A multiagent based framework secured with layered SVM-based IDS for remote healthcare systems

MohammadReza Begli · Farnaz Derakhshan

Received: date / Accepted: date

Abstract Since the number of elderly and patients who are in hospitals and healthcare centers are growing, providing efficient remote healthcare services seems very important. Currently, most such systems benefit from the distribution and autonomy features of multiagent systems and the structure of wireless sensor networks. On the one hand, securing the data of remote healthcare systems is one of the most significant concerns; particularly recent types of research about the security of remote healthcare systems keep them secure from eavesdropping and data modification. On the other hand, existing remote healthcare systems are still vulnerable against other common attacks of healthcare networks such as Denial of Service (DoS) and User to Root (U2R) attacks, because they are managed remotely and based on the Internet. Therefore, in this paper, we propose a secure framework for remote healthcare systems that consists of two phases. First, we design a healthcare system base on multiagent technology to collect data from a sensor network. Then, in the second phase, a layered architecture of intrusion detection systems that uses Support Vector Machine to learn the behavior of network traffic is applied. Based on our framework, we implement a secure remote healthcare system and evaluate this system against the frequent attacks of healthcare networks such as Smurf, Buffer overflow, Neptune, and Pod attacks. In the end, evaluation parameters of the layered architecture of intrusion detection systems prove the efficiency and correctness of our proposed framework.

Keywords Healthcare system · Multiagent system · Intrusion detection system (IDS) · Support vector machine (SVM) · Denial of service (DoS) · User to root attacks (U2R)

1 Introduction

By growing the number of elderly and patients, providing healthcare services becomes difficult. Accordingly, using an intelligent system can facilitate these services. However, such a system should provide healthcare services without interrupting [1]. Consequently, appropriate hardware and software platform must be applied to design and implement healthcare systems. To this end, wireless sensors as a hardware platform can collect data of elderly or patients continuously and the system can provide the right response when it is necessary. On the one hand, the diversity of the data obtained from sensors in a healthcare system makes this data incorrect, unclear, and sometimes contradictory. On the other hand, sensors in an environment and patients cannot aggregate and make decisions based on the received data. To overcome this problem, using multiagent systems would be a good software model to manage these data [1].

Another main issue of healthcare systems is to secure personal data in wireless sensor networks of healthcare systems against attacks. Since healthcare systems are remotely manageable and based on Internet, they are vulnerable to frequent attacks of healthcare systems such as Denial of service (DoS) and User to Root (U2R) attacks. Consequently, attackers can make healthcare networks unavailable by DoS attacks, or a user who has
access to data of a healthcare system can get a higher access level by committing User to Root attacks. Therefore, in this research, we propose a framework that contains two steps. In the first step, we design a layered multiagent-based architecture. In the second step, we introduce a layered architecture to consider intrusion detection systems (IDS) for our agent-based healthcare system. Consequently, we classify agents according to their energy consumption and security of their data. Then, we allocate an intrusion detection system (IDS) [2] to each group of agents.

In multiagent systems (MAS), agents interact with each other autonomously. They do their jobs based on data gathered from sensors without interrupting other processes [1]. Consequently, using multiagent systems is a proper method to design our healthcare system.

In the second step of our framework, we assign intrusion detection systems to the agent-based healthcare system. Consequently, we introduce intrusion detection systems in the following paragraph briefly. Intrusion detection systems monitor and analyze activities in computer systems or computer networks to find out suspicious events that intrude them. Different kinds of Intrusion detection systems can be categorized base on the type of events that they monitor and their implementation [2]. In this paper, we use anomaly and misuse (signature-based) host-based Intrusion detection systems.

Therefore, the purpose of this paper is to propose a framework based on multiagent technology for collecting data from an environment and patients using a secured wireless sensor network at a hospital or a health facility. In this paper, we design an agent-based healthcare system to collect sensor networks data, provide healthcare services, and consider the security of healthcare sensor networks to confront possible attacks.

After this introduction, the rest of this paper is as follows: In the section 2, we shortly discuss related works, which are related to the background of our framework. In the section 3, we explain our proposed framework. The simulation results, which show and evaluate the performance of the framework, are presented in the section 4. In the section 5, first, we discuss our contribution to the improvement of healthcare systems, and then we compare our framework with some similar works in the past. Finally, in the section 6, we end this paper with a conclusion and mention some future works.

2 Related works

This section presents some of the related works about remote healthcare systems, secured healthcare systems, and SVM-based intrusion detection systems. The basic concepts of this section are the prerequisite of our framework.

2.1 Remote healthcare systems

Remote healthcare systems, which monitor the status of patients remotely and widely, consist of three main parts: 1) Some wireless sensors, 2) Sensor analysis and signal analysis to detect problems, and 3) Alert to healthcare staff. Aingeru [3, 4, 5], PANGEA [1, 6], MADIP [7], JTH [8], GerAmi [9], Koutkias [10], Kahuza [11], and Cervantes [12, 13] are examples of this kind of healthcare systems. Among these healthcare systems, PANGEA and MADIP systems are more recent than the others, and Aingeru system is similar to our proposed framework. Consequently, we introduce Aingeru, PANGEA, and MADIP in the following paragraphs briefly.

Aingeru healthcare system is a Java-based system. It also uses the Jade tool, which is a Java-based tool, as an agent platform. In this system, sensors are connected to PDA devices by Bluetooth 1.1 wireless connection, and PDA devices are connected to the Control Center by a GPRS connection. This healthcare system gives intelligent, comprehensive, and constant monitoring of the elderly and patients. Every cared person has a sensor-connected PDA, which is responsible for measuring vital parameters (such as heart rate, amount of oxygen in the blood). The system evaluates data locally (on a PDA) and delivers results to a relevant specialist in an emergency. The control center of a hospital collects all data from patient-connected sensors. Then it stores them in the central database. Physicians can get access to all relevant data of patients through a web-based program. The main components of this system are 1) PDA of a user that is for supervising users, 2) The control center that provides remote services, 3) The health center that gives medical services, and 4) Technical center, which is responsible for maintenance of all infrastructures.

The PANGEA multiagent healthcare system launched and tested at El Residencial La Vega healthcare facility in Salamanca, Spain for 8 months in 2014. In this system, relevant agents respond to condition of an environment based on data of sensors automatically. The following paragraphs are a brief description of the agents in the PANGEA system.

Information Provider Organization: This agent is the interface of the system to communicate with users.

Home Automation Organization: This part includes all agents that are responsible for controlling
sensors in the environment. These sensors are a smoke detector, a temperature sensor, and a presence detection sensor. These agents send all data gathered from these sensors to the ZigBee Supervisor.

ZigBee Supervisor Agent: This agent is responsible for sending data to the database of the system.

Information Agent: This agent is the interface of the database.

Locating Organization: Incorporates all agents that are responsible for controlling sensors of patients to locate them.

Caregiver Organization: Every nurse and physician has one agent that aggregates data related to their activities.

The MADIP is a healthcare system in heterogeneous and wide-range networks such as the Internet or metropolitan and national networks. This system consists of two types of agents including static agents and mobile agents. Static agents offer resources and facilities for mobile agents. Mobile agents operate autonomously and communicate with static agents and host systems by using network infrastructure. The main parts of the MADIP system are as follows: User agent, Diagnostic agent, and resource agent as static agents, physician agent as a mobile agent, knowledge-based data server, and external services.

2.2 Security of agent-based healthcare systems

In the following, we study earlier works about the security of agent-based healthcare systems. The priority concern of healthcare systems is sensitive data protection from unauthorized users. The simple approach in [14] uses the Access Control (AC) mechanism to address this problem. However, traditional AC models are inflexible and difficult to apply in healthcare systems, so this paper proposes two data filtering layers (policies) before returning results to the user, including access policy (public cloud) and privacy policy (private cloud). It introduces an access control model focusing on privacy protection for the healthcare systems. These two sets of policies protect patient records of healthcare systems, so they are accessible securely.

Fog computing provides storage, computing, and networking between end devices and the cloud [15]. Portable devices can be fog servers, where they can perform many tasks such as processing, visualization, and transferring data to the cloud. The main idea of Fog computing is to migrate some tasks of cloud data center tasks to the fog servers on the network edge. Also, Fog computing has proven to be extremely useful in time-sensitive applications such as health care applications [16–18]. Consequently, the use of Fog computing improves security because of its proximity to the devices [19] and accelerates real-time data processing of applications [19]. Since medical information is considered sensitive data, the privacy issue in e-health systems is vital. This issue has been taken care of in [20] by prohibiting unauthorized access and encrypting information before sending it to storage.

The biometric features acquired from biosignals are distinctive and random. Consequently, they can develop security mechanisms for smart healthcare systems. In [21] the Inter-Pulse Intervals (IPIs) extracted from heartbeats are used to generate secret keys to secure WBSNs. These keys are distributed to nodes within and outside the WBSNs to secure data transmission in remote healthcare platforms.

In [22] a three-factor authentication protocol, which is based on Shamir’s threshold scheme, increases the security and privacy of data in healthcare systems and minimizes the communication cost.

The architecture of the healthcare system proposed in [23] is composed of three layers. The first layer, which is the lowest layer and called Sensor Network Tier layer, includes two types of sensors. The first type is the wearable sensor system that pairs with biological sensors (belt attached to caregivers). The second type is the sensors that are located in a building and are responsible for transmitting data of an environment using a wireless or wired network with the ZigBee protocol [24]. The second layer, called mobile computing network tier, includes mobile devices such as PDA devices and laptops that connect to a fixed station using a network infrastructure or a multi-hub network. The third layer, back-end network tier, includes stationary stations and servers that give application layer services for lower layers and is responsible for processing and saving the data received from mobile devices.

The purpose of this architecture is to keep the confidentiality of the data stored in each layer using a digital signature or proper encryption. For example, in the network layer of this sensor network, AES encryption secures the communication between each pair of nodes. Access of devices in the second layer to the data of the first layer is limited, so access is available after authentication. Furthermore, each device in the second layer has a public key and private key pair that is assigned by a third-party entity from the third layer (local server). Hosts in the second layer use this key pair to encrypt access to the first layer.

In [25], the approach is to balance the performance and the security of a sensor-based healthcare system. In this way, this sensor network consists of three parts as follows: the Medical Sensor Network (MSN), the Pa-
tient Area Network (PAN), and a service center. Also proposed security architecture consists of three separate and complementary layers, so there is a security structure for each part of the network.

The MSN layer includes environment sensors such as temperature and humidity sensors and mobile devices such as PDA devices. Symmetric encryption secures the communication between each pair of nodes in this layer. The security layer of PAN, which includes patient-connected sensors, secures medical data associated with MSN-layer nodes (such as physicians and nurses) and a service center. This security layer authenticates devices connected to patients by using a private key. The corresponding security layer of the service center consists of a public key and a certificate. Therefore, components of the PAN and the MSN can receive a pair of private and public keys and a unique identification number (ID) by having the public key of the service center certificate.

To conclude, encryption algorithms are proposed to secure remote healthcare systems in these pieces of research. However, the cryptographic algorithms cannot confront attacks except eavesdropping and data modification, which means these systems are vulnerable to other common attacks of remote healthcare systems such as buffer overflow. Therefore, in this research, we intend to improve this security weakness of earlier remote healthcare systems by considering the energy consumption of sensors and the sensitivity of their data.

2.3 SVM-based IDS

In our proposed framework, we intend to improve the security weakness of remote healthcare systems mentioned in the previous paragraph. For this purpose, we use intrusion detection systems in our proposed framework. We explain the mechanism of intrusion detection systems in the next section. These intrusion detection systems use the support vector machine to classify network traffic. Therefore, in this section, we introduce earlier works about intrusion detection systems to prove the advantages of SVM in comparison to other network traffic classifiers.

In [26], machine-learning methods such as Optimal Power Flow (OPF), SVM, and K-Nearest Neighbors (KNN) collaborate to find abnormal traffic in computer networks. The network traffic contains information such as source and destination IP address, packet count, service type, protocol type, source port, destination port, start time, and end time of a session between two hosts in a network. The focus of this research is on DoS, Brute Force, and Port Scanning attacks. The IDS in this research detects all these three types.

In [27], the IDS consists of the PCA (principal components analysis) method and the SVM. The approach of this research is to select a suitable set of features. NSL-KDD standard data set is used to evaluate the performance of the proposed IDS.

Research [28] describes SVM as one of the best methods to detect abnormal behaviors in networks and proposes an SVM based IDS. It mentions that SVM has a high computational cost, although if the number of features of the training set decreases, the SVM machine will perform better.

Research [29] proposes an SVM-based IDS to identify attacks in enterprise networks. The features are selected by information techniques to learn multiple SVM. According to [29], this method has a higher detection rate than the artificial neural network. Furthermore, some other works in this field prove that SVM performs better than different network traffic classifiers [30, 31].

According to the earlier research, which we reviewed in this section, we got enough background knowledge for our proposed framework. Therefore, in the next section, we describe our framework.

3 System overview

In this section, we introduce our framework for multiagent-based healthcare systems that facilitates the provision of healthcare services and secures the wireless sensor network of healthcare systems against attacks simultaneously.

Multiagent systems help us to integrate data in remote healthcare systems due to the distribution of the data. Each agent has a specific responsibility and interacts with other agents to manage and analyze the data to improve services. Therefore, we design our architecture base on multiagent systems. Consequently, as shown in Figure 1, the first step is to define and plan agents of our system. The second step is to classify agents according to their data and energy capacity. Then, for each group of agents, we consider a proper IDS to secure the sensor network of our healthcare system against attacks.

Therefore, in the first part of this section, we design our multiagent framework and plan agents, capabilities, and goals of them. In the second part of this section, we classify agents according to their data and energy capacity. Then we add a suitable IDS to each group of agents.
3.1 Multiagent design

In this section, we present the multiagent design of our healthcare system. Figure 2, which represents all agents and interactions between them in Tropos methodology, shows the multiagent architecture of our proposed framework. Tropos [32–34] is a software engineering method for designing multiagent systems. This methodology covers all concepts of agents such as goals, programs, and tasks at the development stage. It also focuses on software requirements. The Tropos methodology is about agents and all its related ideas and analysis of primary software needs. The actor diagram is for the stage of determining the basic requirements of the software. In the Tropos methodology, a circle expresses an agent, an ellipsoid shows a goal, a cloud shows a soft goal, and a dashed line implies that there are several sub-systems of the same kind. A soft goal is an ambiguous goal in a system that there is no clear benchmark for achieving. Actors in multiagent systems are agents that play a role in a system. Therefore, according to Figure 2, there are five actors in our proposed framework. In the following paragraphs, we introduce these agents (actors).

**Patient agent** manages all data related to patients. These data include the profile of patients, heart rate, blood pressure, body temperature, and the location of patients. The database center saves these data at the start of admission to a health facility center. Also, real-time sensors of patients collect other necessary data such as blood pressure, heart rate, and body temperature. Presence sensors attached to patients also find the location of patients and detect the presence of patients in their beds. This agent detects the condition of patients after the integration of health monitoring data. After reviewing the collected data, if the patient agent diagnoses the health condition of a patient as unsuitable, it will alert the nurse agent. Also, the patient agent can send his/her request to the nurse agent.

**Nurse agent** manages activities of nurses according to the priorities of them. This agent reports the status of patients to a specific nurse and warns in an emergency. It also requests nurses to do activities and collects reports from them.

**Physician agent** Physicians do their jobs with the help of this agent on portable devices such as tablets, laptops, and smartphones. This agent helps them to monitor the status of patients and receive reports of nurses. Physicians check the condition of patients and the activities of nurses with the help of the physician agent virtually. They can also check the health condition of patients and send out all activities that nurses should do for patients with the help of this agent.

**Ambient agent** controls sensors in an environment include smoke detector sensors and temperature sensors. This agent identifies the condition of an environment after collecting the data of these sensors. If this agent detects an emergency in an environment such as a fire near to patients, it will alert nurses.

**Database agent** is the database interface. It maintains and manages the profile of patients. This agent keeps alert messages with the feedbacks of nurses.

According to Figure 3, after the admission of patients to a healthcare center, the interactions between the agents begin as follows:

1. After collecting data from patients, the patient agent sends identity information of patients, such as name, age, and date of entrance, to the database agent. The database agent saves them in the database.
2. The patient agent analyzes data, including blood pressure, heart rate, and body temperature, to find the health condition of patients. After analyzing the obtained data, if the patient agent detects that the health condition of a patient is unsuitable, it will alert the nurse agent.
3. The patient agent sends the request of the patient to the nurse agent.
4. The ambient agent collects the data of ambient sensors, including smoke detector sensors and temperature sensors, to detect the status of an environment. In an emergency, this agent alerts the nurse agent.
5. The nurse agent sends the activity reports of nurses to the physician agent after nurses react to received alerts.
6. The nurse agent sends activity reports to the database agent to save the alerts and their reactions.
7. The physician agent can request the nurse agent to do treating activities.
8. The physician agent can ask the patient agent to send the health condition of patients.
9. The patient agent responds to the request of the physician agent by sending blood pressure, heart rate, body temperature, etc.

3.2 Layered architecture of intrusion detection systems

As we mentioned before, the second step is securing the healthcare system. We use a clustered wireless sensor network [35] (one of the most common network topologies in sensor networks) in our healthcare system. Because of the difference in activities of each sensor, the probability of an attack is different for each one. Therefore, in the following paragraph, we discuss the mechanism of the IDS for clustered wireless sensor networks in the research [36].

The capabilities of sensors in clustered sensor networks are heterogeneous [37, 38]. Sinks need to collect data from all clusters in these networks, so they have more processing power and use more energy than sensors. Cluster sensors also have more processes than ordinary sensors, so they use more energy. Other sensors do not have the same capacity as cluster heads because they only collect ambient data within their scope. Consequently, the capabilities of sinks are more than cluster heads, and the capabilities of cluster heads are more than other sensors. As a result, sinks and cluster heads are more affected by attacks than ordinary sensors, and they should have better security measures.

We also arrange the agents of our framework and use an IDS suitable for each group of agents with similar reasons. As shown in Figure 4, first, we classify the agents based on the sensitivity of their data and the energy level of their corresponding sensors. In this case, the database agent and other agents (that have data from aggregated sensors) have better security measures than those with restricted data.

The patient agent collects the health data of patients, and the ambient agent collects the data of ambient sensors. Therefore, these two agents have restricted data, which are not valuable for attackers. Consequently, they rarely attack these agents. Furthermore, the wearable sensors of patients have limited energy, so we consider an anomaly IDS for these agents. Anomaly intrusion
Fig. 3 The association of the agents in the proposed framework

detection systems, which have a high detection rate, create a model of normal traffic, and detect network attacks by comparing network traffic with the model. However, anomaly intrusion detection systems identify some normal traffic of networks which has different patterns from the rest as an attack wrongly, so they have a high false-positive rate and low accuracy [36]. Also, they have a low computational cost and low power consumption because of their simple structure, which makes them suitable for both the patient and the ambient agents.

The nurse agent collects the health status of patients and the status of the ambient agents. Then, in an emergency, the nurse agent alerts nurses, and after recording feedbacks of nurses, the nurse agent sends a record of alerts to the database agent. Besides, the physician agent can ask the nurse agent to do a specific action, such as sending the health status of patients. Consequently, the nurse agent and the physician agent collect data from patients and environments, which makes them more likely to be attacked than the patient agent and the ambient agent. The physician agent and nurse agent do not collect data directly from sensors, and they run on mobile devices such as mobile phones, so they have more energy supply than the ambient agent and the patient agent. As a result, we consider a misuse intrusion detection system for the physician agent and the nurse agent. Misuse intrusion detection systems detect the type of attacks in addition to the normal, and attack traffic, so they have a more complex structure, higher processing cost, and more energy consumption than anomaly intrusion detection systems.

The database agent saves profiles of patients, alerts of the patient agent and the ambient agent to the nurse agent, and reports of nurses’ reactions. This agent collects and saves all data of sensors in our healthcare system. Consequently, the database agent is more likely to be attacked than the rest of the agents and requires a better intrusion detection system than the two lower layers in Figure 4. As a result, we consider a hybrid intrusion detection system for this agent. In hybrid intrusion detection systems, an anomaly intrusion detection system and a misuse intrusion detection system complement each other. The anomaly intrusion detection sys-
tem, which has a high detection rate, detects anomaly traffic. Then the misuse intrusion detection system corrects traffic, in which the anomaly intrusion detection system detects abnormal wrongly due to its low accuracy [39]. Finally, the decision-making unit determines the type of traffic. Therefore, hybrid intrusion detection systems use the high detection rate of anomaly intrusion detection systems and the high accuracy of misuse intrusion detection systems.

Table 1 shows the rules of the decision-making unit of the hybrid intrusion detection system. As we mentioned before, anomaly intrusion detection systems have a high detection rate in detecting normal traffic. In the first rule, this feature helps to distinguish normal traffic. We also mentioned that anomaly intrusion detection systems have low accuracy in detecting attacks. The high accuracy of misuse intrusion detection systems modifies this low accuracy in the second and third rules. Consequently, if the misuse IDS does not find an attack that the anomaly IDS detects, so this traffic is normal. If the misuse IDS detects the class of an attack that the anomaly IDS find, then it is an attack. Hybrid intrusion detection systems have more computational cost and more energy usage than anomaly intrusion detection systems and misuse intrusion detection systems because they use two different types of intrusion detection systems at the same time. The database agent has an unlimited energy supply (the database server works with electrical power supply.), so hybrid intrusion detection systems fit the database agent perfectly.

So far, we have introduced details of our proposed framework. In the next section, we discuss how to implement the agents in this framework. Additionally, we evaluate the intrusion detection system in each layer of the framework to prove the correctness of the agents’ classification and assigning an IDS to each layer.

4 Experiment

After the phase of analysis and design, we implement and test our framework. In this section, we focus on the evaluation and implementation results of our healthcare system. Also, we examine our solution by using a dataset, and then we present the run-time and the memory consumption of the intrusion detection systems. Finally, we compare previous works in terms of the security of healthcare systems with our proposed method.

4.1 Implementation of our multiagent-based healthcare system

We implement the agents of our proposed framework with JADE tool (version 4.4) in Java (JDK 8) by using NetBeans 8.2. First of all, we create the required agents from the classes which we have implemented with JADE in Java. As we mentioned previously, we use the following agents in this study: Database agent, Physician agent, Nurse agent, Ambient agent, and Patient agent. The database agent saves and manages the profile of patients under the care and keeps alert messages and feedbacks of nurses. In this study, we create a dataset consist of 1000 patients. These samples of patients include blood pressure, body temperature, heart rate, location of patients, ambient emergency, and ambient temperature samples. The patient agent and the ambient agent can access these data. According to the rules of the patient agent and ambient agent, if the health data of patients and the situation of an environment become abnormal, these agents will alert the nurse agent. We also implement other interactions between the agents, which we described previously.

4.2 The data collection of the intrusion detection systems

As we discussed in Section 2, in earlier research, proper encryption algorithms are proposed in three layers to secure healthcare systems. However, these algorithms
cannot confront common attacks of healthcare systems except eavesdropping and data modification. Therefore, our focus in this study is to propose a healthcare system framework that has tight security against common healthcare system attacks. Consequently, we first study the usual attacks on healthcare systems, which previous research mentions. Then we determine their types according to the general classification of network attacks to get an appropriate sample of network traffic to evaluate the intrusion detection systems of our framework.

Network attacks are classified into four groups [40, 41] as follows: Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and Probe. Also, according to [42-44] spoofing attack, impersonation, the elevation of privileges, DoS attack, eavesdropping, and data modification are the usual attacks of healthcare networks. These attacks, except eavesdropping and data modification, are mainly U2R and DoS attacks.

To implement and evaluate the intrusion detection systems of our proposed framework, we use NSL-KDD [45] dataset. This dataset solves some of the inherent problems of the KDD’99 and is a newer version of that. Therefore, the NSL-KDD has some benefits over the KDD datasets as follows: 1) It does not include redundancy of the data or duplicate records in the train set, so the classifiers are not biased towards the more frequent data. 2) There are no duplicate records in the proposed test sets. Therefore, the performance of the learners is not biased by the methods that have better detection rates on frequent data. 3) The number of selected records from each difficulty group is proportional to the percentage of the related data in the original KDD dataset. 4) The number of records in the train and test sets is reasonable, which makes it affordable to run experiments on this dataset.

To cover more attack types of healthcare systems, we extract U2R and DoS attacks from the attack samples of the NSL-KDD dataset by writing a query in Excel for each attack. Consequently, as Table 2 shows, we have ten datasets of the attacks, and a dataset of normal traffic from the NSL-KDD.

Then, we implement a program in Java environment to create our dataset consists of ten attacks. This dataset contains 10,000 samples consist of 4,000 samples of normal traffic and 300 samples from every ten attacks. We use three datasets because we use three different layers of the intrusion detection systems in our proposed framework.

Table 3 and Table 4 show the type of traffic samples and the number of each one in the test set and the train set for the anomaly, the misuse, and the hybrid intrusion detection systems, respectively. We obtain this information by analysis of the datasets with Weka tool (version 3.9) [46, 47]. In the next part of this section, we implement the intrusion detection systems by using SVM and evaluate them with the datasets.

4.3 The implementation results of the intrusion detection systems

We implement the intrusion detection systems of our proposed framework with R tool (version 3.5.0) [48]. These intrusion detection systems classify the traffic of the network by using support vector machine (SVM) [30]. SVM is one of the most efficient machine learning algorithms in pattern recognition problems, such as classifying traffic of networks and image processing.

In the IDS of each layer of our framework, SVM detects the pattern of abnormal traffic from normal traffic, which is non-linear patterns. Non-linear patterns cannot be easily distinguished and separated, unlike linear patterns, which are easily distinguishable. So non-linear patterns need some process to become easily separable. Consequently, the Kernel function maps the original data to a higher dimensional space to classify non-linear patterns [30].

In the R tool, functions of pattern recognition problems are available in the caret package, and the kernel functions are in the kernlab package. Therefore, we use these two packages in the implementation of the intrusion detection systems of our framework. We use the ksvm function from the caret package to use SVM as a network traffic classifier. The first argument of ksvm function is the attribute of classification. In this study, it is traffic types that can be normal or the name of the attack (abnormal). The second argument declares the dataset that SVM classifies. The last argument names the type of the ksvm function. We use the c-svc type, which is for solving data classification problems. Finally, we name the kernel function. The kernel function, which we use to classify our network traffic, is the radial basis function (RBF in R). After we implement the intrusion detection systems of each layer, we evaluate the parameters of each layer’s IDS. In the following, we discuss and conclude about these parameters.

Table 5 shows the average runtime and memory consumption of the intrusion detection systems of the proposed framework after ten runs. The information in this table shows the correctness of considering the intrusion detection system for each layer of the proposed framework. As we mentioned earlier, the structure of the anomaly IDS is simpler than the misuse and the hybrid IDS. Therefore, it has less runtime and memory consumption than the misuse and the hybrid IDS in Table 5. It means it is suitable for the patient and
| Attack name | Attack type |
|-------------|-------------|
| Back        | DOS         |
| Buffer overflow | U2R       |
| land        | DOS         |
| loadmodule  | U2R         |
| neptune     | DOS         |
| perl        | U2R         |
| pod         | DOS         |
| rootkit     | U2R         |
| smurf       | DOS         |
| teardrop    | DOS         |

| Attack name | Dataset          |
|-------------|------------------|
| Attack      | 1471             |
| Normal      | 4000             |
| Total       | 5471             |

| Traffic type | Dataset          |
|--------------|------------------|
| Attack       | Train set, Test set |
| neptune      | 300, 300         |
| back         | 300, 300         |
| snarf        | 300, 300         |
| bufferoverflow| 30, 20         |
| load module  | 203, 41          |
| perl         | 9, 2             |
| land         | 18, 7            |
| rootkit      | 10, 13           |
| teardrop     | 300, 12          |
| Normal       | Normal 4000, 4000 |
| Total        | 5471, 4997       |

| IDS         | Runtime (s) | Memory usage (MB) |
|-------------|-------------|-------------------|
| Anomaly     | 3.001       | 270.688           |
| Misuse      | 7.784       | 285.486           |
| Hybrid      | 11.374      | 280.138           |

| IDS         | DR (%) | FPR (%) |
|-------------|--------|---------|
| Anomaly     | 95.01  | 9.97    |
| Misuse      | 50.04  | 0.9     |
| Hybrid      | 99.2   | 0.88    |

As we mentioned in Section 2, spoofing, impersonation, the elevation of privileges, DoS attacks, eavesdropping, and data modification are the usual attacks of healthcare networks. According to some earlier research that we discussed before, proper encryption algorithms were proposed in three layers to secure healthcare systems. These algorithms cannot confront attacks except eavesdropping and data modification. Therefore, the main advantages of our proposed framework in comparison with earlier works are as follows: 1) Designing a healthcare system by using the multiagent technology to collect data of the healthcare network. It means we have one agent for each patient and an environment with specific rules. 2) Considering security measures to confront possible attacks other than eavesdropping, besides the provision of healthcare services. 3) Allocation of SVM-based intrusion detection systems appropriate to each group of the agents to save energy and computational cost of the network.

## 5 Our Contributions

As we mentioned in Section 2, spoofing, impersonation, the elevation of privileges, DoS attacks, eavesdropping, and data modification are the usual attacks of healthcare networks. According to some earlier research that we discussed before, proper encryption algorithms were proposed in three layers to secure healthcare systems. These algorithms cannot confront attacks except eavesdropping and data modification. Therefore, the main advantages of our proposed framework in comparison with earlier works are as follows: 1) Designing a healthcare system by using the multiagent technology to collect data of the healthcare network. It means we have one agent for each patient and an environment with specific rules. 2) Considering security measures to confront possible attacks other than eavesdropping, besides the provision of healthcare services. 3) Allocation of SVM-based intrusion detection systems appropriate to each group of the agents to save energy and computational cost of the network.

## 6 Conclusion and future works

Our goal in this paper is to design a healthcare system based on wireless sensor networks and secure it against unauthorized access and network attacks. Consequently, we create a healthcare system with new capabilities. In this system, we consider security measures
appropriate to wireless sensor networks besides providing medical services. For this purpose, after defining the agents and their interactions, the intrusion detection systems are used to confront healthcare network attacks. These intrusion detection systems are proportional to the level of energy and the sensitivity of data of each layer in our framework. Also, the implementation and evaluation of each IDS of the layers prove the correctness of our framework design. We also discuss SVM as an efficient network traffic classifier in our framework. Our proposed framework consists of two steps, so we can implement each step with other methods and tools and compare the results. Consequently, we suggest the following items as the future works: 1) Using a standard medical dataset in the multiagent design phase. 2) Using other learning algorithms to set the rules of the patient agent and the ambient agent to learn the usual behavior of patients and ambient sensors. It might enhance the flexibility of the agents.

References

1. S. Rodríguez, J. F. De Paz, G. Villarrubia, C. Zato, J. Bajo, and J. M. Corchado, Multi-agent information fusion system to manage data from a WSN in a residential home, Information Fusion, 23, 43–57 (2015)
2. S. Thakare, P. Ingle, and B. Meshram, IDS: Intrusion Detection System the Survey of Information Security, International Journal of Emerging Technology and Advanced Engineering Website: www.ijeatec.com, 2, 86-90 (2012)
3. A. Tablado, A. Illarramendi, and M. I. Bag, An Intelligent System for Assisting Elderly People, in the 15th International Symposium Foundations of Intelligent Systems ISMIS 2005, 2005, 466–474
4. M. I. Baghíeí et al., An innovative system that runs on a PDA for a continuous monitoring of people, in 19th IEEE International Symposium on Computer-Based Medical Systems, 2006, 151–156
5. A. Tablado, A. Illarramendi, M. I. Bagues, B. J., and A. Gon, Agents in a system for monitoring elderly people, in 2nd Workshop on Agents Applied in HealthCare, 2004, 47-53
6. R. S. Alonso, D. I. Tapia, G. Villarrubia, and J. F. DePaz, Agent Technology and Wireless Sensor Networks for Monitoring Patients in Residences and Their Homes, in International Conference on Practical Applications of Agents and Multi-Agent Systems PAAMS 2013, 2013, 417–428
7. C. J. Su and C. Y. Wu, JADE implemented mobile multi-agent based distributed information platform for pervasive health care monitoring, Applied Soft Computing Journal, 11, 315-325 (2011)
8. H. Huo, Y. Xu, H. Yan, S. Mubeen, and H. Zhang, An Elderly Health Care System using Wireless Sensor Networks at Home, in 2009 Third International Conference on Sensor Technologies and Applications, 2009, 158–163
9. J. M. Corchado, J. Bajo, and A. Abraham, GerAmi: Improving healthcare delivery in geriatric residences, IEEE Intelligent Systems, 23, 19-25 (2008)
10. V. G. Koutkias, I. Chouvarda, and N. Maglaveras, A multiagent system enhancing home-care health services for chronic disease management, IEEE Transactions on Information Technology in Biomedicine, 9, 528-537 (2005)
11. B. Kaluža, V. Mirchevska, E. Dovgan, M. Luštrek, and M. Gams, An Agent-Based Approach to Care in Independent Living, Lncs, 6439, 177–186 (2010)
12. L. Cervantes et al., Agent-Based Intelligent Decision Support for the Home Healthcare Environment, in Advances in Hybrid Information Technology. ICHIT 2006, 2006, 414–421
13. R. M. A. Mateo, L. F. Cervantes, H. K. Yang, and J. Lee, Mobile agents using data mining for diagnosis support in ubiquitous healthcare, in KES-AMSTA 2007: Agent and Multi-Agent Systems: Technologies and Applications, 2007, 795–804
14. H. X. Son, M. H. Nguyen, H. K. Vo, and T. P. Nguyen, Toward an Privacy Protection Based on Access Control Model in Hybrid Cloud for Healthcare Systems, in International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019). CISIS 2019, ICEUTE 2019, 2020.
15. R. Mahmud, R. Kotagiri, and R. Buyya, Fog Computing: A taxonomy, survey and future directions, Internet of Everything, Internet of Things (Technology, Communications and Computing), 103–130 (2018)
16. A. M. Rahmani, P. Liljeberg, J. S. Preden, and A. Jantsch, Leveraging Fog Computing for Healthcare IoT, Fog computing in the Internet of Things: Intelligence at the edge, 145-169 (2017)
17. M. Mukherjee, L. Shu, and D. Wang, Survey of fog computing: Fundamental, network applications, and research challenges, IEEE Communications Surveys and Tutorials, 20, 1826–1857 (2018)
18. V. Jagadeeswari, V. Subramaniyaswamy, R. Logesh, and V. Vijayakumar, A study on medical Internet of Things and Big Data in personalized healthcare system, Health Information Science and Systems, 6, 1-20 (2018)
19. Y. Guan, J. Shao, G. Wei, and M. Xie, Data Security and Privacy in Fog Computing, IEEE Network, 32, 106–111 (2018)
20. H. Ben Hassen, W. Dghais, and B. Hamdi, An E-health system for monitoring elderly health based on Internet of Things and Fog computing, Health Information Science and Systems, 7, 1-9 (2019)
21. S. Pirbhulal, W. Wu, G. Li, and A. K. Sangaiah, Medical Information Security for Wearable Body Sensor Networks in Smart Healthcare, IEEE Consumer Electronics Magazine, 8, 37–41 (2019)
22. I. Albarki, M. Rasslan, A. M. Bahaa-Eldin, and M. Soh, Robust hybrid-security protocol for healthcare systems, Procedia Computer Science, 160, 843–848 (2019)
23. Y.M. Huang, M.Y. Hsieh, H.C. Chao, S.H. Hung, and J.H. Park, Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks, IEEE Journal on Selected Areas in Communications, 27, 400-411 (2009)
24. P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards, Computer Communications, 30, 1655-1695 (2007)
25. O. Garcia-Morchon, T. Falck, T. Heer, and K. Wehrle, Security for Pervasive Medical Sensor Networks, in Proceedings of the 6th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2009
26. E. M. Kakihata et al., Intrusion Detection System Based on Flows Using Machine Learning Algorithms, IEEE Latin America Transactions, 15, 1988–1993 (2017)
27. H. F. Eid, A. Darwish, A. E. Hassanien, and A. Abraham, Principle Components Analysis and Support Vector Machine based Intrusion Detection System, in 10th International Conference on Intelligent Systems Design and Applications, 2010, 363–367
28. J. Jha and L. Ragha, Intrusion Detection System using Support Vector Machine, International Journal of Applied Information Systems, 25–30 (2013)
29. R. Vijayanand, D. Devaraj, and B. Kannapiran, Support Vector Machine based Intrusion Detection System with Reduced Input Features for Advanced Metering Infrastructure of Smart Grid, in 4th International Conference on Advanced Computing and Communication Systems, 2017
30. A. Pradhan, Support Vector Machine-A Survey, International Journal of Emerging Technology and Advanced Engineering, 2, 82–85 (2012)
31. A. A. Shah, M. S. H. Khialy, and M. D. Awan, Analysis of Machine Learning Techniques for Intrusion Detection System: A Review, International Journal of Computer Applications, 119, 19–29 (2015)
32. P. Bresciani and A. Perini, Tropos: An Agent-Oriented Software Development Methodology, Autonomous Agents and Multi-Agent Systems, 8, 203–236 (2004)
33. R. S. P. Giorgini and J. Mylopoulos, Goal-oriented requirements analysis and reasoning in the tropos methodology, Engineering Applications of Artificial Intelligence, 18, 159–171 (2005)
34. B. Henderson and P. Giorgini, Agent-oriented Methodologies, 20–45. Idea Group Publishing, England: University of London (2005)
35. M. M. Afzar and M. H. Tayarani-N, Clustering in sensor networks: A literature survey, Journal of Network and Computer Applications, 46, 203–226 (2014)
36. S. S. Wang, K. Q. Yan, S. C. Wang, and C. W. Liu, An integrated intrusion detection system for cluster-based wireless sensor networks, Expert Systems with Applications, 38, 15234–15243 (2011)
37. V. Mhatre and C. Rosenberg, Homogeneous vs heterogeneous clustered sensor networks: a comparative study, in IEEE International Conference on Communications, 6, 2004, 3646–3651
38. Y. W. Y. Wang, X. W. X. Wang, B. X. Bin Xie, D. W. D. Wang, and D. P. Agrawal, Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks, IEEE Transactions on Mobile Computing, 7, 698–711 (2008)
39. Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, A global hybrid intrusion detection system for Wireless Sensor Networks, in The 5th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS 2015), 2015, 1047–1052
40. K. Kendall, A database of computer attacks for the evaluation of intrusion detection systems, DARPA, Massachusetts (1999)
41. R. P. Lippmann et al., Evaluating intrusion detection systems: The 1998 DARPA Off-line intrusion detection evaluation, in DARPA Information Survivability Conference and Exposition, 2000, 12–26
42. M. Al Ameen, J. Liu, and K. Kwak, Security and privacy issues in wireless sensor networks for healthcare applications, Journal of Medical Systems, 36, 93–101 (2012)
43. O. O. Olakanni, Lightweight Security and Privacy Scheme for Wireless Body Area Network in E-Health System, International journal of information security science, 6, 26–38 (2017)
44. V. Agrawal, Security and Privacy Issues in Wireless Sensor Networks for Healthcare, in Internet of Things. User-Centric IoT, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2015, 223–228
45. G. Meena and R. R. Choudhary, A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA, International Conference on Computer, Communications and Electronics, 2017, 553–558
46. S. Srivastava, Weka: A Tool for Data preprocessing, Classification, Ensemble, Clustering and Association Rule Mining, International Journal of Computer Applications, 88, 26–29 (2014)
47. S. Singh and M. Jena, A Study on WEKA Tool for Data Preprocessing, Classification and Clustering, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 6, 250–253 (2013)
48. R. Iha and R. Gentleman, R: A Language for Data Analysis and Graphics, Journal of Computational and Graphical Statistics, 5, 299–314 (2012)