Distributed Intrusion Detection Using Mobile Agents in Wireless Body Area Networks

Adedayo Odesile
Computing and Software Systems
University of Washington Bothell
Bothell, WA 98011
Email: adao@uw.edu

Geethapriya Thamilarasu
Computing and Software Systems
University of Washington Bothell
Bothell, WA 98011
Email: geetha@uw.edu

***Abstract*—Technological advances in wearable and implanted medical devices are enabling wireless body area networks to alter the current landscape of medical and healthcare applications. These systems have the potential to significantly improve real time patient monitoring, provide accurate diagnosis and deliver faster treatment. In spite of their growth, securing the sensitive medical and patient data relayed in these networks to protect patients' privacy and safety still remains an open challenge. The resource constraints of wireless medical sensors limit the adoption of traditional security measures in this domain. In this work, we propose a distributed mobile agent based intrusion detection system to secure these networks. Specifically, our autonomous mobile agents use machine learning algorithms to perform local and network level anomaly detection to detect various security attacks targeted on healthcare systems. Simulation results show that our system performs efficiently with high detection accuracy and low energy consumption.**

I. Introduction

Wireless Body Area Networks (WBAN) are emerging as the most promising technology in healthcare applications [1]. These networks consist of wireless wearable, implantable medical devices, mobile devices and networks that provide autonomous, real-time, continuous health monitoring enabling a wide range of medical applications. Since the wireless body area networks deal with sensitive and often life-critical medical information, there are significant security and privacy implications that hinder a wide spread adoption of this technology. Due to limited computational power resources available in the wireless medical and mobile devices, implementing traditional security through prevention techniques is not always feasible or sufficient. Intrusion detection systems (IDS) that monitor and detect various security attacks are essential to provide holistic security in these networks.

Current literature reveals limited work on developing intrusion detection mechanisms for wireless body area networks. Wireless body area networks follow a distributed structure, leading to attacks occurring at multiple attack surfaces. This necessitates a distributed design where intrusion detection system is distributed across the body sensor devices as well as the mobile devices. Mobile agent technology where software agents migrate from one computing node to another enables the desired distributed detection mechanism. While there exists substantial work in literature on using mobile agents for intrusion detection, their feasibility and suitability for wireless body area networks has not been studied yet. In this paper, we develop a hierarchical and distributed IDS for WBANs using autonomous mobile agents, where every node in the network acts as the computing node, and mobile agents migrate and collaboratively perform attack detection.

II. Related Work

The significance and relevance of wireless body area networks has led to several security solutions proposed for these networks in recent literature [2], [3], [4]. While most research on security solutions aim at providing encryption or authentication based solutions, intrusion detection based security solution is currently very limited in this domain. Anandkumar *et.al* conducted experiments on detecting intrusions in earlier implementations of WBANs that were based on IEEE 802.15.4 standard [5]. The authors designed a reputation system to evaluate node communication patterns and blacklist the malicious ones. Intrusion detection system using genetic algorithms to identify aberrations in device activities in WBAN networks was proposed in [6]. 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* originally conceived the use of static autonomous software agents to facilitate multi-level detection at different hierarchies of the network [7]. 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 [8] and MA-IDS [9] 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 the 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 [10] 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 [11], 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 [12]. 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 [13] 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.

In our earlier work, we proposed an initial framework for using mobile agents towards detecting intrusions in wireless body area networks [14]. In this paper, we further develop this framework and build a layered and decentralized hybrid detection system. We provide a detailed description of the design and implementation of our system in the next few sections.

III. Mobile Agents based Intrusion Detection System

In this section, we describe the proposed mobile agents based intrusion detection system. Figure 1 shows the network architecture based on a static in-hospital WBAN topology. The proposed network architecture consists of wireless body sensor nodes such as 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. In this paper, a multiple mobile agents based intrusion detection system is developed for wireless body area networks, where learning and decision making is distributed among different nodes in the 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. Our detection mechanism shown in Figure 2 employs autonomous mobile agents to identify and detect any abnormal activities in the network. In this framework, 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.

A. Detection System Components

In the following we 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 security attack. Each cluster head is responsible for spawning multiple sensor agents for local detection within a clique

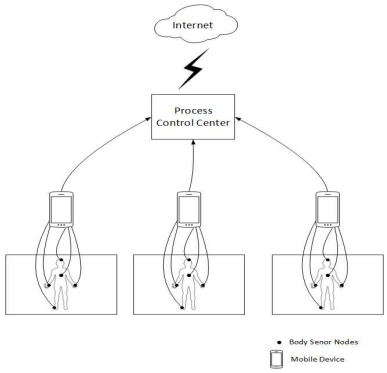

Fig. 1: Static In-Hospital Topology

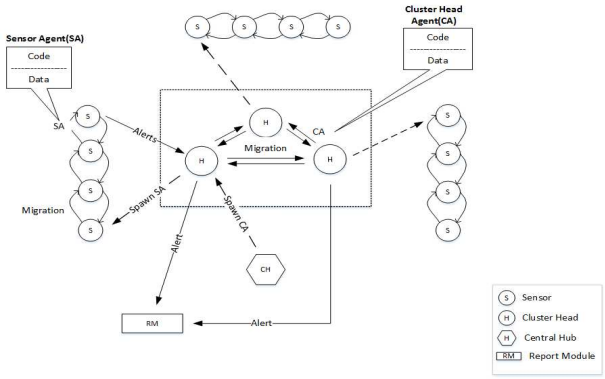

Fig. 2: Mobile Agent based IDS Protocol [14]

of sensors. 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.

2) Cluster Head Agent: The Cluster-Head agent 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. CH 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.

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. Detective Agents are mobile agents dispatched in response to this intervention request to investigate the uncertainty of the detection results. Detective agents operate very 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 stands for the BAN cluster size, and S_A stands for 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.

B. Detection Process

Algorithm 1 gives an overview of the local detection process that occurs within a single cluster of WBAN. Cluster head dispatches several sensor agents for local attack detection. Each sensor agent is trained with a detection algorithm and corresponding data feature set to detect a specific type of attack. The agent traverses through its clique of sensors, waits for a certain amount of time to aggregate data and analyze the gathered data logs for malicious behavior. If the detection was flagged malicious, sensor agent triggers an alarm. If the detection was suspicious but inconclusive, the sensor agent sends an intervention request to CH, which spawns a special detective agent to further evaluate the situation. Algorithm 2 describes the mechanism employed by cluster head agents to hop through all other clusters in the network to perform global attack detection. Cluster head agents are dispatched from each CH and travel through other CHs to analyze the different attack targets. We assume the CH to be a more powerful entity such that it hops from one CH to other without relying on a multi-hop transmission through intermediate sensor nodes. As opposed to sensor agents that instantly classifies a network behavior based on the detection results, CH agents adopt a more distributed approach towards detection. Each CH agent broadcasts its detection result about a particular CH to all other CH agents in the network. Every CH agent is equipped with a data structure for keeping vote tallies about its originator. Assuming the number of CHs is N, once an agent receives $N-1$ unique broadcasts about its owners (originating CH) activities, it relies on the majority vote obtained to determine whether to flag the CH as malicious or benign. This approach ensures detection of compromised cluster heads and prevention of a single point of failure within any cluster.

Algorithm 1 Single WBAN cluster detection algorithm

```
for all att IN attackCategories do
  for all clq IN networkCliques do
    CH.train(SA)
    CH.dispatch(SA)
    for all sensor IN cliqueSensor do
      SA.hop(sensor)
      SA.wait(aggregationTime)
      SA.cumulate(sensor.logs)
      result ← SA.analyze(logs)
      if result IS malicious then
        SA.triggerAlarm()
      else if result IS suspicious then
        SA.sendInterventionRequest(CH)
      end if
    end for
  end for
end for
while TRUE do
  CH.wait(InterventionReq)
  CH.dispatch(DA)
  for all sensor IN networks do
    DA.hop(sensor)
    DA.wait(aggregationTime)
    DA.cumulate(logs)
  end for
  CH.train(DA)
  result ← DA.analyze(logs)
  if result ≠ benign then
    DA.triggerAlarm()
  end if
end while
```

Algorithm 2 Inter-Cluster Detection

```
for all CH IN clusterHeads do
  for all att IN attackCategories do
    CH.train(CA)
    CH.dispatch(CA)
    for all CH IN clusterHeads do
      CA.hop(CH)
      CA.wait(aggregationTime)
      CA.cumulate(sensor.logs)
      result ← CA.analyze(logs)
      CA.addOpinion(CH, result)
      CA.broadCast(result)
      if CA.getOpinion(CH).count ==
      clusterHeads.count − 1 then
        if CA.getOpinion(CH).maliciousCount ≥
        CA.getOpinion(CH).benvolentCount then
          CA.triggerAlarm()
        end if
        CA.clearOpinions(CH)
      end if
    end for
  end for
end for
```

IV. Attack Model and Detection Metrics

In this section, we discuss the following attacks commonly observed in WBAN used in healthcare systems.

- Denial of Service Attacks: 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.
- Data Falsification: An adversary may disrupt the system by forcing the health care providers to continuously respond to false alarms.
- Passive Listening: An adversary may want to obtain financial gains by selling patient's private information, or may use it as a means to harm the patient.

TABLE I: Feature Set for Attack Models

S/N	Attack Category	Feature Set
1.	DoS	Average Incoming/Outgoing Packet Rate, Average Incoming/Outgoing Packet Size, Data Packet Rate, Data Packet Percentage, Agent Packet Rate, Agent Packet Percentage, Other Packet Rate, Other Packet Percentage.
2.	Data Falsification	Sender ID, Received Signal Strength, Time Stamp, Data Value for Differential Temporal Correlation.
3.	Passive Listening	Recipient ID/Address

In addition to the attack classification, we further classify the attacker into different types namely benign, suspicious, malicious, and elusive. Table I gives the details of feature set required for detecting different attacks.

A. Detection Assessment Metrics

To test the efficiency of our detection system, we utilize five popular machine learning algorithms namely: KNN (K-Nearest Neighbors), SVM (Support Vector Machines), RF (Random Forests), DT (Decision Trees), and NBC (Normal Bayes Classifiers). We derived a universal model for every attack category to fit into all five algorithms thereby removing any bias in their comparison. We assessed the efficiency of the learning algorithm and the detection system using the following metrics.

- Accuracy: The accuracy metric is used to determine both the prediction accuracy of the classifier as well as the attack detection accuracy of the system.

$$acc = \frac{T_P + T_N}{T.O} * 100\% \tag{2}$$

  where T_P and T_N are the total number of true positives and negatives respectively, and $T.O$ is the total observations made in the system.
- Cost Ratio: In our medical WBAN scenario, we define cost of the IDS in direct relation to patient's risk level. For instance, it is preferred that a heartbeat monitor raises false alarms in rare occasions than not raising any alarm when a cardiac arrest or hyper-circulation occurs. Hence, we define a greater cost for false negatives as shown in Equation 3.

$$C = \frac{F_N}{F_P} \tag{3}$$

  If F_P is 0 and F_N is greater, cost ratio is defined using Equation 4.

$$C = \frac{F_N}{T_N} \tag{4}$$

- Feedback Reliability: Feedback reliability R is an inverse measure of reliability of the detection algorithm as presented in Equation 5.

$$R = \frac{0.4 * F_P + 0.6 * F_N}{T.O} \tag{5}$$

- Training time: While the above three metrics are used to assess the detection algorithms from a functional standpoint, we also measured the training time (t) to obtain an estimate of resource usage and/or performance.
- Total Rank Score: Total Rank Score is defined as the normal aggregation of values from all the above metrics. This metric is used to rank the different detection algorithms and choose the highest ranked algorithm in our detection system.

$$rank = (\frac{acc}{100} + \frac{C}{C_{max}} + 2 - \frac{t}{t_{max}} - R) \tag{6}$$

  Where t = training time in milliseconds.
- Energy Overhead: This metric is used to assess the efficiency of detection system in terms of its energy consumption. This metric represents the percentage increase in energy usage incurred by the detection protocol and is modeled as a function of execution time and memory usage.

V. Implementation and Results

In this section, we describe our simulation set up and provide a detailed analysis of the results.

A. Experiment Details

We used Castalia WBAN simulator [15] to implement and test our proposed IDS prototype. We generated the training and testing datasets by running simulations under normal, suspicious and malicious settings with their respective labels. Mobile agents were deployed to collect and aggregate sensor logs. Subsequently, a validation phase was carried out where the agents were trained, and their detection results were validated by the test dataset for each algorithm. The number of true and false positives and negatives with their training time were extracted and used to rank the different machine learning algorithms.

TABLE II: Detection Algorithms Rank Score

Algorithm	Rank Score
DT	3.91
SVM	3.73
RF	3.00
NBC	2.99
KNN	2.69

While the values 0, 0.2, and 0.7 were used to emulate benign, malicious and suspicious attackers, the elusive adversary was programmed to change probabilities after each attack using a uniform distribution across 0 to 1, since it is elusive in nature. The detection protocol was tested against all threat levels and relevant results pertaining to defined metrics were extracted, transformed, and analyzed. Our simulation was split into two stages- preliminary stage to derive the most suitable machine learning (ML) algorithm and actual stage to assess the detection system.

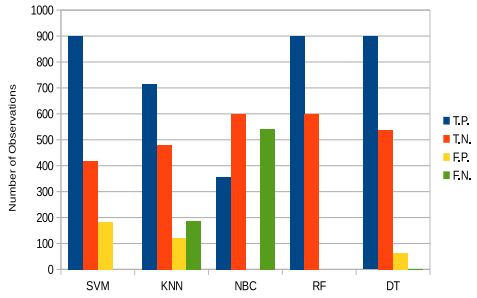

Fig. 3: True Positives vs True Negatives

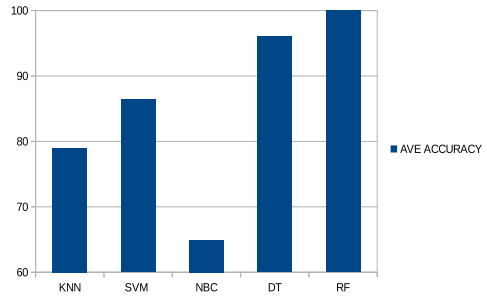

Fig. 4: Prediction Accuracy

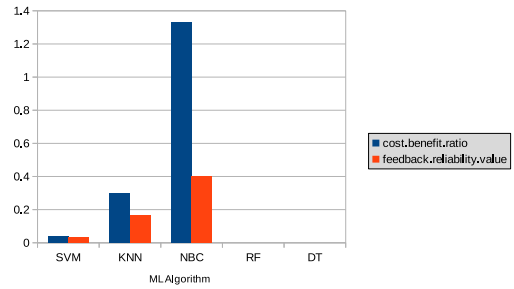

Fig. 5: Cost Ratio and Feedback Reliability Value

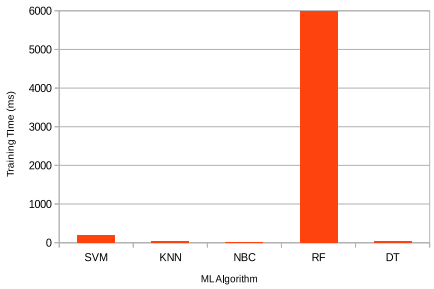

Fig. 6: Training Time

B. Preliminary Phase

In this phase, after training and testing, five ML algorithms (SVM, KNN, NBC, DT, RF) were used for validation and assessed based on the metrics described in the previous section as shown in Figures[3-6]. We used 1500 test samples to validate the classification algorithms. Both KNN and NBC had an accuracy value below 80% thereby rendering them inappropriate for the classifier, regardless of their relatively small training time. Random Forests was highly accurate in classification but incurred too much resource usage in training and was considered unrealistic for running on a low powered sensing device. SVM had a high number of false positives and longer training time compared to Decision Trees (DT). Table II shows the ranking score obtained for the different classification algorithms. DT classifier was chosen based on the outcome of this phase.

C. Actual Phase

In this stage, we designed our measurement process by providing two levels of variations. First, we varied the percentage of compromised sensor nodes and then for each percentage, we varied the probabilities of attacker type i.e. suspicious, malicious, and elusive. We classified the attackers into **dominantly suspicious** to represent a subtle distributed attack, **dominantly malicious** to depict an aggressive adversary, **dominantly elusive** for more sophisticated adversaries, and an equal proportion of all three threat levels. The evaluation metrics, accuracy and energy overhead were used to holistically assess the performance of the system.

1) Detection Accuracy: Detection accuracy was computed as the percentage ratio of the number of correct observations of the attack with respect to the total observations during the simulation period. Figure 7 shows the accuracy plot with varying percentage of threat levels. We observed that the general trend in all four threat level variations increased with the percentage of compromised nodes but declined suddenly at the values between 40-50%. We postulate that this anomaly is probably due to the fairly equal number of benevolent and adversarial nodes leading to a higher level of uncertainty especially for cluster-wide detection from the special agents.

As shown in Figure 9, 99.3% of detection errors were due to false positives because the training set was biased this way to reduce the Cost Ratio (the ratio of error costs of false negatives to positives). Across all threat levels, the suspicious ones had the lowest accuracy on average as they were borderline between benevolent and malicious. Overall, 16,632 observations were made, with an achieved average detection accuracy of 97.21% (Figure 8) and 2.79% detection errors.

2) Energy Overhead: We ran repeated iterations of the system with and without the IDS and recorded traces of energy expended for both communication and computation. As expected, there was no extra computational energy expended without the IDS in place as the sensors merely forwarded measured data to the cluster-heads. A total of 4 cluster-heads and 20 sensors were used and executed over 1 hour of simulation time unit, with the sensors sampling data every 0.4 seconds. As shown in Figure 10, all four cluster-heads consumed 68.05J of energy in total, while the sensors incurred 33.21J of energy by default. With the detection protocol operational, the CHs used 1.16J for computation and 71.12J for communication while the sensors used 0.44J and 34.79J respectively. This resulted in a 6.21% and 6.08% energy overhead for the CHs and sensors respectively, which is deemed acceptable.

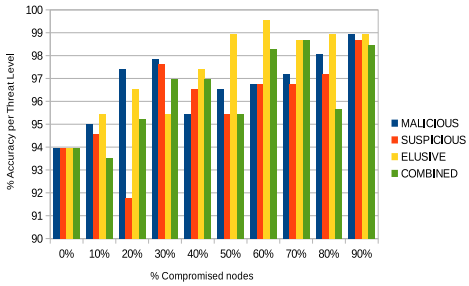

Fig. 7: Detection Accuracy

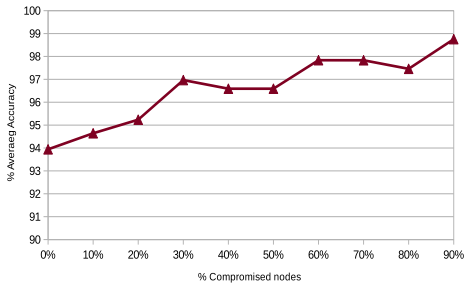

Fig. 8: Average Accuracy

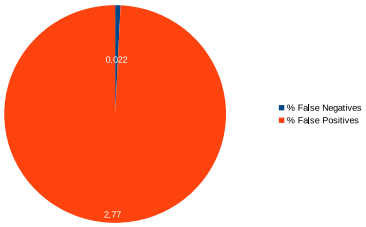

Fig. 9: False-Positives vs False-Negatives

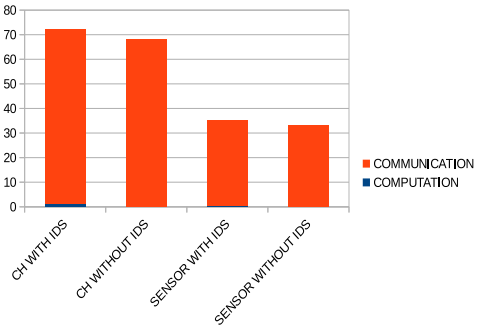

Fig. 10: Total Energy Usage

VI. Conclusion And Future Work

In this work, we conceptualized and implemented a mobile agent based intrusion detection system for wireless body area networks. Using different types of sensor agents, cluster agents and detective agents, we provided a hierarchical and distributed approach to detect various security attacks in these networks. We employed the use of machine learning classifiers on the mobile agents to provide an accurate detection of attacks. We investigated and compared five machine learning classifiers (NBC, KNN, SVM, RF and DT) and chose the most suitable one to implement our IDS. The system was assessed in terms of detection accuracy and energy consumption, and we achieved credible results with different combinations of adversarial sophistication.

References

[1] S.Movassaghi, M. Abolhasan, and J. L. et.al, "Wireless body area networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, pp. 1658–1686, 2014.

[2] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *Wireless Communications, IEEE*, vol. 17, no. 1, pp. 51 –58, february 2010.

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

[4] 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 *2014 IEEE Symposium on Security and Privacy*, May 2014, pp. 524–539.

[5] K. Anandumar, C. Jayaumar, K. Arun, M. Sushma, and R. Vikraman, "Intrusion detection and prevention of node replication attacks in wireless body area sensor networks," *International Journal of UbiComp (IJU*, vol. 3, no. 3, Jul. 2012.

[6] G. Thamilarasu, "iDetect: An Intelligent Intrusion Detection System for Wireless Body Area Networks," *Internaional Journal of Security Networks*, vol. 11, no. 1/2, pp. 82–93, Mar. 2016.

[7] J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isacoff, E. Spafford, and D. Zamboni, "An architecture for intrusion detection using autonomous agents," in *Computer Security Applications Conference, 1998. Proceedings. 14th Annual*, Dec. 1998, pp. 13–24.

[8] P. Kannadiga and M. Zulkernine, "DIDMA: a distributed intrusion detection system using mobile agents," in *Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Network*, May 2005, pp. 238–245.

[9] S.-C. Zhong, Q.-F. Song, X.-C. Cheng, and Y. Zhang, "A safe mobile agent system for distributed intrusion detection," in *Machine Learning and Cybernetics, 2003 International Conference on*, vol. 4, Nov 2003, pp. 2009–2014.

[10] S. B. Riecker Michael and M. Hollick, "Lightweight energy consumption based intrusion detection system for wireless sensor networks," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing. ACM*, 2013.

[11] S.-C. Zhong, Q.-F. Song, X.-C. Cheng, and Y. Zhang, "A safe mobile agent system for distributed intrusion detection," in *2003 International Conference on Machine Learning and Cybernetics*, vol. 4, Nov. 2003, pp. 2009–2014 Vol.4.

[12] O. Kachirski and R. Guha, "Intrusion detection using mobile agents in wireless ad hoc networks," in *IEEE Workshop on Knowledge Media Networking, 2002. Proceedings*, 2002, pp. 153–158.

[13] S. Khanum, M. Usman, and A. Alwabel, "Mobile agent based hierarchical intrusion detection system in wireless sensor networks," *International Journal of Computer Science Issues*, vol. 9, no. 1, 2012.

[14] G. Thamilarasu and Z. Ma, "Autonomous mobile agent based intrusion detection framework in wireless body area networks," in *2015 IEEE 16th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, 2015, pp. 1–3.

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