

Copyright © 2010 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

Senthilkumar Chinnappa Gounder Periaswamy, Dale R. Thompson, and Jia Di,
"Fingerprinting RFID tags," *IEEE Transactions on Dependable and Secure Computing*,
to appear

Fingerprinting RFID Tags

Senthilkumar Chinnappa Gounder Periaswamy, Dale R. Thompson, *Senior Member, IEEE* and
Jia Di, *Member, IEEE*

Abstract— Radio frequency identification (RFID) tags are low-cost devices that are used to uniquely identify the objects to which they are attached. Due to the low cost and small size that are driving the technology, a tag has limited computational capabilities and resources. These limitations constrain the use of conventional encryption algorithms and security protocols to prevent cloning and counterfeiting of an RFID tag. Therefore, we propose to create an electronic fingerprint of a tag based upon the physical attributes of the tag. We have fingerprinted RFID tags based upon their minimum power responses measured at multiple frequencies. The fingerprint can be used effectively to identify the tags in the future with high probability and to detect counterfeit tags. This mechanism does not increase the cost of the tag and can be applied to any existing tag because it is independent of the computational capabilities and resources of the RFID tag.

Index Terms— Authentication, pervasive computing, unauthorized access, wireless sensor networks.

1 INTRODUCTION

RADIO frequency identification (RFID) tags are low-cost devices that are used to uniquely identify the objects to which they are attached. The identifier of the tag can be easily read from the tag and programmed into another tag because most tags do not have any built-in feature to prevent cloning or counterfeiting. Due to the low cost and small size that are driving the technology, a tag has limited computational capabilities and resources. This limitation makes the implementation of conventional cryptographic algorithms and security protocols inefficient.

Even if either a conventional or a lightweight cryptographic-based protocol is implemented, an improper implementation and the use of non-standardized algorithms have led to a determined adversary with sufficient resources breaking it to find the underlying data. A different RFID tag can then be programmed to create a clone, or an emulation device can be programmed to act like the original tag. Once a successful clone has been created, the authentication system will not be able to detect the clone because it uses application-layer data instead of one or more unique physical attributes of the tag. In other words, security in RFID tags is currently a function of what it knows rather than what it is.

The objective of this work is to fingerprint an RFID tag based upon the minimum power response of the tag measured at multiple frequencies. The fingerprint can be used to identify the tag in the future with high probability and to detect counterfeit tags. This work has the potential

to create an electronic fingerprinting system that can effectively prevent anti-counterfeiting in high-value items because security will also be a function of what the tag is. This method can also be used on low-cost tags along with other form of security protocols for identification and authentication because this method is independent of the computational capabilities and resources of the RFID tag. It can be applied as an additional layer of security to any existing tag because it does not require or make any modification to the tag and this does not increase the cost of RFID tags.

We have organized the rest of the paper as follows: Section 2 covers the basics of RFID technology and an overview of the techniques that are currently used to prevent counterfeiting of RFID tags. It also discusses work that is related to the fingerprinting of electronic devices. Section 3 gives the details of the experiment conducted to measure the minimum power response of tags at each frequency. In Section 4, the data from the experiments are analyzed to determine whether minimum power levels are significantly different for each frequency and for different tags. Section 5 summarizes the results and discusses the effects of fingerprinting on the security of RFID tags especially anti-counterfeiting. Section 6 contains proposed future work that can be performed to improve this mechanism.

2 BACKGROUND

2.1 Radio Frequency Identification

Radio frequency identification (RFID) is a technology, which uses radio signals to automatically and uniquely identify objects. It does not require line of sight to work like the barcodes and has a read rate of several hundred per second. EPCglobal Inc. leads the development of the standard for one form of RFID, the Electronic Product Code (EPC) [1], which is the main form of RFID used for retail supply chain.

The system consists of an RFID tag and an RFID read-

- Senthilkumar Chinnappa Gounder Periaswamy is with the Computer Science and Computer Engineering Department, University of Arkansas, Fayetteville, AR 72701. E-mail: schinna@uark.edu.
- Dale.R. Thompson is with the Computer Science and Computer Engineering Department, University of Arkansas, Fayetteville, AR 72701. E-mail: d.r.thompson@ieee.org.
- Jia Di is with the Computer Science and Computer Engineering Department, University of Arkansas, Fayetteville, AR 72701. E-mail: jdi@uark.edu.

er. The reader sends and receives radio frequency signals to communicate with the tag. The RFID tag, which consists of a microchip connected to a radio antenna, modulates the signal it receives depending upon its resident data to communicate back to the reader. The tag sends back data to the reader from its memory, which is usually the identifier of the tag such as the EPC.

An RFID system works in a wide range of frequencies depending on their applications and regulations [2]. They can be broadly classified into Low Frequency (LF) (30 KHz to 300 KHz), High Frequency (HF) (3 MHz to 30 MHz) and Ultra-High Frequency (UHF) (868 MHz – 928 MHz). They are also regulated by the operation guidelines set by various countries. The UHF (902 MHz – 928 MHz) version of RFID is used in the United States for the supply chain due to its relatively long nominal reading distance of nine to twelve feet.

RFID tags can be classified as passive, semi-passive and active depending upon their power source. Passive tags do not have a built in power source and are powered by either induction or electromagnetic radio frequency (RF) signals of the reader. They have limited computational capabilities and resources. They have a lower read range (operating distance) when compared to tags that have their own power source. In spite of these limitations, they are common due to their low cost, size and longer life. Semi-passive tags have their own power source, which are activated when they are interrogated by a reader. Active tags have their own power source and remain active all the time. The semi-passive and active tags have more computational capabilities and resources and they have longer read ranges than the passive tags. However, the built-in power source makes them more bulky and expensive which restricts these tags to high-end applications.

The compelling features, dropping costs and standardizations have enabled the use of RFID in a wide range of applications including manufacturing, supply chain, retailing, payment and administrative systems. In spite of its wide deployment, security and privacy issues have to be addressed to make it a dependable technology. Common security solutions cannot be applied to this technology because of the limited computational capabilities and resources of the RFID tags. The low-cost approach of the system that is driving the technology makes it resource constraint.

2.2 RFID Tags for Anti-counterfeiting

It has been proposed to use RFID tags to prevent counterfeiting of products because each tag is considered to be unique based on its serial number. However, many low-cost passive RFID tags have no explicit anti-counterfeiting features [3][4]. An attacker can simply read the serial number from a target tag (termed skimming) and program it to another tag or emulate the target tag in another type of wireless device [3]. An undergraduate student from University of Waterloo constructed a device that scanned signals from RFID-based entry cards and emulated them to act like the scanned card [5].

According to [3], there is no need for having an anti-

counterfeiting mechanism in the RFID tag if the database generates an alert when a duplicate entry is created by a tag in the system. Such a system-level anti-counterfeiting mechanism is important. However, this system only works when both the original and cloned tags are present in the system at the same time. This also requires a consistent and centralized database. In the case of finding a duplicate entry, there will also be issues on distinguishing between the original and the cloned tag.

A secret proprietary algorithm was used to provide authentication in the MIFARE classic cards. These cards have HF tags and are used in access control systems throughout the world. Exploiting weakness in the stream cipher that was used as random number generator, researchers in [6] were able to recover the key stream. With the recovered key stream, they were able to read and modify certain memory blocks. Although the MIFARE classic cards are HF cards, the attacks demonstrate that a weakness in a cryptographic algorithm can be exploited if they are not rigorously tested.

Power analysis was used to extract passwords from a passive tag in [7]. Power and electromagnetic (EM) attacks were also demonstrated in RFID prototype devices that had hardware and software implemented AES cryptography [8]. This attack needed less than one thousand EM traces to break the algorithm. These attacks demonstrate the need for any cryptographic implementation to be resistant against side-channel attacks. Techniques to mitigate side-channel attacks usually increase the cost and decrease the performance [8].

Several conventional cryptographic-based models have been proposed to prevent unauthorized reading or cloning of tags [9][10][11][12][13][14][15]. The security of these protocols is based on application and communication layers of the RFID tag and they tend to ignore the physical layer. Although they improve security and provide resistance to cloning, we have seen the challenges that need to be faced during their implementation in the previous two paragraphs. Even after a proper implementation, they face challenges from reverse-engineering [17], side-channel [18] and relay attacks [19]. After creation of a duplicate tag with the same data, there is no mechanism to differentiate the original and the duplicate.

We propose a model that fingerprints a passive RFID tag based on the physical characteristics that are difficult to clone. This model does not depend on the resources of the RFID tag and does not require or make any modification to the tag. A passive RFID tag harvests its power from the radio frequency created by the reader. Therefore, we fingerprint an RFID tag based on its minimum power response at multiple frequencies (MPRMF), which is the minimum power required to activate an RFID tag at multiple frequencies. This power is a function of both frequency and manufacturing differences in the tag. We experimentally prove that the MPRMF is unique for each tag and is significantly different for same-model tags.

2.3 Related Work

The work in [20] investigates how RFID tags can be made unclonable by linking it to a physical unclonable function

(PUF). The proposed PUF acts as a secure memory for storing secret keys. The responses of a PUF are not exactly the same each time, although error-correcting codes can be used to create such responses. PUFs are physical structures that respond to challenges that are easy to measure but are hard to predict. In addition, PUFs are difficult to copy or clone. They are embedded in the tag such that any attempt to remove them will either destroy them or modify the values of the responses to challenges. The PUF only communicates with the chip of the tag and is inaccessible to the reader.

The tag goes through an enrollment phase in which a trusted person subjects the PUF to a challenge and possibly some auxiliary data and receives a response. Then, the response, which is like a fingerprint, is either stored in a database or could be printed or stored in the tag. If the fingerprint is stored in the tag for offline verification, the information is signed with the private key of a public/private key algorithm by a trusted authority. Multiple challenges and responses may be measured during enrollment. In the verification phase, the tag first identifies itself with its serial number. Based on the PUF's identity, the verifier sends a random challenge from its database or stored information from the tag along with the corresponding auxiliary data. If the observed response of the PUF matches the enrolled fingerprint from the database or matches the signed fingerprint on the tag, then the tag is deemed authentic; otherwise, the tag is considered a clone.

An intrusion detection approach for Bluetooth networks that uses radio frequency fingerprinting for profiling, Hotelling's T^2 statistics for classification and a decision filter for detecting rogue devices is proposed in [21]. They use the transient portion of the transceiver's signal to identify a Bluetooth transceiver. The transient is the turn-on portion of the signal received from the transceiver. The transient response is dependent upon the hardware characteristics of the transceiver, which is difficult to clone. Fifteen unique features are extracted from the amplitude, frequency and phase components of the transient to create what they call a transceiverprint. The transceiverprint is analogous to the term fingerprint in this work.

In [21], a subset of fingerprints obtained from the captured signals is selected and then enrolled using k-means clustering [22]. In other words, multiple fingerprints are created for the same device and then the outliers are discarded. Then, k-means clustering is used to create fingerprint that represents the measurements. The centroid and covariance matrix created from the subset represents the fingerprint of the transceiver. After creating the transceiver fingerprints, the Hotelling's T^2 statistics is used to determine the similarity between an observed fingerprint and the enrolled fingerprint of a Bluetooth receiver with a given address. The Hotelling's T^2 distance is an extension of the Student's-t statistic to multiple variables that uses a vector of deviations between the observations and the enrolled mean and the enrolled covariance matrix [22]. Since the wireless environment has noise and interference, a decision based upon a single fingerprint may result in an error. To mitigate these errors, a set of fin-

gerprints are independently classified and a decision filter is applied to decide the output based on the multiple observed fingerprints. The threshold of the decision filter is established based on the requirement of the application. The work in [21] on correctly identifying a previously enrolled Bluetooth transceiver demonstrates an average detection rate of ninety seven percent.

The feasibility of radio fingerprinting wireless sensor nodes and analyzing the implications of radio fingerprinting on the security of sensor networking protocols is discussed in [23]. Similar to [21] they use the transient portion of the signal to fingerprint the radio. Five unique features that define a fingerprint are extracted from the amplitude of the transient and the mean and covariance matrix is used to represent each fingerprint. They demonstrate a detection rate of up to seventy percent. It is hypothesized that only using the amplitude is the reason the detection rate is relatively low.

They propose that radio fingerprinting can be beneficial to the security of sensor networks [23]. The fingerprint of nodes can be used in combination with public or symmetric key encryption for message authentication. Fingerprinting of nodes will protect the system against Sybil attacks in which several identities are assigned to the same node and cloning attacks in which the same identity is assigned to multiple nodes. They can also improve security by providing relay and replay protection of signals. On the other hand, fingerprinting can be used against the system by an adversary when sensor anonymity is present or required by the system.

An Ethernet card was remotely fingerprinted by exploiting small, microscopic deviations in the hardware that manifest themselves as differences in clock skews in [24]. This technique does not make any modifications to device and can be performed even without the device's known cooperation. They measured the clock skew by monitoring the difference in TCP timestamps, periodic activities or ICMP Timestamp reply messages. They used a Fourier transform to infer clock skew from the observed times. Their clock skew estimation remains independent of distance, access technology and topology and they successfully demonstrated it over international networks.

According to [25], radio frequency fingerprinting is used on cellular networks with a technology developed by Corsair Communications, Inc. They use several parameters to characterize a fingerprint of a cellular phone. The parameters and characterization of the features remains proprietary. The company has successfully deployed this system known as PhonePrint in base stations of cellular operators. Corsair Communication's parent company TRW Inc. had developed similar systems for the military, which is used to track enemy troop's radio [25][26].

The steady-state portion of the signal was used to identify and track 10 Mbps wired Ethernet cards in [27]. An optimal detector, the matched filter, was used to create signal profiles of the Ethernet cards. They devised variations on the matched filter method depending upon on the device signals to improve results. They used a collection of signals taken over a period of time to developed

adaptive methods that accurately track fluctuations in a signal due to device aging, voltage variations, and temperature changes.

In [28], they proposed to use the initialization state of SRAM's in RFID tags to create a physical fingerprint. They used experimental data from virtual tags to show that a SRAM can be used to identify tags. A simple Hamming distance-based matching was used to observe the identifying qualities.

Different models of high frequency (HF) RFID tags were distinguished using the differences of the waveform in [29] and [30]. HF tags use inductive coupling for communication while the main form of UHF tags communicate in the radiative field. In HF RFID, changes in the reader antenna induce change in the tag antenna and vice versa. This is further explained by the work done in [29] where they used changes in the *reader* antenna to fingerprint the tag. The changes in the reader antenna were more pronounced than the changes in the tag because of inductive coupling. In contrast, there is no inductive coupling in UHF RFID because of the longer transmission path.

The fingerprinting mechanism proposed in this paper is based on variations that are caused due to the manufacturing process of the RFID tags. These variations are difficult to reproduce, predict or control because this type of manufacturing is geared towards mass-producing the tags at a lower cost.

3 EXPERIMENT

The minimum power required for a tag to respond at multiple frequencies was measured using a Voyantic Tagformance Lite system [31] in an anechoic chamber, which was designed for determining the best placement of tags on items and is shown in Fig. 1. The minimum power response was measured using a bottom-up algorithm, which repeatedly sent signals from the reader to the tag starting from -20 dBm incrementing it by 0.01 dBm every time until a response from the tag was detected.

An EPCglobal class-1 generation-2 tag provided by Voyantic for the Tagformance system was used for calibration. The calibration tag was kept in a controlled environment. Before each experiment, the system was calibrated using the calibration tag. The responses of the calibration tag at a distance of one meter in frequencies ranging from 860 MHz to 960 MHz in increments of 1 MHz were preloaded to the system. The Tagformance system calibrated itself by referencing the current measurement with the preconfigured value.

The tags were horizontally polarized along with the antenna during all the measurements. A fixture made of styrofoam was used in the chamber that made sure that all the tags were mounted at same distance and position from the reader antenna during all the measurements. The antenna was mounted to a fixture made of PVC and remained in the same position during all the measurements. The minimum power responses at all the frequencies were measured for hundred passive RFID tags. The minimum power responses were measured six times for a

total of 600 measurements. The time to measure the minimum power response at all the frequencies for one tag was approximately 15 minutes. Fifty of the hundred tags were from a major manufacturer labeled as Manufacturer-1 and they were taken off one roll of tags. Therefore, it is likely that they were manufactured at approximately the same time. The other fifty tags were from another major manufacturer labeled as Manufacturer-2 and they were also taken from one roll. The tags are inexpensive and entry level RFID tags from both the manufacturers.

The minimum power response was measured at frequencies ranging from 860 MHz to 960 MHz in increments of 1 MHz to match the frequencies of the calibration tag. The Tagformance system used dBm as the unit for the power. The values were converted to milliwatts

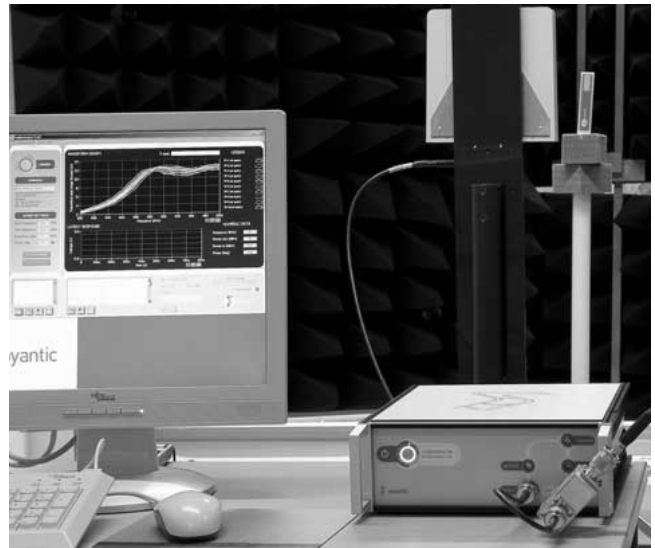


Fig. 1. Voyantic Tagformance Lite.

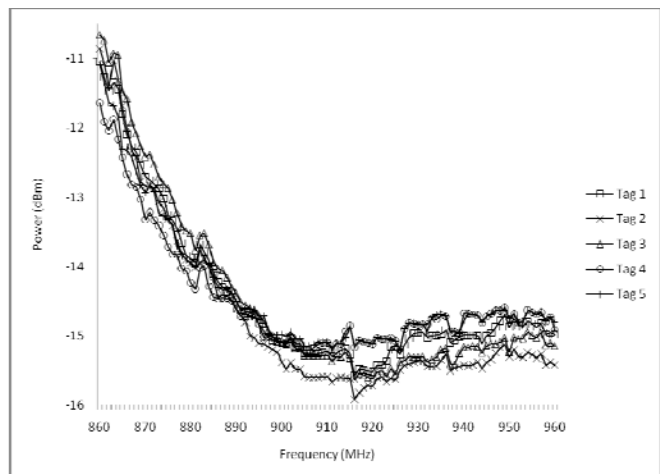


Fig. 2. Minimum power responses of five Manufacturer-1 tags.

for all calculations. During each experiment, the minimum power response measurement was repeated six times for each tag. The Tagformance system measured the minimum power response from 860 MHz to 960 MHz and then started again from 860 MHz for each repetition. The minimum power response curves of five different Manufacturer-1 tags are shown in Fig. 2.

4 ANALYSIS AND RESULTS

The minimum power response at each frequency was considered as a feature of the fingerprint. Each fingerprint of the tag was considered as an instance. The data was analyzed for two different populations of Manufacturer-1 tags and Manufacturer-2 tags. It was also analyzed as a single population with all the tags.

Two-way analysis of variance is a procedure for testing the equality (or inequality) of means of several groups [32]. It analyzes the “effect” when two factors in the experiment change. It can also analyze the interaction between the factors.

Two-way analysis of variance was applied to test the hypothesis that the minimum power responses of tags are affected by frequency and different tags. That is, frequency significantly affects the minimum power responses and the physical characteristic of each tag significantly affects the minimum power response measured at multiple frequencies (MPRMF).

We test the hypothesis at the 1 percent level of significance. The null hypothesis is that there are no differences in the means of the minimum power responses at different frequencies, there are no differences in the means of the minimum power responses for different tags and there is no significant interaction between the two factors. In other words, the means of the minimum power responses at different frequencies are equivalent and the means of the minimum power responses for different tags are equivalent.

Analysis of variance was applied to the experiment of measuring minimum power responses of hundred tags (fifty Manufacturer-1 and fifty Manufacturer-2 tags) for all frequencies and is shown in Table 1. Table 1 also shows the P-values for the test statistics, which is the smallest significance level at which the null hypothesis would be rejected. The F ratio is 2.28×10^4 for the effect of tags on the minimum power responses. Since $F_{0.01, 99, 50500} = 1.36$, which is less than the F ratio, we conclude that the main effect of tags is significant. That is, tags have a significant effect on the minimum power responses. The F ratio is 2.53×10^4 for the effect of frequency on the minimum power response. Since $F_{0.01, 100, 50500} = 1.35$, we conclude that the main effect of frequency is significant. That is, the frequency has a significant effect on the minimum power response. Furthermore, the F ratio is 3.41×10^2 for the interaction between each tag and frequency on the minimum power responses. Since $F_{0.01, 9900, 50500} = 1.03$, we conclude that there is significant interaction between each tag and frequency. Therefore, we reject the null hypothesis and conclude that both the particular tag and the frequency have a significant effect on the minimum power responses. In addition, there is significant interaction between the particular tag and frequency.

Analysis of variance was separately applied to the observed minimum power responses of both types of tags to determine the significance of a particular tag and frequency to one type of tag. Recall that the fifty Manufacturer-1 tags were taken from the same roll of tags and were therefore manufactured at approximately the same time. Therefore, it is likely that any significant difference

TABLE 1
ANALYSIS OF VARIANCE FOR MINIMUM POWER RESPONSES OF MANUFACTURER-1 AND MANUFACTURER-2 TAGS

Source of Variation	Sum of Squares	Degree of Freedom	Mean Square	F ₀	P-value
Tag	1.22	99	1.2×10^{-2}	2.28×10^4	~0
Frequency	1.37	100	1.3×10^{-2}	2.53×10^4	~0
Interaction	1.83	9900	1.8×10^{-4}	3.41×10^2	~0
Error	2.73×10^{-2}	50500	5.4×10^{-7}		
Total	4.46	60599			

TABLE 2
ANALYSIS OF VARIANCE FOR MINIMUM POWER RESPONSES OF MANUFACTURER-1 TAGS

Source of Variation	Sum of Squares	Degree of Freedom	Mean Square	F ₀	P-Value
Tag	8.13×10^{-2}	49	1.65×10^{-3}	1.68×10^3	~0
Frequency	2.97	100	2.97×10^{-2}	3.02×10^4	~0
Interaction	1.57×10^{-1}	4900	3.22×10^{-5}	3.27×10^1	~0
Error	2.48×10^{-2}	25250	9.84×10^{-7}		
Total	3.23	30299			

TABLE 3
ANALYSIS OF VARIANCE FOR MINIMUM POWER RESPONSES OF MANUFACTURER-2 TAGS

Source of Variation	Sum of Squares	Degree of Freedom	Mean Square	F ₀	P-Value
Tag	2.99×10^{-2}	49	6.12×10^{-4}	6.08×10^3	~0
Frequency	6.36×10^{-2}	100	6.36×10^{-4}	6.32×10^3	~0
Interaction	1.27×10^{-2}	4900	2.61×10^{-6}	2.59×10^1	~0
Error	2.53×10^{-3}	25250	1.01×10^{-7}		
Total	1.08×10^{-1}	30299			

in minimum power response is primarily due to manufacturing variances.

Analysis of variance for the minimum power responses of the fifty Manufacturer-1 tags is shown in Table 2. The F ratio is 1.68×10^3 for the effect of tags on the minimum power responses. Since $F_{0.01, 49, 25250} = 1.52$, which is less than the F ratio, we conclude that the main effect of tags is significant. That is, Manufacturer-1 tags have a significant effect on the minimum power responses. The F ratio is 3.02×10^4 for the effect of frequency on the minimum power response. Since $F_{0.01, 100, 25250} = 1.35$, we conclude that the main effect of frequency is significant. That is, the frequencies of Manufacturer-1 tags have a significant effect on the minimum power response. Furthermore, the F ratio is 3.27×10^1 for the interaction between each tag and frequency on the minimum power responses. Since $F_{0.01, 4900, 25250} = 1.05$, we conclude that there

is significant interaction between each tag and frequency.

Analysis of variance for the minimum power responses of the fifty Manufacturer-2 tags is shown in Table 3. The F ratio is 6.08×10^3 for the effect of tags on the minimum power responses. Since $F_{0.01, 49, 25250} = 1.52$, which is less than the F ratio, we conclude that the main effect of tags is significant. The F ratio is 6.32×10^4 for the effect of frequency on the minimum power response. Since $F_{0.01, 100, 25250} = 1.35$, we conclude that the main effect of frequency is significant. Furthermore, the F ratio is 2.59×10^1 for the interaction between each tag and frequency on the minimum power responses. Since $F_{0.01, 4990, 25250} = 1.05$, we conclude that there is significant interaction between each tag and frequency.

K Nearest Neighbor algorithm was used to classify the data. K Nearest neighbor is an instance-based classifier that classifies the current instance to the closest enrolled group by using a distance metric. It considers each instance as a vector and uses the distances between the vectors to find the closest neighbor. This classifier works well when there is little or no prior knowledge about the distribution of data [33].

We used stratified ten-fold cross validation on the classifier to validate our results. In ten-fold cross validation, the data is divided into ten parts. Of the ten parts, the classifier is trained on nine parts and the tenth part is used for validation. This is repeated ten times with each one of ten parts retained for validation exactly one time. The ten individual results are then combined to produce the result. This validation method uses all of the data for both training and validation by repeated sub-sampling and works well when the data available is limited.

We use True Positive rate, False Positive rate and Area under the Receiver Operating Characteristic curve (ROC AUC) as the metrics for the K Nearest neighbor classifier with ten-fold cross validation on the data. True Positive is an instance where a measurement of a tag was positively associated to a correct tag. False Positive is an instance where a measurement was positively associated to an incorrect tag. A higher rate of True Positive and a lower rate of False Positive denote better performance. An ROC curve is a plot of fraction of the True Positives against the fraction of False Positives. The area under the ROC curve represents the probability of a randomly chosen positive matching instance being ranked higher than a randomly chosen incorrect instance. This metric measures the ability of the system to distinguish between a correct and incorrect matching of instances. Therefore a higher ROC AUC denotes better system.

The average True Positive rate for the Manufacturer-1 tags was 94.4% and the False Positive rate was 0.1% with an ROC AUC of 0.999. This denotes that on average 94.4% of the instances that were matched positively to the correct tag. An average of 0.1% instances were positively matched to an instance that was incorrect. The probability of a correctly matching instance getting ranked higher than an incorrectly matching instance is 0.999. The average True Positive rate for the Manufacturer-2 tags was 90.7% and the False Positive rate was 0.2% with an ROC AUC of 0.997.

Finally, the fifty tags of Manufacturer-1 and the fifty tags of Manufacturer-2 were analyzed as a single population of 100. The average True Positive rate for the whole population of Manufacturer-1 and Manufacturer-2 tags is 90.5% and the False Positive rate is 0.1% with an ROC AUC of 0.999.

5 CONCLUSIONS

The results show that the set of minimum power responses at multiple frequencies can be used as a feature to fingerprint a passive RFID. This holds true for not only different-model tags but also for same-model tags that were manufactured using the same design and that were manufactured at approximately the same time.

Using the physical attributes of a tag to create a unique fingerprint as proposed in this paper will provide reliable authentication for the original tag and will detect a counterfeit tag. This method, when combined with other application and communication layer security protocols, will provide robust security for RFID tags. There will not be a need to increase the cost of RFID tags and this method can be applied to any existing tag because it is independent of the computational capabilities and resources of the RFID tag. Fingerprinting will also prevent emulation and relay attacks on RFID tags because mimicking the fingerprint, such as the minimum power response, is practically infeasible. In the event of a duplicate tag arising in the system, the fingerprint can be used to differentiate the original tag from the counterfeit tag.

6 FUTURE WORK

In this paper, we analyzed the use of the MPRMF to fingerprint a passive RFID tag. A fingerprint based on more attributes may give a better fingerprint and we are actively looking for attributes that are unique to the tag and not the reader.

The data can also be analyzed using other statistical methods that suit the data to see if they can improve the performance of the minimum power response. The various physical and environmental conditions that affect the fingerprint of the tag should be studied by measuring the tags using multiple readers and in different environments. In addition, the durability of the fingerprint over time needs to be investigated. The fingerprints need to be measured periodically to determine if the fingerprint changes over time. The components in the tag that cause this variability in these attributes should also be found which would give a better understanding of the fingerprinting system.

Finally, the measurement process can be integrated to RFID reader hardware to reduce cost and increase availability.

ACKNOWLEDGMENT

This work was supported by a grant from National Science Foundation CISE/CNS and the Cyber Trust area support under contract CNS-0716578. The authors wish to thank Bill Hardgrave, Justin Patton, and David Crom-

hout from the University of Arkansas RFID Research Center.

REFERENCES

- [1] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz, ver. 1.1.0, EPCglobal Inc., Dec. 17, 2005. Available: <http://www.epcglobalinc.org>.
- [2] R. Chaudhry, D. R. Thompson, and C. Thompson, *RFID technical tutorial and threat modeling*, ver.1.0, Department of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, Arkansas, Dec. 8 2005. Available: <http://comp.uark.edu/~drt>.
- [3] A. Juels, "RFID security and privacy: a research survey," *Selected Areas in Communications, IEEE Journal on*, vol. 24, pp. 381-394, 2006.
- [4] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-Passports," *Proc. Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm '05)*, 2005.
- [5] J. Westhues, "Hacking the prox card," in *RFID: Applications, Security, and Privacy*, S. Garfinkel and B. Rosenberg, Eds. Reading, MA: Addison-Wesley, 2005, pp. 291-300.
- [6] G. D. Koning Gans, J. Hoepman and F. D. Garcia, "A practical attack on the MIFARE classic," in *CARDIS '08: Proceedings of the 8th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications*, 2008, pp. 267-282.
- [7] Y. Oren and A. Shamir, "Remote Password Extraction from RFID Tags," *Computers, IEEE Transactions on*, vol. 56, pp. 1292-1296, 2007.
- [8] M. Hutter, S. Mangard and M. Feldhofer, "Power and EM attacks on passive 13.56 MHz RFID devices," in *CHES '07: Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems*, 2007, pp. 320-333.
- [9] A. Juels, "Strengthening EPC tags against cloning," in *WiSe '05: Proceedings of the 4th ACM Workshop on Wireless Security*, 2005, pp. 67-76.
- [10] D. N. Duc, J. Park, H. Lee, and K. Kim, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and cloning," *Proc. 2006 Symp. Cryptography and Information Security*, 2006.
- [11] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *First International Conference on Security and Privacy for Emerging Areas in Communication Networks -- SecureComm 2005*, Athens, Greece, September 2005.
- [12] S. S. Kumar and C. Paar, "Are Standards Compliant Elliptic Curve Cryptosystems Feasible on RFID?" *Proc. Workshop RFID Security*, July 2006.
- [13] Yong Ki Lee, L. Batina and I. Verbauwhede, "EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol," *RFID, 2008 IEEE International Conference on*, pp. 97-104, 2008.
- [14] M. Burmester and B. de Medeiros, "The security of EPC Gen2 compliant RFID protocols," in *Proceeding of the International Conference on Applied Cryptography and Network Security, ACNS 2008; Lecture Notes in Computer Science*, 2008.
- [15] M. Burmester, B. de Medeiros and R. Motta, "Robust, anonymous RFID authentication with constant key-lookup," in *ASIACCS '08: Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, 2008, pp. 283-291.
- [16] G. Avoine and P. Oechslin, "RFID traceability: A multilayer problem," in *Financial Cryptography -- FC'05; Lecture Notes in Computer Science*, 2005, pp. 125-140.
- [17] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," in *USENIX Security Symposium*, 2005, pp. 1-16.
- [18] D. Carluccio, K. Lemke, and C. Paar, "Electromagnetic side channel analysis of a contactless smart card: first results," in *ECRYPT Workshop on RFID and Lightweight Crypto*, Graz, Austria, July 2005, pp. 44-51.
- [19] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard systems," in *First International Conference on Security and Privacy for Emerging Areas in Communication Networks -- SecureComm 2005*, Athens, Greece, September 2005.
- [20] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Topics in Cryptology - CT-RSA 2006, the Cryptographers' Track at the RSA Conference 2006; Lecture Notes in Computer Science*, 2006.
- [21] J. Hall, M. Barbeau, and E. Kranakis, "Detection of rogue devices in bluetooth networks using radio frequency fingerprinting," in *IASTED: International Conference on Communications and Computer Networks*, Dec, 2006.
- [22] *NIST/SEMATECH e-Handbook of Statistical Methods*, National Institute of Standards and Technology, 2007. Available: <http://www.itl.nist.gov/div898/handbook>
- [23] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *Third International Conference on Security and Privacy in Communication Networks -- SecureComm 2007*, Sep.17-20, 2007.
- [24] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *Dependable and Secure Computing, IEEE Transactions on*, vol. 2, pp. 93-108, 2005.
- [25] M. J. Riezenman, "Cellular security: better, but foes still lurk," *IEEE Spectrum*, vol. 37, pp. 39-42, 2000.
- [26] R. Jones, *Most Secret war*, Hamilton, 1978.
- [27] R. Gerdes, T. E. Daniels, M. Mina, and S. Russell, "Device identification via analog signal fingerprinting: A matched filter approach," in *Proc. 13th Annual Network and Distributed System Security Symposium*, San Diego, California, Feb 2006.
- [28] D. E. Holcomb, W. P. Burleson, and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in *Proc. Conf. RFID Security*, 2007.
- [29] H. P. Romero, K. A. Remley, D. F. Williams and Chih-Ming Wang, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 57, pp. 1383-1387.
- [30] B. Danev, T. S. Heydt-Benjamin and S. Capkun, "Physical-layer identification of RFID devices," in *Proceedings of the 18th USENIX Security Symposium* USENIX'09, 2009.
- [31] Voyantic Ltd. Available: <http://www.voyantic.com>
- [32] D. C. Montgomery, *Design and analysis of experiments*, New York: John Wiley & Sons, Inc., 2001.
- [33] D. W. Aha, D. Kibler and M. K. Albert, "Instance-Based Learning Algorithms," *Machine Learning*, vol. 6, pp. 37-66, 1991.

Senthilkumar Chinnappa Gounder Periaswamy received his B.E. degree in computer science and computer engineering from Bharathiar University, Coimbatore, India in 2004. He received his M.S. in computer science from University of Arkansas, Fayetteville, AR, USA in 2007. He is a Ph.D. student at the University of Arkansas, Computer Science and Computer Engineering Department. His research interests are radio frequency identification (RFID), computer security, and computer networks.

Dale R. Thompson (M'90–SM'03) received his B.S. and M.S. degrees in electrical engineering from Mississippi State University, Starkville, MS, USA in 1990 and 1992, respectively. He received his Ph.D. in electrical engineering from North Carolina State University, Raleigh, NC, USA in 2000. He worked as an Electronics Engineer in the communications group at the U.S. Army Engineer Research and Development Center in Vicksburg, MS, USA from 1992 to 2000. He is an Associate Professor in the Computer Science and Computer Engineering Department at the University of Arkansas in Fayetteville, Arkansas, USA. His research interests are computer and network systems, security and privacy, and radio frequency identification (RFID).

Jia Di received his B.S. and M.S. degrees in Automation from Tsinghua University, Beijing, China in 1997 and 2000, respectively. He received his Ph.D. from the Electrical and Computer Engineering department of the University of Central Florida, Orlando, FL in 2004. He then joined the Computer Science and Computer Engineering

department of the University of Arkansas, in Fayetteville, Arkansas and is currently an Associate Professor. His research interests include hardware security, asynchronous logic, ultra-low power digital circuit, and digital systems for extreme environments.