Ubiquitous Computing & Security Laboratory

A Mobility-Aware Human-Centric Cyber-Physical System for Efficient and Secure Smart Healthcare

Abdul Razaque , Fathi Amsaad , Musbah Abdulgader , Bandar Alotaibi , Fawaz Alsolami , Duisen Gulsezim,Saraju P. Mohanty , and Salim Hariri

Professor: Park Jong Hyuk

Presented By: Than Than Swe

24 April 2023

SEOULTECH
SEOUL NATIONAL UNIVERSITY OF SCIENCE & TECHNOLOGY

Contents

I. INTRODUCTION

II. RESEARCH PROBLEMS AND CONTRIBUTIONS

III. RELATED WORK

IV. COMPONENTS OF THE PROPOSED MODEL FOR CPS

V. PROBLEM FORMULATION

A. Energy Constraints

B. Flow Constraints

C. Workload Constraints

D. Timing Constraints

E. Privacy Preservation Constraints

F. Quality of Service (QoS) Constraints

Contents

VI. DEVELOPMENT PHASE OF THE PROPOSED MODEL

1) Sensor Advertisements Phase
2) Mobile Sensor Recruitment And Selection Phase
3) Load Balancing Phase
4) Transmission Guaranteed Phase
5) Privacy and Data-Sharing Phase

VII. EXPERIMENTAL RESULTS AND DISCUSSION

VIII.CONCLUSION AND FUTURE WORK

A. Conclusion

B. Future Work

C. Opinion

I. INTRODUCTION

- CYBER–PHYSICAL system (CPS) devices, i.e., sensors, actuators, microprocessors, etc., are gaining importance in IoT applications**.**
- CPS systems combine efficient and real-time applications while focusing on security, energy, mobility, health, and industry.
- 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.
- Using massive networks of sensors and actuators, large environmental areas of CPS can be accessed and revolutionized in real-time.
- 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.
- As an application of CPS, the interconnection between power control systems and edge/fog IoT-based systems can be efficiently analyzed.

Cont.

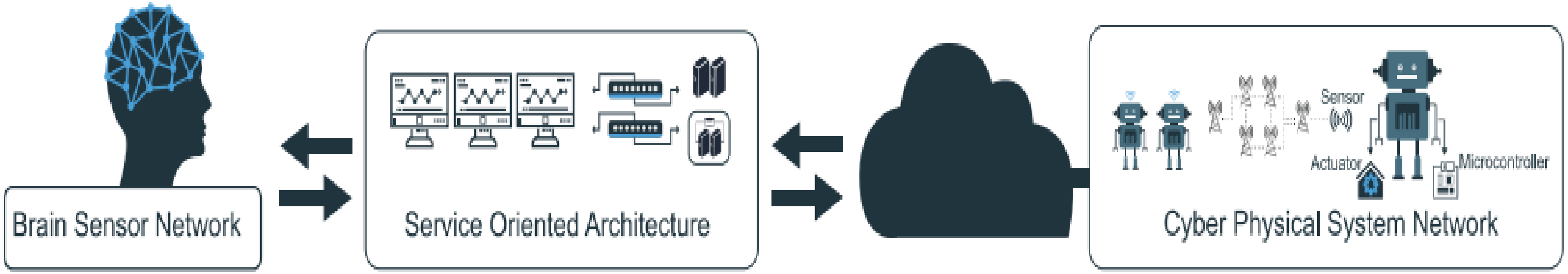


Fig. 1. Overview of the CPS domain.

- Fig. 1 shows an overview of the CPS domain. CPS mobile nodes can detect information over a large wireless area and send it back to the base station (BS) for analysis.
- CPS wireless communication development includes interconnected robots, autonomous vehicles, vehicular ad hoc networks (VANETs), smart grids, etc., creating ideal CPS environment mobile nodes.
- 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.

II. RESEARCH PROBLEMS AND CONTRIBUTIONS

- Despite the aforementioned benefits of the CPSs, many challenges still arise in CPS**s**.
- For example, current mobility systems require CPS sensors during their communications to efficiently communicate sensitive information related to humans, machines, sensors, etc.
- For a balanced throughout and efficient human-centric transmission process, the Quality-of-Service (QoS) and performance issues, including reliability.
- 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, they are vulnerable to new cyberattacks that need to be addressed before they are widely deployed.
- If a CPS mobile node fails to function due to a CPS attack, the whole system becomes comprised and untrusted.
- 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.

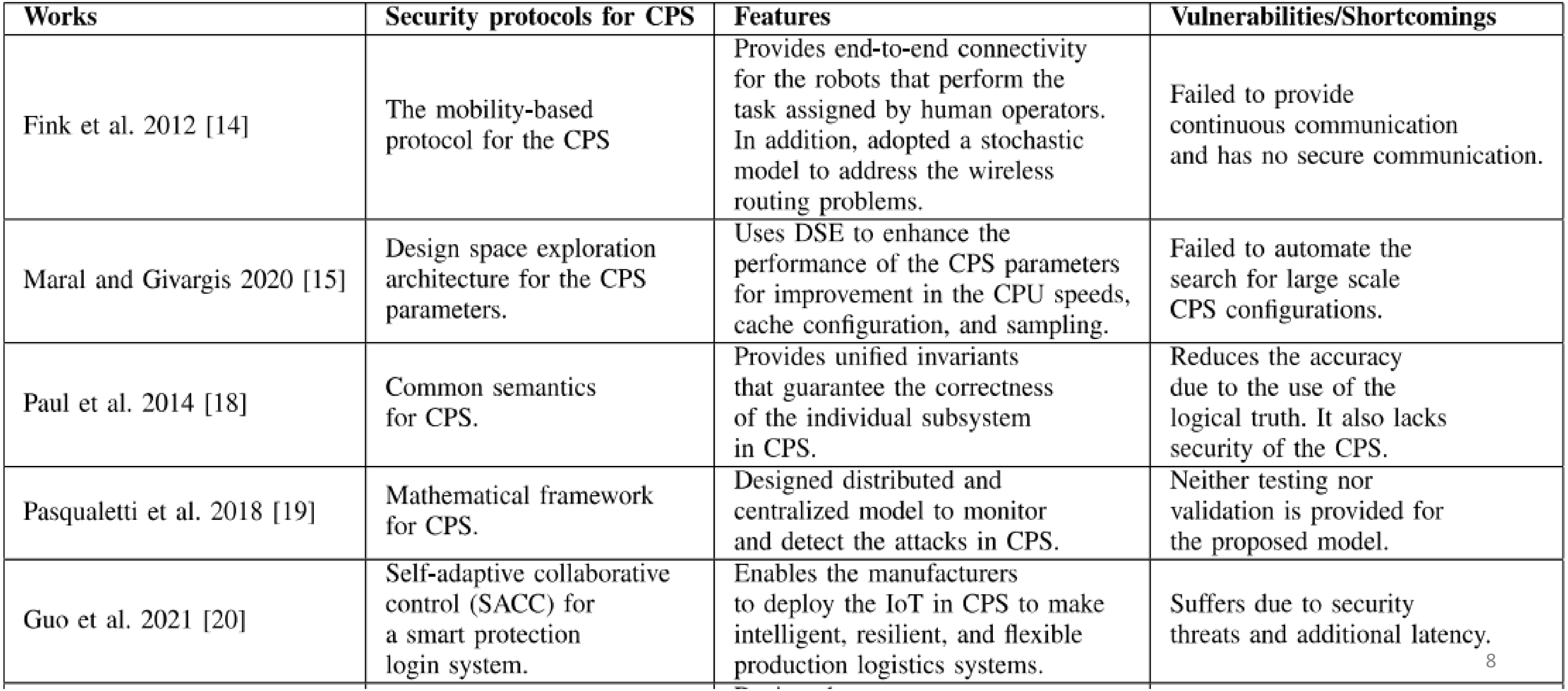
Cont.

The main contributions of this work are as follows.

1. An **efficient and privacy-aware secure human-centric mobility-aware (SHM) 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.
2. 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.
3. 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.
4. 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.

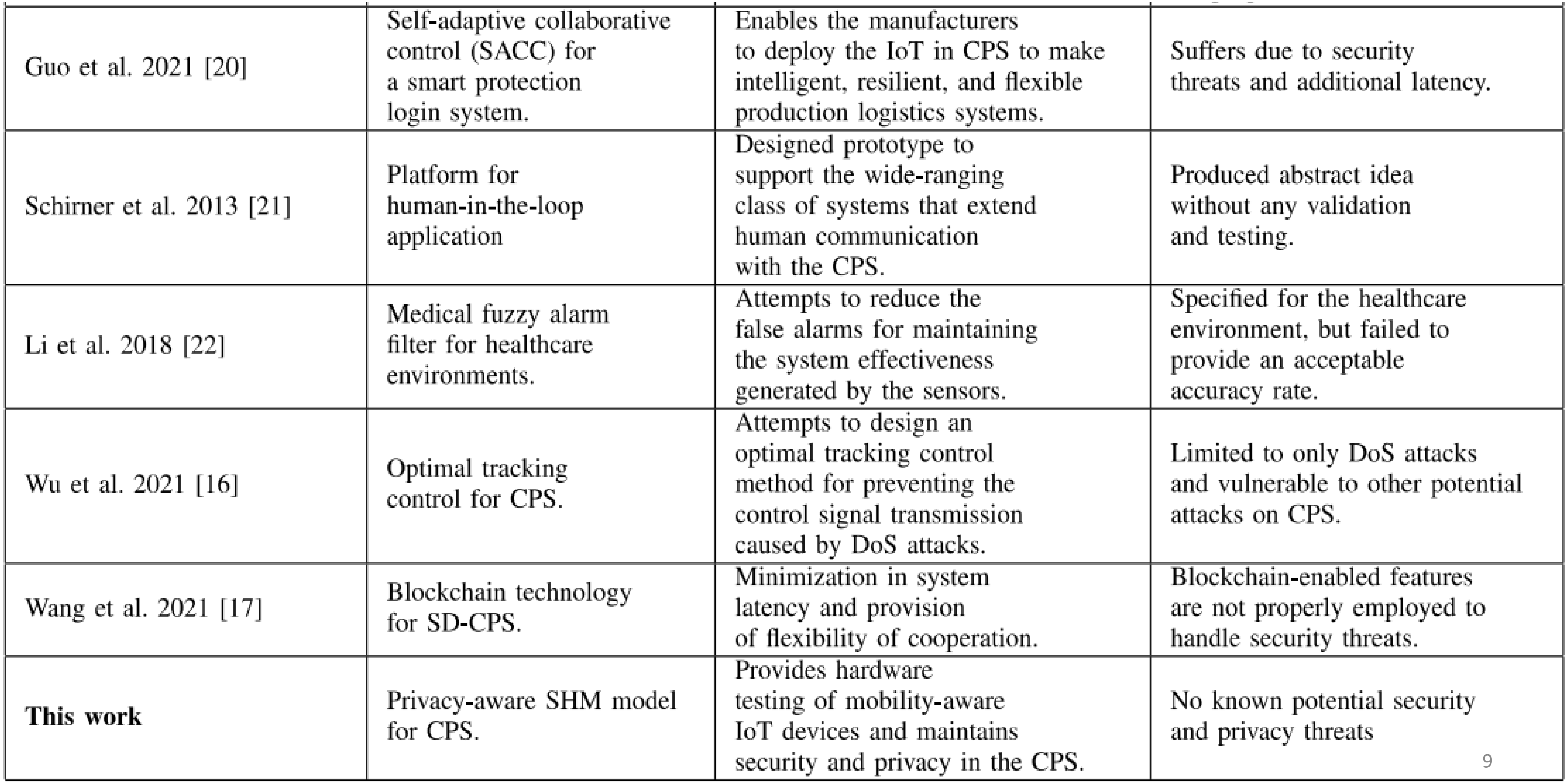
III. RELATED WORK

Table 1
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.

Cont.



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

Cont.

- Table I summarizes the **contemporary related work for handling security in CPS**.
- 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**.
- The proposed Software Defined Network Cyber Physical System (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.
- 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 CPSs mobility is proposed to enhance the resilience and flexibility of manufacturing discrete systems.
- 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.
- 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.
- 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.
- A novel human-centric mobility-aware system model involves **data acquisition**, **data management**, and **IoT features**. The system model comprises four parts, as shown in Fig. 2.
  - **Brain Sensor Network (BSN)**
  - **Data Processor**
  - **Secure Service-Oriented Architecture (SSOA)**
  - **Data Management Domain**

Cont.

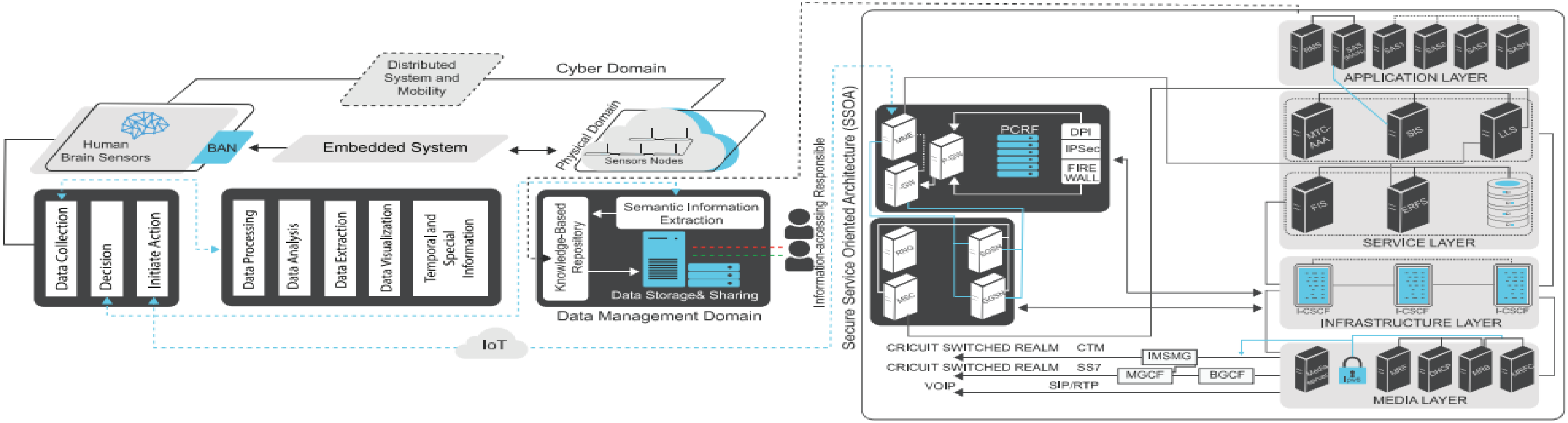


Fig. 2. Framework of the proposed human-centric mobility-aware (SHM) CPS model.

- 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).
- Their IoT-based CPS mobility model is human-centric and covers **two types of sensors**: 1) mobile and 2) 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**.

Cont.

- The stationary sensors are fixed to monitor sleeping patients, whereas mobile sensors monitor moving patients to **gather da**ta and store it on **cloud servers**.
- The model uses BSN, a **brain sensor network**, 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 SSOA**. The SSOA results are reported to the BS 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.
- The brain sensors are attached to the head of the patient. BSN is a **wireless sensor network** (**WSN**) 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.

Cont.

- 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 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: 1) **data collection**; 2) **decision**; and 3) **action initiation.**
- Based on the obtained results, **a decision** is made to **store the information on cloud servers using semantic information extraction.**
- There are two types of servers in the application layer: 1) **a secure authentication server** and 2) **a role-based management server.**
- A secure authentication server is **a unique authentication process** that can protect the user's authentication. It 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.

Cont.

- 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
  1. **Machine-type Communication-authentication, Authorization, And Accounting (MTC-AAA) server**
  2. **Subscriber Information Server (SIS)**
  3. **Location Locator Server (LLS)**
  4. **Feature Integrating Server (FIS)**
  5. **Efficient Route-finding Server (ERFS)**
  6. **Mobile Profile Server (MPS) 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.**

Cont.

- 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**:
  1. **Proxy-CSCF (PCSCF)**
  2. **Serving-CSCF (S-CSCF)**
  3. **Interrogating CSCF (I-CSCF)**
- 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 SIES.

Cont.

- The **SIES** then analyzes the decisions to determine these decisions and whether they need to be stored in the knowledge-based repository.
- The proposed model offers a **visual method** for users to obtain vital information efficiently and rapidly.
- **Cloud-based servers** are adopted as part of thier 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 authorized users, 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

- The authors assume that the SHM model for the CSP is denoted by the interrelated components and composition rules R that are picked from the library (collection) ∀γ.
- Each component involves **a set of attributes** that capture both **functional**, **extra functional,** 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 Tv. 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 by a **specific type τ** and terminal variables including its functionality (tasks or roles).
- Thus, the **overall performance of the SHM model for the CSP SC** can be computed as

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

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 Ct is the total number of components of the system.

Cont.

A. Energy Constraints

Each component and the 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

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

where Ex is the energy of component (C)i and E∼ xy is the consumed energy of the connection for forwarding the signals (or data).

B. Flow Constraints

Assume that flow originates from the source (human) and is transferred to cloud servers through intermediate components and connections. ***The input flow rate Fin*** at Csr i can be expressed as

$$F_{in} = \sum_{x=1}^{|C|} F_r C_i^{sr}.$$

The output flow rate F_{out} for all of the connections can be computed as

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

Where F_r is the flow rate through the connection.

Cont.

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 ci can be determined as

$$c_i = \sum_{x=1}^{|C|} \left(F_r c_y\right) \leq \partial_y .$$

D. Timing Constraints

It refers to the time needed to collect the signal from the source (human) and send it to cloud servers. The entire time of the CPS system T∗ given by

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

where dc is the delay of the component, and BT v is a binary variable that assumes a value of 1 if cx ∈ T; otherwise, it is 0. Thus, the binary variable can be computed as

$$B_v^{\mathbb{T}} = 1 \text{ if } f \sum_{y=1}^{I} \left(P_{xy}^{\mathbb{T}}\right) \vee \left(P_{yx}^{\mathbb{T}}\right)$$

where PT xy is the all possible connections from the source to the destination, and PT yx is the all possible connections from cloud servers to the source (human).

Cont.

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.
- Let the privacy violation of the cloud servers be a Pv, in which the **signal/data temptation** occurs; then, the acquired information at the cloud servers **is not fully confidential.**
- 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 Ti be a threat that affects the component cx which leads to the compromised information.
- Then, privacy preservation no longer remains for the component. Thus, the privacy violation in the cloud servers can recursively be determined as

$$P_{vx} = T_i \bigcup \bigcap_{1 \leq y \leq |c|, eyx \neq 0} P_{vy}$$

Here yx is the yth row and xth column element of the adjacency matrix e of the CPS model. In other words, component cx is attacked when either an attack is generated by an outsider adversary or induced through a malicious insider.

Cont.

F. Quality-of-Service (QoS) Constraints

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

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

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 Wsn from Pn patients is associated with the number of allotted components involved in the data process given by

$$(\mathrm{DR})_{xy} = \sum_{c_i \in C_t} \left(\mathrm{Co}_{xy}^{c_i}\right) F_r \quad \forall x \in X, y \in Y$$

Here, $\mathrm{Co}_{xy}^{c_i}$ is an associated connection between the two components.

They observe that the more components are assigned to the source, the higher the data rate that can be attained. Thus, the delay for Wsn(**d**) can be calculated as

$$W_{sn}(d) = \frac{D_s}{(\mathrm{DR})_{xy}}.$$

Assume that the data received through the BAN from the source (human) are distributed with the associated **WSN** with a fixed probability. The data influx rate in WSN is flowing successfully.

VI. DEVELOPMENT PHASES OF THE PROPOSED MODEL

- The proposed **CPS 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: 1) mobile and 2) 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 BS.
- 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:

1**) Sensor Advertisements Phase**

2) Mobile Sensor Recruitment And Selection Phase

3) Load-balancing Phase

4) Transmission Guaranteed Phase

5) Privacy and Data-Sharing Phase.

Cont.

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).
- 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 BS.
- The mobility of mobile sensors is controllable. The sensors can communicate within the communication range using a multi-hop process. The remaining energy of the sensors (RESs) defines the RLS.
- 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.

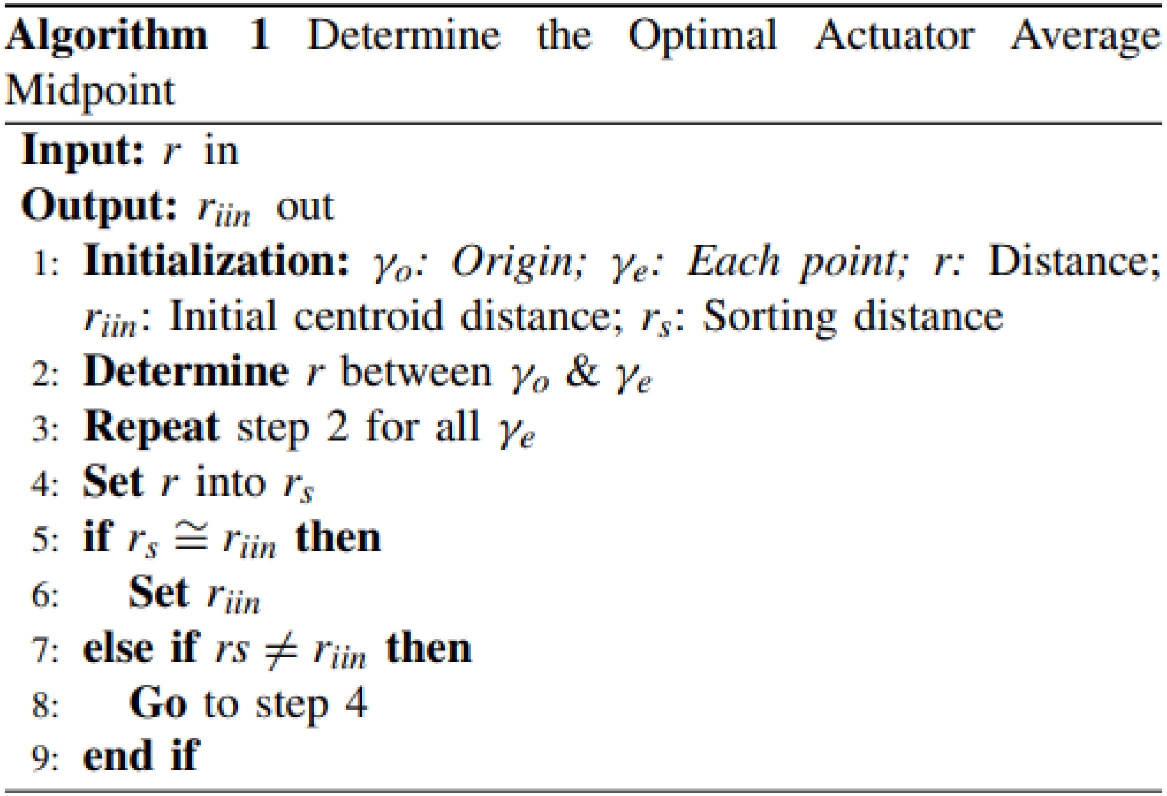
Cont.

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.

Cont.

- To **avoid back transmissions**, an average midpoint of the actuator should be determined.
- Therefore, Algorithm 1 is employed to determine the actuator that should be closer to the 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).



Algorithm 1 Determine the Optimal Actuator Average Midpoint

```
Input: $r$ in
Output: $r_{iin}$ out
1: Initialization: $\gamma_o$: Origin; $\gamma_e$: Each point; $r$: Distance;
   $r_{iin}$: Initial centroid distance; $r_s$: Sorting distance
2: Determine $r$ between $\gamma_o$ & $\gamma_e$
3: Repeat step 2 for all $\gamma_e$
4: Set $r$ into $r_s$
5: if $r_s \cong r_{iin}$ then
6:     Set $r_{iin}$
7: else if $rs \neq r_{iin}$ then
8:     Go to step 4
9: end if
```

Cont.

- 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 and 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 the worst case is O(log n).

Cont.

- Based on the midpoint, the sensor decides to send the data either to the actuator or the BS, 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 BS compared to Actuator-2.
- As a result, additional energy is consumed, and the delay is extended. Thus, the proposed algorithm is applied to determine the midpoint to reduce the delay and improve energy efficiency.

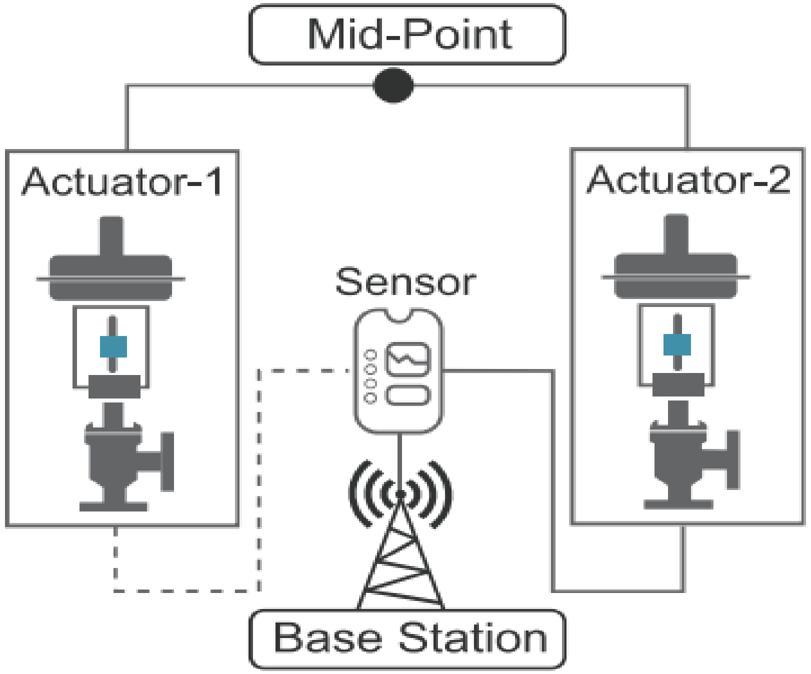


Fig. 3. Average midpoint of the optimal actuator.

Cont.

The **sensor pervasive mobility** (SPM) model adding a layer of mobile sensors (patients) between the accessing points and the sensor layers is shown in Fig. 4.

1) **Sensor Layer**: It 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.

2) **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.

3) **Connective Layer**: Servers with access to the Internet with strengthened power, storage, and processing capabilities.

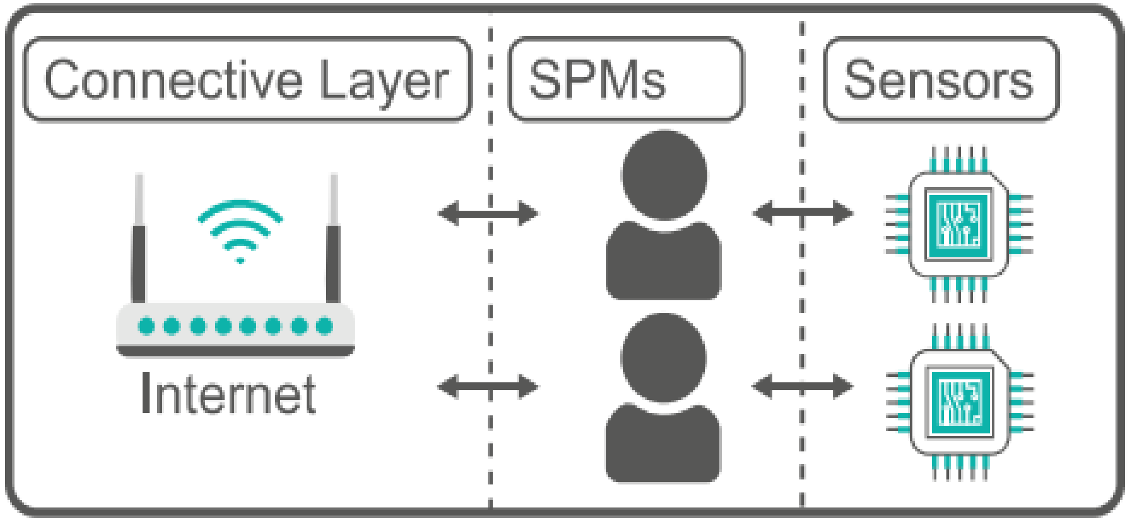


Fig. 4. Three layers of the SPM model.

Cont.

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.**

C. Load-Balancing Phase

- Once **the actuator** completes the sensors’ borrowing process, **then the BS initiates its execution process**.
- The BS sends the query to the exciting area using **the shortest pa**th. The sensor first receives the query request that sets its priority = φ and then forwards the query process inside the region to let other sensors know that the BS 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.**

Cont.

D. Transmission Guaranteed Phase

- This phase is more critical because it **includes two types of sensors**:

  1) static and

  2) 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.
- This 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.**

Cont.

E. Privacy and Data-Sharing Phase

- This phase provides a secure method for sharing the data and delivery process among the sensors.
- Assume that the sensor shares$\Delta\varrho$ out of the forwarded data, such that Δd required blocks to regenerate the data.
- Thus, each sensor is loaded with the same $\Delta\varrho \times \Delta d$ matrix $V = [x_i, q]$,
- When a sensor is triggered, sensor k collects its reading in a core buffer of length Δd The block reading can be expressed as follows: $B_r = [b_{k,1}, b_{k,2}, b_{k,3}, \ldots, b_{k,\Delta d}]$.
- 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:

$$S = [b_{k,1}, b_{k,2}, b_{k,3}, \ldots, b_{k,\Delta d}] \times [x_i, q].$$

When the actuator receives $\Delta\varrho$ shares, it is in the position of regenerating the data. Assume that it receives Sk = [Sk,q1, Sk,q2,Sk,q3, …., Sk,q Δd . Thus, the reading can be obtained by resolving

$$S_k = \begin{cases} b_k, 1x_1, q_1 + b_k, 2x_2, q_2 + b_k, 3x_3, q_3 + \cdots \\ \quad +b_k, \Delta d x_{\Delta d}, q1 = s_{k,q1} \\ bk, 1x_1, q_2 + b_k, 2x_2, q_2 + b_k, 3x_3, q_3 + \cdots \\ \quad +b_k, \Delta d x_{\Delta d}, q2 = s_{k,q2} \\ b_k, 1x_1, q_3 + b_k, 2x_2, q_2 + b_k, 3x_3, q_3 + \cdots \\ \quad +b_k, \Delta d x_{\Delta d}, q3 = s_{k,q3} \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ b_k, 1x_1, q\Delta d + b_k, 2x_2, q\Delta d + b_k, 3x_3, q\Delta d + \cdot\cdot \\ \quad +b_k, \Delta d x_{\Delta d}, q\Delta d = s_{k,q\Delta d} \end{cases}$$

VII. EXPERIMENTAL RESULT AND DISCUSSION

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

A. Experimental Setup and Model Prototype

- The proposed SHM consists of SSOA, 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.
- 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 field-programmable gate arrays (FPGAs).
- Figs. 6 and 7 show a proof of concept of the prototype of the proposed secure SHM CPS model and an implementation instance of the prototype; respectively.

Cont.

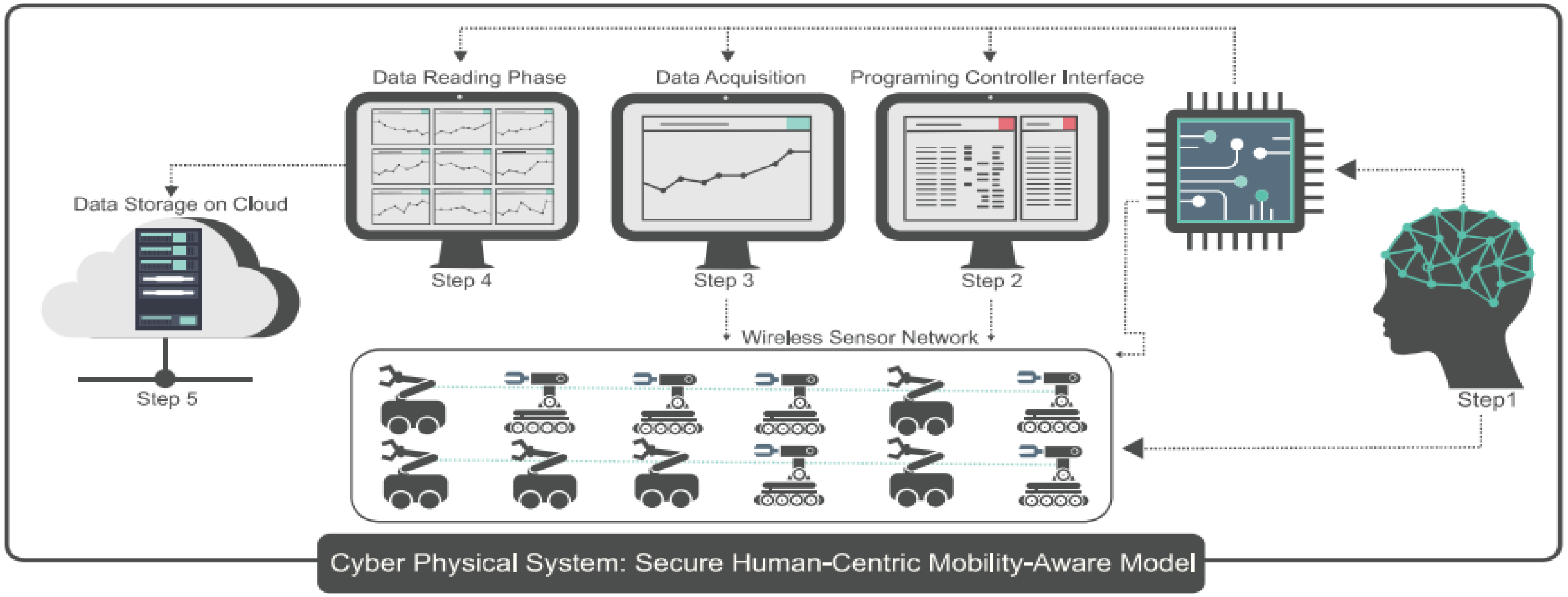


Fig. 6. Proposed prototype for the SHM CPS model.

As seen in the figures, the prototype involves hardware and software features.

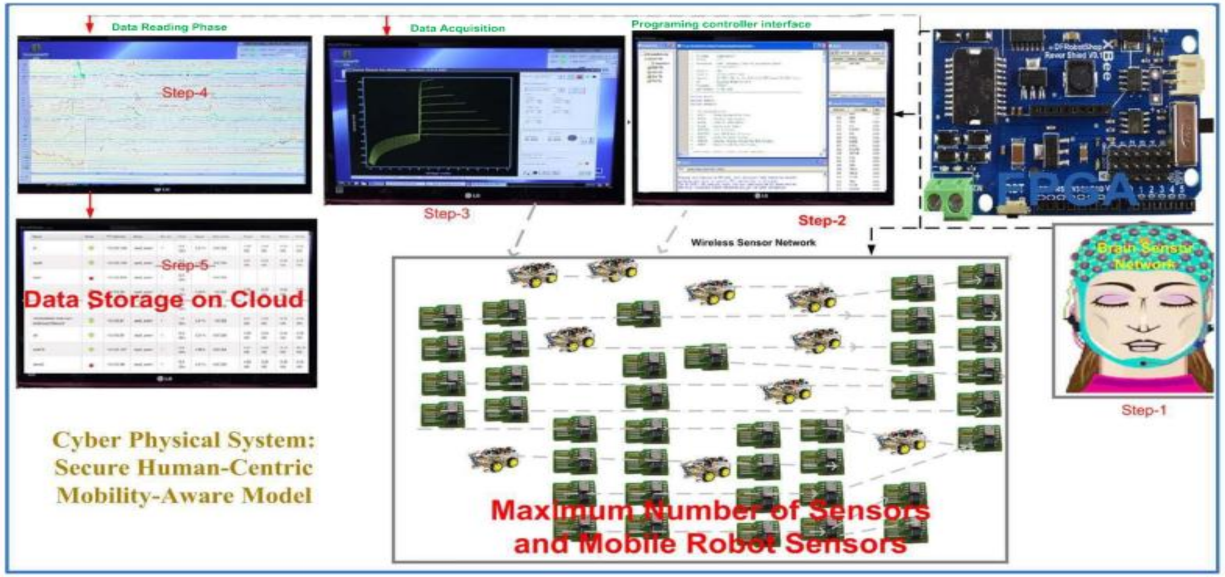
The **hardware part** is based on an

1) **FPGA-based real-time clock (RTC)** that provides flexible parallelism and

2) Microcontrollers are embedded in the FPGA to obtain **energy efficiency and reusability**.

Cont.

- 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.



Data Reading Phase
Data Acquisition
Programing controller interface
Step-4
Step-3
Step-2
Srep-5
Data Storage on Cloud
Wireless Sensor Network
FPGA
Brain Sensor Network
Step-1
Cyber Physical System: Secure Human-Centric Mobility-Aware Model
Maximum Number of Sensors and Mobile Robot Sensors

Fig. 6. Proposed prototype for the SHM CPS model.

Cont.

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:

  1) average throughput;

  2) hop-by-hop delay;

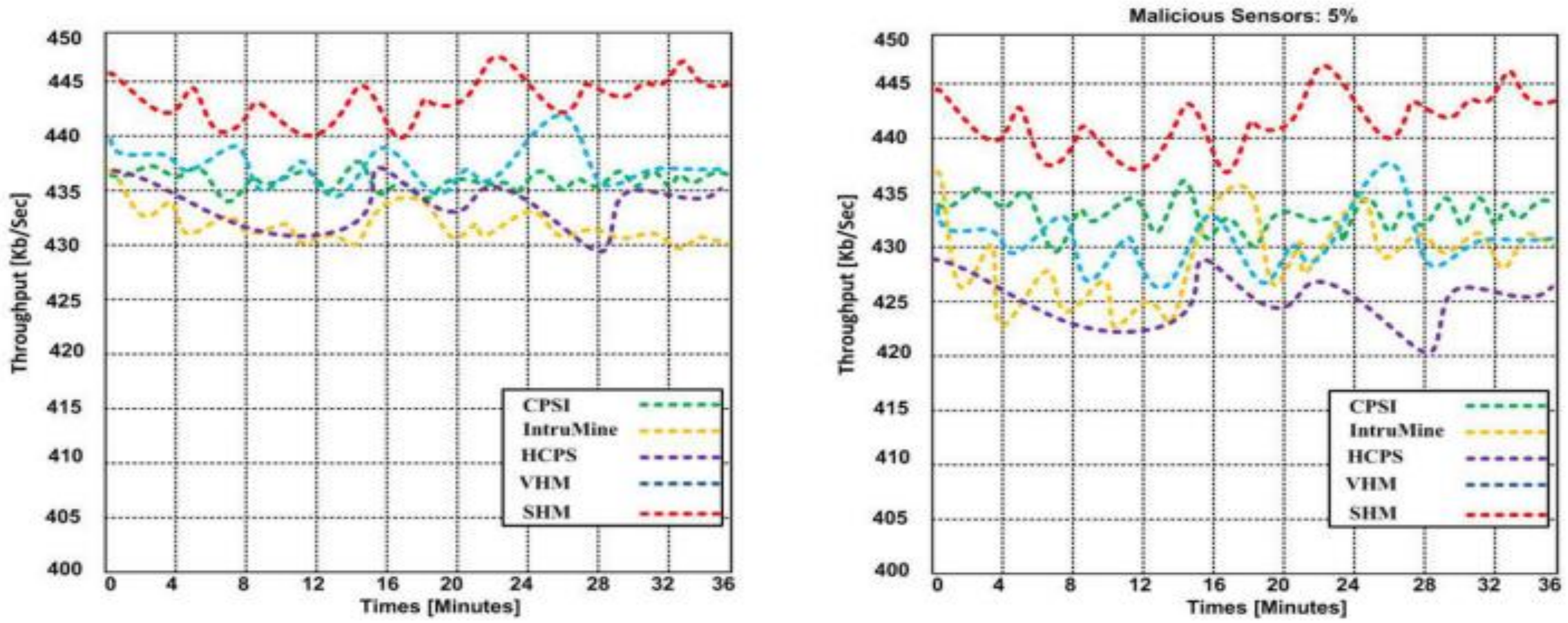
  3) sensors' lifetime;

  4) energy consumption;

  5) 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.

Cont.



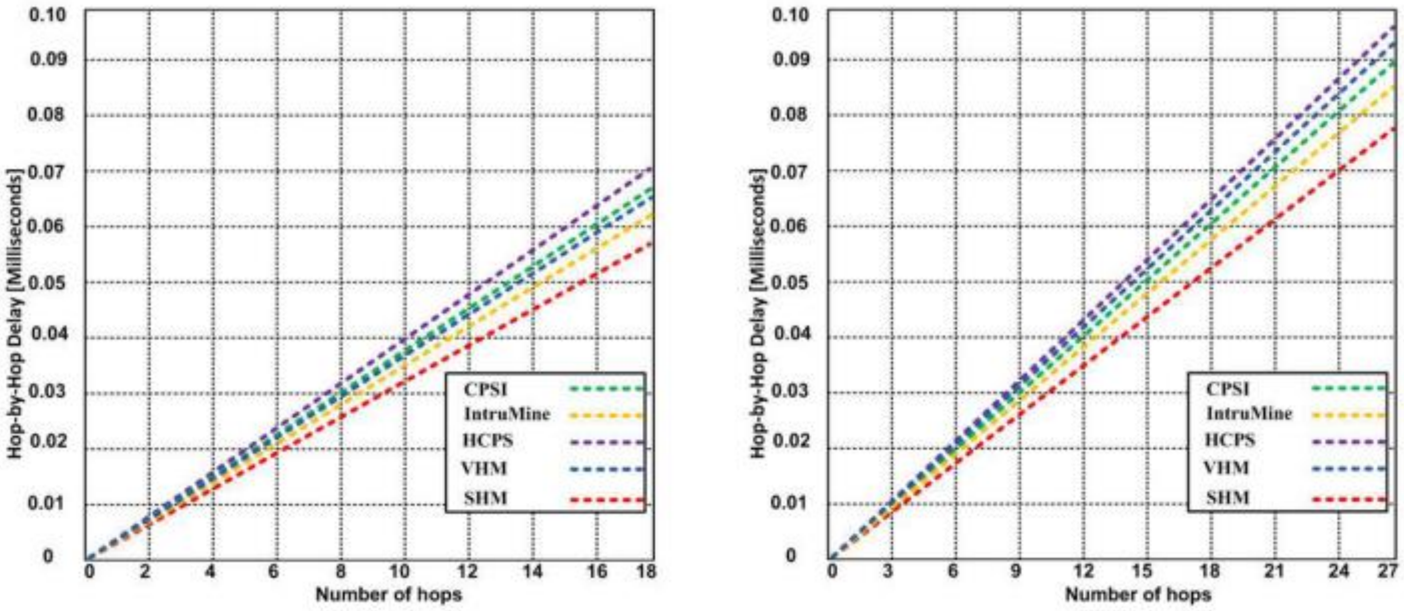
(a)   (b)

Fig. 8(a) and (b) indicate the tradeoff between the average throughput and the testing time, (a) without malicious sensors, and Fig. 8(b) with 5% of malicious sensors activated, respectively.

Fig. 8(a), the average throughput increases, and the system becomes more efficient and stable.

Cont.

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.

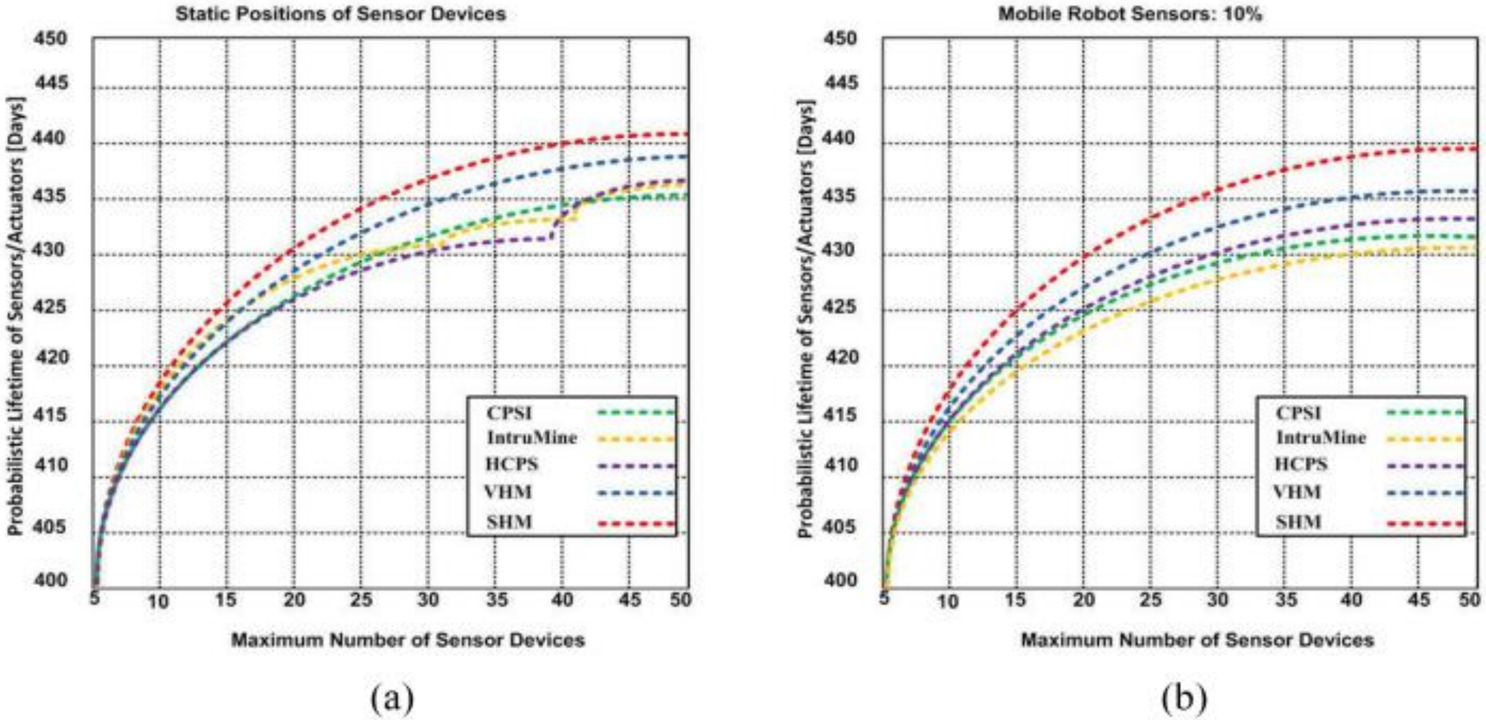


(c) (d)

Fig. 8. (c) and (d) positive correlation between the number of hops and the hop-by-hop delay.

Cont.

3) Sensors' Lifetime: Fig. 9 (a) and (b) indicate the tradeoff 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.



(a)

(b)

Fig. 9. (a) and (b) Lifetime of the network with sensors/actuators for the proposed SHM model and competing protocols.

Cont.

4) Reliability: It 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, whereas other competing models have 99.3%–99.44% reliability, as shown in Fig. 9(d).

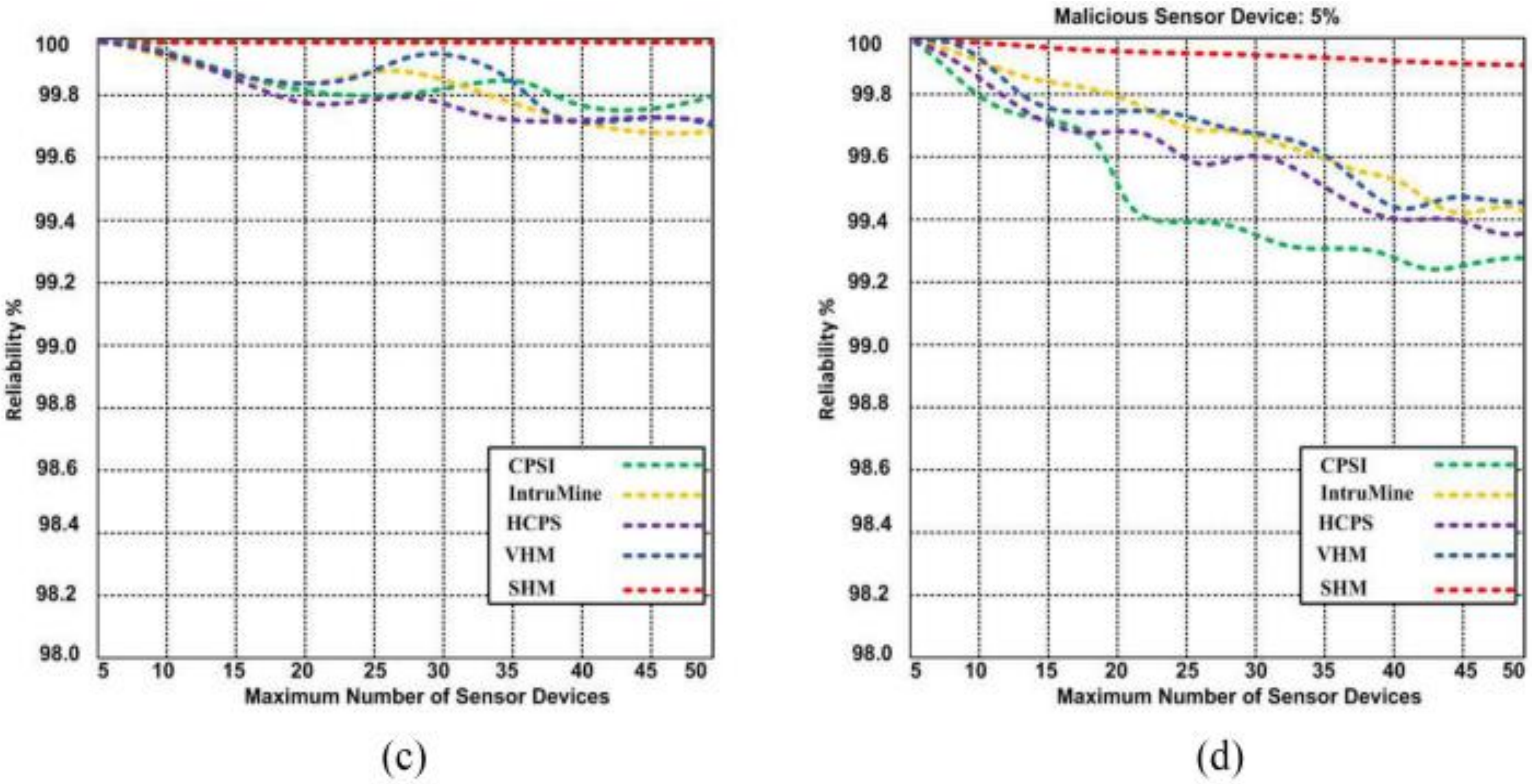
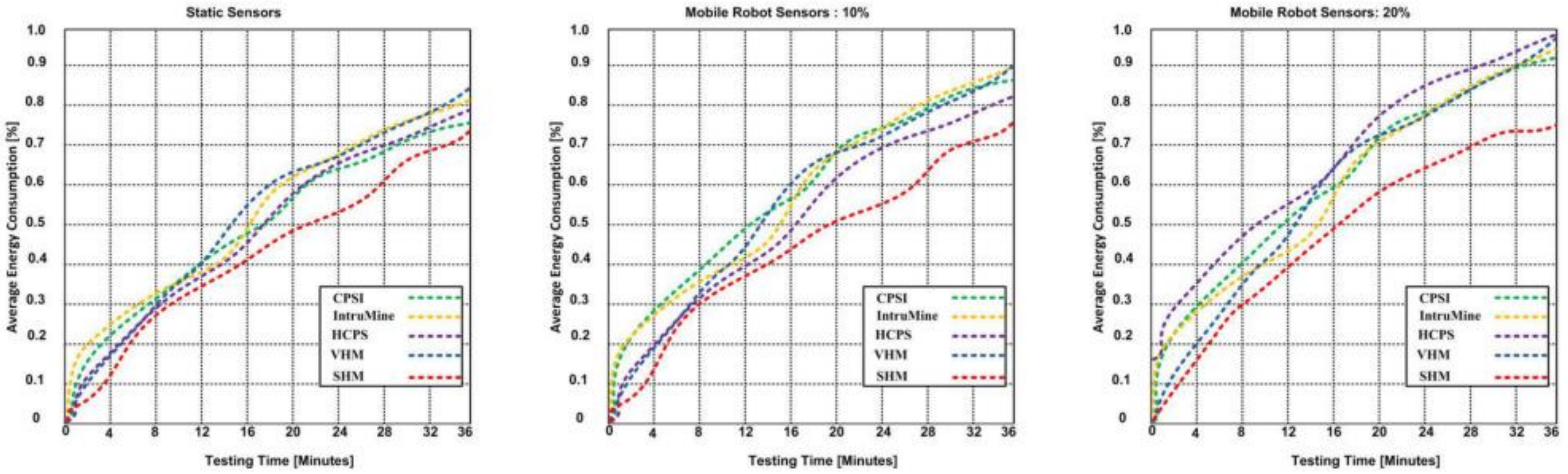


Fig. 9. (c) and (d) Reliability of the SHM model and other contending protocols: (c) without and (d) with 5% malicious sensors.

Cont.

C. Energy Consumption

Energy consumption refers to the energy that is consumed by IoT devices to accomplish tasks and actions.



(a) (b) (c)

Fig. 10(a) and (b) demonstrate the average energy consumption with 10% and 20% of mobile robot sensors activated. Fig. 10(c) explicitly indicates the better performance of the SHM model, as this paper's proposed SHM model consumed 0.72 J of energy throughout the testing process.

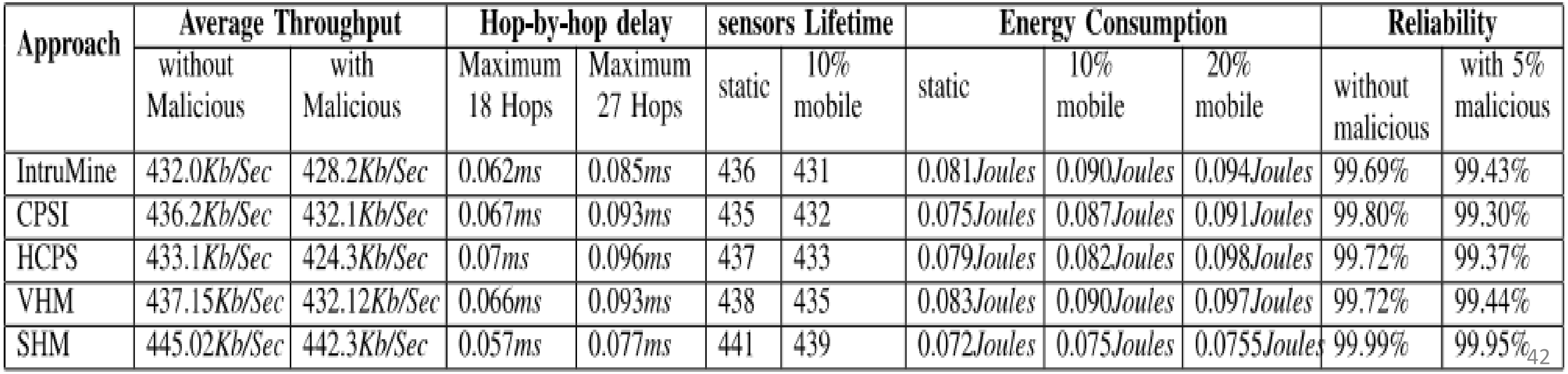
Cont.

D. Analytical Comparison

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

Table II

PERFORMANCE COMPARISON OF THE PROPOSED APPROACH WITH COMPETING APPROACHES

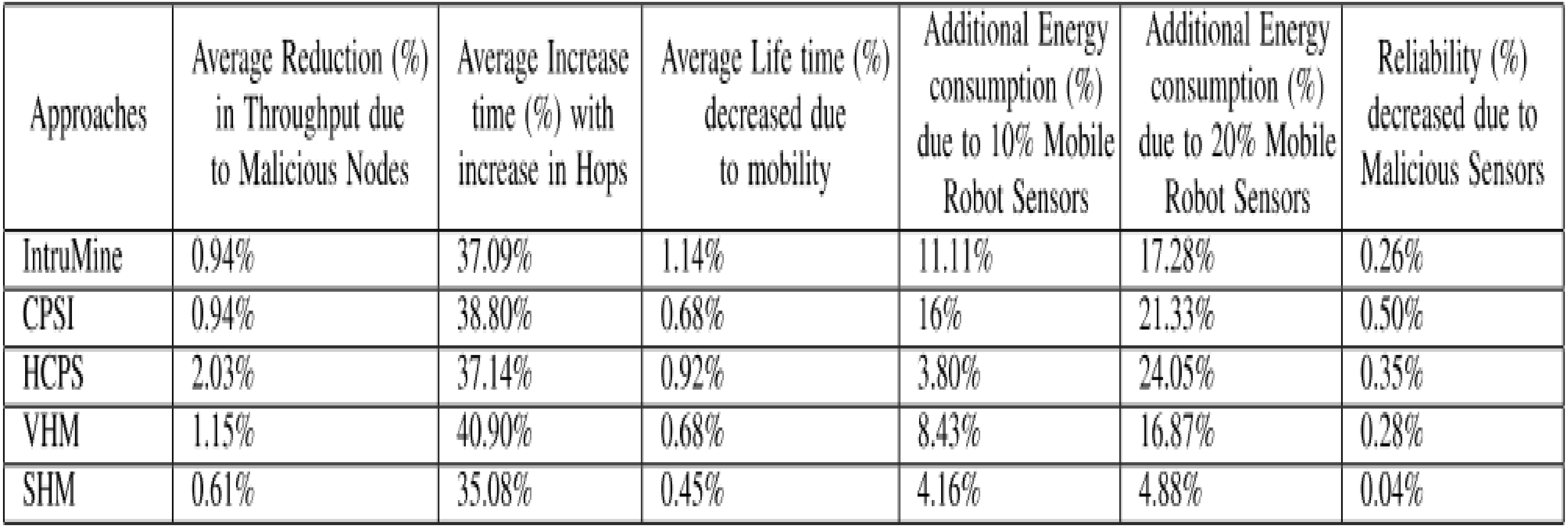


Approach	Average Throughput		Hop-by-hop delay		sensors Lifetime		Energy Consumption			Reliability	
	without Malicious	with Malicious	Maximum 18 Hops	Maximum 27 Hops	static	10% mobile	static	10% mobile	20% mobile	without malicious	with 5% malicious
IntruMine	432.0*Kb/Sec*	428.2*Kb/Sec*	0.062*ms*	0.085*ms*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

Cont.

Table III

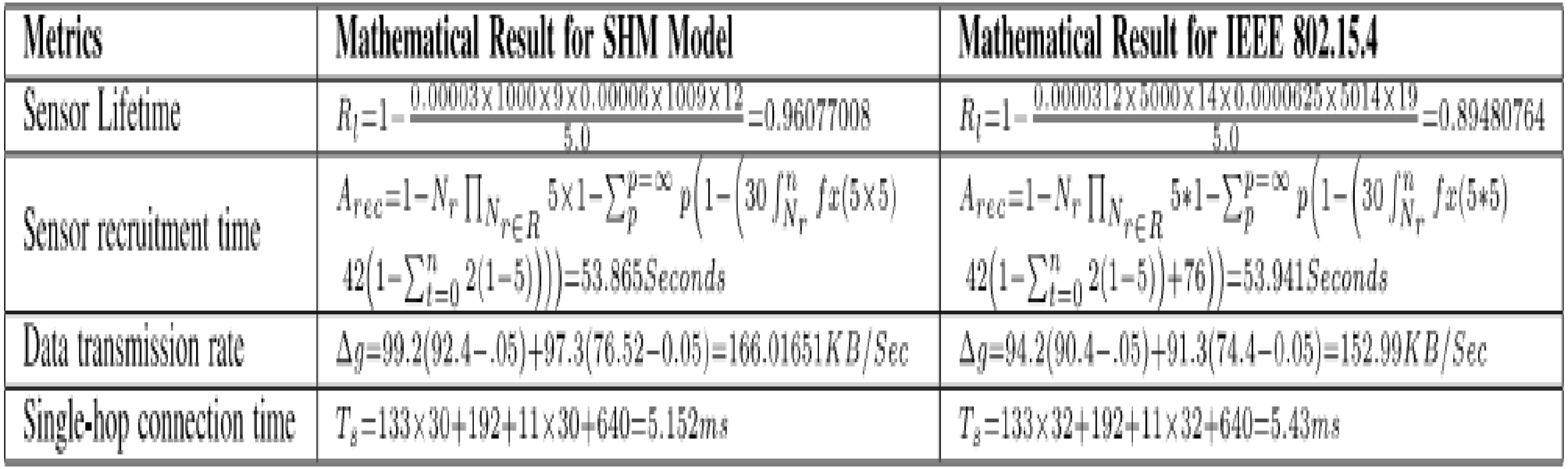
PERCENTAGE OF AVERAGE PERFORMANCE (%) OF THE PROPOSED SHM MODEL AND COMPETING APPROACHES



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%

Cont.

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	$R_l=1-\frac{0.00003\times1000\times9\times0.00006\times1009\times12}{5.0}=0.96077008$	$R_l=1-\frac{0.0000312\times5000\times14\times0.0000625\times5014\times19}{5.0}=0.89480764$
Sensor recruitment time	$A_{rec}=1-N_r\prod_{N_{r\in R}}5\times1-\sum_p^{p=\infty}p\Big(1-\Big(30\int_{N_r}^{n}fx(5\times5)$ $42\Big(1-\sum_{t=0}^{n}2(1-5)\Big)\Big)\Big)=53.865Seconds$	$A_{rec}=1-N_r\prod_{N_{r\in R}}5*1-\sum_p^{p=\infty}p\Big(1-\Big(30\int_{N_r}^{n}fx(5*5)$ $42\Big(1-\sum_{t=0}^{n}2(1-5)\Big)+76\Big)\Big)=53.941Seconds$
Data transmission rate	$\Delta g=99.2(92.4-.05)+97.3(76.52-0.05)=166.01651KB/Sec$	$\Delta g=94.2(90.4-.05)+91.3(74.4-0.05)=152.99KB/Sec$
Single-hop connection time	$T_s=133\times30+192+11\times30+640=5.152ms$	$T_s=133\times32+192+11\times32+640=5.43ms$

- As seen in Table IV, compared to the **IEEE 802.15.4 standard**, this paper's proposed SHM model is slightly faster in the sensor recruitment process time.
- 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. Therefore, this proposed model covers **both static and mobile robot sensors.**

VIII.CONCLUSION AND FUTURE WORK

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

A. Conclusion

- This paper's proposed SHM model is tested in **a realistic environment** compared with the IntruMine, CPSI, HCPS, and VHM models.
- The results demonstrated that this paper's SHM model outperforms the other models in **both static and mobile testing environments.**
- Their model maintains **the tradeoff between energy efficiency and throughput.** The results prove their 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 CPSs.
- Furthermore, the SHM model produces **the lowest hop-by-hop time** compared with competing models.

Cont.

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.**
- The authors 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, also aim to **remove these shortcomings before designing the product.**

Cont.

C. Opinion

- The SHM model has been utilized in this article to ensure the dependability and protection of information from the sensors of static and mobile robots **throughout communication, transmission, data sharing, and privacy phases.**
- Due to the capability of **handling both static and mobile sensors**, their transmission guaranteed phase is able to utilize a **real varied infrastructure.**
- In this paper, they need to make a 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.**
- Managing accurate data collection is **one of the challenges that CPS faces**, and to tackle this problem, a semantic information extraction module is also utilized in this context.
- In the end, the model they have proposed significantly improves **the quality of transmission** by facilitating data aggregation.

THANK YOU