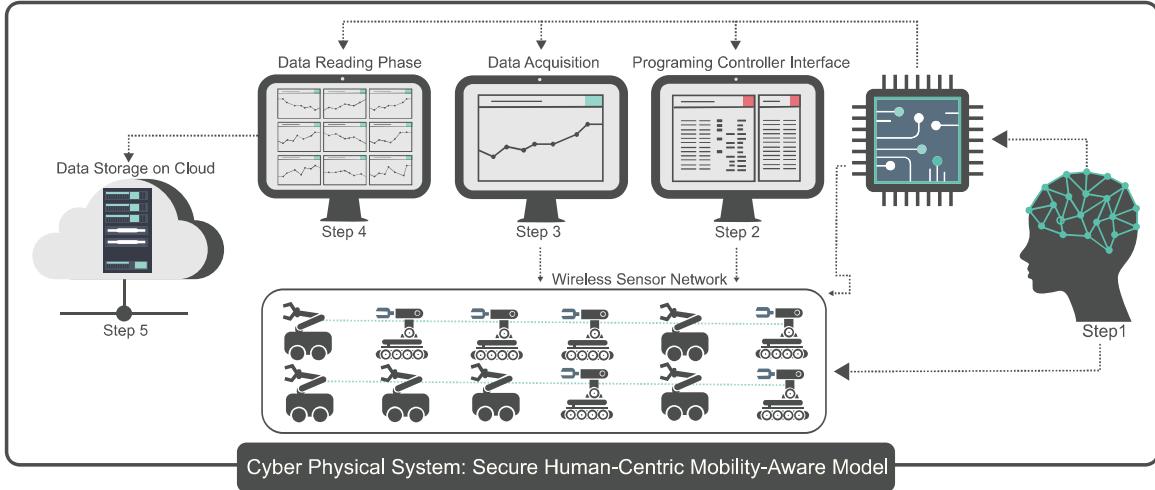


Fig. 6: A proposed prototype for the SHM cyber-physical system model.

aggregator sensor accumulates as $\Delta m_{k1}, q + \Delta m_{k2}, q$. The given messages can be expressed in the following equations.

$$\Delta m_{k1}, q + \Delta m_{k2}, q = \sum_{i=0}^{\Delta d} (b_{k1}, i + b_{k2}, i + b_{k3}, i) x_i, q \quad (31)$$

Upon receipt of Δd messages, the actuator regenerates each task as follows:

$$A_{tr} = \sum_{i=0}^n \gamma \varepsilon (b_{k1} + b_{k2}, \dots, b_{kn}) + T\Delta \quad (32)$$

where $\gamma \varepsilon$ is the decision variable, A_{tr} is the task regenerated by the actuator, and $T\Delta$ is the task processor.

VII. EXPERIMENTAL RESULTS AND DISCUSSION

This section explains the experimental results regarding the experimental setup, performance metrics, and discussion of the results.

A. Experimental setup and model prototype

The proposed SHM consist of secure service-oriented architecture (SSOA), brain sensor network (BSN), cloud services, and the data management domain. A real-time prototype is developed and tested in the neurological surgery ward in the RSCN in Nur-Sultan, Kazakhstan, where patients of the ward have been monitored, and their important signs and physical and physiological constraints are recorded. Many NeuroSky headsets have been used, which provide multiple channels of electroencephalogram (EEG) recordings from the dry electrode positioned at the ear lobe. NeuroSky contains ThinkGear technology that allows the headset to interface with the wearers' brainwaves, and its sensor touches the forehead and reference points situated on an ear pad. Thus, the onboard chip keeps all data, as recorded data are used to evaluate the patients' health conditions.

The primary purpose of this prototype is to monitor continuously moving and static patients as a prototype to monitor the activities of doctors and other staff by embedding

additional microprocessors in the real hardware using Filed programmable Gate Arrays (FPGAs). Figs 6 and 7, show a proof of concept of the prototype of the proposed Secure SHM cyber physical system model and the an implementation instance of the prototype; respectively. As seen in the figures, the prototype involves hardware and software features. The hardware part is based on a 1-field-programmable gate-array (FPGA)-based real-time clock (RTC) that provides flexible parallelism; 2-microcontrollers are embedded in the FPGA to obtain energy efficiency and reusability. The interface has been developed for FPGA to maintain parallelism based on EV12DS460A and comprises the dual-channel, 14-bit, 9-GSPS, and Arria V GZ from Intel. The static robot helps convert the brain signals into a robot signal using multiple linear regression to support a deep neural network model, which can be later easily stored and analyzed. The naive Bayes algorithm was used for stress classification, which takes less computational time than multilayer perceptron and support vector machine algorithms. On the other hand, the mobile robot sensor helps determine the mobility of the proposed SHM.

The mobility-based model is programmed in C++ language to monitor moving neuro patients. The model is designed and implemented to meet real-world requirements using the Java platform. A greater focus is placed on SSOA to maintain privacy and data-sharing processes. For better security and privacy, the model the xfDNN library is used to obtain the knowledge-based repository features for data storage. Also, xDNN processing engine is used with a machine learning suite to store the Amazon Elastic Compute Cloud (EC2) data that come through a knowledge-based repository decision. The distance between the neurological ward and the management office (where systems are set up to observe the patients' information) is approximately 100 meters. Thus, we physically installed a maximum of 50 flexible sensor devices. The reason behind this philosophy is to determine and justify a scientific contribution of different parameters (e.g., average throughput, hop-by-hop delay, energy consumption, and reliability). Fur-

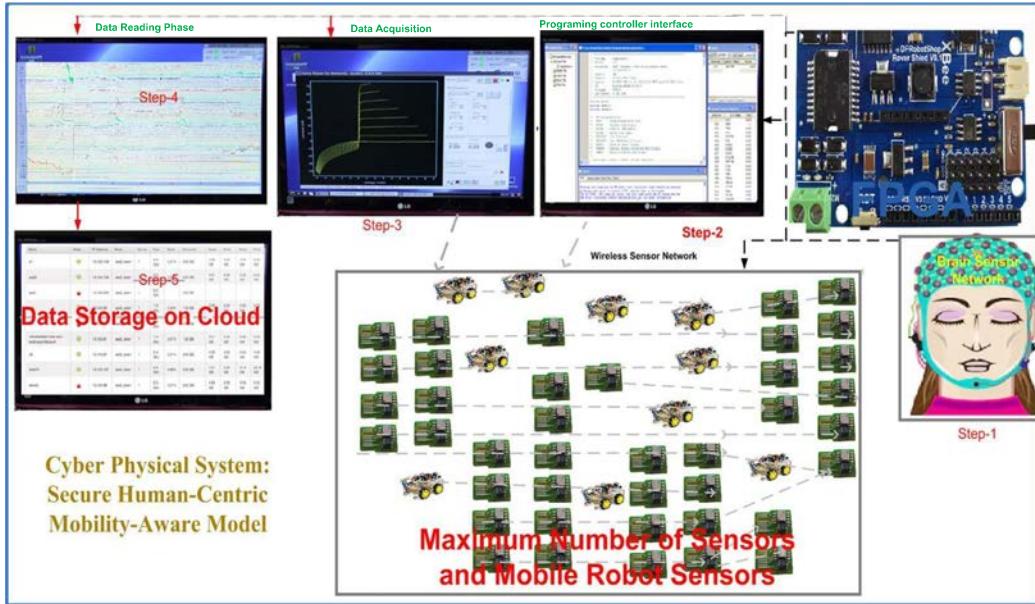


Fig. 7: Implementation steps of the proposed SHM cyber physical system prototype.

thermore, testing processes have also been conducted with other methods over the next four days: IntruMine [25], a cyber-physical security infrastructure (CPSI) [26], a healthcare cyber-physical system (HCPS) [27], and a virtual heart model (VHM) [11]. The received data are shared with the neurological specialist of RSCN to confirm the validity of the obtained data.

Due to patient privacy, the real-time testing environment, including pictures of patients, staff, doctors, and attendants, is not shared. However, the working prototype is given in Fig. 7. In the proposed model, the data collection process continued for 36 minutes. The collection data time is much longer during mobility, and overhead is expected due to noise. Thus, features of [28, 29, 30] algorithms are used to remove the noise from the speech/data to avoid overhead. The normal movements and reactions of the static and moving neurosurgical patients were measured, who were experiencing treatment for epilepsy, and they could listen to continuous communication. The patients mainly carried out breathing and muscle movements to the sense of touch and absorption. The activities were not painful but sometimes seemed slightly unpleasant. The position of the robot was set as mobile and static. The robot consists of a microcontroller with an ARM Cortex-M4 processor and 12 identical smart ports. It also uses a Backlit LCD for performing simple operations. The mobile sensor robots concurrently communicate with the controller wirelessly. Each mobile robot can talk to a maximum of 12 devices.

B. Performance Metrics

Performance metrics are defined as figures and data representative of SHM model abilities and overall reliability. Based on the obtained data, MATLAB is just used for graph generation to view the measurements of the following parameters as a means of comparison:

- ▷ Average Throughput

- ▷ Hop-by-Hop Delay
- ▷ Sensors' Lifetime
- ▷ Energy Consumption
- ▷ Reliability

1) Throughput performance: The throughput is used to record the number of network data transmissions in a particular period. A much higher throughput creates higher efficiency, which means a smaller delay in the network data transmission, faster transmission speed, and more sensitivity to external influences. Thus, the performance of the whole network improves. Figs. 8(a) and 8(b) indicate the trade-off between the average throughput and the testing time, without malicious sensors and 8(b) with 5% of malicious sensors activated, respectively. As seen in Fig. 8(a), the average throughput increases, and the system becomes more efficient and stable. We monitored the patients using static sensors and with 20% of mobile sensor robots activated. We conclude that the average throughput increased in the SHM model. According to the definition of throughput, the formula for throughput is defined as follows.

Suppose that there are m sensors in this system, the density of sensors is ρ , and the single-hop delay of each sensor in many cases is $\delta_p^{z,\mu}$, as follows:

$$T_p = \sum_{i=0}^m \frac{\eta_k^d}{\delta_p^{z,\mu}} \quad (33)$$

where η_k^d represents the amount of data sent from the sensor device to the actuator. Additionally, the sum of data that one sensor receives and generates equals all the data it sends. It only records the data sent because the amount of data received and sent is the same. The number of data transmissions per second can be represented as the quotient of the amount of the data and delay.

The throughput of the numbers of sensors in the WSN and the number of data transmissions of the whole system

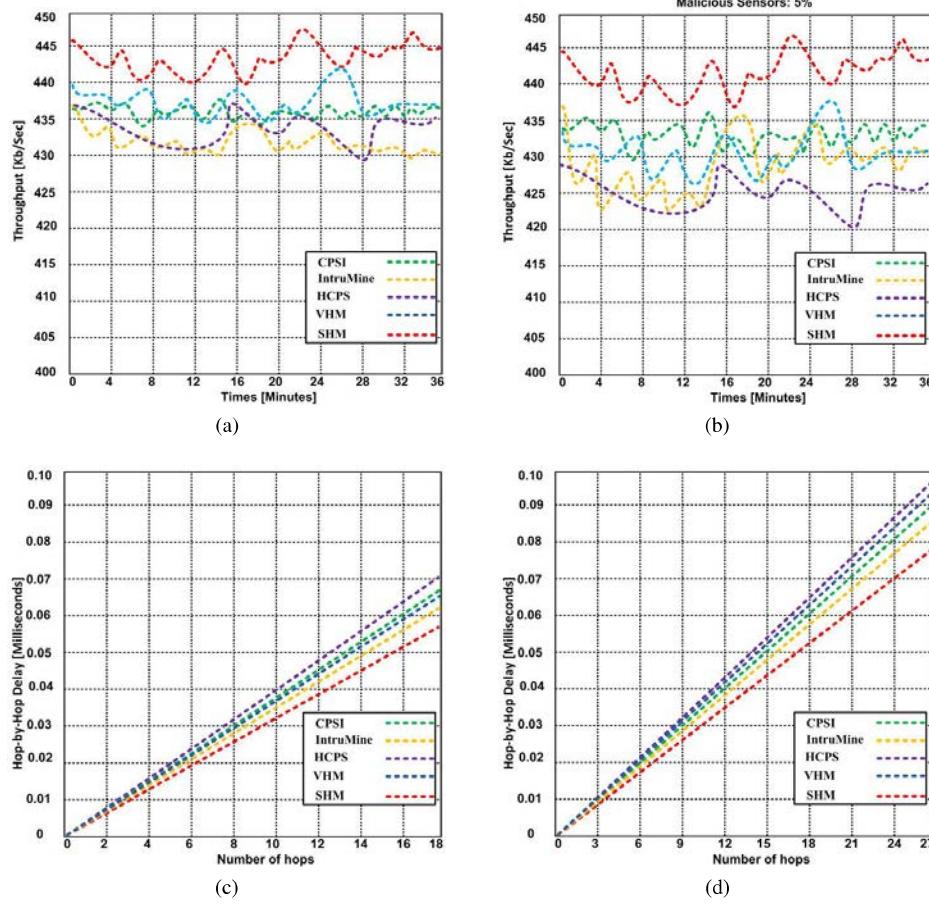


Fig. 8: (a) and (b) show the average throughput performance: (a) without malicious sensors, (b) with 5% malicious sensors; (c) and (d) show the positive correlation between the number of hops and the hop-by-hop delay.

are equivalent in unit time. Due to the randomness of the distribution in the sensor network, the throughput can be approximately represented by the average throughput of a single sensor device and the number of sensors participating in the entire network. Let p_{rn} be a positive real number that denotes the minimum requirement of mobile/static sensor node k . The long-term throughput $T_p^{\mathbb{T}}$ of node k using random variable $\omega_d^z(k)$ with employed policy $\partial_{\rho}^{(z,\mu)}$ can be determined as

$$T_p^{\mathbb{T}} := \lim_{I_c \rightarrow \infty} \frac{1}{I_c} \sum_{I_c=1}^{I_c^{\vee}} \omega_d^z(k) \cdot \partial_{rho}^{z,\mu} \times (DR)_{xy} \times t_c \quad (34)$$

I_c is the interference constraint related to the channel, $(DR)_{xy}$ is the transmitted data rate, and t_c is the total time the node transmits and receives data.

We created the malicious nodes in Fig. 8(b), which are only proficient in launching wormhole and HELLO flood attacks. The transmission is considered malicious if the conforming message's geographical location is made up or communicated with different power ranges.

Thus, we set 5% of sensors as malicious based on dissimilar power ranges. A sensor is considered malicious if a malicious transmission is broadcast. As a result, upon receiving a message, the sensor is classified as malicious in the system. The

ACC RMS sensor consists of a built-in RSSI function that is activated. It produces an analog output signal at its pin that is inversely proportional to the input signal range. An analog/digital converter (A/DC) is used to measure the voltage from the pin. Received signal strengths R_{ss} for antenna $\dashv q'$ on sensor node k for transmission Tr can be determined as

$$R_{ss} = g(\theta) + T_{pow} + R_{vm} \quad (35)$$

$$g(\theta) = \left(<(k, Tr) u_p + (\dashv q') \right) \Delta$$

Substituting the value of $g(\theta)$:

$$R_{ss} = \left(<(k, Tr) - u_p + (\dashv q') \right) \Delta + T_{pow} + R_{vm} \quad (36)$$

where $g(\theta)$ is the gain (dB) of the sensor's antenna at the angle θ , T_{pow} is the transmission power, R_{vm} is the model of the random variability to cope with recurring measurements at different locations, and u_p is an unidentified placement of the receiving node.

2) *Hop-by-Hop Delay*: In networking, the hop-by-hop delay refers to the amount of time that the packet takes to reach the node (hop) and the time taken by the packet to leave the node. Figs. 8(c) and 8(d) represent the trade-off between the number of hops and the hop-by-hop delay. As the number of hops increases, the hop-by-hop delay increases. We

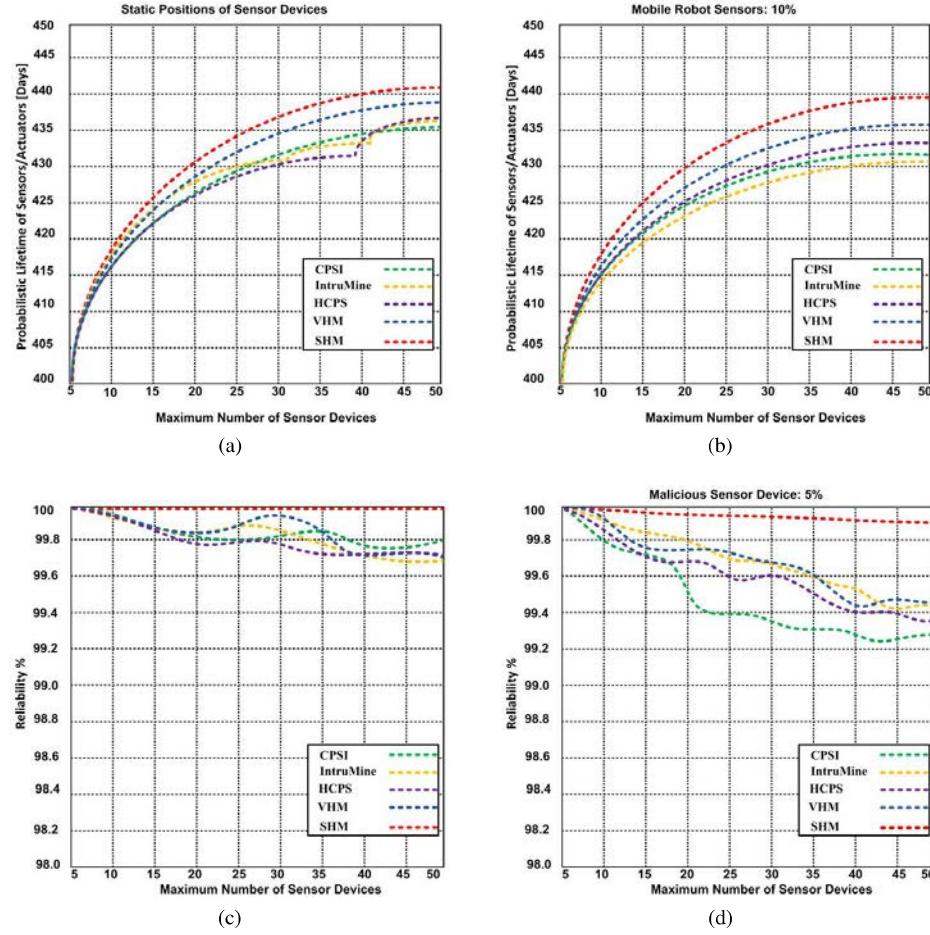


Fig. 9: (a) and (b) show the lifetime of the network with sensors/actuators for the proposed SHM model and competing protocols. (c) and (d) show the reliability of the SHM model and other contending protocols: (c) without and (d) with 5% malicious sensors.

tested both static and mobility-aware situations for SHM and other contending models. We used a similar situation for our proposed and other contending models and observed that the hop-by-hop delay is the lowest in SHM. The standard average delay A_{de} for n hops can be obtained as follows:

$$A_{de} = \sum_{t=0}^n \frac{t_{sl}}{C_{tl}} \times \frac{t_{sl}}{2} \quad (37)$$

where t_{sl} is the small time slot reserved either for listening or sleeping of the node, and C_{tl} is the length of the duty cycle time for a sensor device. Each sensor device sends the preamble pr before transmitting the data (frames). Thus, each sensor device requires P_n preamble sensors that are forwarded to h_{tot} total number of hops. Thus, the sensor device requires a total number of slots S_{tot} .

$$A_{de} = (n - 1)pr(t_{sl}) \times \frac{t_{sl}}{2} + P_n(t_{sl}) \times \frac{t_{sl}}{2} \quad (38)$$

where $(n - 1)$ is the time for the first slot, t_{sl} is the small time slot reserved either for listening or sleeping of the node, and C_{tl} is the length of the duty cycle time for a sensor device.

3) *Sensors' Lifetime*: Figs. 9(a) and 9(b) indicate the trade-off between the number of sensors/actuators and the sensors/actuators' lifetime. The lifetime of the sensors should

increase with an increase in the number of sensors for performance improvement. These experiments were performed on the IntruMine, CPSI, HCPS, VHM, and SHM models using a similar number of sensors and setup (maximum 50 sensors). We compared these results with the performance of the SHM model in static and mobility-aware situations. The testing results with the static sensors depicted in Fig. 9(a) show a better performance of the SHM model than the other four models. Additionally, our proposed model is compatible with mobile sensors. The results demonstrated that our proposed SHM model outperforms the contending protocols. The probabilistic average lifetime of the proposed SHM model is estimated at 441 days. In comparison, other competing models show a probabilistic average lifetime of 335-338 days with static sensors, as shown in Fig. 9(a).

In Fig. 9(b), 10% of mobile sensor robots have been used that affect the lifetime. The results demonstrated that the proposed SHM model has a 439-day lifetime, whereas other contending models show 431- to 435-day lifetimes. This finding demonstrates that our proposed approach reduced the lifetime by two days with 10% of mobile sensor robots activated, whereas the competing models reduced the lifetime by approximately three days. Therefore, the results confirm our proposed model's effectiveness and show its advantage

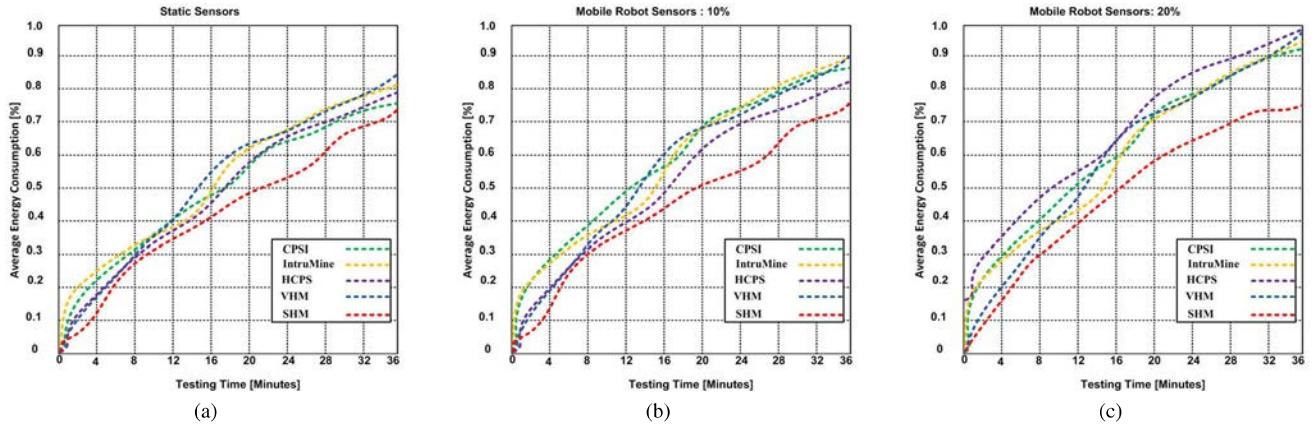


Fig. 10: (a) and (b) show the energy consumption with 10% and 20% mobile robot sensors for the SHM model and other competing models. (c) shows the average energy consumption of the SHM model and other contending models during different time periods with static sensors.

over other contending models in static and mobility-aware situations.

4) Reliability: Reliability refers to the model's capability to continually perform its required function on demand without deterioration or failure. Fig. 9(c) shows the SHM model's reliability and other competing models without malicious sensors and with 5% of malicious sensors activated (an installed malicious model that enforces the sensors to behave disorderly). As shown in the figure, the SHM model is more reliable than other contending models. The SHM model shows 99.99% reliability compared to other contending models, which possess 99.69-99.8% reliability. When 5% of malicious sensors are activated, the proposed model's reliability decreases slightly to 99.95%, whereas other competing models have 99.3-99.44% reliability, as shown in Fig. 9(d).

The results demonstrate that the overall performance of the proposed SHM model is more reliable than other contending models. We assume that the total number of successful data S_{dt} (successful storage of the data from source to cloud servers) is effectively stored. Thus, some data are not attacked and are considered protected data P_{dt} , and some data become victims by the attacker and are considered attack data A_{dt} . Thus, the reliability ratio R_{ratio} of the SHM model can be obtained as:

$$R_{ratio} = \frac{(S_{dt})}{S_{dt} - 1} \left\{ 1 - \frac{\sum P_{dt} \times A_{dt}}{S_{dt} - 1} \times V_{dt} \right\} \quad (39)$$

where \sum is the sum, and V_{dt} is the variation in all the data.

The results demonstrate that the proposed model is highly reliable when activating mobile sensors.

C. Energy Consumption

Energy consumption refers to the energy that is consumed by IoT devices to accomplish tasks and actions. Figs. 10(a) and 10(b) demonstrate the average energy consumption with 10% and 20% of mobile robot sensors activated. The results indicate that the competing models consumed more energy as the interval increased than the SHM model. When 10% of mobile robot sensors were activated to check the moving patients,

the SHM model consumed 0.75 joules, and other models consumed approximately 0.81-0.91 joules, as shown in Fig. 10(a). The results confirm that our proposed SHM model consumed 7.1-17.2% less energy. Similarly, when 20% of mobile robot sensors were activated, the SHM model consumed 0.755 joules, while contending models consumed 0.91-0.98 joules, as shown in Fig. 10(b). The energy consumption is of high significance for any model to ensure that the model performs effectively. The experimental results show the effectiveness of static and mobile sensor robots. The testing process with static sensors/actuators depicted in Fig. 10(c) explicitly indicates the better performance of the SHM model, as our proposed SHM model consumed 0.72 joules of energy throughout the testing process. However, the contending protocols consumed 0.75-0.83 joules during the same time. This result demonstrates that our proposed SHM model consumed 3.2- 11.4% less energy with static sensors/actuators.

D. Analytical comparison

This subsection provides an analytical comparison between the performance and efficiency of the proposed model and the competing state-of-the-art models and the IEEE 802.15.4 wireless standard protocol. Table II and Table III summarize the comparison results between the proposed SHM model and other models. The two tables clearly show that our proposed SHM model exhibits a better performance with an increased number of static and mobile sensors than the competing model.

This confirms the effectiveness of the proposed SHM over other contending models. Most of the existing CPS only use the standard IEEE 802.15.4 [31], but the performance of the existing CPS is affected due to use of the IEEE 802.15.4 standard protocol. The reason for the performance of the existing CPS is that the sensor nodes in the IEEE 802.15.4 standard make a query process that takes additional overhead. Thus, the data admission rate D_{ar} can be calculated as

$$D_{ar} = D_{arf} (M_{sr} - R_{sam}) + D_{arf} (M_{lr} - R_{sam}) \quad (40)$$

where D_{arf} is the data admission rate factor in the case of the short-term query miss ratio, D_{arf} is the data admission rate

TABLE II: Performance Comparison of the proposed approach with competing approaches.

Approach	Average Throughput		Hop-by-hop delay		sensors Lifetime		Energy Consumption			Reliability	
	without Malicious	with Malicious	Maximum 18 Hops	Maximum 27 Hops	static	10% mobile	static	10% mobile	20% mobile	without malicious	with 5% malicious
IntruMine	432.0Kb/Sec	428.2Kb/Sec	0.062ms	0.085ms	436	431	0.081Joules	0.090Joules	0.094Joules	99.69%	99.43%
CPSI	436.2Kb/Sec	432.1Kb/Sec	0.067ms	0.093ms	435	432	0.075Joules	0.087Joules	0.091Joules	99.80%	99.30%
HCPS	433.1Kb/Sec	424.3Kb/Sec	0.07ms	0.096ms	437	433	0.079Joules	0.082Joules	0.098Joules	99.72%	99.37%
VHM	437.15Kb/Sec	432.12Kb/Sec	0.066ms	0.093ms	438	435	0.083Joules	0.090Joules	0.097Joules	99.72%	99.44%
SHM	445.02Kb/Sec	442.3Kb/Sec	0.057ms	0.077ms	441	439	0.072Joules	0.075Joules	0.0755Joules	99.99%	99.95%

TABLE III: Performance Comparison of the proposed approach with competing approaches.

Approaches	Average Reduction (%) in Throughput due to Malicious Nodes	Average Increase time (%) with increase in Hops	Average Life time (%) decreased due to mobility	Additional Energy consumption (%) due to 10% Mobile Robot Sensors	Additional Energy consumption (%) due to 20% Mobile Robot Sensors	Reliability (%) decreased due to Malicious Sensors
IntruMine	0.94%	37.09%	1.14%	11.11%	17.28%	0.26%
CPSI	0.94%	38.80%	0.68%	16%	21.33%	0.50%
HCPS	2.03%	37.14%	0.92%	3.80%	24.05%	0.35%
VHM	1.15%	40.90%	0.68%	8.43%	16.87%	0.28%
SHM	0.61%	35.08%	0.45%	4.16%	4.88%	0.04%

TABLE IV: Analytical comparison of SHM and IEEE 802.15.4.

Metrics	Mathematical Result for SHM Model	Mathematical Result for IEEE 802.15.4
Sensor Lifetime	$R_l = 1 - \frac{0.00003 \times 1000 \times 9 \times 0.00006 \times 1009 \times 12}{5.0} = 0.96077008$	$R_l = 1 - \frac{0.0000312 \times 5000 \times 14 \times 0.0000625 \times 5014 \times 19}{5.0} = 0.89480764$
Sensor recruitment time	$A_{rec} = 1 - N_r \prod_{N_r \in R} 5 \times 1 - \sum_p^{p=\infty} p \left(1 - \left(30 \int_{N_r}^n f_x(5 \times 5) 42(1 - \sum_{t=0}^n 2(1-5)) \right) \right) = 53.865 \text{Seconds}$	$A_{rec} = 1 - N_r \prod_{N_r \in R} 5 \times 1 - \sum_p^{p=\infty} p \left(1 - \left(30 \int_{N_r}^n f_x(5 \times 5) 42(1 - \sum_{t=0}^n 2(1-5)) + 76 \right) \right) = 53.941 \text{Seconds}$
Data transmission rate	$\Delta g = 99.2(92.4 - 0.05) + 97.3(76.52 - 0.05) = 166.01651 KB/Sec$	$\Delta g = 94.2(90.4 - 0.05) + 91.3(74.4 - 0.05) = 152.99 KB/Sec$
Single-hop connection time	$T_s = 133 \times 30 + 192 + 11 \times 30 + 640 = 5.152ms$	$T_s = 133 \times 32 + 192 + 11 \times 32 + 640 = 5.43ms$

factor in the case of the long-term query miss ratio, M_{sr} is the short-term miss ratio, R_{sam} is the sampling and randomization time, and M_{lr} : long-term miss ratio.

Hence, the effective data capacity D_c over the single-hop transmission is of paramount significance because the positive effective data capacity may lead to increased throughput and efficiency. We assume that the collected data from a source D_{cs} (data obtained from a patient) require a stable connection and that the entire connection consists of multiple hops. Thus, the single-hop connection time is Ct_{sh} , and the effective data capacity can be determined as

$$D_c = \frac{D_{cs}}{Ct_{sh}} \times C_{pi} \quad (41)$$

where C_{Pi} is the capacity at the physical interface.

As seen in Table IV, compared to the IEEE 802.15.4 standard, our proposed SHM model is slightly faster in the sensor recruitment process time, as shown in Table IV. The table results confirm that in the proposed SHM, the sensor advertisement and load-balancing phases are more efficient. SHM shows better performance than IEEE 802.15.4 regarding the sensor's remaining lifetime after the advertisement process, the data admission rate during the query process, and the single-hop connection time. For further analysis, the competing models, for example, the model proposed in [23], only include static sensors. In contrast, our proposed model covers static and mobile robot sensors. Two phases are included in our SHM model to ensure the information reliability and security of static and mobile robot sensors during communication: transmission guarantee and privacy and data-sharing phases. Handling static and mobile sensors, our transmission guaranteed phase uses an actual heterogeneous infrastructure. As a result, contention-free transmission is realized. Moreover, our

privacy-aware sharing is helpful for data aggregation as well, which reinforces transmission quality. As one future research direction, we plan to design a specific range where sensors can directly send data to the selected BS without redundant calculation to improve the SHM model performance. Furthermore, existing competing models were purely designed for simulation and emulation purposes. On the other hand, our proposed SHM model is purely designed for hardware devices. One of the challenges of a CPS is how to manage data collection accurately; this problem is also addressed using a semantic information extraction module.

VIII. CONCLUSIONS AND FUTURE WORK

This section reiterates the goals and objectives and summarizes the key evidence and findings for the reader. Additionally, it provides directions for the extension of current work.

A. Conclusions

This paper introduced a secure human-centric mobility-aware (SHM) model to analyze both human and physical domains. The proposed model consists of four parts: BSN, data processor, SSOA, and data management. The BSN detects the patients' physical and physiological constraints and transmits the information to an actuator, controller, and mobile robot sensor (physical domain). The data processor includes three sections: data collection, decision, and initiate action. An SSOA ensures both security and QoS while performing actions. Semantic information extraction, knowledge-based repositories, and cloud servers are included in the data management domain, where responsible people can access and share data. The SHM model realizes human-to-machine interaction and improves efficiency while ensuring data security

to avoid privacy problems. It consists of five modules: a sensor advertisement phase, mobile sensor recruitment and selection phase, load-balancing phase, transmission guarantee phase, and privacy and data-sharing phase. The sensor advertisement phase helps stationary and mobile robot sensors advertise their lifetime within the network and calculate the RLS to define the initial energy level. The mobile sensor recruitment and selection phase helps find sensors from other clusters (first from a neighbor, then from a nonadjacent domain) for the cluster that does not have enough sensors and aims to improve throughput and reduce the latency. The query-forwarding load acts as a sensing device and receives data from the query-receiving sensor in the load-balancing phase. This process helps reduce the load of the actuator. The transmission guaranteed phase ensures contention-free transmission at different transmission power levels to adapt to the environment's change. Because security is a great concern in WSNs, the privacy and data-sharing phase provides a secure way of sharing and delivering data among sensors, which is also helpful for data aggregation. Our proposed SHM model is tested in a realistic environment compared with the IntruMine, CPSI, HCPS, and VHM models. The results demonstrated that our SHM model outperforms the other models in both static and mobile testing environments. Our model maintains the trade-off between energy efficiency and throughput. The results prove our claim that the SHM model consumes less energy and produces increased average throughput. The testing results showed that the SHM model demonstrated a higher lifetime in static and mobile systems compared to other competing models designed for cyber-physical systems. Furthermore, the SHM model produces the lowest hop-by-hop time compared with competing models. Additionally, the reliability of the SHM model is better than that of other competing models, as confirmed through both malicious and nonmalicious situations. The reason for obtaining better performance in our proposed SHM approach is mobility-supported features. Second, the midpoint is determined such that the sensor decides to send the data to the actuator or the base station based on the midpoint. This choice helps protect data loss and provides an opportunity to send faster data. As a result, it leads to higher reliability and throughput and less energy consumption. Third, contending approaches experienced slight problems on the hardware platform because they were primarily designed for simulation purposes. On the other hand, the proposed system is particularly designed for real devices and tools.

B. Future Work

Future research will focus on integrating the SHM model with the recurrent neural network to improve the QoS and focus on the extensive study of human behavior. We will plan to design a specific range where the sensors should directly send the data to the selected BS without redundant calculation that will help to improve the SHM model performance. The integration process of hardware devices and software tools restricts mobility and slightly affects the energy when handling static and mobile robot sensors. Thus, in the future, we also aim to remove these shortcomings before designing the product.

ACKNOWLEDGEMENT

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number IFPIP: 855-611-1442" and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

REFERENCES

- [1] S. Kim, Y. Won, I.-H. Park, Y. Eun, and K.-J. Park, "Cyber-physical vulnerability analysis of communication-based train control," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6353–6362, 2019.
- [2] T. Shah, A. Yavari, K. Mitra, S. Saguna, P. P. Jayaraman, F. Rabhi, and R. Ranjan, "Remote health care cyber-physical system: quality of service (qos) challenges and opportunities," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 40–48, 2016.
- [3] K. Song, K. Anderson, and S. Lee, "An energy-cyber-physical system for personalized normative messaging interventions: Identification and classification of behavioral reference groups," *Applied Energy*, vol. 260, p. 114237, 2020.
- [4] Y. Zhang, Z. Guo, J. Lv, and Y. Liu, "A framework for smart production-logistics systems based on cps and industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4019–4032, 2018.
- [5] G. Tanganeli, L. Cassano, A. Miele, and C. Vallati, "A methodology for the design and deployment of distributed cyber-physical systems for smart environments," *Future Generation Computer Systems*, vol. 109, pp. 420–430, 2020.
- [6] B. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, "Fog/edge computing-based iot (feciott): Architecture, applications, and research issues," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4118–4149, 2018.
- [7] S. Li, Q. Ni, Y. Sun, G. Min, and S. Al-Rubaye, "Energy-efficient resource allocation for industrial cyber-physical iot systems in 5g era," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2618–2628, 2018.
- [8] M. Gushev, "Dew computing architecture for cyber-physical systems and iot," *Internet of things*, vol. 11, p. 100186, 2020.
- [9] K. D. Singh and S. K. Sood, "5g ready optical fog-assisted cyber-physical system for iot applications," *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 2, pp. 137–144, 2020.
- [10] A. Razaque, F. Amsaad, M. J. Khan, S. Hariri, S. Chen, C. Siting, and X. Ji, "Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain," *IEEE Access*, vol. 7, pp. 168774–168797, 2019.
- [11] Z. Jiang, M. Pajic, and R. Mangharam, "Cyber-physical modeling of implantable cardiac medical devices," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 122–137, 2011.
- [12] K.-K. R. Choo, M. M. Kermani, R. Azarderakhsh, and M. Govindarasu, "Emerging embedded and cyber physical system security challenges and innovations," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 235–236, 2017.
- [13] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.
- [14] J. Fink, A. Ribeiro, and V. Kumar, "Robust control for mobility and wireless communication in cyber-physical systems with application to robot teams," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 164–178, 2011.
- [15] M. Amir and T. Givargis, "Pareto optimal design space exploration of cyber-physical systems," *Internet of things*, vol. 12, p. 100308, 2020.
- [16] C. Wu, W. Pan, G. Sun, J. Liu, and L. Wu, "Learning tracking control for cyber-physical systems," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 9151–9163, 2021.
- [17] D. Wang, N. Zhao, B. Song, P. Lin, and F. R. Yu, "Resource management for secure computation offloading in software-defined cyber-physical systems," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 9294–9304, 2021.
- [18] T. Paul, J. W. Kimball, M. Zawodniok, T. P. Roth, B. McMillin, and S. Chellappan, "Unified invariants for cyber-physical switched system stability," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 112–120, 2013.
- [19] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control*, vol. 58, no. 11, pp. 2715–2729, 2013.

- [20] Z. Guo, Y. Zhang, X. Zhao, and X. Song, "Cps-based self-adaptive collaborative control for smart production-logistics systems," *IEEE transactions on cybernetics*, vol. 51, no. 1, pp. 188–198, 2020.
- [21] G. Schirner, D. Erdogmus, K. Chowdhury, and T. Padir, "The future of human-in-the-loop cyber-physical systems," *Computer*, vol. 46, no. 1, pp. 36–45, 2013.
- [22] W. Li, W. Meng, C. Su, and L. F. Kwok, "Towards false alarm reduction using fuzzy if-then rules for medical cyber physical systems," *IEEE Access*, vol. 6, pp. 6530–6539, 2018.
- [23] R. M. Sandoval, A.-J. Garcia-Sanchez, and J. Garcia-Haro, "Improving rssi-based path-loss models accuracy for critical infrastructures: A smart grid substation case-study," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2230–2240, 2017.
- [24] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 27–40, 2017.
- [25] L.-A. Tang, J. Han, and G. Jiang, "Mining sensor data in cyber-physical systems," *Tsinghua Science and Technology*, vol. 19, no. 3, pp. 225–234, 2014.
- [26] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2011.
- [27] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-cps: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88–95, 2015.
- [28] J. J. Song and J. C. Johnson, "Method and apparatus of increasing speech intelligibility in noisy environments," Oct. 2 2012, uS Patent 8,280,730.
- [29] M. R. Ram, K. V. Madhav, E. H. Krishna, N. R. Komalla, and K. A. Reddy, "A novel approach for motion artifact reduction in ppg signals based on as-lms adaptive filter," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 5, pp. 1445–1457, 2011.
- [30] V. Kılıç, M. Barnard, W. Wang, and J. Kittler, "Audio assisted robust visual tracking with adaptive particle filtering," *IEEE Transactions on Multimedia*, vol. 17, no. 2, pp. 186–200, 2014.
- [31] A. Razaque and K. Elleithy, "Least distance smart neighboring search (ldsns) over wireless sensor networks (wsns)," in *2013 European Modelling Symposium*. IEEE, 2013, pp. 549–554.



Abdul Razaque is a Professor in the Department of Computer Engineering at International Information Technology University, Almaty, Kazakhstan. He received a Ph.D. degree in Computer Science & Engineering from the University of Bridgeport, USA, in 2014. His research interests include wireless sensor networks and cloud computing security. He served on the Editorial Board for several international journals, including serving as the Editor-in-Chief for International Journal for Engineering and Technology (IJET), Singapore.



Fathi Amsaad is an Assistant Professor at the School of Information Security and Applied Computing (SISAC), Eastern Michigan University (EMU). He earned a Ph.D. degree in Engineering from the University of Toledo (UT), Ohio, in 2017. His research expertise lies in smart and cyber physical systems security (SCPSS) areas. He served on the Editorial Board for several peer-review journals as a guest editor, an IEEE conferences track/session chair, and a reviewer of many conferences and peer-reviewed IEEE/ACM journals.



Musbah Abdulgader is an Assistant Professor at Norfolk State University. He received his Ph.D. degree from the Electrical Engineering and Computer Science Department, The University of Toledo, Toledo, OH, USA. His research interests include swarm intelligence, evolutionary algorithms, optimization techniques, computational intelligence systems, neural networks, fuzzy systems, wireless sensor networks, security, and their applications. He is Active IEEE member.



Bandar Alotaibi received a B.Sc. degree (Hons.) in Computer Science-Information Security and Assurance Emphasis from the University of Findlay, USA, an M.Sc. degree in Information Security and Assurance from Robert Morris University, USA, and a Ph.D. degree in Computer Science and Engineering from the University of Bridgeport, USA. He is currently an associate professor with the Department of Information Technology, University of Tabuk. His research interests include network security, mobile communications, the IoT, and wireless networks.



Fawaz Alsolami received the M.A.Sc in Electrical and Computer Engineering from University of Waterloo, Canada, in 2008, and his Ph.D. degree in Computer Science from KAUST University, Thuwal, Saudi Arabia, in 2016. Fawaz joined computer science at King Abdulaziz University as an assistant professor of Computer Science. His research interests are artificial Intelligence, machine learning and data Mining, and combinatorial optimization. He has been the chairman of the Computer Science department at King Abdulaziz University since 2018.



Duisen Gulsezim has received her BS degree in Computer Engineering and Security from International IT University, Almaty Kazakhstan. Her research interests include cybersecurity, cryptographic methods, and design of secure biometric systems.



Saraju P. Mohanty (Senior Member, IEEE), received the bachelor's degree (Honors) in electrical engineering from the Orissa University of Agriculture and Technology, Bhubaneswar, in 1995, the masters degree in Systems Science and Automation from the Indian Institute of Science, Bengaluru, in 1999, and the Ph.D. degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2003. He is a Professor with the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science Foundations (NSF), Semiconductor Research Corporation (SRC), U.S. Air Force, IUSSTF, and Mission Innovation. He has authored 400 research articles, 4 books, and invented 7 granted/pending patents. His Google Scholar h-index is 44 and i10-index is 168 with 8000 citations. He is a recipient of 13 best paper awards, Fulbright Specialist Award in 2020, IEEE Consumer Electronics Society Outstanding Service Award in 2020, the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, and the PROSE Award for Best Textbook in Physical Sciences and Mathematics category in 2016. He has delivered 11 keynotes and served on 12 panels at various International Conferences. He has been the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine (MCE)" during 2016–2021 and serves on the editorial board of 6 journals/transactions.



Salim Hariri Salim Hariri (Senior Member, IEEE) received the M.Sc. degree from Ohio State University in 1982, and the Ph.D. degree in computer engineering from the University of Southern California in 1986. He is a Professor with the Department of Electrical and Computer Engineering, University of Arizona, and the Director of the NSF Center for Cloud and Autonomic Computing. His current research focuses on autonomic computing, cybersecurity, cyber resilience, secure critical infrastructures, and cloud security.