PHY-IDS: A Physical-layer Spoofing Attack Detection System for Wearable Devices

Wenqing Yan
Uppsala University, Sweden
wenqing.yan@it.uu.se

Sam Hylamia
Uppsala University, Sweden
sam.hylamia@it.uu.se

Thiemo Voigt
RISE SICS, Sweden
Uppsala University, Sweden
thiemo@sics.se

Christian Rohner
Uppsala University, Sweden
christian.rohner@it.uu.se

ABSTRACT

In modern connected healthcare applications, wearable devices supporting real-time monitoring and diagnosis have become mainstream. However, wearable systems are exposed to massive cyber-attacks that threaten not only data security but also human safety and life. One of the fundamental security threats is device impersonation. We therefore propose PHY-IDS; a lightweight real-time detection system that captures spoofing attacks leveraging on body motions. Our system utilizes time series of physical layer features and builds on the fact that it is non-trivial to inject malicious frames that are indistinguishable with legitimate ones. With the help of statistical learning, our system characterizes the signal behavior and flags deviations as anomalies. We experimentally evaluate PHY-IDS's performance using bodyworn devices in real attack scenarios. For four types of attackers with increasing knowledge of the deployed detection system, the results show that PHY-IDS detects naive attackers with high accuracy above 99.8% and maintains good accuracy for stronger attackers at a range from 81.0% to 98.9%.

CCS CONCEPTS

• **Security and privacy → Intrusion/Anomaly detection**;
• **Human-centered computing → Wearable devices**.

KEYWORDS

Physical-layer security, Spoofing attacks, Wearables, Machine learning, Time series analysis

ACM Reference Format:
Wenqing Yan, Sam Hylamia, Thiemo Voigt, and Christian Rohner. 2020. PHY-IDS: A Physical-layer Spoofing Attack Detection System for Wearable Devices. In *Proceedings of ACM Workshop on Wearable Systems and Applications (WearSys '20).* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3396870.3400010

WearSys '20, June 19, 2020, Toronto, ON, Canada

ACM ISBN 978-1-4503-8013-3/20/06…$15.00
https://doi.org/10.1145/3396870.3400010

1 INTRODUCTION

In body area networks (BANs), wirelessly connected wearable devices play an influential role in the revolution of healthcare applications, such as vital signs monitoring for remote monitoring and diagnostics. Although these systems support critical functionality, a lack of proper security protection is quite common [8]. Most reported security attacks are related to spoofing attacks where a malicious party impersonates another device because it can be exploited to launch many other sophisticated attacks. Through spoofing attacks, adversaries can not only report false data but also mislead the diagnose of the user's physical health condition and create life-threatening errors in subsequent treatment.

Spoofing attacks forge higher layer identities, such as MAC and IP addresses, or compromise authentication protocols [7]. Physical layer features in wireless channels are difficult to modify at will because of the spatial separation of sender and receiver and are preferable in security threat prevention. Our system analyses the time series of received signal strength indicator (RSSI), which is the power level of a received frame measured at the receiver's antenna. It is non-trivial for an attacker to send frames that are received with a signal level indistinguishable from the legitimate data sent over a dynamic wireless channel. A physical layer spoofing detection system is an essential complement to protect wearable devices against potentially life-threatening attacks.

Using RSSI to detect spoofing devices is not new, but all existing research require the RSSI measurements from several access points in a stationary setup [1, 11]. These approaches rely on clustering algorithms to analyze the overall RSSI statistics, which are sensitive to device positional changes. In BANs, human body movement makes it impossible to apply existing methods to distinguish spoofing attackers [14]. Moreover, wearable devices are generally designed with limited processing capability, storage space and power resources. Therefore, in practical implementation, security systems that require either multiple supporting devices, a large amount of data or heavy computation algorithms are problematic.

To fill in the gaps, we propose PHY-IDS, a spoofing intrusion detection system (IDS) specifically for wearable devices leveraging body motion and lightweight statistical algorithms. PHY-IDS can identify a single frame from an impersonating device by analyzing RSSI time series. With body movement, the RSSI behavior of off-body devices differ from the on-body devices, and the on-body devices at different positions also differ from each other. This diversity in feature dynamics is used to identify frames that violate the

regular pattern of the wireless signal from legitimate wearables. In particular, easy-to-collect audit data and light algorithms make it easy to deploy our system on wearable constrained devices. In this work, we make the following contributions:

(1) We propose a purely RSSI based IDS to detect spoofing attacks under body motions. With the help of statistical learning methods, our system uses distinct low-resolution patterns in wireless links to identify a single suspicious frame from malicious devices.
(2) We propose one naive and three smart attack models that acquire increasing knowledge of the deployed system and have learning capability.
(3) The system is evaluated with wearable devices on different positions in real attack scenarios, including on-body and off-body attackers. The results show that our system can detect naive attackers accurately, and maintains good accuracy even for sophisticated attackers.

The rest of paper is organized as follow. An overview of the related work is given in Section 2. Then, Section 3 defines the problem and observations of unique BAN channel characteristics. In Section 4, the PHY-IDS detailed system design are presented, followed by attack models in Section 5. After that, Section 6 presents the experiment setup and evaluation results. We finally conclude this paper in Section 7.

2 RELATED WORK

In this section, we introduce three types of related work to defend spoofing attacks. The first approach limits the communication range, the second builds on cryptographic mechanisms, and the last one is the detection of anomalies, either based on cross-layer or physical-layer information.

(1) *Proximity-based Methods*: For BAN security protection, limiting the communication range is an intuitive method to secure wearable systems since devices are constrained to a body. A suitable option is near-field communication technology, but research shows that an attacker with a high-gain antenna can access devices even outside the intended range [4]. The ultrasonic distance-bounding scheme introduced by Rasmussen et al. [9] solves this vulnerability but requires extra sonic transceivers. Our system utilizes the differences in signal behavior to detect adversaries and hence mitigates this vulnerability without any hardware modification.

(2) *Physical Layer as Source of Randomness*: The unique physical properties of the wireless medium are powerful sources of randomness that can be used for secure key generation [10, 12]. Shi et al. [12] leverage the signal strength characteristics along with body movements to achieve authenticated key generation between each wearable and a hub, but the proposed system suffers from low key generation rate and ignores the possibility of on-body attackers. DLINK [10] improves the bit rate five times higher than previous research, which makes the key generation mechanism more robust in various fading channel conditions. However, these cryptography-based schemes still face the risk of key leakage, as well as replay attacks, which can bypass the cryptographic protection using the same legal management structure [6].

(3) *Cross-layer Anomaly Detection*: MedMon [15] is a wearable anomaly detection framework that requires a security monitor

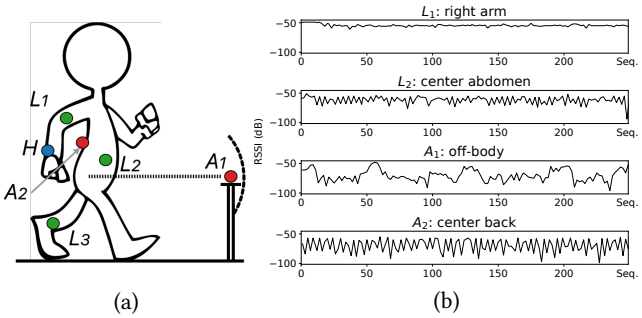


Figure 1: (a) Motes placement: Hub: wrist (H); Legitimate nodes: right arm (L_1), center abdomen (L_2), and left ankle (L_3); Attackers: fixed on surrounding furniture (A_1) (distance between test person and (A_1) changing between 25cm to 400cm), attached on tester body (A_2). (b) RSSI signal behavior among different channels in BANs, when human walking indoors.

across multiple network layers. A large number of features extracted from different receiving process are required including RSSI, time of arrival, data payload, packet repeating rate, etc. For each feature, an individual security policy with predefined threshold is used to detect malicious behavior. PHY-IDS implements a learning-based detection framework with single feature time series, which not only avoids the cumbersome multi-layer monitoring architecture but also simplifies the tedious threshold presetting process.

(4) *Physical-layer Anomaly Detection*: Detecting spoofing attacks with RSSI in static wireless networks has been studied previously [1, 3, 11], building on the observation that received signals reflect the propagation environment or the wireless interface at the nodes (i.e., fingerprinting). These approaches assume static environments that are sensitive to movements since channel variation makes the detection difficult. Huang et al. [5] devised a motion invariant authentication system for wearable systems based on the idea of removing the motion features at the cost of computationally complex feature extractors, deep neural networks and intense RSSI sampling process. Our system makes use of the channel variation due to movement instead, and achieves the spoofing attack detection under motion with a lightweight real-time intrusion detection system and a much lower sampling rate.

3 PROBLEM DEFINITION

3.1 System Model

Our wearable system is a wireless network composed of N on-body nodes, including sensors, actuators, and one hub. In this paper, we consider a star topology in which all nodes connect to the central hub with one-hop bidirectional links. Depending on their functionality, nodes are attached to different body areas, for example, a glucose sensor on the arm, a pacemaker in the chest, a plantar pressure under the foot, and a fitness tracking band on the wrist. The hub is a device such as a smartwatch, responsible for aggregating, processing, and relaying data to remote data centers.

3.2 Security Goal

We focus on detecting spoofing attacks in BANs, that is, external transmitters (attackers) impersonate legitimate nodes and try to send false data or false critical commands to a node in the network.

The objective of PHY-IDS is to differentiate between legitimate and malicious packets based on the physical layer characteristics of received wireless frames.

Our system provides real-time investigation for every single incoming frame without any additional hardware. It is installed on off-the-shelf wearable devices as plug-ins. The key idea of PHY-IDS is to verify whether a received frame fits into the feature time series of signals coming from a legitimate device. In this paper, we consider both naive attackers and strong attackers, who are aware of the detection system and intend to remain undetected and hide their malicious frames by manipulating their physical layer transmissions to follow the expected behavior of the legitimate signals closely. We will present the detailed attack model in Section 5.

3.3 RSSI Behavior of Wearable Devices

In BANs, the radio channel depends on plenty of parameters, such as individual body shape, body movement, node placement, and device hardware. Miniutti et al. [2] have reported that the channel behavior in BAN is scenario-dependent. Figure 1(b) shows the RSSI time series we collected when a person walks indoors. The channel dynamics differ notably depending on the placement of the transmitter. With the receiver placed at the tester's right wrist, the variation of the signal coming from the center abdomen is higher than that from the right arm. Non-line-of-sight channels, for example, from the center back tend to vary more. On-body channels are more stable than channels of off-body nodes. These differences in individual channel dynamics and physical signal behaviors provide the foundation to distinguish the transmitter of different signals.

4 SYSTEM DESIGN AND ALGORITHM

In this section, we describe the PHY-IDS framework to detect malicious frames injected by spoofing attackers. Figure 2 is a system overview, which contains four steps. PHY-IDS requires every node collecting the RSSI of each received frame.

The first time deploying a device, the system runs step ① in an arbitrary environment under movements to collect training time series. In this step, the hub broadcasts a steady stream of probe packets to emulate the real traffic, and the node records the RSSI time series. Then a learning algorithm in step ② will model the RSSI behavior of the legitimate wireless signal. The complexity of learning algorithms is considered too expensive for resource-constrained devices so that we execute them off-line in a powerful device such as a hub. After the individual wearable device downloads back its model, the real-time detection ④ runs locally to ensure timely detection.

During the regular communication of the wearable devices, our system monitors the RSSI metric for each incoming frame. Then, based on the MAC address in the received frame header, the system chooses the corresponding pattern to analyze each sample and justify its legitimacy. Note that for bidirectional links, the RSSI has the symmetric property[13]. Signals in two directions of the same link share an identical RSSI pattern. Thereby, in step ③, the model can be loaded on both the hub and resource-constrained nodes.

Our system uses an autoregressive model as the time series prediction model, which is trained with a historical RSSI trace. The task of the model is to predict the upcoming value $\widehat{x_i}$ with the lagged

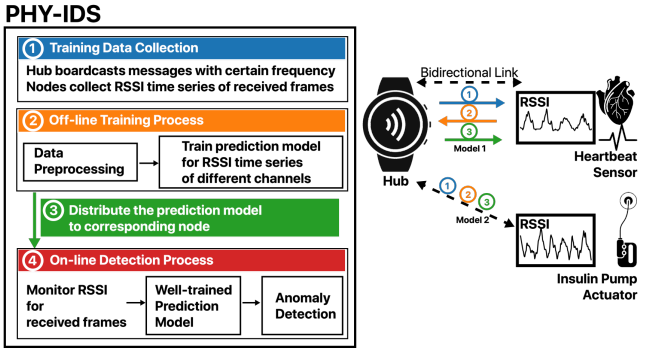


Figure 2: System overview of PHY-IDS

records in a size n sliding window $X_{i-1} = \{x_{i-1}, x_{i-2}, ..., x_{i-n}\}$ as:

$$\widehat{x_i} = f(X_{i-1}) \tag{1}$$

where $f(\cdot)$ is a well-trained prediction model. Once the model is sufficiently trained, in the detection process, the prediction error can be calculated as the Euclidean distance between the predicted and observed value as:

$$Error = |\widehat{x_i} - x_i| \tag{2}$$

A high error tags a significant deviation from the expected behavior. When the prediction model captures time-series accurately, the system can detect anomalies that violate legitimate behavior with simple thresholding algorithms.

4.1 Prediction Models

To identify a suitable model of RSSI time series forecasting, we compare two models, namely autoregression (AR) and long short term memory (LSTM). The former yields a linear model and the latter is a recurrent neural network. Learning is the optimization process to minimize the target error function w.r.t. model coefficients W in the training dataset as below, where $f(\cdot)$ is the model function and R is the regularization term.

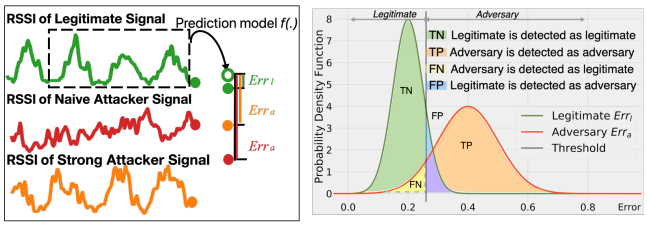
$$\min_W \sum |f(W, X) - x_i|^2 + R \tag{3}$$

4.1.1 Autoregression. In time series analysis, a linear forecasting model is modeled as below:

$$f(W, X_{i-1}) = w_0 + w_1 x_{i-1} + ... + w_n x_{i-n} \tag{4}$$

where n represents the n_{th} autoregression order that is equal to the prediction window size, and W is the coefficient set $\{w_0, w_1, ..., w_n\}$. The linear regression assumes the data has the Markov property, that is, the current sample only depends on the previous samples. We add an L1 regularization term $\alpha|W|$ in the model that estimates the sparse coefficients. It has a feature reduction side effect that efficiently reduces the computing complexity in the prediction stage. To train the model, we use a coordinate descent solver that keeps iterating until the target function converges.

4.1.2 Long Short Term Memory. It is one type of recurrent neural network (RNN) applied to sequential data prediction. It is good at non-linear modeling for long-range sequences. Different from standard neural networks, RNN uses the hidden states to capture the information about the computational results of the previous time step. Our model is constructed by stacking one input layer, one output layer, and two LSTM layers with the rectified linear unit as an activation function. In our experiments, we train the model with different hyper-parameters and evaluate their performance to find a suitable setup for each dataset.



(a) Attacking scenario (b) Detection threshold optimization

Figure 3: (a) RSSI of malicious signal deviates from the expected behavior of legitimate signal. (b) Error distribution differs between legitimate and adversary transmitters.

4.2 Anomaly Detection

In order to identify frames from malicious transmitters, the on-line detection system computes the error in Equation 2 as the anomaly score for every incoming frame. An alarm is triggered whenever $Error > \theta$ for threshold θ. Multiple anomaly detection algorithms can be applied to this binary classification task except for the vanilla method with a fixed threshold. However, it is worth pointing out that finding the best-performing classification is not in the scope of our paper. For this work, we optimize the θ choice with Equation5 and derive the best ideal accuracy of our system based on the statistics of different attacks in our adversary model. Assume the legitimate incoming signal has an error score of Err_l, and the adversary signal is Err_a. Statistically speaking, Err_l and Err_a are two random variables that follow different distribution as shown in Figure 3 Different θ settings divide the density plot into four parts, TP (true positive), FP (false positive), TN (true negative) and FN (false negative).

$$\max_{\theta}\{Accuracy\} = \max_{\theta}\{\frac{TP+TN}{TP+TN+FP+FN}\} \tag{5}$$

5 ADVERSARY MODEL

We do not constrain the attacker's location. However, we assume that in most scenarios, there is a low probability that an adversary is located next to legitimate nodes. We classify attacks into four groups based on their knowledge of our system. We assume L is a legitimate node and A is an attacker. After training, $f_L(\cdot)$ is the legitimate prediction model. In real-time detection, L records the RSSI series X_L for incoming frames as prediction model inputs. Due to the open nature of the wireless medium, malicious attackers can eavesdrop the on-going communications passively and record the local RSSI as X_A. To fool the detection system, all attackers target to forecast the legitimate RSSI trace accurately and fool our detection system with a low error score.

(1) *Naive Attacker*: The first attack vector does not know anything about our detection system. It transmits frames with fixed transmit power without any efforts to evade our system inspection. This is the most naive attacker we use as a benchmark to show what is achievable with PHY-IDS.
(2) *Model-stealing Attacker*: The second attacker knows the well-trained model $f_L(\cdot)$ our system uses, but can not get access to any legitimate nodes' real-time RSSI. The attacking model is $\widehat{x} = f_L(X_A)$.
(3) *Training Data-stealing Attacker*: The third attacker first appears early in initial training data collection. When legitimate nodes are collecting training data, the attacker eavesdrops the same frames and locally records the RSSI. After that, it intercepts the legitimate RSSI trace and trains his own prediction model $f_{A-L}(\cdot)$ mapping the relation between attacker data and legitimate data. In the detection period, it is only a passive eavesdropper and can not compromise any nodes. Thereby, the attacking model is $\widehat{x} = f_{A-L}(X_A)$.
(4) *Mimic Training Attacker*: The final attack vector deploys an emulation attacking setup on another person to collect pseudo training data for nodes L' and A', which is an imitation of the previous attack. The attacking model is a pseudo version of the previous attack $\widehat{x} = f_{A'-L'}(X_A)$.

6 EVALUATION

In this section, we evaluate PHY-IDS on a prototypical setup. First of all, we show that compared to a neural network, our AR model performs better in RSSI prediction with a lower computational cost. Afterward, we evaluate the ability of our system to detect different attackers based on signal physical characteristics. In the end, we analyze the system cost and compatibility, and also introduce a parameter choosing guideline.

6.1 Experimental Setup

We set up a wearable prototype with six Firefly motes that feature IEEE 802.15.4-compliant transceivers. The onboard transceiver is a Texas Instruments CC2520 chip with a ceramic antenna. As shown in Figure 1(a), three motes act as proxies for wearable devices worn on different body areas (arm, abdomen and ankle), one as hub fixed on the wrist and the other two as attackers (off-body and on-body).

We measure average RSSI during one packet reception as one sample. In all experiments, the hub broadcasts packets every 5 ms with a fixed transmission power of 0 dBm, and the other motes record the RSSI time series under user walking scenario. In our configuration, to reach a high RSSI sampling rate, we use a packet sending frequency of 200 Hz. In practice, the packets are sent at a lower speed. In order to maintain the sampling rate, the system can sample RSSI more than once during one packet transmission.

In the experiment, two volunteers participated, one male and one female. For data collection, we asked them to wear the motes and walk 10 mins in their normal ways. We test our system in an office corridor with regular furniture around. In this lively wireless environment, the signals are interfered by nearby objects as well as other signal sources such as WiFi and Bluetooth devices.

We implement PHY-IDS in `Python` using the `Sciki-learn` and `Keras` library. For model evaluation, the train and test data is split as 70/30 for all our experiments. For a appropriate sliding window size choice, each dataset calculates the autocorrelation and partial autocorrelation function with lag range from $[0\,s, 30\,s]$. Based on the most correlated lagged range, we go for a fair choice with 10 s for all datasets. To amplify the behavior characteristics caused by dynamic channels, we normalize data and range in value from 0 to 1 before applying a prediction algorithm. It also can help optimizer speed up the training process and reduce the chances of getting stuck in local optimums. We train the prediction model individually for every

dataset from different legitimate nodes. The hyper-parameters are optimized for each model. To tune the parameters, the autoregression model implements a grid search with ten-fold cross-validation, and the neural network uses manual search because of the ample parameter space. To assess the impact of sampling rates on prediction accuracy, we downsample all our data originally 200 Hz sampling rate to (100, 50, 20, 10, 8, 4, 2, 1 Hz).

6.2 Model Suitability

We evaluate prediction model performance with normalized mean absolute error (NMAE) defined as below, where x_i is the actual RSSI value at time i, $\hat{x_i}$ is the estimation value and n is the size of test set.

$$\text{NMAE} = \frac{\sum_{i=1}^{n} |x_i - \hat{x_i}|}{\sum_{i=1}^{n} x_i} \tag{6}$$

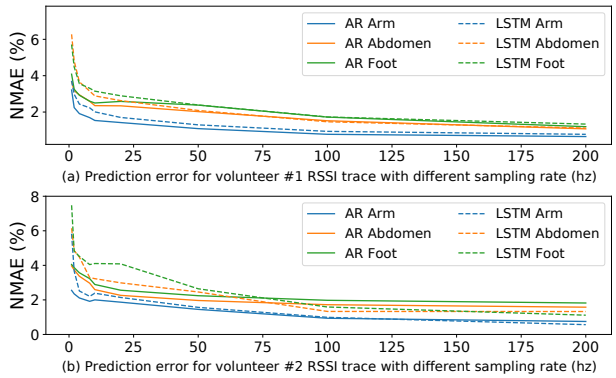


Figure 4: Prediction performance of autoregression (AR) and long short term memory (LSTM)

Figure 4 is the detailed prediction performance of two models with different sampling rates. It covers six datasets collected from two volunteers with three legitimate nodes each. Although the prediction error changes as the sampling rates vary, both models hold a good accuracy level. The best prediction error of 1% would imply an average accuracy of 99%, which means both models can nicely capture the mapping between history data in window X_{i-1} and the current time sample x_i. In general, it is clear that autoregression performs slightly better than the neural network, especially with low sampling rates. This may because the current time-series correlation is dominated by linear relationships, which is not the strength of recurrent neural networks. Alongside this, the sizeable hyper-parameter space of the neural network might be another reason. It challenges us to find the optimum network structure for each dataset. In contrast, autoregression only has one hyper-parameter α that is much easier to traverse entirely and figure out the best model configuration.

Another observation is that the prediction error increases for both models when resampling at lower rates. A higher resolution provides more information within the tested range that helps models capture the dynamic channel details. However, the impact of the sampling rate on prediction error is not linear. Figure 4 shows that prediction errors have rapid changes in the low sampling range below 20 Hz. The Nyquist-Shannon sampling theorem can explain this. When the sampling rate is higher than two times signal frequency, perfect reconstruction is guaranteed possible. The human body effective natural moving frequency is below 2 Hz, so, in theory, 4 Hz should be the lowest boundary to capture the dynamic channel behavior under walking. When the sampling rate is lower than the theoretical bottom line as the left side of error lines, it is difficult to track the signal behavior due to a lack of information. One the other hand, the figure also shows that choosing a too high sampling rate does not make a significant difference.

Besides that, our models have generalizability across different node positions and testers. However, sensor placement indeed influences model performance. For sensor position at the arm, the models have lower error rates. More likely, complex movement in the channel between foot and hub introduces higher random noise, which negatively affects prediction performance. We also compare the experiments on two testers. Although an individual has a unique gait pattern, the prediction error is at the same level on the datasets from two testers. It indicates that our models can capture the characteristics of the dynamic channel under the walking movement.

6.3 Detecting Spoofing Attacks

In this section, we show the ability of PHY-IDS to detect four levels of spoofing attacks mentioned in Section 5. To do so, we simulate the strong attacks using the data collected from real experiments. In the following experiments, we use AR as the prediction model with 10 Hz as the sampling rate. Based on the empirical error distribution of the attacker, we optimize the threshold setting and infer the theoretical detection accuracy based on the method shown in Section 4.2.

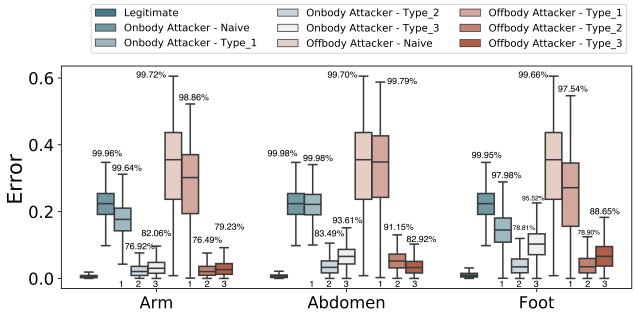


Figure 5: The error performance of four attackers: naive attacker (Naive); model-stealing attacker (Type_1); training data-stealing attacker (Type_2); mimic training attacker (Type_3). The number on top of each box is the accuracy of detecting spoofing attacks from both on-body and off-body malicious devices in different scenarios.

Error statistics of each attacker are shown in Figure 5, and we mark the individual detection accuracy on top of each box. As a benchmark, our system can detect naive attackers with an accuracy above 99.8%. This accuracy holds for all scenarios, which means both on-body and off-body attacks have distinct physical channel behavior from legitimate nodes. Similarly, the model-stealing attack

is also easy to detect. Since a model is trained for a specific channel, the well-trained model does not fit with the physical feature time series of any other channels. Emulating the attacking setup on another person helps the attacker to learn the legitimate channel behavior, but entirely fooling our system is still impossible. The detection accuracy of the mimic training attacker is approx 87.0% on average. The training data-stealing attack is considered as the strongest model, which has enough information to train a separate algorithm mapping the relationship between the eavesdropped RSSI and legitimate time series. However, it is still detectable by our system with an accuracy around 81.0%. In general, due to the open nature of the wireless medium, the attacker can receive the same signal, which is not enough to estimate features of the signal received by the victim receiver. Without access to the legitimate RSSI time series, we consider that learning all signal behavior details is unlikely even for adversaries with learning capability.

6.4 System Cost and Compatibility

We first compare the computational complexity of autoregression and LSTM. For model training, AR has a overall complexity of $O(n^3+n^2t)$, where n is the sliding window size and t is the number of training samples. For standard univariate LSTM with K memory cells, n lagged time steps, t training samples and m epochs, the computational complexity is $O(4mt(K^2+Kn+K))$. When K and m are large, training the LSTM model is much more expensive than AR. For our design, model prediction complexity is another important factor to assess system cost. To predict one sample, the AR model has a complexity of $O(n+1)$. Compared to one single recurrent layer in LSTM model, this is a very low computational level. In practical scenarios, our system distributes the on-line detection components to the wearable nodes. For these resource-constrained devices, AR with low computational cost and higher prediction accuracy is an appropriate choice.

We also notice that the model input dimension is a parameter critical to the system operating cost. The model requires a high sampling rate to capture the complete signal behavior, which implies a larger window size n as input. This not only increases the calculation load but also challenges the resource consumption related to data collection, storage, and preprocessing. In a nutshell, choosing the sampling rate is a two-fold question: it should not be lower than the human body movement frequency but can not be too high to affect other operating functions on the devices. The specific choice should base on the actual deployment.

For PHY-IDS to detect spoofing attacks, a steady stream of legitimate data has to be transmitted. Streaming applications such as real-time health monitoring and Bluetooth earphones are ideal for our system to track received signal behavior. If the wearable device only occasionally generates data, the burst of traffic will result in the first few frames not being well detected due to incomplete prediction window filling. Hence, we also designed an backward detection mode that uses frames coming after $X_{i+1} = \{x_{i+1}, x_{i+2}, ..., x_{i+n}\}$ to verify the previous RSSI x_i with our autoregressive model $f(X_{i+1})$, triggered by the reception of x_i. The NMAE difference between the backward model and the normal forward model is less than 0.15%. This ensures that PHY-IDS can inspect every received frame in different transmission modes and is compatible with deployed applications.

7 CONCLUSION

In this work, we propose a novel real-time spoofing detection system to augment wearable device security protection under body motion. Our system leverages physical layer signal behavior to distinguish legitimate devices from malicious attackers. For different levels of spoofing attacks with increasing knowledge of deployed system, the experimental results demonstrate that PHY-IDS can detect naive attacks with 99.8% average accuracy and still maintain 81.0% for the strongest attacker with full knowledge and advanced learning capability. It is a promising step towards using wireless-link characteristics for spoofing attack detection in BANs.

ACKNOWLEDGMENTS

This project is supported by the Swedish Foundation for Strategic Research (Grants RIT17-0020).

REFERENCES

[1] Yingying Chen, Wade Trappe, and Richard P Martin. 2007. Detecting and localizing wireless spoofing attacks. In *4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*.
[2] Miniutti Dino and et al. 2008. *Narrowband Channel Characterization for Body Area Networks.* Technical Report.
[3] Daniel B Faria and David R Cheriton. 2006. Detecting identity-based attacks in wireless networks using signalprints. In *Proceedings of the 5th ACM workshop on Wireless security*.
[4] Ernst Haselsteiner and Klemens Breitfuß. 2006. Security in near field communication (NFC). In *Workshop on RFID security*.
[5] Yong Huang, Mengnian Xu, Wei Wang, Hao Wang, Tao Jiang, and Qian Zhang. 2019. Towards motion invariant authentication for on-body IoT devices. In *IEEE International Conference on Communications (ICC)*.
[6] Zhiping Jiang, Jizhong Zhao, Xiang-Yang Li, Jinsong Han, and Wei Xi. 2013. Rejecting the attack: Source authentication for wi-fi management frames using csi information. In *IEEE Conference on Computer Communications (INFOCOM)*.
[7] Pengfei Liu and et al. 2019. Real-time Identification of Rogue WiFi Connections Using Environment-Independent Physical Features. In *IEEE Conference on Computer Communications (INFOCOM)*.
[8] Lily Hay Newman. 2019. A Model Hospital Where the Devices Get Hacked on Purpose. Retrieved April 14, 2020 from https://www.wired.com/story/defcon-medical-device-village-hacking-hospital/
[9] Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S Heydt-Benjamin, and Srdjan Capkun. 2009. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM conference on Computer and communications security (CCS)*.
[10] Girish Revadigar, Chitra Javali, Wen Hu, and Sanjay Jha. 2015. DLINK: Dual link based radio frequency fingerprinting for wearable devices. In *IEEE 40th Conference on Local Computer Networks (LCN)*.
[11] Yong Sheng, Keren Tan, Guanling Chen, David Kotz, and Andrew Campbell. 2008. Detecting 802.11 MAC layer spoofing using received signal strength. In *IEEE Conference on Computer Communications (INFOCOM)*.
[12] Lu Shi, Jiawei Yuan, Shucheng Yu, and Ming Li. 2015. MASK-BAN: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks. *IEEE Internet of Things Journal* (2015).
[13] Kannan Srinivasan and Philip Levis. 2006. RSSI is under appreciated. In *Proceedings of the 3rd workshop on embedded networked sensors*.
[14] Stéphane Van Roy and et al. 2012. Dynamic channel modeling for multi-sensor body area networks. *IEEE Transactions on Antennas and Propagation* 61, 4 (2012).
[15] Meng Zhang, Anand Raghunathan, and Niraj K Jha. 2013. MedMon: Securing medical devices through wireless monitoring and anomaly detection. *IEEE Transactions on Biomedical circuits and Systems* (2013).