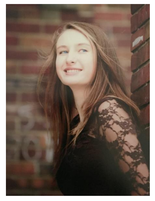
Physical Layer Security

Gabrielle Beck - University of Michigan
Kevin Ponce Garcia - University of Puerto Rico at Arecibo
Advisors: Dr. Tao Shu – Auburn University, Rui Zhu – Oakland University

1 Objectives

- Explore potential vulnerabilities in physical layer security methods like link signatures (LS) for wireless networks in an indoor office setting

2 Introduction

Because of the computational limitations of wireless networks and the growing uncertainty about the security of current cryptographic schemes, new methods of encrypting communication between transmitters and receivers have been proposed. One such method is physical layer security: it leverages the unique physical properties of a channel for location authentication or for extracting secret keys. The strength in physical layer security lies in how channels are considered to be reciprocal and uncorrelated: reciprocal because a channel measured at either end will give out similar measurements and uncorrelated because two channels separated by more than half of a wavelength are assumed to be unrelated to each other.

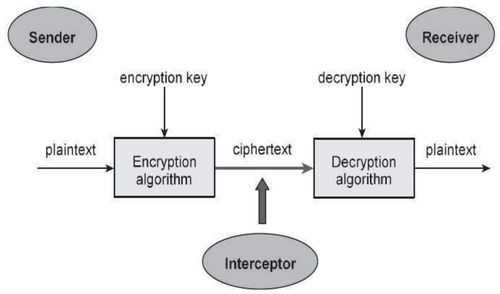


Figure 1. General Encryption Framework

However, some of these decorrelation assumptions have been proven not to hold in specific cases based on previous work, for example, the one ring model. Thus, it may be possible for hackers to obtain an estimation of the specific channel properties between a pair of transmitters and receivers in order to perform a spoofing attack or to compromise their secret key, under specific circumstances.

3 Experimental Setup

Simulation platform: MATLAB

Dataset from Motorola Labs, Florida Communications Research Lab and the University of Utah [1]

Topology model: the measurement campaign consisted of 44 nodes locations, as show in figure 2.

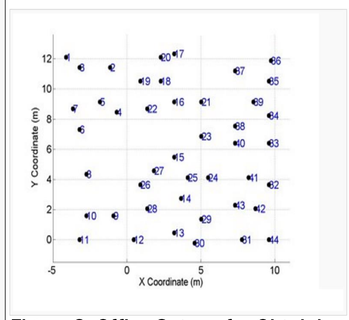


Figure 2. Office Set- up for Obtaining Transmitter/Receiver

- Dataset contains link signatures for 44*43=1892 links, so between any pair of nodes
- 5 distinct measurements performed at different times for each link
- In total the database recorded over 9300 traces for the link signature
- The data set was used to test a temporal link signature base on machine learning algorithms.

Estimating the link signature:

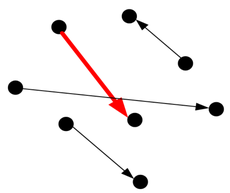


Figure 3. Set-up of Attack Model

- Used links of different transmitter x and receiver x locations to estimate LS of interest
- Besides Multivariate Linear regression, different transmitters/receivers used varied from 5 to 20 of the total dataset

[1] N. Patwari, A. O. Hero, M. Perkins, N. S. Correal, R. J. O'Dea, Relative Location Estimation in Wireless Sensor Networks, IEEE Transactions on Signal Processing, vol. 51, no. 8, August 2003, pp. 2137-2148.

4 Results

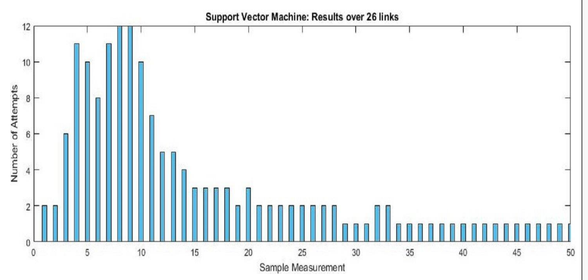


Figure 4. Number of Attempts to Guess portions of LS

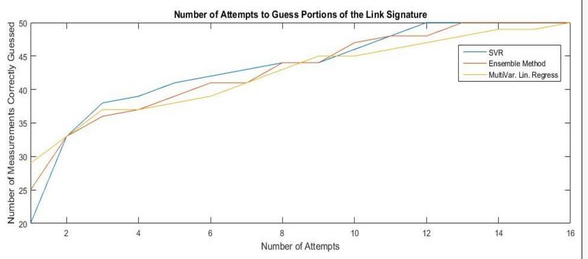


Figure 5. Portion of LS discoverable by Number of Attempts

We tested over 26 different links, quantizing into 32 bins using the following Machine Learning Algorithms: Ensemble Methods, which is an adaptation of Decision Tree and support vector regression. The links were also tested with multivariate linear regression. Links were tested multiple times in order to get the best results possible. The same parameters were not used on all of the links tested. Overall, Support Vector Regression had the overall lowest max number of attempts: 12 (see figure 4). In comparison, ensemble methods had an average of 13 and Multivariate Linear Regression had an average of 16 (see figure 5 for analysis). For reference, we would expect brute force to have an average of 16 attempts on each of the 50 measurements sampled.

5 Analysis and Future Work

Our results suggest that link signatures would be vulnerable to these attacks under specific circumstances: the variability in how well an ML can guess specific link signatures suggests that in some environments, using link signatures would not be very safe. The environment must be inherently dynamic in order to ensure a certain amount of security. It is also important to note that sampling past a certain amount of time leads to very deterministic keys. Any actual practical implementation would need to cut off sampling after a certain amount of time to avoid creating a compromised key.

We suggest that future works consider looking at specific environmental features that effect channel predictability and looking more into statistical learning frameworks that take into consideration various known channel distributions.

6 Conclusion

Under specific circumstances, it is undeniable that there exists great insecurity in link signature methods. However, more research in a known environment must be done in order to say what conditions are needed and where unknown transmitters and receivers must be placed to find vulnerabilities.

We also note that poor implementation practices such as using duplicates of the key, not using transformations to create uncorrelated components, etc. will greatly damage the integrity of any existing key and it may be important to take this into consideration during error correction.

7 Acknowledgment

This research work was conducted at Oakland University in the UnCoRe program - REU site supported by the National Science Foundation under Grant No. CNS-1460897. Any opinions, findings, and conclusions or Recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

More Details may be found at : http://cse-reu.secs.oakland.edu