Specific Emitter Identification for Enhanced Access Control Security

J.N. Samuel[1] and W.P. du Plessis[1]
Email: jeevanninansamuel@gmail.com, wduplessis@ieee.org
[1]Department of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa

***Abstract*—This paper presents the application of specific emitter identification (SEI) to access control and points out the security caveats of current radio-based access remotes. Specifically, SEI is applied to radio frequency (RF) access remotes used to open and close motorised gates in residential housing complexes for the purposes of access control. A proof-of-concept SEI system was developed to investigate whether it is possible to distinguish between the RF signals produced by two nominally-identical access remotes. It was determined that it is possible to distinguish between the remotes with an accuracy of 98%.**

I. Introduction

Access remotes are used to open gates to residential estates, houses and garages. On this basis they provide security as only people with the remote are able to gain access to these areas, akin to a key. However, the signal produced by these remotes can easily be read from low-cost software-defined radios (SDRs) and reproduced by another radio transmitter [1]. This allows for illegitimate access to residential estates, houses and garages. This motivates the need for making access remotes robust against replay attacks and cloning.

SDRs are radios whose hardware implementation is either replaced by corresponding software components or configurable via software [2]. Recently the concept of SDR has matured due to advancements in hardware and software technology to the point where anyone can purchase a SDR for $10 to $15 [3]. In particular the RTL2832U-based SDRs fit in this category of low-cost SDR. They consist of a number of models based on the tuning chip that they utilise. Three of the tuning chips used are the Raphael R820T, the Elonics E4000 and the Fitipower FC tuning chips. The R820T SDR can tune from 24 MHz to 1766 MHz [3], while the Elonics E4000 can tune between 52 MHz to 2200 MHz, though with a frequency gap between approximately 1100 MHz and 1250 MHz. Regardless of the type of tuner used, the RTL2832U receiver can sample data at up to 3.2 Msps and has an 8-bit analogue-to-digital converter (ADC) resolution. However, it has been found that the RTL2832U can only sample data reliably (i.e. without dropping samples) at sampling rates lower than 2.56 Msps [3]. While these low-cost SDRs have relatively low ADC resolution and tuning range, they are sufficient for eavesdropping on radio communications.

Connected to a software application such as GNU Radio [4], an SDR can be used to listen to radio transmissions in its tuning range and to store these transmissions in a digital format. This makes it easier to perform replay attacks provided the assailant has a radio transmitter capable of transmitting on the same frequency as the captured communications. The HackRF is the cheapest SDR capable of receiving and transmitting radio communications at $299 [5]. Access remotes are thus vulnerable to replay attacks since they perform access control by transmitting radio signals.

Specific emitter identification (SEI) is a technique used to uniquely identify radio transmitters, even those of the same make and model, using only their transmitted radio signals [6]. This means of identification is possible due to hardware tolerances in the radio frequency (RF) circuitry created during manufacturing [7]. SEI is also referred to as radio-frequency fingerprinting (RFF) or physical-layer identification. SEI aims to alleviate the mimicing or spoofing of the identities of radio devices as the identifying characteristics produced by SEI are inherently difficult to spoof [8], [9]. In this way, SEI is used to enhance the security of communication networks using wireless devices.

A typical approach used in SEI is to maintain a library of signal characteristics (or features) that uniquely identify a variety of emitters, and comparing the incoming signal of an emitter to the library of feature sets. The identifier (or label) of the feature set that best matches the incoming signal is assigned to it [6], [10]. An implicit requirement of this approach is that the feature sets cluster. This implies that feature values from a particular emitter are similar and repeatable for all signals produced by the emitter while appreciably distinct from feature values produced by a different emitter [6].

This paper demonstrates how conventional RF access remotes can be uniquely identified using low-cost SDR receivers and SEI. The success of this demonstration suggests that this is a viable approach to increasing the security which can be achieved using conventional RF access remotes.

Section II presents the design and implementation of a proof-of-concept software system that performs SEI to distinguish between two nominally-identical access remotes. Section III describes the results obtained from the study. Section IV concludes the paper.

This work is based on the research supported in part by the National Research Foundation (NRF) (Grant specific unique reference number (UID) 85845). The NRF Grantholder acknowledges that opinions, findings and conclusions or recommendations expressed in any publication generated by the NRF supported research are that of the author(s), and that the NRF accepts no liability whatsoever in this regard.

978-1-5090-2473-8/16/$31.00 ©2016 IEEE

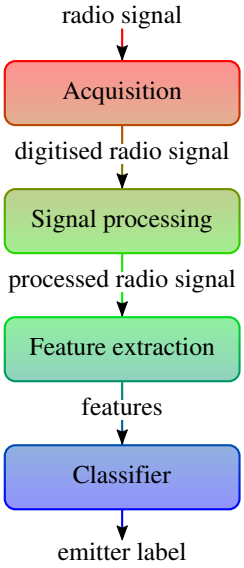


Fig. 1. SEI system overview.

II. System Description

The overall SEI system depicted in Fig. 1 consists of the following elements which will be considered below.

1) The acquisition system acquires the RF signals produced by the access remotes. It then stores the data in a digital format for later processing.
2) Signal processing is then performed on the stored digital RF signals to remove any arbitrary variances in the signals that may distort the signals and affect signal classification.
3) The feature-extraction subsystem then extracts distinct features from the processed RF signals.
4) The classifier subsystem then takes the extracted features and builds an association between the radio signals and the transmitters from which they were produced.

A. Operating Characteristics of RF Access Remotes

RF access remotes operate in the industrial, scientific and medical (ISM) band at 433 MHz [11], [12]. This band is intended for the operation of equipment designed to use local RF energy for purposes other than telecommunications [13].

These access remotes transmit a modulated sequence of bits to the gate's receiver in order to open or close the gate. This usually takes the form of pulse width modulation (PWM) in which a logical 0 is represented by a short pulse, and a logical 1 is represented by a long pulse [1]. This simple form of modulation makes these access remotes susceptible to replay attacks allowing for illegitimate access to residential estates, houses and garages. This simple modulation scheme also allows for access remotes to be programmed by cloning the signal from another access remote [11].

For the development of this system, two RF access remotes that open the gate to a residential complex were considered. Each remote was distinctly labelled (A and B) as shown in Fig. 2.

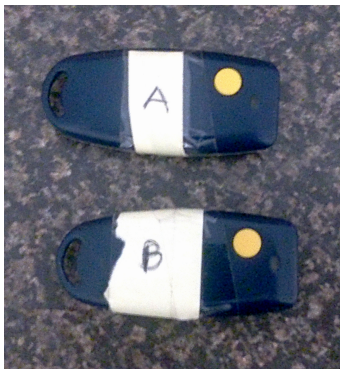


Fig. 2. Access remotes utilised for the development of the proof-of-concept SEI access control system.

Fig. 3. RTL2832U SDR with a Raphael R820T tuner.

The signal characterisitics of the RF access remotes will be described in Section II-B during the elaboration of the signal acquisition setup.

B. Signal Acquisition

The signal acquisition system consists of two processes, namely the recording process and burst extraction process.

For signal recording, an RTL2832U SDR with an R820T tuner, shown in Fig. 3, was utilised and interfaced through a GNU Radio applet. The selected SDR is a relatively inexpensive SDR that can sample signals at up to 3.2 Msps and has 8-bit ADC resolution [3]. The SDR receiver was configured as shown in Table I.

The applet was run for 80 s while the button on the remote was continously pressed for the duration of 80 s. After the 80 s, the applet stored the recorded samples in a binary file for later processing.

The recorded samples were then investigated in order to identify the characteristics of the signals produced by the access remotes. A single burst produced by an access remote is shown in Fig. 4. It is observed that the access remotes' signals consist of a 10.4-ms start pulse followed by twelve modulated pulses comprising a burst with a total duration of 13.6 ms. The start pulse is used for the detection of a signal produced by an access remote. The encoded burst pulses are seen to utilise PWM (as mentioned earlier) in which the a short pulse corresponds to a 0 and a long pulse corresponds to 1. Based on this, each access remote transmitted the same bit sequence of 011001100001.

TABLE I
RECEIVER PARAMETERS.

Receiver parameter	Value
Low-noise amplifier (LNA) gain	5 dB
Center frequency	433.91 MHz
Sampling rate	1 Msps
Distance from receiver	20 cm

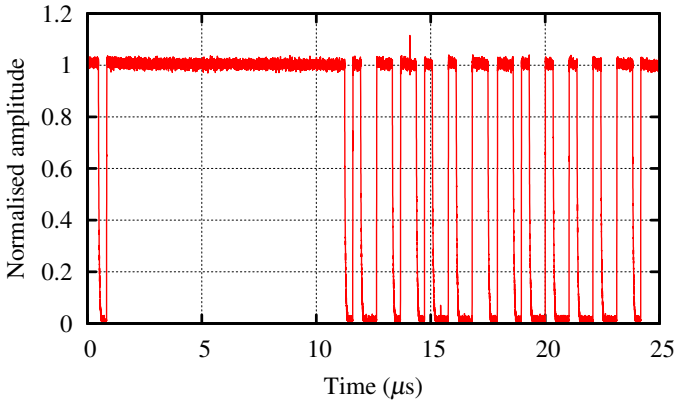


Fig. 4. Captured signal from access remote A.

In order to extract the individual access-remote bursts, burst extraction was performed on the digitally-stored RF signals produced by each access remote. A threshold algorithm was utilised to extract the individual bursts and is described in Algorithm 1. Essentially the algorithm parses the amplitude of the recorded samples and checks the number of consecutive samples above the theshold (the mean value of all the amplitude samples). If the number of consecutive samples is at least 90% of the preceeding start pulse length (i.e. 10.4 ms as mentioned earlier), then a burst has been detected. The algorithm then extracts the complex in-phase and quadrature samples from the current search index to 13.6 ms later, which as mentioned earlier, is the approximate burst length. These extracted data constitute a single access remote burst. In this case, the search window is advanced by the sum of the start pulse length (i.e. 10.4 ms) and the burst length (i.e. 13.6 ms). If no burst is detected, the search index is advanced by 100 samples to continue parsing the data in a small window. For the development of this proof-of-concept system, more than a thousand bursts were extracted for each remote.

C. Signal processing

Following recording of the access-remote signals and extraction of bursts, the individual bursts are then further processed in order to remove any arbitrary variances in the bursts that are due to noise, amplitude variances and phase offsets.

The first step taken in processing is filtering out noise. This is typically done by first down-converting the recorded burst to its baseband frequency and then applying a low-pass filter to the signal [14]. In order to correctly filter the noise, the bandwidth of a burst had to be identified. This was done by taking the Fourier transform of a single burst and visually inspecting which frequency bins had the most energy, as shown

Data: Complex samples **s**
Result: Array of extracted bursts
amp ← absolute(**s**);
threshold ← mean(amp);
searchIndex ← 0;
burstCount ← 0;
while *searchIndex < total number of samples in amp* **do**
  window ← [searchIndex to searchIndex + 10.4 ms];
  if *Σ(amp[window] > threshold) > 90% of window length* **then**
    increment burstCount;
    extractionWindow ←
    [searchIndex:searchIndex+window+13.6 ms];
    burstArray[burstCount] ← **s**[extractionWindow];
    increment searchIndex by (10.4 ms + 13.6 ms);
  else
    increment searchIndex by 100 samples;
  end
end
return burstArray;

Algorithm 1: Algorithm for burst extraction.

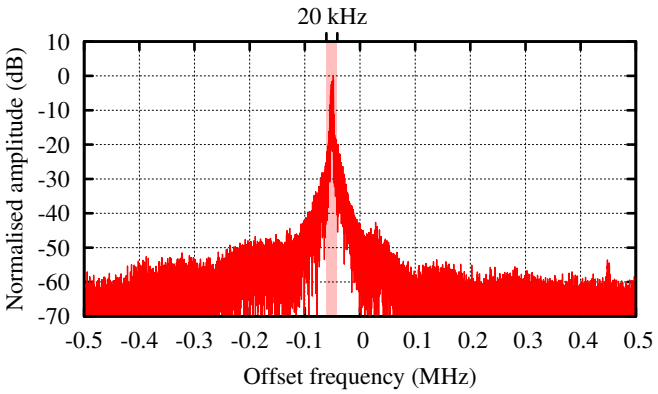


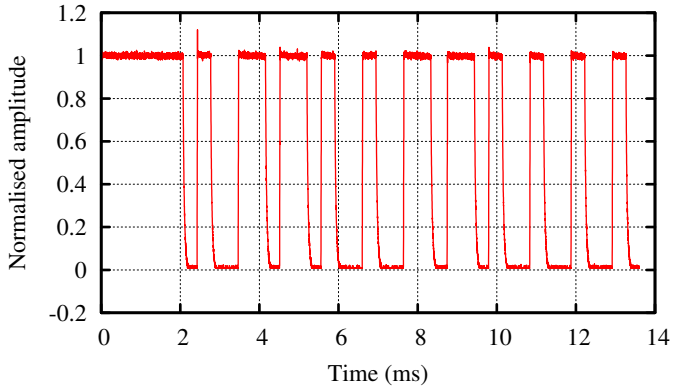
Fig. 5. Magnitude of frequency spectrum computed over a single burst.

in Fig. 5. In this way, the burst bandwidth was determined to be 20 kHz. Thus a finite impulse response (FIR) low-pass filter with a 3 dB cut-off frequency of 10 kHz was utilised in order to filter out noise. The FIR filter consisted of 10 000 coefficients and used a Hamming window.

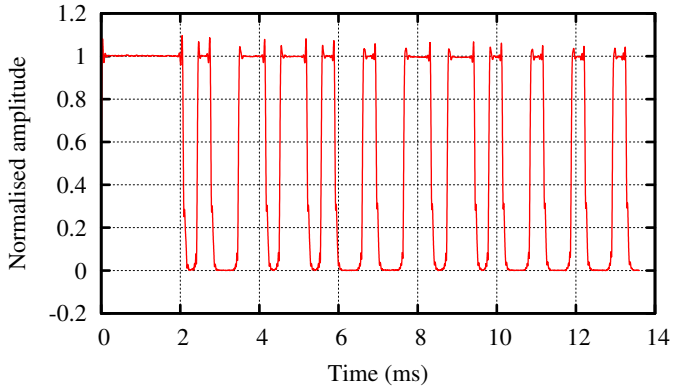
The effect of filtering is demonstrated in Fig. 6 which shows filtered and unfiltered bursts in Figs 6(a) and 6(b), respectively.

Following filtering, the amplitude representations of each burst need to be normalised between 0 and 1 so as to allow bursts recorded at different amplitudes to be compared. This prevents the feature extraction subsystem from producing feature vectors that differ due to amplitude variances between bursts. This would cause the misclassification of bursts even if they were produced from the same access remote.

Similarly, frequency offsets in the phase representations of each burst can cause misidentifications by the classifier. A

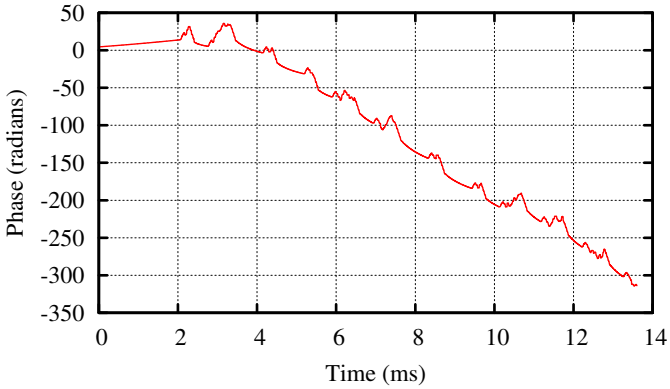


(a) Unfiltered.

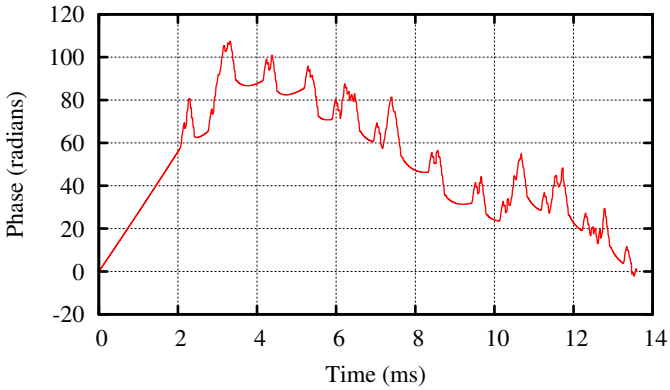


(b) Filtered.

Fig. 6. Amplitude representation of an access remote burst.



(a) Without frequency offset correction.



(b) With frequency offset correction.

Fig. 7. Phase representation of an access remote burst.

phase representation of a burst with and without a frequency offset is shown in Figs 7(a) and 7(b), respectively.

D. Signal difference inspection

Once signal processing is complete, only then can the true differences between the signals produced by each access remote be determined.

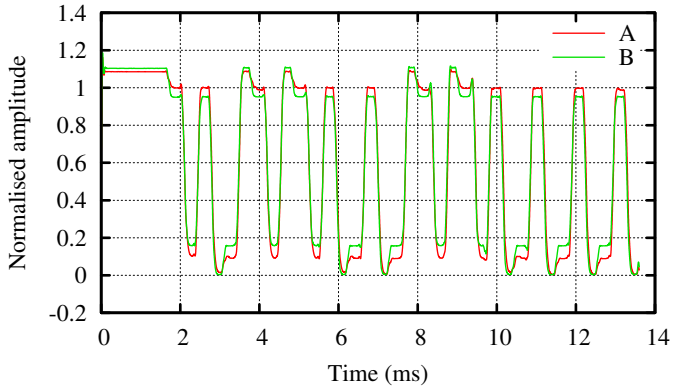
Observing the differences between mean amplitude representations of 100 bursts produced by the individual access remotes, shown in Fig. 8(a), it is seen that there are distinct differences in the amplitude representations. However, these differences are not consistent as shown in Fig. 8(b). The average amplitude representation over the first 100 bursts for access remote A differs from the average amplitude representation for the next 100 bursts. The same holds true for access remote B. As mentioned earlier, for SEI to be successful it is imperative that the characteristics of the signal produced by a specific transmitter be consistent for all signals produced by that transmitter, while being appreciably distinct from the characteristics produced by another transmitter. Based on this observation, the amplitude representations of the access remotes are unlikely to achieve the ultimate goal of classifying the bursts emitted by them.

Observing the differences between the mean phase representations over 100 bursts of access remotes A and B alone (Fig. 9(a)), it is seen that the phase representations for each key differ significantly. As shown in Fig. 9(b), the post-processed mean phase representations do not exhibit the inconsistencies seen in the amplitude representations. As seen in Fig. 9(b), the mean phase representation for the first 100 bursts of access remote A is similar to mean phase representation for the next 100 bursts. The same holds true for access remote B. These phase differences are more distinct than the differences seen in the amplitude representation. On this basis, the phase representations of the access remotes would be better for the purposes of SEI.

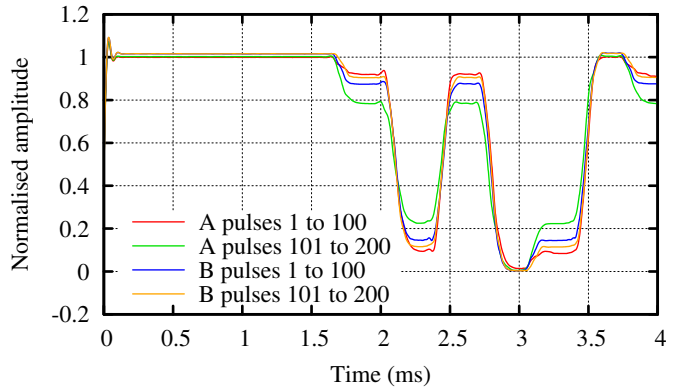
E. Feature Extraction

While it is possible to present the entire amplitude or phase representation to the classifier, this would be inefficient and may hinder the classification accuracy. This is because each sample in the phase and amplitude representations would be treated as a feature leading to an exorbitant number of features. Instead, a set of values that effectively summarises the shape of each representation are calculated. These values then serve as the features for each signal representation and the process is called feature extraction [15].

Statistical measures, namely variance, standard deviation, skewness and kurtosis, are typically used in the SEI of wireless devices such as Global System for Mobile Communications (GSM) cellular telephones [14]. For the development of this system, statistical feature extraction was utilised and is de-

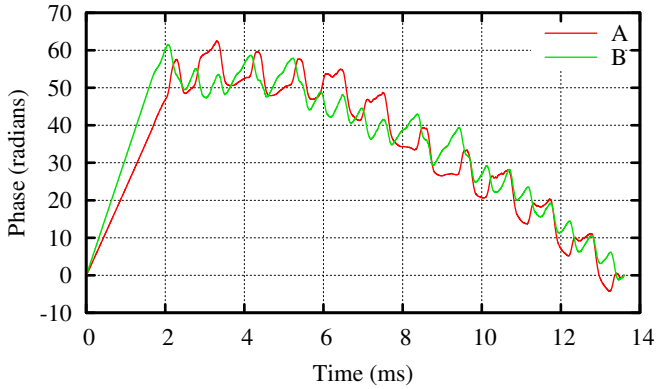


(a) One set of averaged data.

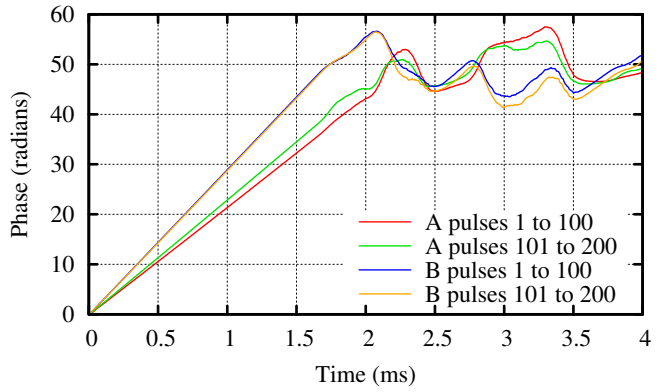


(b) Comparison between different sets of averaged bursts.

Fig. 8. Mean amplitude representation of 100 bursts.



(a) One set of averaged data.



(b) Comparison between different sets of averaged bursts.

Fig. 9. Mean phase representation of 100 bursts.

scribed in Algorithm 2. Each signal representation (the mean phase and amplitude representations over a certain number of bursts) is divided into a number of equally sized sub-regions (NR). For each sub-region, the variance, standard deviation, skewness and kurtosis are calculated. These statistical values are then standardised using [14]

$$[\sigma, \sigma^2, \gamma, k] = \frac{\text{mean}([\sigma, \sigma^2, \gamma, k])}{\text{standard deviation}([\sigma, \sigma^2, \gamma, k])}. \quad (1)$$

Once statistical measures have been calculated for each sub-region, the variance, standard deviation, skewness and kurtosis are calculated over the whole signal representation. The number of sub-regions determined to work best for GSM cellphones was 5 [14], which leads to a total of 24 features per signal representation. Once the statistical features have been calculated for each signal representation, they are concatenated with the first 24 features corresponding to amplitude features and the latter 24 corresponding to phase features. The 48 features in total represent a single feature vector.

The average representation of the features for each access remote is shown in Fig. 10, with the amplitude and phase features in Figs 10(a) and 10(b), respectively.

F. Signal Classification

Once a set of feature vectors have been established, classification can take place. In order to perform classification, the feature vectors have to be segmented into training and test groups for each access remote. The training feature vectors serve to build an association between the feature vectors and the access remotes from which they were derived. This is done by presenting the classifier with a feature vector and an associated access remote label for all feature vectors in the training group. The test group of feature vectors is then used to evaluate the performance of the classifier. In this phase, each feature vector in the test group is presented to the classifier without a label, and the classifier returns the label of the access remote it deems most likely to correspond to the feature vector [16]. It is important to note that the training and test groups of feature vectors must be derived from different bursts. For the development of this system, training feature vectors were derived from the first 200 bursts for each remote. Test feature vectors were derived from bursts 200 to 1 000 for each remote.

The classifier utilised was a kth nearest neighbour (KNN) classifier. KNN computes a distance d between an m-dimensional input feature vector $\mathbf{x}$ to a number of training feature vectors $\mathbf{t_r}$ (with the same dimensionality). The label of $\mathbf{x}$ is based on the most occurring label of its k nearest neighbours, where k is a positive integer [16]. The distance measure utilised in the implementation of KNN is the Man-

Data: Array of access remote bursts
Result: Feature vector of statistical features
amplitude representation of burst ←
mean(absolute(low-pass filter(access remote bursts)));
amplitude representations of burst ←
normalise(amplitude representation of burst);
phase representation of burst ← mean(angle(low-pass filter(access remote bursts)));
phase representations of burst ← remove phase offset from phase representation of burst;
NR ← 5;
for *each representation* **do**
  N ← number of samples in representation;
  s ← ⌊ N/NR ⌋;
  for $m = 1$ *to NR* **do**
    g ← m × s;
    d ← (g-s)+1;
    segment ← representation from samples d to g;
    feature_vector(m) ← standardise([σ σ^2 γ k of segment]);
  end
  feature_vector(m+1) ← standardise([σ σ^2 γ k of entire representation]);
end
final_feature_vector ← concatenate feature_vector 1 to NR+1;
return final_feature_vector;

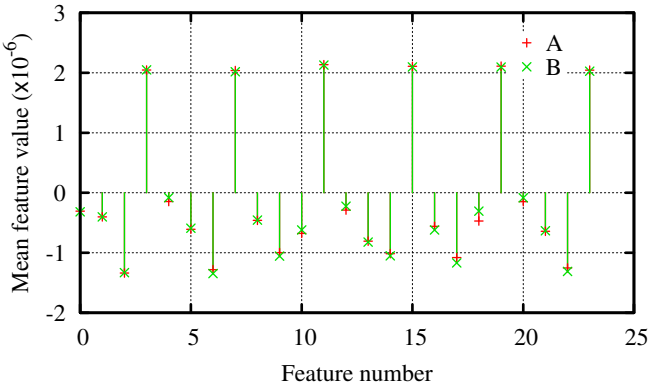
Algorithm 2: Algorithm for feature extraction.

hattan distance calculated by

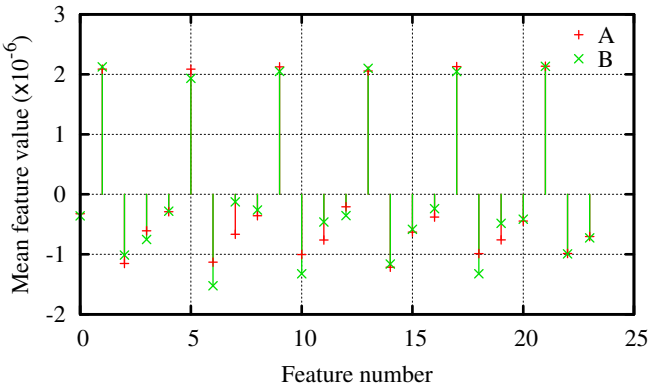
$$d = \sum_{i=1}^{m} |\mathbf{x(i)} - \mathbf{t_r(i)}|. \quad (2)$$

Manhattan was the chosen distance measure due to the fact that Manhattan distance is best suited for features that measure dissimilar properties [16]. Given that feature extraction process considers amplitude and phase measures, Manhattan distance is apt for evaluating distance.

Once the distances for all feature vectors are computed, the labels of the k feature vectors corresponding to the lowest distance (nearest neighbours) are considered. The most occurring label among the k nearest neighbours is then assigned to $\mathbf{x}$. For this process, k is usually set to an odd number to avoid ties [16]. However, for the development of this SEI system, only the average feature vector per access remote was maintained in the memory of the KNN classifier. That is to say, only two feature vectors were presented to the KNN classifier for training, with each one corresponding to the mean of all training feature vectors produced by a particular access remote. Thus, k was set to 1. The processing detail for the KNN classifier is shown in Algorithm 3.



(a) Amplitude features.



(b) Phase features.

Fig. 10. Average representation of the features.

III. Results

As mentioned earlier, feature vectors are derived by taking the mean representations of phase and amplitude over a certain number of bursts. In order to determine the effect that number of bursts utilised during feature extraction had on classification, the following two classification scenarios were considered.

1) Classification scenario 1 – Feature vectors were derived over 50 bursts.
2) Classification scenario 2 – Feature vectors were derived over 10 bursts.

The confusion matrices are shown in Table II. A summary of the classification accuracy (taken as the mean across the diagonal of the confusion matrix) for each of the scenarios and features used is shown in Table III.

The performance of the system is determined by how well the classifier is able to identify the bursts of the access remotes. Based on Table III, it is seen that the KNN classifier can identify bursts from access remotes A and B with an accuracy of at least 98% provided phase features are utilised. When amplitude features are used exclusively, the accuracy drops to between 53% and 55% depending on the number of bursts utilised to form a feature vector. Furthermore, the high accuracy for phase features in classification scenario 2 indicates that as few as ten bursts can be used to form a feature

Data: Feature vector ($\mathbf{x}$), training feature vectors ($\mathbf{t_r}$), class labels l and value for k
Result: Class labels and mean distance from nearest neighbours for each $\mathbf{x}$
P $\leftarrow$ number of feature vectors $\mathbf{x}$;
Q $\leftarrow$ number of training feature vectors $\mathbf{t_r}$;
for $p = 1$ *to* P **do**
  for $q = 1$ *to* Q **do**
    $\mathbf{x}' \leftarrow \mathbf{x(p)}$;
    $\mathbf{t_r}' \leftarrow \mathbf{tr(q)}$;
    $d(q) \leftarrow \sum_{i=1}^{m} |\mathbf{x}'(\mathbf{i}) - \mathbf{tr}'(\mathbf{i})|$;
  end
  Sort d in ascending order;
  Sort l based on sorted indices of d;
  if $k > 1$ **then**
    nearest_neighbours $\leftarrow$ l from 1 to k;
    class_result(p) $\leftarrow$ most_occurring_class(nearest_neighbours);
    distance_result(p) $\leftarrow \frac{1}{k} \sum_{i=1}^{k} d(i)$;
  else
    class_result(p) $\leftarrow l(1)$;
    distance_result(p) $\leftarrow d(1)$;
  end
end
return class_result and distance_result;

Algorithm 3: Algorithm for the KNN classifier.

TABLE II
CLASSIFICATION ACCURACY.

	Features used					
	Amplitude		Phase		Amplitude and phase	
	A	B	A	B	A	B
Classification scenario 1						
A	6.25%	93.75%	100%	0%	100%	0%
B	0%	100%	0%	100%	0%	100%
Classification scenario 2						
A	10%	90%	97.5%	2.5%	96.25%	3.75%
B	0%	100%	1.25%	98.75%	0%	100%

vector distinct enough to provide accurate classification. As a result, an access remote will only need to be sampled for less than a quarter of a second in order to produce the number of bursts required for accurate identification.

IV. CONCLUSION

In conclusion, the development of a proof-of-concept SEI access control system for RF access remotes proved successful. Offline classification was performed on RF bursts produced by two access remotes. When the phase features of the bursts were utilised, the bursts could be identified as belonging to a specific access remote with an accuracy in excess of 98%. Furthermore, this classification can theoretically be performed by sampling bursts produced by an access remote for less than a quarter of a second. In light of these observations, SEI has been shown to hold tremendous potential to enhance the security of RF access remotes by providing physical-layer identification of the individual remotes and consequently makes these remotes less susceptible to replay attacks.

TABLE III
SUMMARY OF CLASSIFIER PERFORMANCE.

Classification scenario	Features used	Classification accuracy
1	Amplitude and phase	100%
1	Amplitude	53.13%
1	Phase	100%
2	Amplitude and phase	98.125%
2	Amplitude	55%
2	Phase	98.125%

REFERENCES

[1] T. Watorowski. (2016, July) H4ck33D – hacking a 433MHz remote control. http://mightydevices.com/?p=300.
[2] M. Dillinger, K. Madani, and N. Alonistioti, "Introduction," in *Software Defined Radio: Architectures, Systems and Functions*, ser. Wiley Series in Software Radio. Chichester, England: Wiley, 2005, pp. xxxiii–xxxiv.
[3] (2016, July) rtl-sdr – OsmoSDR. [Online]. Available: http://sdr.osmocom.org/trac/wiki/rtl-sdr
[4] (2016, July) GNU Radio. [Online]. Available: http://gnuradio.org
[5] (2016, July) NooElec – HackRF One software defined radio – SDR receivers – software defined radio. [Online]. Available: http://www.nooelec.com/store/sdr/sdr-receivers/hackrf-one.html
[6] K. I. Talbot, P. R. Duley, and M. H. Hyatt, "Specific emitter identification and verification," *Technology Review Journal*, vol. 11, pp. 113–133, 2003.
[7] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys*, vol. 45, no. 1, pp. 6:1–6:29, Dec. 2012.
[8] M. Williams, M. A. Temple, and D. Reising, "Augmenting bit-level network security using physical layer RF-DNA fingerprinting," in *Global Telecommunications Conference (GLOBECOM 2010)*, Miami, USA, Dec. 2010, pp. 1–6.
[9] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improving intra-cellular security using air monitoring with RF fingerprints," in *IEEE Wireless Communications and Networks Conference (WNC10)*, Sydney, Australia, Apr. 2010.
[10] D. Zanetti, V. Lenders, and S. Capkun, "Exploring the physical-layer identification of GSM devices," Swiss Federal Institute of Technology Zurich, Department of Computer Science, Tech. Rep., 2012.
[11] (2016, July) SENTRY learning 1/3/4 button 433MHz (binary, inverted trinary, SMART). http://www.martin-electronics.co.za/Learning_B_T_F_433Mhz.aspx.
[12] (2016, July) SENTRY binary remote control transmitter three button (433Mhz) – SENTRY remote. http://www.taskltd.com/task-online-store/remote-control-transmitters/binary-transmitters-433mhz/sentry-binary-transmitter-three-button-433mhz.html.
[13] ITU. (2016, July) Article 1: Terms and definitions. http://life.itu.int/radioclub/rr/art01.htm.
[14] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improved wireless security for GMSK based devices using RF fingerprinting," *International Journal of Electronic Security and Digital Forensics*, vol. 3, no. 1, pp. 41–59, Mar. 2010.
[15] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2nd ed. New York, USA: Wiley-Interscience, 2000.
[16] S. Russell and P. Norvig, *Artificial Intelligence A Modern Approach*. New Jersey, USA: Pearson Education, 2010.