Autonomous Agent Based Intrusion Detection for WBANs

Adedayo Odesile, University of Washington, Bothell

PROBLEM STATEMENT AND GOALS
WBANs have recently emerged as the advocated means for remote physiological telemetry particularly in the medical space. Regardless of the significant benefits procured by this technology, its fundamental standard design does not entirely account for adequate security within its respective devices. The sensitivity of data relayed in such networks cannot be overemphasized being rated as the most valuable and private class of personal information in [1]. Secondly, the network dynamism and resource constraints that characterizes WBANs and other similar networks in the IoT space makes it relatively easy for an adversary to illegally extract, replay or modify transmitted data, or bring down devices with simple power draining DoS attacks. Such consequences are more dire in the WBAN space as they could lead to physical harm or loss of life to the victim.

The current WBAN standard specified by the IEEE 802.15 TG 6 [2] made some improvements over previous similar standards (i.e. Zigbee, Bluetooth) by providing multiple security profile options for end devices. However, these are cryptographic based solutions which are feasible on higher powered medical devices like the fitbit but may be beyond the computational capacities of micro IMDS (Implanted Medical Devices). Other alternatives such as trust based and intrusion detection have been proposed in a centralized and distributed fashion but still pose challenges in scalability, redundancy, and communication over-head.

Our current research explores alternative paradigms in sensor level security to address these security challenges without a significant compromise on efficiency.

APPROACH
We employ a novel approach which entails the use mobile code (autonomous agents) to distribute computation work load in a scalable and distributed fashion without incurring significant communication overhead. We assume a typical WBAN topology with macro and micro sensors all relaying sensed data to a central cluster-head which is usually a smart phone or its equivalent. We pre-load cluster-heads with the training sets modelled based on features that could be used to detect DoS or foreign device presence such as packet influx/efflux and RSSIs (Received Signal Strength Indicators). New sensor agents are instantiated and trained with chosen ML algorithm on the cluster-heads before dispatch into different cliques of the WBAN sensors. On visiting a sensor, a sensor agent collects cumulated logs and run them through its pre-trained algorithm to detect any anomalies. The same approach was applied at the higher level of the network hierarchy in environments with multiple interacting WBANs such that cluster-head agents are also dispatched across multiple cluster-heads to carry out distributed intrusion detection. Certain advantages are realized from the use of mobile code such as ease of deployment and update, reduction in communication overhead since agent does not need to travel with training set, scalability, and fault tolerance.

CONCLUSION AND FUTURE WORK
The current iteration of the system was ran on a simulation and assessed based on detection accuracy, and energy consumption. We believe similar results could be attained on actual devices as we put some effort in ensuring our energy usage model was approximately close enough to actual hardware devices. While we consider testing our system on actual hardware as a possible future activity, we intend to focus on handling agent packet loss and preventing injection of malicious agents into the network as our paramount priority.

REFERENCES
Autonomous Agent Based Intrusion Detection for Body Area Networks
Adedayo Odesile
University of Washington, Bothell.

Problem Statement and Goals

- WBANs are mostly employed in the healthcare space.
- The financial value ascribed to medical records tend to provoke more cybercrimes.
- WBAN is a subset of the sensor network domain which consist of devices commonly targeted for data breaches.
- This is due to the inability of most of these devices to provide enough computational resource for carrying out traditional data and network security measures.
- Traditional sensor level intrusion detection methods are characterized by scalability, redundancy, an energy constraints.

Approach

- Conceptualized a lightweight alternative that meets scalability, and fail-safe requirements without compromising efficiency.
- Used mobile code at different hierarchies of the network to significantly reduce communication overhead.
- We were able to design a control protocol that distributes the workload according to device’s computational power, i.e. train on cluster-heads and analyze on sensors.
- We implemented and tested simulations of the system against various attack models, and got promising results in detection accuracy, and resource overhead.

Results

- RESULTS: Our test results show an increasing trend in accuracy as % compromised nodes rises due to the training set being slightly biased to resulting in more false positives than negatives. Various features such as packet influx, received signal strength indicators, etc. were incorporated into the model to detect DoS related activity and signal interference from malicious nodes extracting data.
- CHALLENGES/FUTURE WORK: We intend to address the challenges arising from the possibility of agents going missing in transit and malicious agents being injected into the network. We also plan to increase the overall accuracy by improving the training models.