A framework for detecting MAC and IP spoofing attacks with network characteristics

Jaegwan Yu*, Eunsoo Kim*, Hyoungshick Kim*, and Jun Ho Huh**
*Sungkyunkwan University, Republic of Korea
{jaegwan, eskim86, hyoung}@skku.edu
**Honeywell ACS Labs, USA
junho.huh@honeywell.com

***Abstract*—This paper presents a spoofing attack detection framework based on physical network characteristics (e.g., received signal strength indicator, round trip time and link quality indicator) that cannot easily be mimicked by artificial means. Unlike most previous studies that are sensitive to changes in network conditions, we propose a spoofing attack detection method, which is highly robust to the changes of network conditions over time. The proposed framework can monitor devices' physical network characteristics in real time and check if any significant changes have been made in the monitored measurements to effectively detect device spoofing attacks. To demonstrate the feasibility of the proposed framework, we analyzed how the RSSI values of packets were changed with varying physical distances in a real ZigBee (IEEE 802.15.4) network environment.**

1. Introduction

Wireless network technologies (e.g., ZigBee, WiFi, and Bluetooth) make network device configuration and management more convenient. However, these technologies could also lead to potential risks of cyber attacks which raise serious security and privacy concerns for users. For example, a user's home devices and files could be illegally accessed by unauthorized neighbors via a wireless communication channel unless a proper access control scheme is deployed.

In many home network applications, media access control (MAC) address is popularly used for designing access control schemes (hereafter called *MAC-based* access control) where only whitelisted MAC addresses are accessible on a private network [1]. It enables a network administrator to manage a list of valid MAC addresses to limit access to resources on home devices only to authorized devices. However, this approach has several weaknesses in both security and usability. Tech-savvy end-users can easily spoof MAC addresses. Also, maintaining a whitelist of acceptable MAC addresses could be a challenging task for casual users.

In order to overcome the limitations of a MAC-based access control scheme, one possible solution is to analyze devices' physical characteristics which are hard to imitate. There have been several previous studies to solve this problem using the physical properties of wireless signals. Faria et al. [2] introduced an idea of using the Received Signal Strength Indicator (RSSI) reported by access points in order to detect misbehaving devices because RSSI could be assumed to be a measurement which is not only hard to forge arbitrarily but also highly correlated to a device's location. Chen et al. [3] also proposed a similar technique based on the devices' RSSI to use the K-means clustering algorithm to detect spoofing attacks. Sheng et al. [4] developed proprietary software to design a more robust RSSI monitor by removing duplicates and synchronizing timestamps. Jokar et al. [5] presented spoofing detection method based on the spatial correlation property of RSSI. They attained a 94.75 percent detection rate with a 0.56 percent false positive rate using only one monitoring access point (AP). They attained a 99 percent detection rate with no false positives when using four monitoring access points. However, the majority of those approaches require a set of multiple traffic measurement devices to achieve high accuracy and reliability, which may not be acceptable in small network environments (e.g., home networks) where only a single access point is available.

In this paper, we propose a novel spoofing attack detection method using the information about the target device's physical network characteristics collected in a given time-interval. We develop a spoofing attack detection algorithm based on a dynamically updated threshold, which is robust to the changes of network conditions. Our experiments were performed on ZigBee (IEEE 802.15.4) rather than WiFi but the proposed technique can work well regardless of the underlying protocol being used. Our key contributions can be summarized as follows:

- Unlike previous approaches based on globally observed measurements, we develop a spoofing attack detection method which is highly robust to the changes of network conditions over time. To improve the accuracy of the proposed algorithm, we consider several physical network features of devices, and monitor inconsistencies between packet sequences (observed during different time intervals) with respect to those network features.
- To demonstrate the feasibility of the proposed detection method, we analyzed how the RSSI values

of packets are affected from changing physical distances in a real network environment.

The rest of this paper is organized as follows. Section 2 describes a possible attack scenario to explain the motivation of our study. In Section 3, we present the proposed detection technique with devices' physical network characteristics. In Section 4, we measure how RSSI values are affected by varying physical distances. In Section 5, we discuss key implementation challenges.. Related work is discussed in Section 6. Finally, we conclude in Section 7.

2. Threat model

This section describes a practical attack scenario that involves an attacker illegally accessing a victim's device, and discusses the limitations of existing MAC-based access control.

2.1. Attack scenario

Let us consider a scenario where an attacker is carrying a laptop with various client applications installed, and is parked outside a victim's home. Using known wireless protocols and client applications, the attacker tries to directly connect to the victim's home device, e.g., a smart TV. If the victim does not properly follow standard practices for home network security (e.g., using the default password on the smart TV), the attacker could easily access and watch recorded TV, view photos, or download documents stored on the victim's device.

Wireless networks are inherently prone to security problems. Unlike a wired network, a wireless network is accessible to anyone in the vicinity. Hence, a security mechanism should be deployed to prevent such attack attempts so that only the authorized can access to the resources. Using *MAC-based* access control list is a popularly used security practice because it is simple to deploy. In the next section, we will explain why existing MAC-based access control mechanisms are not robust against spoofing attacks.

2.2. Limitations of MAC-based access control

The most widely available and used defense mechanism is to use an access control list (ACL) with devices' network addresses. A security administrator creates specific rules that allow registered devices to access the network resources. Source/destination IP and MAC addresses can be used for defining those rules. That is, request messages or packets are ignored or dropped when those messages or packets were sent by a device that is not included in the ACL. MAC addresses are more popularly used than IP addresses because IP addresses can often be assigned dynamically assigned.

However, several limitations exist in this approach. First, for casual users, it is really cumbersome to maintain an ACL with the latest changes of devices and services. If the coverage of the ACL is insufficient, it can incur a significant usability penalty that finally result in discouraging users from using ACL-based access control mechanisms. To make matters worse, the actual security of MAC-based access control schemes have been weaker than expected because MAC addresses can also be spoofed by tools that some experienced users can easily use [6]. MAC spoofing is a technique used to change the MAC address assigned to a Network Interface Card (NIC) to a different address. By changing it to a trusted, known MAC address, an attacker can bypass MAC-based access control mechanisms. Ogle et al. [7] showed that many hotel networks were vulnerable to MAC address spoofing attacks that can be used to monitor and redirect traffic. Similarly, Ahmad et al. [8] showed that an attacking device on the same wireless network can simply send spoofed address resolution protocol (ARP) replies to victim devices even when a strong security mechanism such as WiFi Protected Access Pre-Shared Key (WPA-PSK) is used to authenticate and validate devices on the wireless network.

3. Proximity based access control

To overcome the existing limitations of MAC-based access control, we propose a proximity-based access control scheme that is capable of detecting attacks that originate from outside the victim's house and use MAC spoofing. We first explain the proposed detection method at a high level, and discuss several physical characteristics that can be used for detection.

3.1. Proposed detection method

The key idea of the proposed method is to monitor a device's physical characteristics and check if there are any significant changes in the measurements of those characteristics to detect an unauthorized device trying to access the network from outside a victim's house.

Physical network characteristics of a device such as "signal strength" are highly related to its physical location. Therefore, we use such characteristics as a fingerprint for a device that can be independently observed. Figure 1 shows the description of our method with the time series of the collected packets. We use the term of *detector* to represent a device to monitor the changes in other device's physical network characteristics.

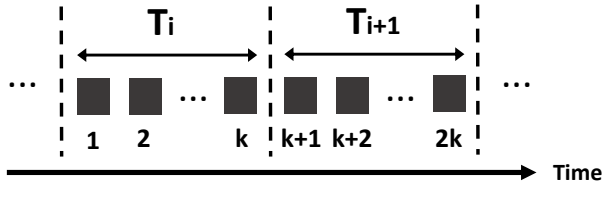


Figure 1. Time series of the collected packets with two time intervals.

If a device's physical network characteristics are statistically consistent, the packets in a time window T_i and the

packets in the next time window T_{i+1} have similar physical network characteristics. Consequently, if the two packets collected from an identical network device (with the same IP and MAC addresses) during the two subsequent time intervals have a significantly different network characteristics and the physical location of that device is not changed, it could be used as an evidence of a spoofing attack.

There are, however, many challenges involved in developing this method. We identified the following research questions to drive the design process: "What types of network features could be used for this purpose?" "What is the best time window size for the proposed framework?" "How can we compare the network characteristics of packets between two subsequent time intervals?" and "How can we determine a threshold α of significant changes in the measurement of physical characteristics?"

3.2. Candidate features

In ZigBee networks, the following three features are generally considered to measure a device's physical characteristic that cannot be mimicked easily.

"RSSI" is a metric to indicate the power level of a received radio signal implemented in IEEE 802.11. The higher the RSSI value the stronger the received signal. There is no standard format nor particular physical parameter for obtaining RSSI value in mW or dBm. Thus, each vendor making chip-sets uses its own unit.

"RTT" is a time delay which is the sum of two propagation delays of a request packet to be sent and response packet to be received. RTT is affected by not only the physical distance between network entities, but also other factors such as packet loss rate and queuing delay in the operating system.

"LQI" is a metric used to estimate the link quality of a received signal implemented in IEEE 802.15.4. It represents how easily a received signal can be demodulated by accumulating the magnitude of the error between ideal constellations and the received signal over the 64 symbols immediately following the sync word. LQI is calculated by measuring the number of successful modulations from the physical layer, and this is relevant to the error rate of the received packets.

3.3. Candidate similarity measures

If the similarity between two subsequent packet sequences is greater than a predefined threshold α, the case is treated as an anomaly.

For this purpose, we need to have a proper similarity measure between two packet sequences. In this paper, we suggest the two following similarity measures: (1) Euclidean distance and (2) DTW distance because the two measures are widely used for time series classification.

Given the two packet sequences $p = (p_1, p_2, \cdots, p_k)$ and $q = (q_1, q_2, \cdots, q_k)$, the Euclidean distance D_{Euc} between p and q is calculated as

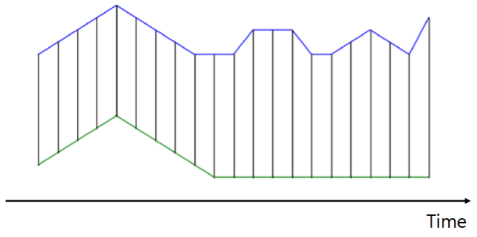
$$D_{Euc} = \sqrt{(p_1 - q_1)^2 + \cdots + (p_k - q_k)^2}$$

where $p_i - q_i$ is defined as the weighted sum of the differences between the observed values for each feature (i.e., RSSI, RTT and LQI). If we assume that there are n features to be observed, $p_i - q_i$ is calculated where $p_i = (p_{i1}, p_{i2}, \cdots, p_{in})$ and $q_i = (q_{i1}, q_{i2}, \cdots, q_{in})$ as

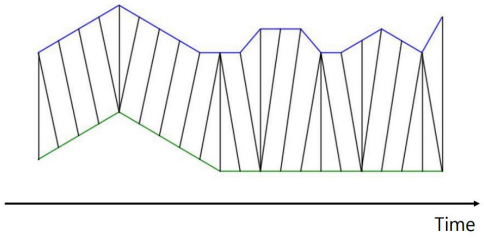
$$p_i - q_i = \sqrt{(w_1 \cdot (p_{i1} - q_{i1}))^2 + \cdots + (w_n \cdot (p_{in} - q_{in}))^2}$$

where w_j denotes the relative importance of the jth feature. We can estimate the relative importance of each feature using a feature selection algorithm.

We also used the DTW (Dynamic Time Warping) algorithm [9] to measure the time-series similarity by minimizing the effects of time-shifting and distortion. In the case of Euclidean case (see Figure 2(a)), the ith element from a sequence matched the ith element of another sequence. However, DTW finds the optimal alignment of two sequences and measures the similarity between the optimally aligned elements (see Figure 2(b)).



(a) Euclidean distance.



(b) DTW distance.

Figure 2. Euclidean distance vs DTW distance.

4. Experiment

We tested the feasibility of the proposed detection method by analyzing how the RSSI values of packets changed with varying physical distances.

4.1. Datasets

We used two Probee Zu10 modules based on the Ze10 hardware of Sena Technologies to measure RSSI values for ZigBee packets. RSSI values were measured by a command provided in the ZigBee module.

The basic process of measuring the statistical properties of packets is as follows. First, we fixed the position of the first device with the ZigBee module and then placed the

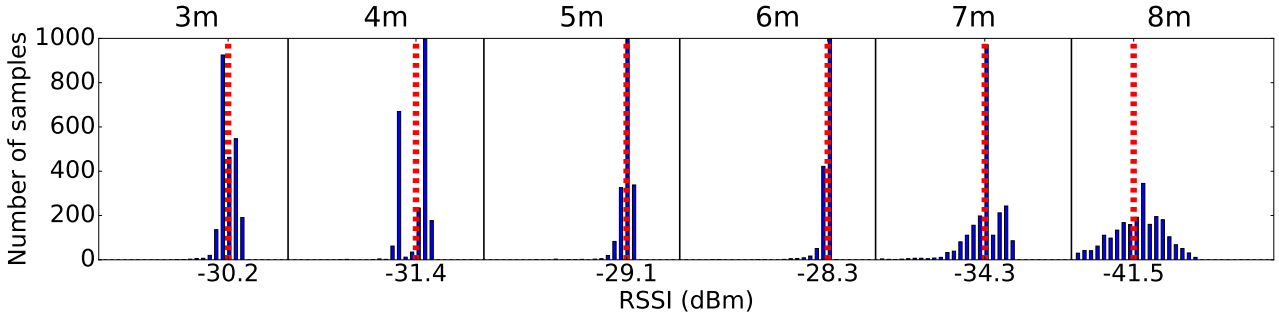


Figure 3. Histograms and mean (red dotted lines) of RSSI measured from 3, 4, 5, 6, 7, and 8 meters (from the left to rightward).

second device with the same ZigBee module approximately m meters away from the first device with $m = 3, 4, 5, 6, 7$ and 8. After placing those devices, we started sending a packet with 70 bytes from the first device to the second device and recorded RSSI value for the received packet. We repeated this procedure 2,300 times every 1.5 seconds, respectively, for all m meters. That is, we collected 13,800 ZigBee packets in total.

This data collection process was performed at a university laboratory. This laboratory consists of a single room that could be interfered with a lot of WiFi signals (sharing the same 2.4GHz bandwidth range with ZigBee) generated by other wireless devices inside and/or around the room. Arguably, this environment could represent the worst case scenario in real-world home environments. It was our intention to show that the proposed method can facilitate accurate detection in such noisy environments.

4.2. Results

Figure 3 shows the distributions of measured RSSI values. Unlike our expectations, the strength of the received signal was at the maximum (-28.3dBm) when the distance to the device was 6 meters. This implies that the measurement of RSSI alone might not be sufficient to distinguish ZigBee devices within 6 meters. Therefore, we need to consider additional features such as RTT and LQI to improve the accuracy of the proposed detection method.

Hopefully, the distributions of measured RSSI values at 7 and 8 meters are far from the other distributions; they have not only significantly smaller mean signal strengths (-34.3dBm and -41.5dBm) but also larger standard deviations than the other distributions. Therefore, if we collect a time series of RSSI data, we might distinguish devices that are located at more than four meters.

5. Key challenges

To deploy the proposed framework in the real-world. we need to address the following four key challenges.

5.1. Unreliable network characteristics

As Section 4 demonstrates the distributions of RSSI, the measured network characteristics may not be sufficiently reliable. Also, it could be difficult to distinguish the locations of devices in close proximity (e.g., within 3 meters). Therefore, we need to find several network features that are also reliable, and are significantly affected by varying physical distances.

5.2. Modification of physical characteristics

In this paper, we assumed that devices' physical characteristics will remain unchanged. However, several physical characteristics such as RSSI and RTT can often be changed (and even controllable) in practice. Therefore, a sophisticated attacker might try to boost the signal strength of her device by using an amplifier to mimic victim device's network characteristics. However, we note that it will be extremely difficult for attackers to mimic a victim's physical characteristics without the knowledge about the victim (e.g., the physical distance between the verifier and victim device). As part of future work, we will try to demonstrate that the proposed framework is still robust enough against such attack scenarios.

5.3. Initial setup for generating fingerprints

To use the proposed framework, we initially need to analyze a device's network characteristics to generate the device's fingerprint (or profile) before using the device. This may incur a usability penalty because the initial setup process should be repeated whenever a new device connection is established. Moreover, this setup process could be compromised in theory if an attacker could poison the training data at the initial setup process for a new device. Therefore, it is integral to complete the initial setup process within a short time interval.

5.4. Power consumption

The main idea of the proposed system is to continuously monitor devices' network characteristics in real time

by gathering their physical signals and analyzing them. Inherently, it requires more power consumption that may not be acceptable for devices with low battery capacity. Therefore, we need to develop a monitoring process, e.g., with a small number of signal samples, to effectively reduce power consumption on the proposed framework.

6. Related work

This section surveys a number of previous work for spoofing detection method using RSSI.

Misra et al. [10] proposed a method to detect spoofing attacks in a wireless sensor network using WiFi signals collected by multiple monitoring Access Points (APs). This study also suggested a constant threshold to distinguish devices at different locations. The signal strength difference at the same location does not exceed 2.5dBm on average. However, those results were just analyzed by using the MATLAB simulation without conducting experiments in a physical environment.

Chen et al. [3] proposed a method for identifying the locations of attackers with four monitoring APs. They developed the method using K-means classification assuming that devcies' RSSI values follow a Gaussian distribution. They attained a detection accuracy of 95% (with 5% false positive rate) in WiFi and ZigBee network environments. Jokar et al. [5] developed a similar technique based on the spatial correlation property of RSSI. They achieved detection accuracies of 94.75% (with 0.56% false positive rate) and 99% (with no false positive rate), respectively, using one and four monitoring APs.

Sheng et al. [4] used a Gaussian mixture model rather than a single Gaussian distribution. Since modern RF communication chipsets and drivers use a diversity antenna to increase the reliability and stability of network connectivity, RSSI values exhibit multimodal distributions. Based on this observation, they developed a spoofing detection achieving a detection accuracy of 97.8% (with 3% false positive rate).

Those previous studies define various probabilistic models to better understand RSSI signals. However, probabilistic models generally require large amounts of labeled training data. This weakness discourages users to use such techniques. Unlike previous methods that were heuristically designed with RSSI alone, we propose a generic framework based on the concept of a similarity to measure the physical difference between subsequent packet sequences, which can be naturally extended to use multiple network features with a small number of samples.

7. Conclusion

In this paper, we introduced a novel approach to overcome the limitations of MAC-based access control schemes that can be easily bypassed with spoofing techniques. We developed a generic framework to detect suspicious network devices with their inherent physical characteristics (e.g., RSSI) that are hard to imitate. To show the feasibility of the proposed framework, we analyzed how the RSSI values are affected with varying physical distances. For this experiment, we collected a total of 13,800 packets from real ZigBee devices, and demonstrated that the RSSI values measured from devices 7 and 8 meters away from the verifying device (that runs our detection mechanism) are significantly different to the RSSI values measured from devices that were within 6 meters.

The experiments we conducted so far presented promising preliminary results. We plan to extend this work by fully implementing the proposed framework, and performing more thorough feasibility and performance evaluations with several more physical characteristics (e.g., RTT and LQI).

Acknowledgments

This work was supported by the NRF (National Research Foundation of Korea) grant funded by the Korea government (No. 2014R1A1A1003707), the IITP (Institute for Information & communications Technology Promotion) grant funded by the MSIP (Ministry of Science, ICT and Future Planning) (No.R-20160222-002755), and the KISA (Korea Internet & Security Agency) grant funded by the MSIP (H2101-16-1001). This research was also supported by the MSIP under the ICT R&D program (R0166-15-1041) and the ITRC (Information Technology Research Center) support program (IITP-2016-R0992-16-1006) supervised by the IITP.

Authors would like to thank all the anonymous reviewers for their valuable feedback.

References

[1] Y.-X. Lim, T. Yer, J. Levine, and H. L. Owen, "Wireless intrusion detection and response," in *Proceedings of Information Assurance Workshop*, 2003.

[2] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using singalprints," in *Proceedings of ACM Workshop on Wireless Security*, 2006.

[3] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *Proceedings of 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2007.

[4] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 mac layer spoofing using received signal strength," in *Proceedings of 27th IEEE Conference on Computer Communications*, 2008.

[5] P. Jokar, N. Arianpoo, and V. C. Leung, "Spoofing detection in ieee 802.15. 4 networks based on received signal strength," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2648–2660, 2013.

[6] J. Wright, "Detecting wireless lan mac address spoofing." White paper, 2003.

[7] J. Ogle and M. P. Talbert, "Hotel network security: a study of computer networks in us hotels," tech. rep., Cornell University School of Hotel Administration, 2008.

[8] M. S. Ahmad, "WPA Too!," in *DEFCON*, 2010.

[9] M. Müller, *Information Retrieval for Music and Motion*, ch. Dynamic Time Warping, pp. 69–84. Springer Berlin Heidelberg, 2007.

[10] S. Misra, A. Ghosh, P. Sagar, M. S. Obaidat, *et al.*, "Detection of identity-based attacks in wireless sensor networks using signalprints," in *Proceedings of IEEE International Conference on Green Computing and Communications*, 2010.