IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 1, 2020, accepted September 16, 2020, date of publication September 23, 2020,
date of current version October 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3026260

An Intrusion Detection System for Internet of Medical Things

GEETHAPRIYA THAMILARASU, ADEDAYO ODESILE, AND ANDREW HOANG
Department of Computing and Software Systems, University of Washington Bothell, Bothell, WA 98011, USA

Corresponding author: Geethapriya Thamilarasu (geetha@uw.edu)

ABSTRACT Internet of Things (IoT) is making strong advances in healthcare with the promise of transformation in technological, social and economic prospects, paving the way for a healthy future. Medical devices equipped with wireless communication enable remote monitoring features and are increasingly becoming connected to each other and to the Internet. Such smart and connected medical devices referred to as the Internet of Medical Things have enabled continuous real-time patient monitoring, increase in diagnostic accuracy, and effective treatment. In spite of their numerous benefits, these devices open up newer attack surfaces thereby introducing multitude of security and privacy concerns. Attacks on Internet connected medical devices can potentially cause significant physical harm and life-threatening damage to the patients. In this research, we design and develop a novel mobile agent based intrusion detection system to secure the network of connected medical devices. In particular, the proposed system is hierarchical, autonomous, and employs machine learning and regression algorithms to detect network level intrusions as well as anomalies in sensor data. We simulate a hospital network topology and perform detailed experiments for various subsets of Internet of Medical things including wireless body area networks and other connected medical devices. Our simulation results demonstrate that we are able to achieve high detection accuracy with minimal resource overhead.

INDEX TERMS Wireless body area networks (WBAN), Internet of Medical Things, intrusion detection, mobile agents, machine learning, healthcare security.

I. INTRODUCTION

Internet of Things (IoT) is an emerging paradigm, where the network of physical objects embedded with sensors aim to seamlessly integrate physical and digital world. IoT revolution, largely driven by advances in wireless communications, sensor networks, mobile devices and cloud computing is redesigning modern healthcare and transforming healthcare delivery and reliability. Internet of Medical Things (IoMT) is a connected ecosystem of sensors, wearable devices, medical devices and clinical systems, that enable various healthcare applications such as remote health monitoring, fitness programs, chronic diseases, and elderly care with reduced costs, timely response and increased quality of treatment [1], [2]. Wireless body area networks (WBAN) that consists of wearable and implanted medical devices connecting to and monitoring various parts of the body are a major component of Internet of Medical Things. While Internet connected medical devices offer several benefits, they also raise serious security and privacy concerns especially as healthcare systems deal with sensitive and often life-critical medical information [3]. Statistics show that the healthcare industry has endured the most cybersecurity attacks in the past few years [4]. Attacks on Internet connected medical devices can potentially cause significant physical harm and life-threatening damage to the patients. For instance, hacks on medical insulin pumps can lead to over dosage of insulin and potentially kill patients. Connected cardiac device such as a pacemaker can be hacked also endangering patients' life. Researchers have demonstrated various attacks on medical devices including eavesdropping, message alteration, fake data injection, and denial of service attacks that can compromise patient security, safety and availability of critical systems [5].

Traditional IT security solutions lack the context of connected medical devices. Current research on security in this domain focuses on implementing authentication, encryption and trust based solutions for implanted and wearable medical devices [6]–[8]. Such cryptography based solutions are often computationally expensive and challenging to implement on resource constrained medical devices. Physical layer

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

security has recently emerged as an alternative to cryptography, exploiting physical layer properties of the network system to improve security of IoT systems [9]. However, challenges such as weak adversary models or assumptions about wireless channel need to be addressed before physical layer security solutions can be adopted by practical systems [10]. In this work, we adopt another alternative approach to cryptographic security solutions and propose a machine learning based intrusion detection solution using mobile agent technology. While there exists substantial work in literature on using mobile agents for intrusion detection, research on their feasibility and suitability in connected medical devices does not currently exist.

The main objective of this research is to develop a robust and efficient system that addresses the security requirements within the connected health space. Specifically, we develop hierarchical and distributed attack detection mechanism in connected health devices using autonomous mobile agents, where every node in the network acts as the computing node, and mobile agents migrate, learn and collaboratively perform attack detection. In our earlier research, we developed an initial framework using mobile agents for WBAN [11], [12] and provided a comparison analysis of our system with other mobile agent based intrusion detection. In this paper, we significantly expand our research to address both device and network level anomaly detection across the entire spectrum of Internet of Medical Things.

A. OUR CONTRIBUTIONS

To the best of our knowledge, we consider this research to be the first attempt at utilizing mobile agents to facilitate low-footprint intrusion detection within the medical space. Our main contributions include:

- Design of a scalable, fault-tolerant, and robust architecture for mobile agent driven intrusion detection for Internet of Medical Things
- Design and implementation of machine learning to detect network level security attacks in Internet of Medical Things
- Implementation of a polynomial model for detecting device level anomalies using statistical regression.

II. BACKGROUND AND RELATED WORK

In this section, we first provide a background on Internet of Medical Things and Wireless body area networks, followed by an overview of security and privacy attacks and a review of current security solutions in the domain of Internet of Things in healthcare. We then summarize mobile agent based intrusion detection solutions.

A. INTERNET OF MEDICAL THINGS

The Internet of Medical Things/Smart Connected Health is a variant of the IoT networks adapted to the healthcare space. It is a hierarchical network constituted by a diagnostic/sensing, data aggregation, routing, and data service layer. The diagnostic/sensing layer comprises of two broad categories of devices, which are the sensing and smart imaging devices. Sensing devices range from a network of low-powered sensors attached/implanted in patient for direct observation of physiological phenomena (Wireless Body Area Networks), to sensors attached to smart-beds, smart ambulances, etc. On the other hand, imaging devices utilize various forms of physical media to approximate visual or acoustic images of patient's internal organs. Typical examples are smart MRI and Ultra-Sound scanners, smart X-Ray machines, etc. The routing layer typically consists of internet gateways, internal and external routers, while the data service layer encompasses the different servers used to either analyze, redact, or persist patient's medical information.

B. WIRELESS BODY AREA NETWORK (WBAN)

Wireless body area network consists of wireless wearable or implanted devices in a human body, that sense and relay physiological data from patient to enable continuous patient monitoring, diagnosis and effective treatment. A typical WBAN follows a star topology with sensors relaying data to a central cluster-head as shown in Figure 1.

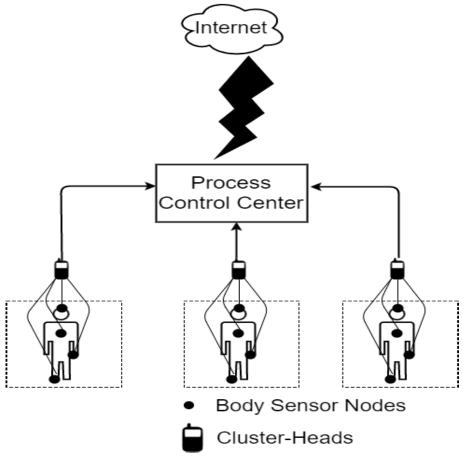

FIGURE 1. Wireless Body Area Network (Category A network).

C. SECURITY ATTACKS AND CURRENT SOLUTIONS

A number of studies on privacy attacks demonstrate that through simple eavesdropping attack, patients' private and sensitive medical information can be exposed to unauthorized entities [13]. Kumar *et al.* examined attacks that threaten patient's data integrity by intercepting physiological data and subsequently altering them to induce errors in diagnostic inferences [14]. This type of security attack has serious consequences as wrong diagnosis could lead to physical injuries or death of patient in extreme cases. Researchers have also demonstrated that routing attacks on wireless body area networks, such as selective forwarding, sinkhole and Sybil attacks can potentially lead to medical information being compromised en route to its destination (gateway device, cloud, hospital server etc.) [15], [16]. Attacker nodes can choose to drop the critical information from reaching its destination or attract all data to itself for selfish reasons.

Several solutions have been proposed to address the aforementioned security concerns in smart medical networks [6]–[8], [17]–[21]. IEEE 802.15.6 standard for WBAN provides a pre-installed cryptographic security suite with options for authentication and confidentiality. However, the inherent cryptographic protocol still possess design flaws that exposes other vulnerabilities [22]. A number of other cryptographic security measures were proposed for efficient key management and encrypted communications in connected healthcare networks [6], [7]. Other security solutions considered trust based mechanisms, to evaluate trust of every node in the network [8], [18]. Several physical layer security solutions such as artificial noise injection, anti-eavesdropping signal design and cooperation-based secure transmission techniques have also been developed to secure wireless communications [23], [24]. Unlike the traditional cryptographic approaches, physical layer security solutions takes advantage of the intrinsic characteristics of wireless channels to achieve keyless secure transmission via signal design and signal processing. Soderi *et.al* proposed a new transceiver architecture design to secure wireless communication by using a jamming receiver with a spread spectrum watermarking method [25]. The authors showed that their solution makes eavesdropping challenging and achieves larger secrecy capacity. Spread spectrum based schemes however suffer from code distribution and management challenges. Cipriani *et.al* proposed a solution using noise as the carrier of information, enabling secure channel for wireless systems without any priori knowledge between source and the destination [26]. Artifical Noise (AN) injection is an effective means to create the channel quality advantage for the legitimate transmission link. However, most of these schemes rely on the deployment of multiple antennas at the transmitter, which is a challenge in low-cost and resource constrained IoT devices.

Intrusion detection systems (IDS) are a commonly used security control to monitor and examine network/system traffic and identify anomalies and suspicious behaviors. While IDS solutions are well developed for wireless networks, these security measures are limited in the fields of wireless body area networks and especially in IoT connected healthcare systems. Anandkumar *et.al* conducted experiments on detecting intrusions in earlier implementations of WBANs that were based on IEEE 802.15.4 standard [18]. The authors designed a reputation system to evaluate node communication patterns and blacklist the malicious ones. In [17], an Intrusion detection system using genetic algorithms was developed to identify aberrations in device activities in the context of WBAN networks.

D. MOBILE AGENT BASED INTRUSION DETECTION

Use of mobile agents in intrusion detection systems has been well explored in traditional computer networks due to their ease of deployment, reduced network traffic, and resiliency. Balasubramaniyan *et al.* [27] originally conceived the use of static autonomous software agents to facilitate multi-level detection at different hierarchies of the network. Although, the architecture allows for scalability and dynamism, the purely hierarchical nature renders it inapplicable for wireless body area networks that require a more distributed protocol.

DIDMA [28] and MA-IDS [29] are similar to our proposed architecture with the use of both static and mobile agents. These systems however dispatch the mobile agents to local hosts only when the manager receives a request. Single point of failure at the manager limits resilience of the system. It is also evident that these systems may not be applicable for use in resource constrained networks such as WBAN. A lightweight mobile agent based IDS proposed in [30] has significant advantages with reduced power consumption but this approach does not provide distributed detection and is limited to detecting only a few selective types of attacks.

In [29], the authors proposed a relatively versatile protocol that consists of a compound static agent on every host running three different sub-agents to analyze file access, privilege usage, and network access respectively. While this system is robust, single point of failure at the managerial level was a noteworthy weakness. This protocol is also designed for traditional systems with files and user privileges that differ from sensors on a patient's body.

A decentralized intrusion detection system using mobile agents was explored for wireless sensor networks in [31]. While data gathering happens on a per-node basis with static agents, actual detection takes place at cluster-heads selected by a custom clustering algorithm. A similar architecture with more layers and sophistication was employed by [32] using a signature based intrusion detection to match patterns of known suspicious activity. Neither of these systems are designed to work with WBANs that differ from typical wireless sensor networks in terms of their heterogeneity and attack surfaces. Security solutions for connected medical devices are required to cope with network mobility, computational power, and communication constraints. To address these challenges permeating existing solutions, we propose a distributed mobile agent based intrusion detection framework. We employ a layered and decentralized hybrid architecture with mobile agents performing intrusion detection at different hierarchies of the network. In our earlier work, we proposed an initial framework for using mobile agents towards detecting intrusions in wireless body area networks [11], [12]. In this paper, we further extend this framework to build the intrusion detection system for Internet of Medical Things comprising of both WBAN and other connected medical devices.

III. NETWORK ARCHITECTURE AND IDS REQUIREMENTS

We consider a typical architecture of connected medical devices in a hospital networking environment as shown in Figure 2. The data acquisition layer in this system consists of wearable systems such as wireless body area networks, smart and connected things such as smart bed as well as

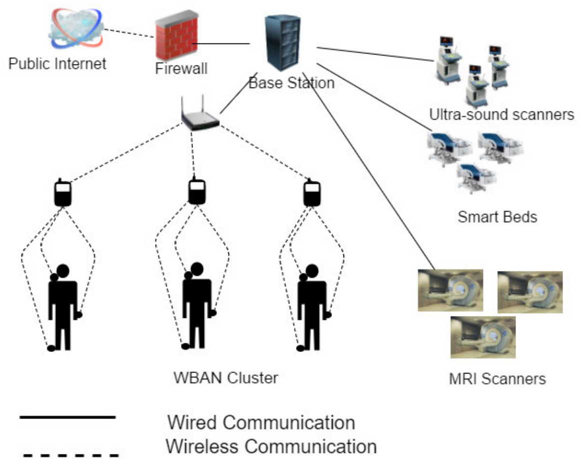

FIGURE 2. **IoMT network architecture.**

traditional diagnostic systems such as MRI, ultrasound etc. The sensors in wireless body area networks includes wearable or implantable sensors, placed in and around patients' body. These sensor nodes monitor, collect and relay the data to local gateway nodes or cluster heads, and perform data processing, aggregation and/or provide distributed storage. IEEE 802.15.6 standard is used for WBAN communication with corresponding cluster head/gateway device. Smart beds and other connected medical devices (MRI, ultrasound) connect either using wireless or wired communication to the hospital network.

A. IDS REQUIREMENTS

In addition to the security threats described earlier, an effective intrusion detection system must consider other non-functional requirements. The detection system should be scalable, fault-tolerant, conservative, easily deployable, and extensible without significant compromise on its efficiency in providing adequate security. In order to achieve these requirements, we design a hierarchical hive of mobile agents independently but cooperatively to perform intrusion detection across different segments of the network. The following outlines how the proposed mobile agent based detection addresses each of the requirements:

- **Scalability:** In a connected medical network, a potential point of contention is the cluster-head for the sensing devices. However, mobile agents are executed and propagated autonomously without continuous reliance on the cluster-head. Hence, an increasing number of nodes within the network will only lead to increase in number of required agents. This impacts the cluster-heads during agent instantiation and initial dispatch.
- **Fault Tolerance:** As mobile agents are capable of adjusting their itineraries according to changes in available routes, the system can survive multiple node failures. However, if the cluster-head fails, the WBAN (sensing layer of the IoMT network) ceases to exist considering that the cluster-head is responsible for data aggregation and communication coordination across the sensors.
- **Conservativeness:** The use of mobile agents ensures that the computationally demanding task for intrusion detection is distributed across the network. This is done such that available resources are used optimally without overloading or under utilizing any particular node. Also, since the agents are considerably smaller than the size of aggregated network traffic data, there is less communication overhead in transmitting agents.
- **Ease of Deployment:** The entire system can be easily deployed on the cluster-head while the agents automatically propagate into the network.
- **Extensibility:** Existing agents can be terminated by control commands from the cluster-head while newly extended ones are dispatched.

B. ATTACK MODEL

In this section, we describe the attack models specific to the Internet of Medical Things environment.

1) DENIAL OF SERVICE (DoS)

We consider our adversary to possess the ability to hijack and reprogram sensor nodes to pump data at a faster/slower rate, or randomly transmit noise. We model this attack such that an adversary might be interested in endangering a patient's life for hostage-ransom benefits or personal grudges by ensuring doctors/nurses do not receive emergency alerts when necessary. DoS attacks can be launched through several methods as described below:

- **Sender Radio Exhaustion**: This attack is targeted at nodes transmitting information. It is carried out by increasing the rate of transmission, resulting in increased energy usage of the sender eventually leading to battery exhaustion.
- **Receiver Radio Exhaustion**: This attack is launched by compromising multiple transmitters and sending a flood of packets to the receiver. The continuous reception and processing of packets inadvertently leads to increased energy usage and exhaustion of the receiver node.
- **Decoy Packets**: In this attack(also focused on the receiver node), the malicious node transmits random noise signals to act as decoys for the receiver. Nodes receiving the packets become pre-occupied with noise filtering and are unable to perform their normal network operations. The cluster-head is a common victim of such attacks.
- **Sink Holes**: In this routing based DoS attack, transmitted data is misdirected to an attacker node instead of the intended receiver node.

2) DATA FABRICATION AND FALSIFICATION

In data fabrication attack, adversaries can computationally fabricate invalid data unrelated to any physical phenomena observed by body sensors. In data falsification attack, an adversary may disrupt the system by forcing the health care providers to continuously respond to false alarms. This kind of attack is fairly easy to execute in WBANs which communicate through connectionless protocols, thereby not requiring any sort of pre-authentication or handshake. Any device that can transmit within the radio frequency of respective sensors can be used to generate false data for the cluster-head. However, execution of such attacks on wired devices such as the smart scanners are more challenging as the computing chip needs to be physically accessed and reprogrammed.

Data driven attacks can be highly consequential because they tend to provide misleading results which could lead to wrong and potentially dangerous actuator response, prescriptions, or even lack of any required medical response. The common motivations behind these attacks are:

- To inflict harm by causing patient to receive misinformed/misdirected medical response to certain conditions.
- To increase operational costs of medical organizations by introducing a lot of false alarms and unnecessary incidence response.

Again, we consider our adversary to be powerful enough to hijack a sensor and modify sensed data.

3) PRIVACY/DATA BREACH

This encompasses all form of attacks that results in unauthorized access to private medical information. The most common way of executing such attacks is through a passive listening radio device tuned to the same broadcast frequency of the wireless medical devices. More sophisticated adversaries can remotely reprogram a node in the network to route private data to a certain location. Although data breaches may not have immediate consequences, it can be used as a medium for blackmail on larger scale. The common motivations behind these attacks are:

- To gain leverage for coercing compromised individuals into performing certain deeds including parting with some finances.
- For financial gains in the cyber black market.
- To induce medical institutions into making payments to avoid facing disciplinary action from certain health regulation bodies.

Our adversary is assumed to be capable of mirroring packets to unauthorized destinations. Detecting passive listeners is however outside the scope of our research.

IV. IDS FOR INTERNET OF MEDICAL THINGS

We propose a novel multiple mobile agents based intrusion detection system for Internet of Medical Things, where sensing, learning and decision making is distributed among different nodes in the network. Our detection mechanism employs autonomous mobile agents with machine learning algorithms to identify and detect any abnormal activities in the network. In particular, our system focuses on providing both device-centric and network-centric intrusion detection.

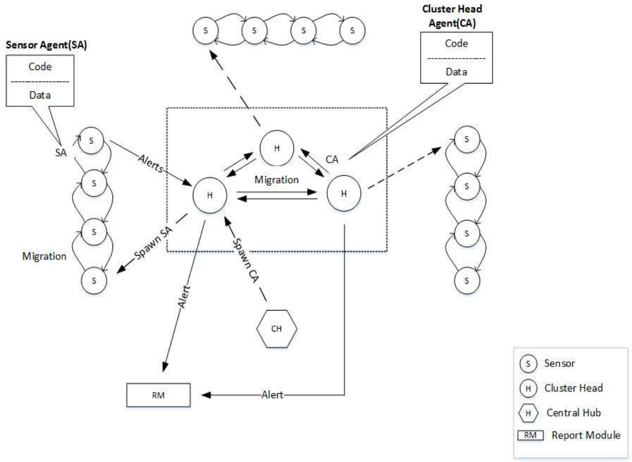

FIGURE 3. Mobile agent based IDS protocol [11].

In Figure 3, the sub-networks of WBAN (three shown as an example) are connected via cluster heads (mobile gateway device). Each mobile agent traverses only among sensors within a given sub-network. Sensor agents are capable of performing local detection using the attack features available in the limited sensing region, while gateway nodes and servers are capable of performing global attack detection.

A. DETECTION SYSTEM COMPONENTS

In the following we first describe the different types of mobile agents involved in the detection process.

1) SENSOR AGENT

The sensor agent is an autonomous mobile program responsible for detecting a specific category of attack. Each cluster head is responsible for spawning multiple sensor agents for local detection within a clique of sensors. The sensor agents are preloaded with two sets of parameters as outlined in Table 1. The first set includes variables that guide the agent's trajectory and state management, while the other set is derived from training algorithms to be used for detection purposes. The fixed size of an agent's state is 10 bytes, while the size of the variable parameters is dependent on the number of devices designated to an agent as well as the type of detection algorithm. Each sensor agent traverses the nodes within its set itinerary and performs local detection in each node by aggregating the logs accumulated over a period of time.

When the sensor agent executes the intrusion detection algorithm, it produces a *malicious* flag that triggers an alarm response, or a *normal* flag that does nothing (migrate to next node in itinerary) or a *suspicious* flag that triggers an intervention request. The "suspicious" state is introduced to reduce detection errors (false positives/negatives) which is critical to WBANs. Traditional detection algorithms use binary classification that sometimes hinders distinction between benign and malicious activities. For instance, certain legitimate activities could cause temporary network spikes on the single

TABLE 1. Sensor agent parameters.

Parameter	Category	Description
Id	Operational	A numeric identifier used for tracking a single SA instance
Clique Index	Operational	A numeric identifier for the group of sensors SA is assigned to within the WBAN cluster.
Detection Model	Security	An encapsulation of the parameters and algorithms used in carrying out network/device intrusion detection.
Cluster-Head Id	Operational	A numeric identifier for the originating cluster-head.
Aggregation Delay Period	Operational	The duration for which a SA waits for logs to accumulate on a sensor before aggregating and running them through its detection algorithm.
Detection Type	Security	A field that identifies SA's detection algorithm as Machine learning (ML) or Polynomial Regression (PR).
Itinerary	Operational	A list of sensors within the SA's network clique which defines its trajectory.

Algorithm 1 Sensor Agent Protocol Algorithm

```
Require: $SA.isTrained \equiv true$
  $wait(aggregationDelay)$
  for all $logEntry$ $FROM$ $entries[lastAggIndex]$ do
    $SA.cumulate(logEntry)$
  end for
  $result \leftarrow SA.analyzeEntries()$
  if $result \equiv MALICIOUS$ then
    $SA.triggerAlarm()$
  else if $result \equiv SUSPICIOUS$ then
    $SA.triggerCHInterventionRequest()$
  end if
  $SA.hop(next\_node\_in\_itinerary)$
```

Algorithm 2 Cluster-Head Agent Protocol Algorithm

```
Require: $CA.isTrained \equiv true$
  $wait(aggregationDelay)$
  for all $logEntry$ $FROM$ $entries[lastAggIndex]$ do
    $CA.cumulate(logEntry)$
  end for
  $result \leftarrow SA.analyzeEntries()$
  if $CA.getCHId() \neq currCH.getId()$ then
    $CA.broadcast(\{result, currCH.getId()\})$
  else
    $finalResult \leftarrow CA.computeMajorityVote()$
    if $finalResult \equiv MALICIOUS$ then
      $CA.triggerAlarm()$
    end if
  end if
  $CA.hop(next_node_in_itinerary)$
```

device or a more sophisticated adversary could distribute its attack vectors across the entire network. The suspicious class represents activities that are considered benign but could potentially indicate a large scale distributed malicious attack. Introducing the *suspicious* classification gives the system a benefit of doubt that warrants further investigation. Algorithm 1 describes the process of the sensor agent.

2) CLUSTER HEAD AGENT

The Cluster-head agent (CA) is another instance of an autonomous mobile program designed to detect anomalies among cluster-heads within multiple interconnected WBAN clusters. They are similar to the sensor agents in that they have a pre-defined itinerary, trained model and are also capable of targeting different attack types. CA agents however operate in a more distributed manner to provide global attack detection across inter-connected clusters in WBAN. To facilitate the inter-node communication between the cluster head agents, a cache of the IDs of all dispatched CH agents within the same target attack group is maintained. A cluster head agent can be static or mobile depending on the network configuration. A static CA resides on its originating cluster head and performs intrusion detection at regular intervals, while a mobile CA works similar to a sensor agent where it traverses nodes (cluster-heads) within its defined trajectory and performs localized detection. Algorithm 2 summarizes the execution flow of the cluster-head agent.

3) DETECTIVE AGENTS

When the detection module of a sensor agent is unable to characterize the network behavior as malicious or normal, it initiates an intervention request. The request consists of the agent and sensor ID. On reception of such request, the Cluster head (CH) creates a signature from the request attributes, and caches it to prevent responding to duplicate requests. Cluster head spawns a special agent known as Detective Agents in response to this intervention request and populates its itinerary with the addresses of every sensor within the local cluster to investigate the uncertainty of the detection results. These agents sweep through the entire cluster, gathering network activity data in the process, and reporting back to the originating CH. The collected data is run through a conflict resolution detection algorithm which is trained for a group of sensors as opposed to the per-sensor SA (sensor agent) training set. A negative classification of data implies the possibility of a distributed intrusion across nodes within the scanned cluster. Such attacks have very subtle impacts when examined on a per-device scale. Detective agents operate differently from the other agents in that they scan the entire cluster with an aggregation time given by D_A where:

$$D_A = \frac{C.S}{B.S} * S_A \tag{1}$$

and C.S is clique size, B.S is the BAN cluster size, and S_A denotes the defined sensor agent aggregation time. This measure is used to ensure that the detective agents take at most the same time as a sensor agent does in scanning a clique to traverse the entire cluster. Subsequently, the detective agent trains itself with global datasets available in the CH and runs its detection analysis on the aggregated data, triggering an alarm if the attack detection result is flagged as malicious.

Algorithm 3 summarizes the process flow of the detective agents.

Algorithm 3 Special Agent Protocol Algorithm

```
Require: $SA.interventionRequest.isNew()$
    $CH.train(SP)$
    for all $sensors\ IN\ cluster$ do
        $SP.cumulate(logEntry)$
    end for
    $SP.hop(CH)$
    $result \leftarrow CH.analyzeEntries()$
    if $result \equiv MALICIOUS$ then
        $CH.triggerAlarm()$
    end if
    $invokeAfter(cacheInvalidationFunc, validPeriod)$
```

B. NETWORK LEVEL INTRUSION DETECTION

Increased network connectivity in medical devices results in larger attack surfaces in this domain. Attacks can occur at any part of the network and adversely impact network operations and survivability. To detect attacks at the network level, we first utilize multiple network traffic variables such as rate of packet influx/efflux and network throughput and obtain the representation of a normal network state. We then deploy standardized machine learning algorithms to analyze and interpret the multi-variate data and determine normal and abnormal network behaviors.

1) DATA COLLECTION AND TRANSFORMATION

In the first step of network level intrusion detection, data collection and transformation module characterizes network traffic using wide range of features such as total packet size, number of packets etc. As these features have disparate ranges, we normalize each feature with the following series of equations. $\{\forall j : j \in F\}$ and all data entry (rows) i of the training set with n entries, where j is a data dimension/feature and F is the defined feature set:

$$x_{(i,j)} = x_{(i,j)} - \mu(j) \tag{2}$$

$$\sigma(j) = \sqrt{\frac{1}{n}\sum_{i=0}^{n}(x^2)} \tag{3}$$

$$x_{(i,j)} = \frac{x_{(i,j)}}{\sigma(j)} \tag{4}$$

where $x_{(i,j)}$ is a scalar value at data entry i and feature j, $\mu(j)$ is the mean for all $x_{(i,j)}$ for a feature j, and σ is the corresponding standard deviation.

2) PRINCIPAL FEATURE EXTRACTION

We use principal component analysis (PCA) technique for feature extraction. PCA is a multi-step mathematical transformation that is widely used for feature selection. The main goal of PCA is to reduce dimensionality of the features by identifying strongly correlated features and either combining them or by selecting the feature with highest relevance.

Suppose we have a training vector set of N vectors, we use the following procedure for PCA.

1) Derive co-variance matrix C from the normalized training data D

$$C = \frac{1}{N-1}DD* \tag{5}$$

D^* is the conjugate transpose of training set matrix D, x_i is a row vector representing a data entry in D.

2) Derive the eigenvalues and eigenvectors for matrix C using the OpenCV library.

3) Sort the eigenvalues in decreasing order and choose the first corresponding eigenvectors called principal components.

4) $\{\forall v : v \in V\}$ where V is the set of eigenvectors for C, we compute the cumulative energy content $g|v|$ as

$$g|v| = \sum_{i=0}^{v} g|i| \tag{6}$$

5) In the final thinning process, we chose a value L such that $\frac{g|L|}{g|v|} \geq 0.9$. Any eigenvector with a $g|v|$ lesser than $g|L|$ is discarded as representing a redundant dimension with little or no significant impact on the data trend. The final output $D^{|}$ of the PCA is each data entry projected on the remaining eigenvectors that has been normalized as unit vectors since all computations were carried out on z-scores not actual data values.

$$D^{|} = \begin{pmatrix} \vec{x_1}.\vec{v_1} & \vec{x_1}.\vec{v_2} & \cdots & \vec{x_1}.\vec{v_k} \\ \vec{x_2}.\vec{v_1} & \vec{x_2}.\vec{v_2} & \cdots & \vec{x_2}.\vec{v_k} \\ \vdots & \vdots & \ddots & \vdots \\ \vec{x_n}.\vec{v_1} & \vec{x_n}.\vec{v_2} & \cdots & \vec{x_n}.\vec{v_k} \end{pmatrix} \tag{7}$$

where v_i is the ith eigenvector from the selected k eigenvectors.

C. DEVICE INTRUSION DETECTION WITH POLYNOMIAL REGRESSION

Connected medical devices pose a huge cybersecurity threat as attacks on these devices can delay care or trigger clinical errors. Attacks such as data falsification/fabrication involves illegal modification or synthesis of device data. In 802.15.6 standard based WBAN, individual sensing/imaging devices communicate directly with the cluster head. An attack on these individual devices do not affect the data flow of the network other devices to the cluster-head. To detect intrusions at the device level, we define a model that profiles normal sensor device data and use it as a baseline to detect anomalous device readings. While the network state is dependent on various factors across the network, device state is solely dependent on device specific information such as system calls, timestamps and previous sensor readings. As this corresponds to a time-dependent regression problem, we use polynomial regression to model our intrusion detection. This involves building a model as an n-order polynomial equation which is a function of one or more independent variables. The polynomial equation is used to forecast/predict sensor data and if the deviation from expected value exceeds a set threshold, the system flags an alarm and reports an anomaly. The model is continually updated from benign device data in real-time to ensure model adapts to changes in the network. Device level detection is performed only at the individual sensor devices and not at the cluster head. Instances of sensor agents are created such that there exists one SA for device level detection for every group of sensor devices within a cluster. Polynomial regression for the proposed intrusion detection system involves the following stages.

1) DATA COLLECTION

We consider both wireless sensing devices (WBAN) as well as the medical imaging devices as data collection sources for device level detection. Data is however collected independently from each of these sources. Data collection process assumes benign network conditions to prevent the model from being corrupted by malicious data. Data is extracted as a tuple of timestamp and sensor scalar value for sensing devices, while data from imaging devices is transformed in real-time from a pixel matrix P to a scalar value s.

$$V(P_{i,j}) = \vec{V}_{i,j} = \begin{pmatrix} \mu_r \\ \mu_g \\ \mu_b \end{pmatrix} \tag{8}$$

$$f(\vec{V}_{i,j}) = h(\ \vec{(\vec{i},j)}).\vec{V}_{i,j} \tag{9}$$

$$\vec{h}((\vec{i,j})) = \begin{pmatrix} g(|(\vec{i,j})|)Mod255 \\ gg(|(\vec{i,j})|)Mod255 \\ ggg(|(\vec{i,j})|)Mod255 \end{pmatrix} \tag{10}$$

$$s = \mu(f(\vec{V}_{i,j})) \tag{11}$$

where the pair (i, j) represents the 2-dimensional index of each sub-matrix of the entire pixel. We divide the pixel matrix P into 16 sub-matrices $P_{1,1}$ to $P_{4,4}$. In Equation 8, we convert each sub-matrix to a 3-D vector with each dimension representing the average red, green, and blue channel values respectively. Equation 9 defines a function f that converts the 3D vector into a scalar by computing its inner-product with function h. h is defined to compute a hash of the sub-matrix indices i, j in form of a 3-D vector to ensure the position of the sub-matrix is factored in. The first element of the hashed vector is the output of a function g generating a 32-bit hash of the magnitude of vector (i,j) modulo 255, where 255 is the maximum value of a color channel within the 24-bit color depth specification. The second and third elements were derived from g being applied twice and thrice to the vector (i,j) respectively. The scalar value of the entire matrix P is subsequently computed in Equation 11 as the mean of all scalars from the sub-matrices. Although the conversion process is fairly complex, it incurs fewer computational resources when compared to other matrix representations such as the eigenvalues.

2) MODEL CONSTRUCTION

Since physiological data is approximately closer to varying sine/cosine functions and are considerably difficult to approximate linearly, we develop a dynamic polynomial regression to address security anomalies at the device level. Using a polynomial model ensures a closer approximation of the data trend. Secondly, its dynamism keeps it up to date with the latest valid changes in data trends. As shown in Equation 12, our polynomial model is built as a function of time.

$$y^{|} = m_n t^n + m_{n-1} t^{n-1} + \ldots + m_1 t + m_0 \tag{12}$$

where m_n to m_0 are derived coefficients, and n is the polynomial order. In computing the coefficients, we construct a coefficient matrix C as shown in Equation 13. The matrix is subsequently row-reduced to its echelon form with the element of its right-most column vector being the desired coefficients m_{0-n}.

$$C = \begin{pmatrix} n & \sum_{i=0}^{n} t & \cdots & \sum_{i=0}^{n} t^n & \sum_{i=0}^{n} y \\ \sum_{i=0}^{n} t & \sum_{i=0}^{n} t^2 & \cdots & \sum_{i=0}^{n} t^{n+1} & \sum_{i=0}^{n} yt \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sum_{i=0}^{n} t^n & \sum_{i=0}^{n} t^{n+1} & \cdots & \sum_{i=0}^{n} t^{2n} & \sum_{i=0}^{n} yt^n \end{pmatrix} \tag{13}$$

For continuous update of the model to newer trends, every agent that performs device-level detection maintains state information containing unique elements ($\sum_{i=0}^{n} t \ldots \sum_{i=0}^{n} t^{2n}$) of the coefficient matrix. Subsequent data samples classified as benign are cumulated with the existing state matrix. The matrix is eventually expanded and row-reduced to its echelon form, thereby generating a new set of coefficients for the model.

TABLE 2. Radio level network simulation parameters.

Parameter	Sensor Value	Cluster-head Value	Wired Devices Values
Data rate.	1,024 kbps	147,456 kbps	1,002,400 kbps
Modulation Type.	DIFFQPSK	DIFFQPSK	N/A
TX range/power usage.	-10 dBm/3.0 mW	-1 dBm/29 mW	-0.001dBm/14 mW
Available Energy.	1,872 kJ	Rechargeable	Connected
Retransmission Interval.	100 ms	100 ms	100ms

3) DETECTION PROCESS

The sensor and cluster-head mobile agents are responsible for performing network level and device level intrusion detection at the diagnostic and aggregating hierarchy of the network respectively. For the sake of clarity, we delineate the WBAN sensing devices and the other types of smart medical devices by classifying them as category A and B respectively. The detection process followed by the mobile agents is outlined as follows:

- The cluster-heads (CH) are preloaded with training sets for both network and device level detection.
- In the category A network (WBANs), two separate instances of mobile code instance known as sensor agents (SAs) are created and trained for network and device level detection respectively.
- Both instances of SAs are duplicated until there is one network and device detection sensor agents for every group of devices within the cluster.
- The SAs are propagated throughout the WBAN to their respective trajectories to perform localized detection.
- The SAs only travel with the state of their trained detection algorithm, excluding the training dataset. This ensures agents are minimal in size, thus minimizing communication overhead with each hop.
- On arrival at a sensor node, a SA aggregates network activity or device data depending on its role as a network or device intrusion detection agent.
- SA runs aggregated information through its detection algorithm and classifies them as either benevolent, in which case it migrates to the next node, or malicious thereby triggering an alarm, or suspicious where an intervention request is made to the CH.
- Once a CH receives an intervention request, a special agent is instantiated and dispatched to sweep the entire cluster for network activity or device data. This mechanism is effective in case of sophisticated adversaries that tend to distribute their attack vectors across the network.
- SA delivers the aggregated information to the CH which in turn runs it through an instance of the algorithm trained for cluster-scale detection. In this case, the classification result is binary, either benign or malicious.
- In a single cluster WBAN, an instance of a static (no migration) cluster-head agent (CH) is spawned to perform localized network intrusion detection at set intervals.
- Device-level intrusion detection is not executed at this hierarchy of the network as the cluster-heads do not measure any data.
- For every CH, a mobile CA is created and trained, with each of them independently traversing the networks of CHs for localized cluster-head intrusion detection.
- A CA does not trigger alarms immediately after detecting malicious network patterns. Instead, it shares its detection results with other CAs.
- The receiving CA adds the result to its cache, designed to store multiple detection results from every CA.
- On complete culmination of every CA's opinion about its originating CH, the decision is based on a majority. If half or less of the other CAs reported the CH as benevolent, then an alarm is triggered.
- A similar process is carried out for the category B devices. However, in this case, the agents do not travel directly from one device to another. The mobile agents migrate through the central network router which serves as a communication gateway across the devices.

V. EXPERIMENT SETUP AND ATTACK MODEL

In this section, we describe our simulation setup, attack models and assessment metrics. We simulate Internet of Medical things that consists of heterogeneous devices communicating using different network protocols. We consider a combination of wireless sensing devices using either zigbee or the 802.15.6 WBAN standard. Our system also includes other smart and connected devices such as the ultra-sound scanners or MRI machines running on DICOM network protocol. To address the communication protocol disparity, we ensure the proposed system is designed to be oblivious to the differences between the network standards.

We conducted our simulations on OMNeT based Castalia-3.2 simulator [33] specifically tailored for wireless body area networks. In addition to the preloaded IEEE 802.15.6 and 802.15.4 implementations, the simulator also allows for an accurate emulation of network implementations across the entire protocol stack with full customizability. Additionally, its inherent radio model is versatile enough to simulate constructive and destructive interference, RX to TX to sleep transitions, and energy usage computations.

Table 2 lists the simulation parameters used for our experiments. Based on these parameters, we were able to emulate benign and compromised network scenarios, generate training data, and develop corresponding algorithms for both network and device-level detection

A. ADVERSARIAL MODEL IMPLEMENTATION

We categorize the attackers into **dominantly suspicious** to represent a subtle distributed attack, **dominantly malicious**

TABLE 3. Attack implementations.

Attack	Category	Launch Point(s)	Implementation
Sender Radio Exhaustion	DoS	During packet transmission	Increasing the sampling and transmission rate of a sensing device exponentially.
Receiver Radio Exhaustion	DoS	During packet transmission	A group of malicious sensors target a victim and flood it with data packets.
Decoy Packets	DoS	During packet transmission	Sent noise to the CH as opposed to meaningful data packet.
Sink-holes	DoS	Both packet reception and transmission	Selective or no transmission of sensed data to CH.
Data falsification	Data driven attack	Right after an incoming sample of sensor/image data	Modifying sensed data before transmission to the CH.
Illegal Transmitter	Privacy Breach	During packet transmission.	Transmission of data to an illegal destination other than the CH.

for an aggressive adversary, **dominantly elusive** for more sophisticated adversaries, and an equal proportion of all three threat levels. We present the simulated attacks, attack launch points and their implementation details briefly in Table 3.

B. ALGORITHM ASSESSMENT AND SELECTION

We train five supervised machine learning algorithms, namely, SVM (Support Vector Machines), DT (Decision Trees), NBC (Naive Bayes Classifier), KNN (K-Nearest Neighbor), and RF (Random Forests) to test our proposed intrusion detection system. We evaluate the performance of these algorithms using the following metrics:

Accuracy: Classification accuracy is a metric widely used to assess ML algorithms. This metric provides an estimate for the algorithm's correctness based on the training and test data sets. This is the ratio of correct classifications to the total number of test classifications as shown in equation 14.

$$x_a = \frac{t_n + t_p}{T} * 100\% \tag{14}$$

where x_a is the percentage accuracy, t_n and t_p are the number of true negatives and positives respectively, and T is the total number of classifications.

Cost-Benefit Ratio (CBR): This is a contextual metric for evaluation of a ML based intrusion detection algorithm based on its operational consequences [34]. It is defined as the ratio of false positives (f_p) to false negatives (f_n) or its inverse depending on which classification error incurs more costs. In the context of medical networks, a false negative is considered more consequential as it could result in loss of lives. For instance, in case of medical devices such as insulin pumps, a false negative classification can trigger excess injection of insulin into the patient's body causing significant harm to the patient.

An algorithm may have a relatively low number of false positives and higher false negatives, resulting in a large CBR that approaches infinity as false positives approach zero or an algorithm can result in relatively low false negatives and high false positives which results in a low CBR that approaches zero as false negatives gets smaller. In both cases, the algorithm with classification errors (high or low) has the tendency to possess low or even zero CBR. This shows that high number of errors does not necessarily imply higher cost or vice-versa. As a result, we define cost benefit ratio x_c in Equation 15 as:

$$x_c = \frac{2f_n + f_p}{f_p + t_n + t_p} \tag{15}$$

In this case, the accuracy is also factored in by including t_n and t_p. As t_p increases, the influence of f_p in x_c decreases with that of f_n increasing, resulting in a controlled increase in x_c. Conversely, a controlled decrease in x_c is realized as t_n increases.

Feedback Reliability Ratio (FBR): The feedback reliability ratio is an inverse measure of the reliability of a machine learning based intrusion detection system [35]. It is defined as the ratio of a weighted error sum to the total number of observations as shown in equation 16.

$$x_f = \frac{W_n * f_n + W_p * t_p}{T} \tag{16}$$

where W_n and W_p are weights assigned to the false positives and negatives respectively on a scale of 0 - 1. We experimented with several weight combinations, which led to the following conclusion; the condition $W_p < Wn \bigwedge W_p > 0.5\ W_n$ must hold to reflect an accurate estimate of their inverse reliability while maintaining the property of associating higher risks with false negatives.

Training Time: Machine learning consists of two phases of computation- training and classification. Our experimental results show that each ML algorithm took roughly the same time for classification but varied significantly in training time. As a result, we establish the training time as the dominant factor in computing power usage. We examined a simplistic model of micro-controller/processor computational energy usage in equation 17 [36]. It is evident that runtime is the only variable within the model, implying that energy usage is a function of time.

$$x_e = C * f * V^2 * t \tag{17}$$

where C is the computing chip's capacitance, f is the clock frequency, V is the total voltage dissipated per unit time, and t is the computation time.

Rank: This is a normalized aggregation of results from the other metrics which is used to rank each algorithm. The rank x_r is presented in equation 18 as:

$$x_r = \frac{x_a}{100} - \frac{x_c}{max(x_c)} - x_f - \frac{x_t}{max(x_t)} + 3 \qquad (18)$$

where x_t is the training time and the value 3 is used for inverting the three negatives.

VI. IMPLEMENTATION RESULTS AND ANALYSIS

We conducted a thorough implementation of our detection system based on the following three categories:

1) **Detection Type:** Network Intrusion Detection, Device Intrusion Detection.
2) **Adversarial Composition:** Dominantly malicious, dominantly suspicious, dominantly elusive, randomly distributed.
3) **Percentage of Compromised Nodes:** 10 - 90%.

The different attack strategies (malicious, suspicious, and elusive) are implemented using attack probabilities. The attack probability $P(0 < P < 1)$ determines the likelihood of an adversary launching an attack. While an attack probability of 0.7 and 0.2 is defined for malicious and suspicious attackers, the elusive ones are designed to be relatively difficult to classify. The elusive adversary constantly changes its attack probability over a uniform distribution between 0 - 1. Hence, they oscillate erratically across benign, suspicious, and malicious states.

A. TESTING MACHINE LEARNING ALGORITHMS

We first evaluated five commonly used ML algorithms for intrusion detection, namely, SVM (Support Vector Machines), DT (Decision Trees), NBC (Naive Bayes Classifier), KNN (K-Nearest Neighbor), and RF (Random Forests).

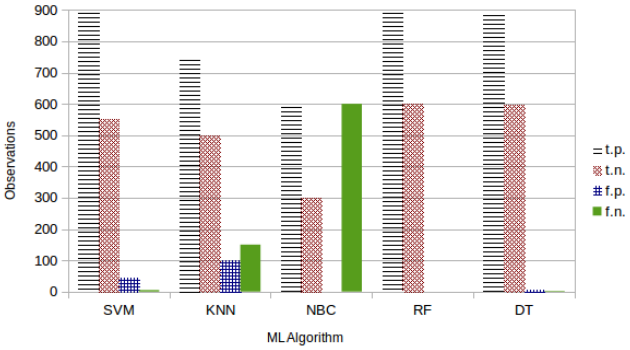

FIGURE 4. True positives vs true negatives.

1) CLASSIFICATION ACCURACY

Figure 4 shows the classification accuracy of machine learning algorithms. A total of 1,500 observations are made for the sensor and cluster-head traffic respectively. For sensor accuracy tests, we use 600 malicious, 300 suspicious, and 600 benign classes of data respectively. On the other hand, the cluster-head traffic was tested with 900 malicious, and 600 benign network data considering that classification at the cluster-head level is binary. KNN and NBC algorithms produced a high number of false classifications, rendering them unsuitable for our system. The remaining three algorithms (SVM, DT, and RF) performed with significantly higher level of accuracy. Random Forest gained the highest classification accuracy of approximately 100% and KNN and SVM suffered from relatively higher number of false positives. DT performed better with fewer false positives and fewer false negatives. We also assessed the learning algorithms for other metrics such as resource usage to establish a more concrete measure of their suitability to the system.

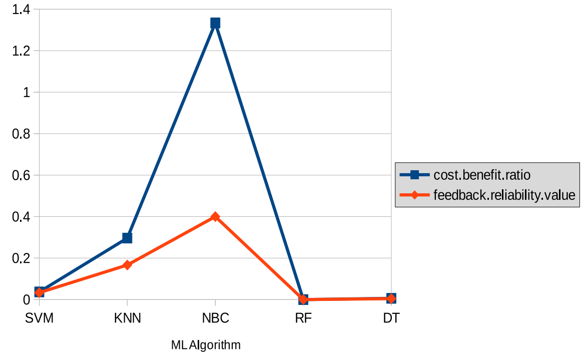

FIGURE 5. Cost ratio and FBR.

2) COST-BENEFIT RATIO

As depicted in Figure 5, the NBC learning algorithm failed considerably with high number of false negatives, which is a critical factor in determining the resultant cost benefit ratio. Although, KNN's CBR is order of magnitudes lesser than that of NBC, its performance was poor in comparison with the remaining algorithms. The CBR value of RF was zero as there were no false classifications and SVM had a slightly higher value than DT due to its higher number of false negatives.

3) FEEDBACK RELIABILITY VALUE

Figure 5 shows the feedback reliability value, with NBC and KNN scores, order of magnitudes higher compared to other ML algorithms. The Feedback reliability value is a direct inverse representation of reliability of ML classification algorithm with respect to the data model.

4) TRAINING TIME

Figure 6 presents the time taken to train in milliseconds over a total of 11,059 training data entries for each ML algorithm. The training time dictates the computational resource consumption of a ML algorithm on an actual computing chip. The RF algorithm performed poorly with a training time exponentially longer than its counterparts. Although SVM experienced longer training time than the NBC, KNN, and DT algorithms, it is still deemed to be feasible for execution on a cluster head. The KNN and NBC performed the best with a training time lesser than 20 ms.

TABLE 4. Polynomial coefficients.

Order	Coefficients
1st	m_0 = 104.527, m_1 = 0.000198
2nd	m_0 = 106.736, m_1 = -0.00229, $m_2 = 5.197 * 10^{-7}$
3rd	m_0 = 73.599, m_1 = 0.058684, $m_2 = -1.817 * 10^{-5}$, $m_3 = -3.565 * 10^{-12}$
4th	m_0 = 71.132, m_1 = 0.0678, $m_2 = -2.51 * 10^{-5}$, $m_3 = 1.4 * 10^{-9}$, $m_4 = 2.227 * 10^{-15}$
5th	m_0 = 53.526, m_1 = 0.176, m_2 = -0.000174, $m_3 = 7.246 * 10^{-8}$, $m_4 = -1.090 * 10^{-11}$, $m_5 = 2.237 * 10^{-20}$

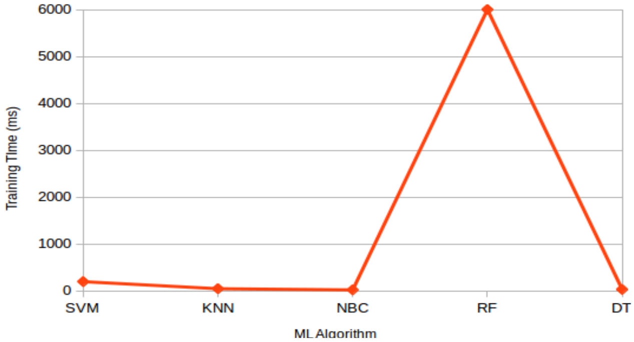

FIGURE 6. Training time.

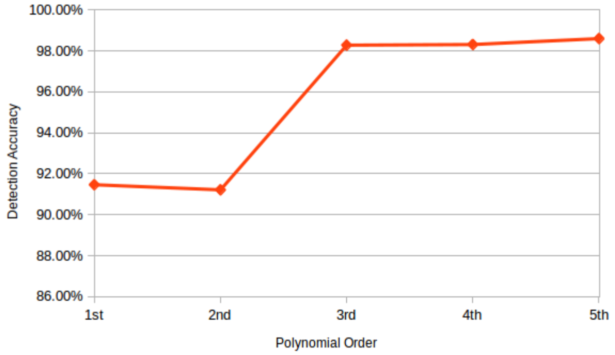

FIGURE 8. Order vs accuracy.

5) FINAL RANKING

Figure 7 presents the results of the final ranking score. With lower classification accuracy, NBC and KNN algorithms resulted in a lower aggregated score. The high computational of RF negatively impacted its final score regardless of its high values of accuracy, CBR, and FRV. Decision tree (DT) and SVM had close rankings, however DT performed better in the overall ranking due to SVM's high false positives rate.

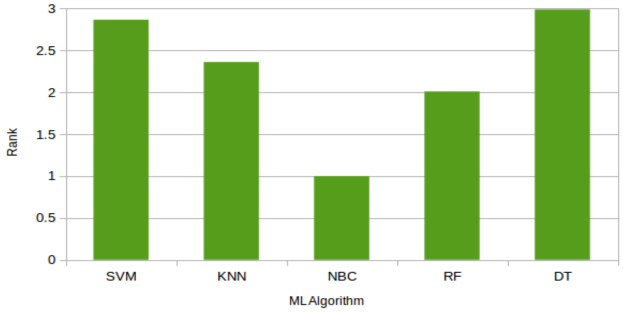

FIGURE 7. Final rank score.

B. TESTING POLYNOMIAL REGRESSION

Following the data collection and model construction process, we ran tests to find the optimal value of the polynomial order n. While higher order polynomials are considered to be more accurate, they are subject to over-fitting concerns. Also, incrementing n implies an exponential increase in coefficient matrix size, and the time it takes to construct it. Figure 8 shows the resulting accuracy for each polynomial order. The coefficients derived for each polynomial order used is presented in Table 4. We observe a slight decline in accuracy between the linear and quadratic model due to the inherent property of quadratic equations possessing a single global maxim/minim. This impedes the possibility of approximating periodic data which usually have several minima and maxima. The increase in prediction accuracy from the cubic to the fifth order model is considered not significant enough to warrant the extra computational resources required. As a result, we chose the cubic model for our implementation.

C. IDS EVALUATION OF WBAN (CATEGORY A DEVICES)

We use the network topology seen in Figure 1 for our simulation. Each WBAN cluster consists of 5 sensors and 1 clusterhead. Figures 9 to 14 present the results for both network level and device level intrusion detection with varying percentage of compromised nodes and adversarial compositions.

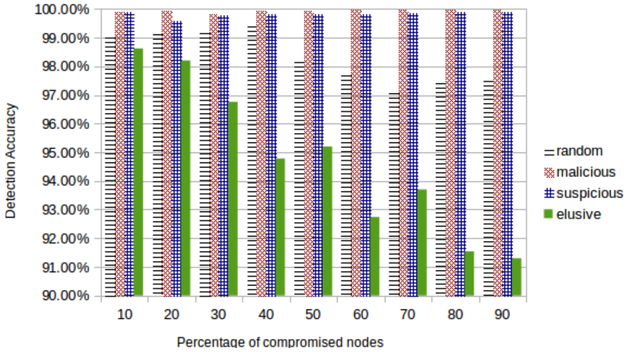

FIGURE 9. Network detection accuracy (WBAN cluster).

Figures 9 and 10 show that the classification accuracy of malicious adversaries is significantly higher than suspicious,

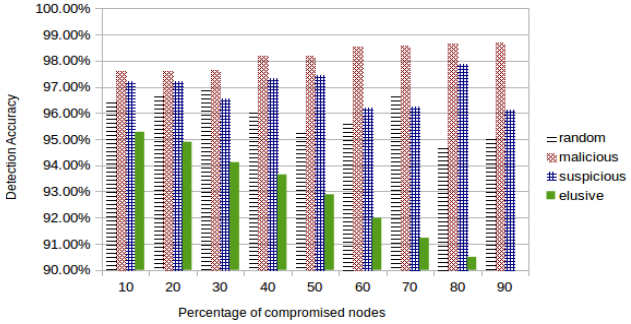

FIGURE 10. Device detection accuracy (WBAN cluster).

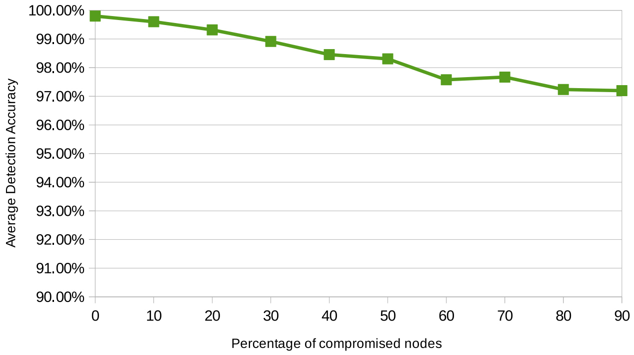

FIGURE 11. Network intrusion detection average accuracy (WBAN).

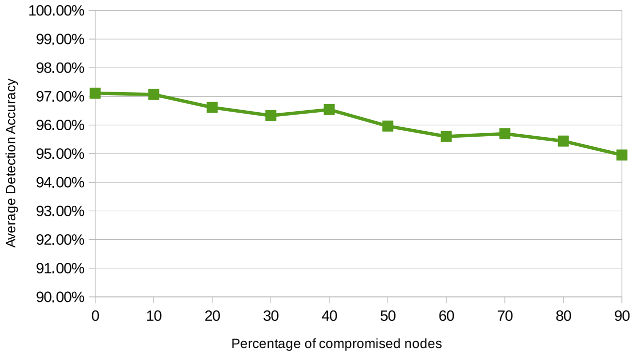

FIGURE 12. Device intrusion detection average accuracy (WBAN).

and elusive adversaries due to their overt approach. The system is less efficient against the elusive adversaries due to their erratic transitions from benign to malicious roles. The same trend is observed for device-level detection with polynomial regression (PR). However, the average accuracy is lower for PR possibly due to the irregular nature of the simulated patient ECG data. By using a more stochastic data trend, we test the limits of our detection system in areas of extreme uncertainties.

Figures 11 and 12 show that the average detection accuracy declines steadily for both network and device intrusion detection with increasing number of elusive adversaries in the network as percentage of compromised nodes increases. From our observations in Figures 13 and 14, the system performs best at an accuracy of 99.6% and 98.2% for network and device-level intrusion detection respectively, when the

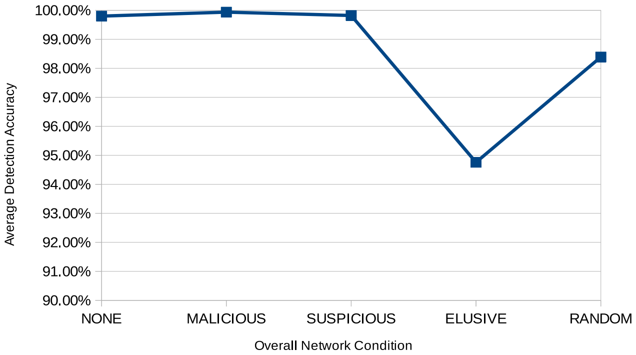

FIGURE 13. Network intrusion detection accuracy per adversary (WBAN cluster).

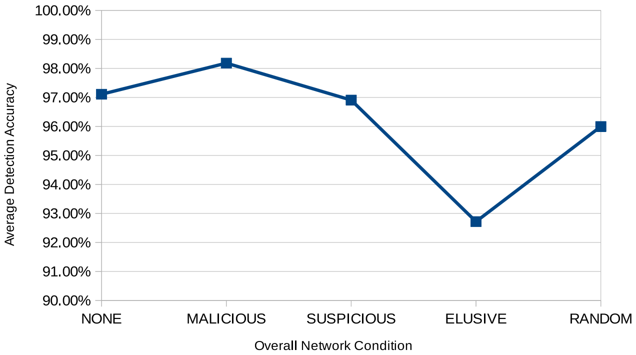

FIGURE 14. Device intrusion detection accuracy per adversary (WBAN cluster).

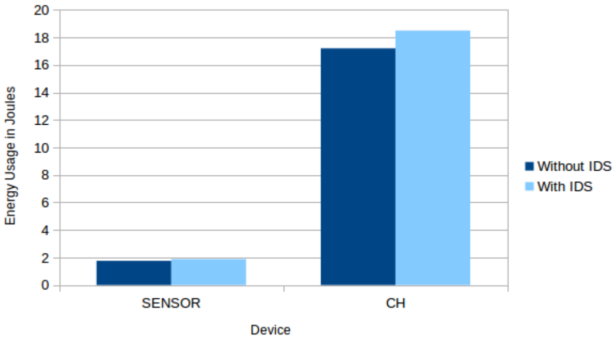

FIGURE 15. Energy usage per device (WBAN cluster).

percentage of malicious adversaries is high. However, when a greater percentage of the network adversaries are elusive in nature, we achieve a lower detection accuracy of 94.9% and 92.8% for network and device-level intrusion detection respectively

In addition to testing the system accuracy, we also measured energy consumption to assess the robustness of the system. We focused on communication and computation energy sources in our model. We extracted the values of communication energy consumed by each device's radio and derived the computational energy as a function of computation time in Equation 17. Figure 15 shows the results of energy consumption with and without the use of intrusion detection system. The results show that an average of 5.2% and 7.03% energy

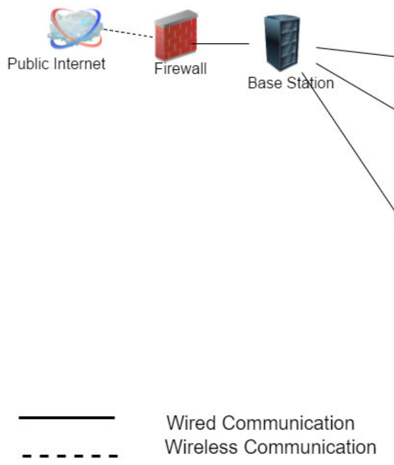

FIGURE 16. Simulated cat B network topology.

overhead occurs on sensors and cluster-heads with intrusion detection system. We find this energy overhead tolerable for an intrusion detection system.

D. IDS EVALUATION OF SMART MEDICAL DEVICES (CATEGORY B DEVICES)

In addition to wireless body area networks, we also simulated, a network of category B devices, composed of smart and connected higher powered devices such as smart beds, smart MRI and scanners etc. (Figure 16). These connected devices differ from WBAN sensing devices in terms of their network connectivity (wired or wireless) and higher computational capabilities.

We repeated our experiments and measure detection accuracy for network and device intrusion detection under varying adversarial compositions. Figures 17 to 18 presents the detection accuracy of category B devices.

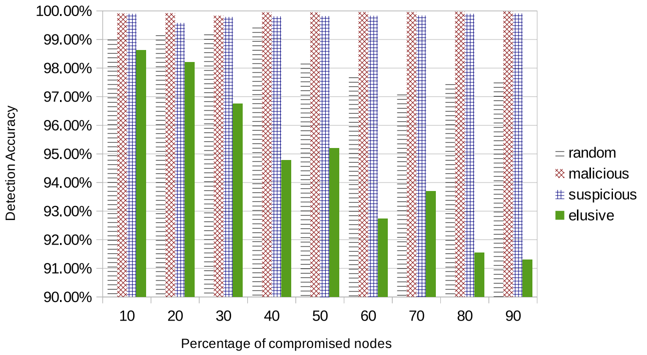

FIGURE 17. Network intrusion detection accuracy (Category B devices).

Simulation results obtained for category B devices nearly follow the same trend as the observations for the WBAN cluster. The system performed best against malicious nodes and was significantly less effective against elusive adversaries for both network and device intrusion detection. However, the overall network intrusion detection accuracy was slightly higher than that of the WBAN clusters. This is possibly due to the fact that, category B devices include wired connectivity to the Internet and hence have increased network bandwidth (Table 2), little or no interference, less packet retransmissions and a more regulated flow of traffic. One notable observation is the significant decrease in accuracy from the network to device intrusion detection. This is due to the application of our regression algorithm on image data from imaging devices. We use an approximation of the pixel matrix into a scalar value derived by Equations 8 to 11. This has a slight negative impact on the accuracy of our regression algorithm, but resulted in exponential decrease in computational time from using Eigenvalues. The best case accuracy is 99.9% and 97.81% for network and device-level detection respectively. In the worst case scenario, an accuracy of 95.72% and

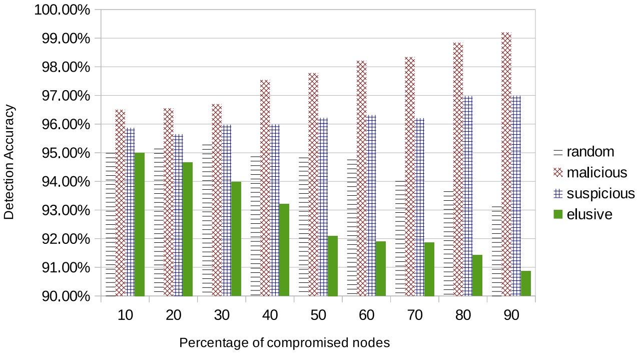

FIGURE 18. Device intrusion detection accuracy (Category B devices).

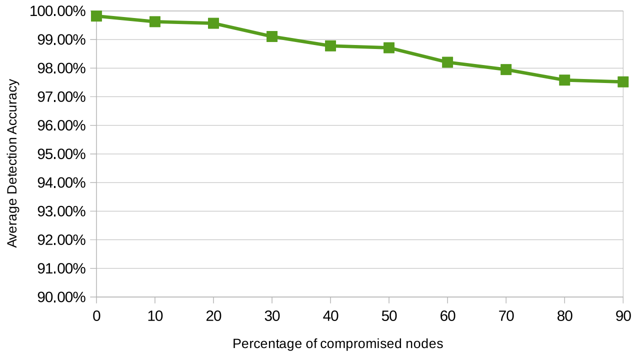

FIGURE 19. Network intrusion detection average accuracy (Category B devices).

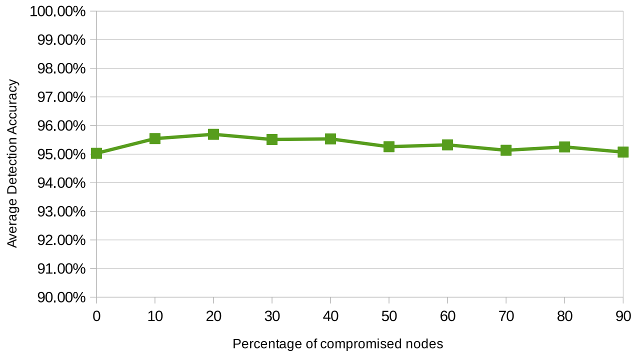

FIGURE 20. Device intrusion detection average accuracy (Category B devices).

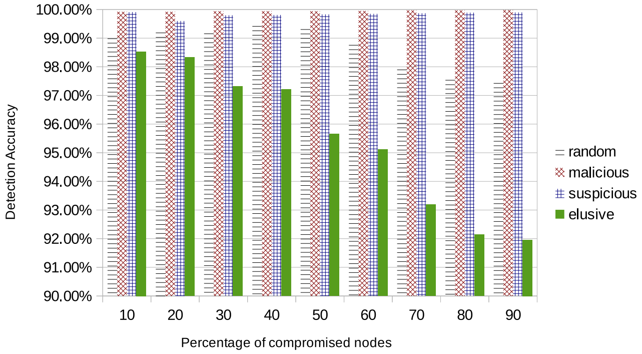

FIGURE 21. **Network intrusion detection accuracy (Smart health grid).**

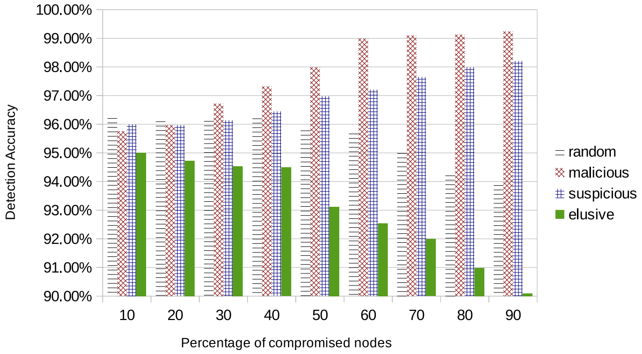

FIGURE 22. **Device intrusion detection accuracy (Smart health grid).**

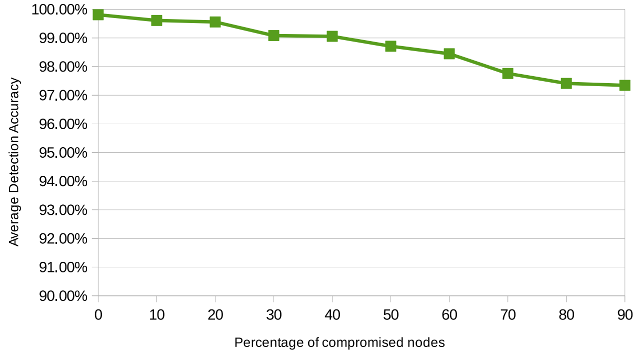

FIGURE 23. **Network intrusion detection average accuracy (Smart health grid).**

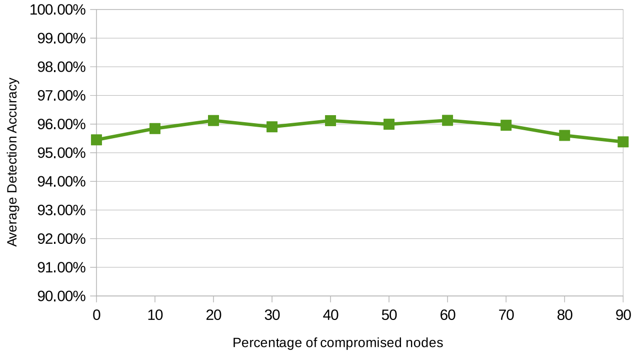

FIGURE 24. **Device intrusion detection average accuracy (Smart health grid).**

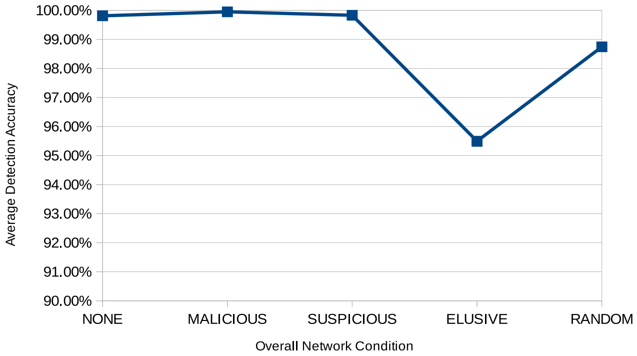

FIGURE 25. **Network intrusion detection accuracy per adversary (Smart health grid).**

92.91% is realized for both levels of detections respectively. The relationship between the adversarial composition and system accuracy is very similar to that of the WBAN Cluster.

E. IDS EVALUATION OF INTERNET OF MEDICAL THINGS

After independently testing the two subsections of the network, we evaluated of the network as a whole, as shown in Figure 2. In this phase of the experiment, we combined both classes of devices to form a complex network of multiple variants of wireless medical sensing and imaging devices.

Since category B devices generate most of the network traffic, they contributed most to the network IDS accuracy trend. In the combined IoMT network, the system had a best case accuracy of 99.8% and 97.93% for network and device intrusion detection respectively. The worst case accuracy was recorded to be 95.21% and 93.17% for both detection levels respectively.

Table 5 displays the comparative system performance for each type of network. The WBAN cluster performed best in device-level IDS and worst in network IDS. Conversely, the category B devices performed best in network IDS, and worst in device IDS, while the combined IoMT network demonstrated moderate performance for both types of detection.

1) SCALABILITY TEST

In the final phase of the experiment, we tested the system for scalability by running repeated simulations with increasing number of devices. In each run, we measured the average energy consumed by the cluster-head and observed its relationship to the number of devices. The result presented in Figure 27 shows that our system scales well with increasing number of devices. The difference in CH energy usage between a 2 and 5 cluster network (10 and 25 devices) is approximately 1 Joule. The single cluster network consumed a relatively low amount of energy due to the absence of extra communication amongst multiple cluster-heads.

We tested a total of 72 varying simulations for each network type with an overall best and worst case detection accuracy of 99.9% and 92.91% respectively out of 216 simulations in total. The system also incurred an energy overhead between 5-7% for both network devices and cluster-heads.

TABLE 5. Comparative system performance.

Network Type	Network IDS	Device IDS
WBAN-Cluster	1	3
Category B Devices	3	1
Smart-Health-Grid	2	2

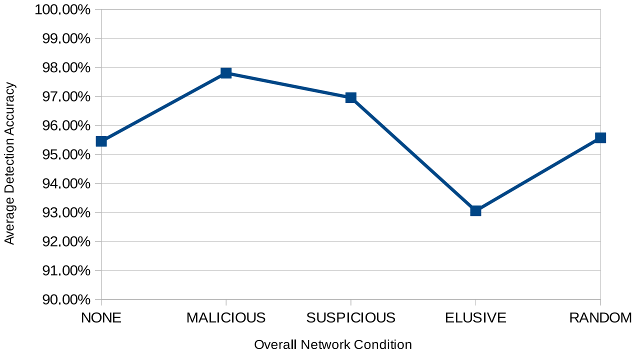

FIGURE 26. Device intrusion detection accuracy per adversary (Smart health grid).

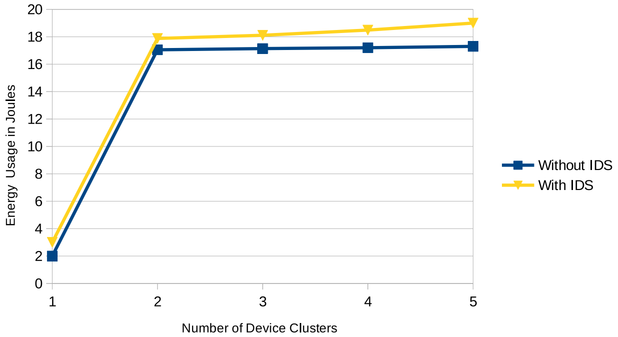

FIGURE 27. Energy usage with increasing clusters (5 devices per cluster).

Our results strongly proves the effectiveness of our system in providing adequate security for IoMT networks with smart and connected devices.

VII. CONCLUSION

In this research, we designed and developed a novel mobile agent driven intrusion detection prototype for Internet of Medical Things using machine learning for detecting intrusions at the network and device level respectively. We tested different polynomial orders for accuracy as well as efficiency and conclude that the third order polynomial was most appropriate for approximating the model without incurring higher computational resources. We evaluated our detection system by emulating different use-case scenarios with network and device level detection executing in parallel and obtained promising results in terms of accuracy. In our future research, we plan to further reduce device specific energy consumption of the detection system. We also plan to examine alternative algorithms such as state graphs for analyzing change in sensor data trends as opposed to regression which deals with actual sensor data samples.

REFERENCES

[1] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, ''The Internet of Things for health care: A comprehensive survey,'' *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.

[2] D. V. Dimitrov, ''Medical Internet of Things and big data in healthcare,'' *Healthcare Inform. Res.*, vol. 22, no. 3, pp. 156–163, 2016.

[3] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, ''Security and privacy in the medical Internet of Things: A review,'' *Secur. Commun. Netw.*, vol. 2018, Mar. 2018, Art. no. 5978636.

[4] *IBM 2016 Cost of Data Breach Study—United States*, I. Corp, Washington, DC, USA, Sep. 2016.

[5] T. Yaqoob, H. Abbas, and M. Atiquzzaman, ''Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3723–3768, 4th Quart., 2019.

[6] R. V. Sampangi, S. Dey, S. R. Urs, and S. Sampalli, ''A security suite for wireless body area networks,'' 2012, *arXiv:1202.2171*. [Online]. Available: http://arxiv.org/abs/1202.2171

[7] A. S. Sangari and J. M. L. Manickam, ''Public key cryptosystem based security in wireless body area network,'' in *Proc. Int. Conf. Circuits, Power Comput. Technol.*, Mar. 2014, pp. 1609–1612.

[8] W. Li and X. Zhu, ''Recommendation-based trust management in body area networks for mobile healthcare,'' in *Proc. IEEE 11th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Oct. 2014, pp. 515–516.

[9] L. Sun and Q. Du, ''A review of physical layer security techniques for Internet of Things: Challenges and solutions,'' *Entropy*, vol. 20, no. 10, p. 730, Sep. 2018.

[10] W. Trappe, ''The challenges facing physical layer security,'' *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[11] G. Thamilarasu and Z. Ma, ''Autonomous mobile agent based intrusion detection framework in wireless body area networks,'' in *Proc. IEEE 16th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2015, pp. 1–3.

[12] A. Odesile and G. Thamilarasu, ''Distributed intrusion detection using mobile agents in wireless body area networks,'' in *Proc. 7th Int. Conf. Emerg. Secur. Technol. (EST)*, Sep. 2017, pp. 144–149.

[13] T. Dimitriou and K. Ioannis, ''Security issues in biomedical wireless sensor networks,'' in *Proc. 1st Int. Symp. Appl. Sci. Biomed. Commun. Technol.*, Oct. 2008, pp. 1–5.

[14] P. Kumar and H.-J. Lee, ''Security issues in healthcare applications using wireless medical sensor networks: A survey,'' *Sensors*, vol. 12, no. 1, pp. 55–91, Dec. 2011.

[15] G. Kambourakis, E. Klaoudatou, and S. Gritzalis, ''Securing medical sensor environments: The codeblue framework case,'' in *Proc. 2nd Int. Conf. Availability, Rel. Secur.*, Apr. 2007, pp. 637–643.

[16] N. Nasser and Y. Chen, ''SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks,'' *Comput. Commun.*, vol. 30, nos. 11–12, pp. 2401–2412, Sep. 2007.

[17] G. Thamilarasu, ''IDetect: An intelligent intrusion detection system for wireless body area networks,'' *Int. J. Secur. Netw.*, vol. 11, nos. 1–2, p. 82, 2016.

[18] K. M. Anandkumar, C. Jayakumar, P. A. Kumar, M. Sushma, and R. Vikraman, ''Intrusion detection and prevention of node replication attacks in wireless body area sensor network,'' *Int. J. UbiComp*, vol. 3, no. 3, pp. 1–10, Jul. 2012.

[19] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, ''IMDGuard: Securing implantable medical devices with the external wearable guardian,'' in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.

[20] H. Wang, H. Fang, L. Xing, and M. Chen, ''An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN),'' in *Proc. IEEE Int. Conf. Commun.*, Jun. 2011, pp. 1–5.

[21] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, ''SoK: Security and privacy in implantable medical devices and body area networks,'' in *Proc. IEEE Symp. Secur. Privacy*. Washington, DC, USA: IEEE Computer Society, May 2014, pp. 524–539.

[22] M. Toorani, "On vulnerabilities of the security association in the IEEE 802.15.6 standard," 2015, *arXiv:1501.02601*. [Online]. Available: http://arxiv.org/abs/1501.02601

[23] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.

[24] S. Li, "Security and vulnerability in the Internet of Things," in *Securing the Internet of Things*, S. Li and L. D. Xu, Eds. Boston, MA, USA: Syngress, 2017, ch. 3, pp. 49–68. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128044582000032

[25] S. Soderi, L. Mucchi, M. Hämäläinen, A. Piva, and J. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 7, p. e3142, 2017.

[26] L. Mucchi, L. Ronga, and L. Cipriani, "A new modulation for intrinsically secure radio channel in wireless systems," *Wireless Pers. Commun.*, vol. 51, no. 1, pp. 67–80, 2009.

[27] J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isacoff, E. Spafford, and D. Zamboni, "An architecture for intrusion detection using autonomous agents," in *Proc. 14th Annu. Comput. Secur. Appl. Conf.*, Dec. 1998, pp. 13–24.

[28] P. Kannadiga and M. Zulkernine, "DIDMA: A distributed intrusion detection system using mobile agents," in *Proc. 6th Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput. 1st ACIS Int. Workshop Self-Assembling Wireless Netw. (SNPD/SAWN)*, May 2005, pp. 238–245.

[29] S.-C. Zhong, Q.-F. Song, X.-C. Cheng, and Y. Zhang, "A safe mobile agent system for distributed intrusion detection," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 4, Nov. 2003, pp. 2009–2014.

[30] M. Riecker, S. Biedermann, and M. Hollick, "Lightweight energy consumption based intrusion detection system for wireless sensor networks," in *Proc. 28th Annu. ACM Symp. Appl. Comput. (SAC)*, 2013, pp. 1784–1791.

[31] O. Kachirski and R. Guha, "Intrusion detection using mobile agents in wireless ad hoc networks," in *Proc. IEEE Workshop Knowl. Media Netw.*, Jul. 2002, pp. 153–158.

[32] S. Khanum, M. Usman, and A. Alwabel, "Mobile agent based hierarchical intrusion detection system in wireless sensor networks," *Int. J. Comput. Sci. Issues*, vol. 9, pp. 101–108, Jan. 2012.

[33] *Omnet++ WBAN Projects | Wireless Body Area Network Projects*, Open-Sim Ltd., 2011.

[34] J. Ulvila and J. Gaffney, "Evaluation of intrusion detection systems," *J. Res. Nat. Inst. Standards Technol.*, vol. 108, pp. 453–473, Nov. 2003.

[35] U. Banerjee, G. Batra, and K. V. Arya, "Feedback reliability ratio of an intrusion detection system," *J. Inf. Secur.*, vol. 3, no. 3, pp. 238–244, 2012.

[36] Y. Zhang, Y. Liu, L. Zhuang, X. Liu, F. Zhao, and Q. Li, "Accurate CPU power modeling for multicore smartphones," Microsoft Res., Redmond, WA, USA, Tech. Rep. MSR-TR-2015-9, Feb. 2015.

GEETHAPRIYA THAMILARASU received the M.S. degree in electrical engineering, in 2004, and the Ph.D. degree in computer science and engineering from the University at Buffalo, in 2009. She is currently an Assistant Professor with the Department of Computing and Software Systems, University of Washington Bothell, where she leads the Mobile Embedded and Wireless Security (MEWS) Research Group. She has authored and has published several papers in leading international journals and peer-reviewed conferences in networking and security. Her research interests include wireless network security, wireless and mobile health systems, machine learning for security, wireless body area networks, and the Internet of Things. She is a professional member of IEEE, ACM, and the Society of women engineers. She has served in many roles as the Program Committee Chair, the Session Chair, and an Organizing Committee Member at various networking conferences, including IEEE International Conference on Computer Communications and Networks, the ACM Conference on Embedded Networked Sensor Systems, and the ACM International Joint Conference on Pervasive and Ubiquitous Computing.

ADEDAYO ODESILE received the bachelor's degree in computer science from Babcock University, Nigeria, and the M.S. degree in computer science and software engineering from the University of Washington Bothell. His research interest includes cyber security for emerging technologies. During the course of his graduate study, he designed and implemented distributed intrusion and anomaly detection algorithm capable of running on low-powered wireless body area network devices. He has published and coauthored in major IEEE conferences. He currently works on applying distributed computing techniques in improving security, system efficiency, resiliency, and throughput.

ANDREW HOANG is currently pursuing the bachelor's degree in computer science with the Paul G. Allen School of Computer Science and Engineering, University of Washington, with a focus in data science. His research interests include computer vision, natural language processing, and machine learning. He is particularly interested in the intersection of the two, and in how to incorporate external knowledge into neural models.