Tiako P.F. (ed) *Intelligent Computing and Consumer Support Applications*. Chronicle of Computing. OkIP
© 2023 Oklahoma International Publishing https://doi.org/10.55432/978-1-6692-0003-1_8

# A Novel Agent-Based Intrusion Detection System for Wireless Body Area Network

Lynda Sellami[a], Khaled Sellami[a], Piere F Tiako[b]

*[a]LMA Laboratory, Faculty of Exact Sciences, University of Bejaia, Algeria*
*[b]Center for IT Research and Development, Tiako University, Oklahoma, USA*

*Abstract*

*The objective of e-health is to assist patients in improving health care through integrating a wireless body network, communication infrastructure, and hospital network. The patient monitoring system assists patients in better understanding their health daily. The mobility and dynamism offered by e-health services expose the health system to the risk of attacks and intrusions. However, securing patient information and confidentiality is essential to ensure quality care. Current research on security in e-health focuses on implementing authentication, encryption, and trust-based solutions for implanted and wearable medical devices. These solutions are often computationally expensive and challenging to implement on medical devices with limited resources. This paper proposes a novel intrusion detection system based on agent technology to protect patients' medical data. The proposed method detects network-level intrusions as well as anomalies in sensor data. Our model was experimented with by simulating a hospital network topology. Our simulation results demonstrate that we can achieve high detection accuracy.*

*Keywords: E-Healthcare, Wireless Body Area Network, Security, Intrusion Detection System, Agent Technology*

## I. Introduction

The Internet of Things (IoT) is a dynamic and heterogeneous network of interconnected (Habib & Leistr, 2013) objects, where objects communicate and exchange information (SUNDMAEKER & al., 2010) and integrate real-world information into networks (X-ETP Group, 2010). To facilitate patients' lives with quick medical responses from doctors, the existing healthcare system uses communication capability and support for a dynamic IoT environment to develop a patient monitoring system (PMS) (Abie & Balasingham, 2012; Sellami, 2016).

The security of health services is an essential issue for patients and health professionals, given the importance and confidentiality of the data that these services use, share, and transfer to ensure quality care. The mobile, dynamic, and ubiquitous aspect of the services offered by E-health exposes the health system to the risk of attacks and intrusions. Therefore, it is necessary to secure personal data and healthcare records (Sellami & al., 2021).

In this paper, we propose developing an intrusion detection (IDS) to detect and identify altered patient medical data in the body area network (BAN) by reporting and notifying healthcare professionals to provide abnormal services. The approach is applied and tested on a simulated medical dataset to prove the effectiveness and feasibility of the proposed solution in detecting unauthorized activities in eHealth environments.

The rest of the paper is organized as follows: Section 2 presents the E-health system. Section 3 discusses security objectives and requirements. Section 4 details our proposal. We show some experimental results on a simulated medical dataset evaluating our solution in section 5. Finally, the conclusion and the perspectives are described in section 6.

## II. E-health System Architecture

E-health offers health services and information to improve health care and the well-being of people (Saleem & al., 2011 ; Ziaie, 2013). It is based on patient monitoring by ensuring personalization, availability, and mobility. Personalization concerns the patient's expectations, their adaptation to treatment, and the medical device. Availability and mobility guarantee the operation of the solution in all places. A PMS monitors the health status of patients. It is composed of three parts (figure 1): (1) The Body Area Network (BAN) includes the actual patient, the medical sensors, and the patient's smartphone. (2) Communication networks connecting the BAN to a hospital network. (3) hospitals and healthcare enterprises (Li & al., 2010).

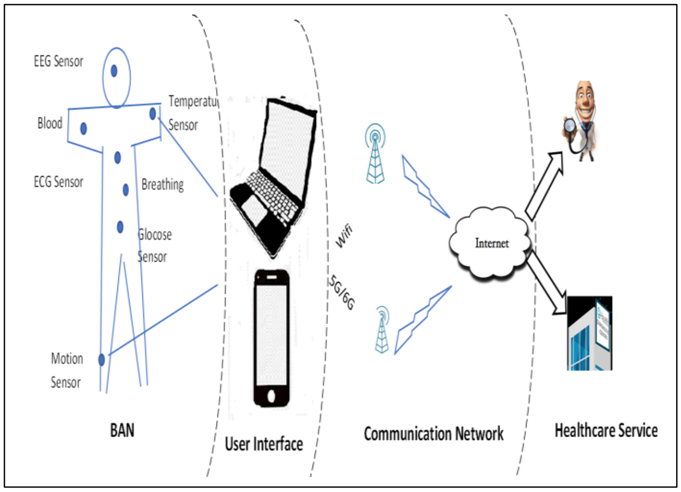


Fig. 1. Patient Monitoring System Architecture (Ghamari & al., 2016)

The patient's body is equipped with medical sensors to support the patient. The medical sensor reacts to the

* Corresponding author E-mail: slynda1@yahoo.fr

modification of the vital parameters of the patient. It takes care of the collection of the critical parameters recorded at the level of the patient's device (smartphone). The vital parameters collected are transmitted; via the communication network; at the health center (hospital and health care enterprises). The transmitted medical data is evaluated, and a decision is taken by the health professionals of the hospital and the health company.

## III. Security Objectives and Requirements

The primary objective of security in e-health is data security and patient privacy. Data security relies on the secure transfer of the patient's vital signs t to the hospital. For PMS, security concerns the entire system; the BAN, the communication, and the hospital network. The security of the BAN involves the safety of the data collected, namely, confidentiality, integrity, availability, and data authentication. For the communication network, security deals with the data transferred, confidentiality, integrity, reliability, data accuracy, and data authentication. For the hospital network, security deals with the data processed and evaluated; data confidentiality, data integrity, data availability, patient and data authentication, physical security, and access control. In this article, we focus on security issues at the BAN.

### *A. Security in the BAN*

The Body Area Network (BAN) (Ghamari & al., 2016) is a wireless networking technology consisting of placing miniature devices (sensors) on, around, or in the human body to collect vital parameters or act on specific situations. These sensors interconnect and communicate with each other via radio frequencies. They can communicate with a remote service center.

The BAN's security concerns the data's safety (Al-Rimawi & al., 2016). Data confidentiality ensures the non-disclosure of data collected and stored, exchanged by the sensors, and transmitted. This data includes information about the patient's private life and the disease; disclosing this data may compromise the diagnosis. Data integrity protects the data from all modifications during storage and transfer. Modifying data leads to an erroneous diagnosis. Data availability is about ensuring that healthcare personnel have access to patient data. Any delay in access or inability to access information may prevent the patient's treatment data authentication process.

### *B. Security Threats*

Due to inherent vulnerabilities in wireless communication, BAN is vulnerable to various security threats. To protect data and devices from loss or theft, awareness, and training of the patient on the use of sensors and devices are essential. The authentication consists of detecting and identifying falsified data. The BAN uses the patient's device for data collection and transmission, such as a smartphone (Hodgkiss & al., 2021). The patient can install monitoring software to share data to protect his devices from unauthorized access.

Several threats put BAN at risk (Habib & al., 2014). We summarize them in the following:

*1) Frequency jamming:* By using an external device, an adversary interferes with BAN frequencies, rendering devices and network components unresponsive, leading to network blockage (Bengag & al., 2020; Jaitly & al., 2017).

*2) Data collision:* this is a threat to the BAN link layer communication. An adversary tries to intercept and modify a data frame by transmitting at the same frequency that is used by the actual node, which creates a threat to the availability of data in the BAN (Chowdhury & Sen, 2018).

*3) Compromised data routing:* is a threat to network layer communication in the BAN. To hijack data, an adversary exploits vulnerabilities in routing protocols (Malik & al., 2018).

*4) Data flooding:* is an attack on the transport layer in the BAN. An adversary sends connection requests several times, thus inducing the saturation of memory resources (Malik & al., 2018; Anwar & al., 2018).

*5) Lack of data synchronization:* is a threat at the transport layer in the BAN. An adversary sends a retransmission request for missing frames to desynchronize the pre-established connection (Malik & al., 2018).

*6) Repeated retransmission of frames:* can exhaust resources and degrade network performance. Data wave ping threatens patient privacy and safety; an adversary intercepts a message for further analysis (Malik & al., 2018; Liu & al., 2021).

*7) Denial of services (DoS):* an attack occurs when overall traffic exceeds the total system capacity. Adversary hijacks and reprograms sensor nodes to pump data at a faster/slower rate or transmits noise randomly (Raymond & al., 2008; Ramkumar & al., 2010; Premkumar & al., 2020).

## IV. Proposed Work

We recall that our work aims to solve the detection problem of attacks at the medical data level. We propose a functional model for the protection of the medical network using a new intrusion detection system based on several agents, where the detection, the learning, and the decision-making are distributed between different nodes of the network.

### *A. System Architecture*

Our detection system is focused on the sensor and the network. The architecture of our network is composed of three levels, figure 2:

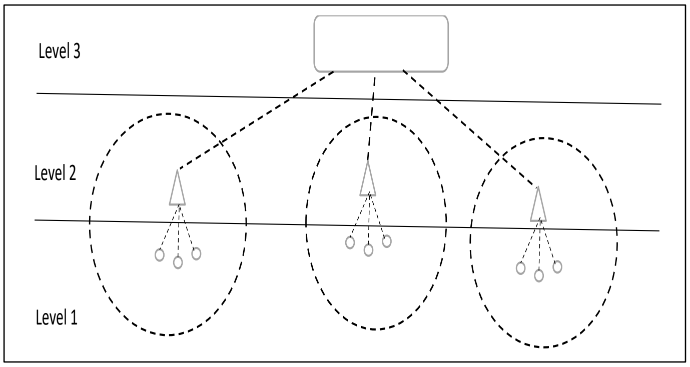


Fig. 2. System Architecture

*1) The first level:* Represents the nodes of the network of sensors. Each node has a static agent which collects information and data at the node level.

A mobile agent is responsible for moving between neighbors (cluster nodes). It is also responsible for monitoring and detecting anomalies.

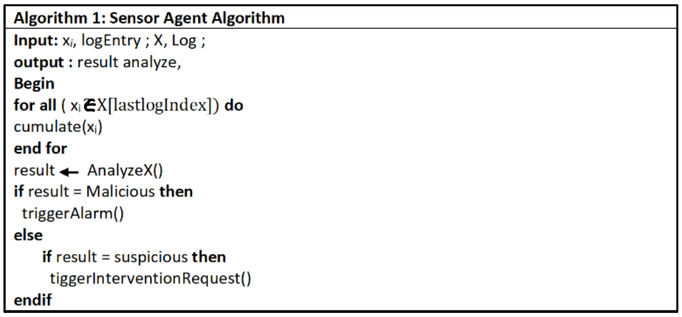
*2) The second level:* It is represented by a control agent residing at the level of the heads of the cluster. It is responsible for monitoring the state of mobile agents. It participates in cooperative detection.

*3) The third level:* It is the highest level and represents the trusted server which is the principal agent. It monitors all other agents and nodes. It acts as an administrator on a network.

### B. Detection system components

In this section, we describe the different types of agents involved in the detection process.

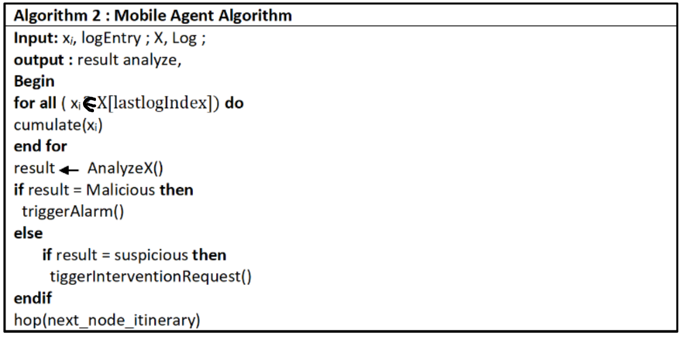
*1) Sensor Agent (SA):* The SA is installed at sensor nodes; it is a program responsible for collecting data and information from each node. The Sensor Agent performs local detection in each node by aggregating the logs accumulated over time.



```
Algorithm 1: Sensor Agent Algorithm
Input: $x_i$, logEntry ; X, Log ;
output : result analyze,
Begin
for all ( $x_i \in$ X[lastlogIndex]) do
cumulate($x_i$)
end for
result ← AnalyzeX()
if result = Malicious then
  triggerAlarm()
else
    if result = suspicious then
      tiggerInterventionRequest()
endif
```

The sensor agent performs local node discovery by aggregating logs accumulated over time. When the sensor agent executes the intrusion detection algorithm, we have three possible cases: (1) it produces a malicious flag that triggers an alarm response, (2) a regular flag that does nothing, (3) or a suspicious indicator that triggers an intervention request.

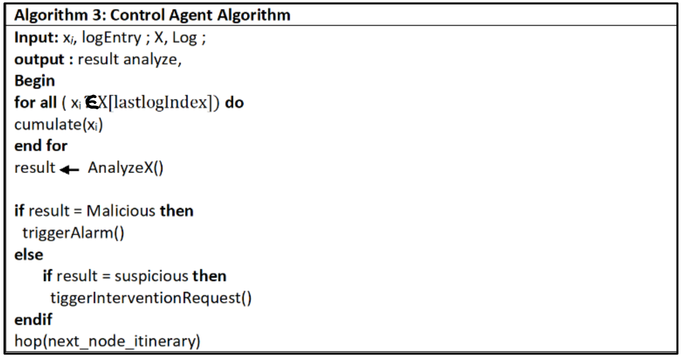
*2) Mobile Agent (MA):* The MA is responsible for detecting a specific attack category. Each mobile agent traverses the nodes in its defined route and performs local discovery in each node by aggregating the logs accumulated over time. When executing the intrusion detection algorithm, the Mobil Agent produces a malicious flag that triggers an alarm response, a regular flag that does nothing, or a suspicious flag that initiates a request for intervention.



```
Algorithm 2 : Mobile Agent Algorithm
Input: $x_i$, logEntry ; X, Log ;
output : result analyze,
Begin
for all ( $x_i \in$ X[lastlogIndex]) do
cumulate($x_i$)
end for
result ← AnalyzeX()
if result = Malicious then
  triggerAlarm()
else
    if result = suspicious then
      tiggerInterventionRequest()
endif
hop(next_node_itinerary)
```

Each mobile agent traverses the nodes in its defined route and performs local discovery in each node by aggregating the logs accumulated over time. When the mobile agent executes the intrusion detection algorithm, it either produces a malicious flag that triggers an alarm response, a regular flag that does nothing (migrating to the next node in the route), or a suspicious indicator that starts an intervention request.

*3) Control Agent (CA):* The CA is the cluster head agent; it detects anomalies among the cluster heads within several interconnected WBAN clusters. CA agents provide global attack detection on interconnected clusters in WBAN. They have a predefined route and a trained pattern and can also target different types of attacks.



```
Algorithm 3: Control Agent Algorithm
Input: $x_i$, logEntry ; X, Log ;
output : result analyze,
Begin
for all ( $x_i \in$ X[lastlogIndex]) do
cumulate($x_i$)
end for
result ← AnalyzeX()

if result = Malicious then
  triggerAlarm()
else
    if result = suspicious then
      tiggerInterventionRequest()
endif
hop(next_node_itinerary)
```

The control agent (CA) is an instance of an autonomous mobile program designed to detect anomalies among cluster leaders within multiple interconnected WBAN clusters. CA agents operate more widely to provide global attack detection on interconnected clusters in the WBAN. They are similar to Sensor Agents in that they have a predefined route. They can target different types of attacks.

## V. Experimentation

The Internet of Medical Things consists of heterogeneous devices communicating. This section simulates the Internet of Medical Things using different network protocols. We describe our simulation setup, attack patterns, and evaluation metrics.

We used the Castalia (Caslatia, online) WBAN simulator based on OMNeT (Omnet, 2011) designed for wireless body area networks to implement and test our proposed IDS prototype. Training and testing datasets by running simulations are generated. Agents are deployed to collect and aggregate sensor logs. The test dataset is validated by the detection results.

Attacks are categorized into benign, malicious, and suspicious. The detection protocol has been tested against all threat levels, and the relevant results relative to the defined metrics have been extracted, transformed, and analyzed.

Table 1 shows the results of the analysis. We sent bad packets and good packets to test and simulate the system. Bad packets (by default) are effectively identified and eliminated. Table 1 shows that the detection rate (DR) and the rate of normal behavior (NB) are very high.

TABLE I. DETECTION RESULTS

| Normal data size (KB) | Intrusion data size (KB) | Normal behavior | Level I detection | Level II detection | Level III detection | Detection rate |
|---|---|---|---|---|---|---|
| 50 | 40 | 50 | 15 | 20 | 5 | 100% |
| 150 | 80 | 150 | 30 | 20 | 30 | 100% |
| 200 | 100 | 200 | 50 | 30 | 19 | 99,83% |

Our IDS model detects new attacks coming from inside and outside the network that try to affect proper network functioning.

*Performance:* An intruder attack's detection rate (DR) is the rate of accurately detected records observed as malicious attacks.

$$DR = \frac{TP}{TP + FN} \qquad (1)$$

Where,

TP is the true positive detection rate, which is the number of malicious recordings correctly detected according to the intrusions' classification.

- FN is the false negative detection rate which is the no. Falsely detected recordings are classified as legitimate activities.
- False Positive Rate (FPR) is the False Positive Rate that is the no. Recordings are misclassified as attacks.

$$FPR = \frac{FP}{TN + FP} \qquad (2)$$

Where,

- TN is the True Negative rate, the number of legitimate recordings incorrectly classified as an intrusion.
- FP is the false positive rate that evaluates the no. Incorrectly detected records.

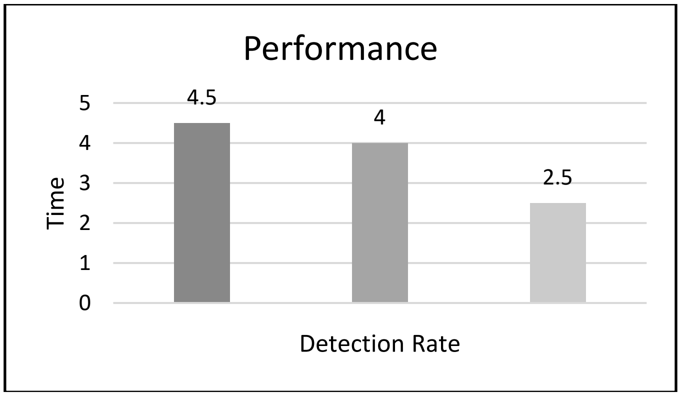


Fig. 3. Performance

Figure 3 shows that the detection rate increases each time the true positive rate increases. The false positive rate depends on the true positive rate.

## VI. CONCLUSION

To assist patients and caregivers, e-health offers home health devices and applications that focus on ease and flexibility, exposing the E-Health system to numerous Internet attacks and anomalies. Developing traffic monitoring methods to detect attacks in e-health systems and networks is imperative.

The main objective of this work is to ensure the security of the medical data of BAN patients. Our approach helps control the security of patient medical data against misuse. This process involves finding anomalies that could lead to possible attacks and taking action against those attacks. The proposed model ensures the overall security of health records in the BAN, thus avoiding errors in the diagnosis and treatment of patients.

We have carried out pilot experiments to evaluate our method. The results show that our model gives good precisions.

We plan to conduct a more experimental evaluation by collecting patient data with more attributes in the future, such as adverse drug reactions, Healthcare-associated infections (HAIs), surgical errors, laboratory errors, and documentation errors.

## REFERENCES

Habib, K., & Leister, W. (2013). Adaptive Security for the Internet of Things Reference Model. 6th Norwegian Information Security Conference, NISK, 13-24.

SUNDMAEKER, H., GUILLEMIN, P., FRIESS, P., & Woelfflé S. (2010). Vision and challenges for realising the Internet of Things. Cluster of European research projects on the internet of things, European Commision, 3(3), 34-36.

X-ETP Group. (2010). Future Internet Strategic Research Agenda, Version 1.1, European Future Internet X-ETP Group, 1-73, 2010.

Abie. H.. & Balasingham, I. (2012). Risk-Based Adaptive Security for Smart IoT in eHealth, BodyNets, 269-275.

Sellami, L., Sellami, K., & Tiako, PF. (2016). Detection of New Attacks on Ubiquitous Services in Cloud Computing and Against Measure. Advanced Science Letters 22 (10), 3168-3172.

Sellami, L., Idoughi, D., Sellami, K., & Tiako, PF. (2021). Detection and Preventing Approach for Electronic Medical Records in E-Health. In 2021 OKIP International Conference on Advances in Health Information Technology (AHIT). Oklahoma International Publication, USA.

Saleem, S., Ullah, S., & Kwak, K. S. (2011). A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks. Sensors; 11(2), 1383-1395.

Ziaie, N. (2013). e-Health Security Issues and Solutions, Master of Science Thesis, University of Gothenburg. Göteborg. Sweden.

Li, M., Lou, W., & Ren, K. (2010). Data Security and Privacy in Wireless Body Area Networks, Wireless Communications, IEEE, 17(1), 51-58, February.

Ghamari, M., Janko, B., Sherratt, RS. Harwin, W., Piechockic, R., & Soltanpur. C. (2016). A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environment, Sensors 16, 6( 831). https://doi.org/10.3390/s16060831

Al-Rimawi, R., Dwairej, D., Masadeh, A., Ahmad, M. & Al-Ananbeh. E. (2016). E-health Concept Development and Maturity in Literature. Journal of Health, Medicine and Nursing. ISSN 2422-8419. An International Peer-reviewed Journal. 29.

Hodgkiss, J., Djahel, S., & Zhang, Z (2021). A New Attack Method Against ECG-Based Key Generation and Agreement Schemes in Body Area Networks, in IEEE Sensors Journal, 21(15), 17300-17307, doi: 10.1109/JSEN.2021.3079177.

Habib, K., Torjusen, A. & Leister, W. (2014). A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth, SMART 2014, July 20 - 24, 32-37.

Bengag, A., Bengag, A., & Moussaoui. O. (2020). Effective and Robust Detection of Jamming Attacks for WBAN-Based Healthcare Monitoring

Systems. In International Conference on Electronic Engineering and Renewable Energy, 169–174. Springer, Singapore.

Jaitly, S., Malhotra, H., & Bhushan, B. (2017). Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey. In International Conference on Computer, Communications and Electronics (Comptelix). IEEE, 559-564.

[15] Chowdhury, S.K., & Sen, M. (2018). Survey on Attacks on Wireless Body Area Network. Conference on Computational Intelligence & IoT (ICCIIoT) 2018. At: National Institute of Technology Agartala, Tripura, Indi.

a, pp 636-644.

Malik, M.S.A., Ahmed, M., Abdullah, T., Kousar, N., Shumaila, M. N. & Awais. P. M. (2018). Wireless Body Area Network Security and Privacy Issue in E-Healthcare. (IJACSA) International Journal of Advanced Computer Science and Applications, 9(4)

Anwar, M., Abdullah, A.H., Butt, R.A., & Ashraf, M.W. Securing. (2018). Data Communication in Wireless Body Area Networks Using Digital Signatures. Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan, 23(2).

Liu, Q., Mkongwa, K.F., & Zhang, C. (2021). Performance issues in wireless body area networks for the healthcare application: a survey and future prospects. SN Applied Sciences 3.

Raymond, D.R., Midkiff. S.F. (2008). Denial-of-service in wireless sensor networks: Attacks and defences. IEEE Pervasive Computing.7(Pt 1), 74-81

Ramkumar, M. (2010)Proxy aided key pre-distribution schemes for sensor networks. In: Paper Presented at the IEEE International Conference on Performance, Computing, and Communications; 461-68

Premkumar, M., & Sundararajan, T. V. P. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. Microprocessors and Microsystems, v 79, 103278.

Castalia home. [Online]. Available:https://castalia.forge.nicta.com.au/index.php/en/

Omnet++ WBAN Projects | Wireless Body Area Network Projects, OpenSim Ltd., 2011.