GMM based Semi-Supervised Learning for Channel-based Authentication Scheme

Nikhil Gulati[1], Rachel Greenstadt[2], Kapil R. Dandekar[1] and John M. Walsh[1]

[1]Department of Electrical and Computer Engineering, Drexel University
[2]Department of Computer Science, Drexel University,
Philadelphia, PA 19104
Email: ng54@drexel.edu, greenie@cs.drexel.edu, dandekar@ece.drexel.edu, jwalsh@ece.drexel.edu,

***Abstract*—Authentication schemes based on wireless physical layer channel information have gained significant attention in recent years. It has been shown in recent studies, that the channel based authentication can either cooperate with existing higher layer security protocols or provide some degree of security to networks without central authority such as sensor networks. We propose a Gaussian Mixture Model based semi-supervised learning technique to identify intruders in the network by building a probabilistic model of the wireless channel of the network users. We show that even without having a complete *apriori* knowledge of the statistics of intruders and users in the network, our technique can learn and update the model in an online fashion while maintaining high detection rate. We experimentally demonstrate our proposed technique leveraging pattern diversity and show using measured channels that miss detection rates as low as 0.1% for false alarm rate of 0.4% can be achieved.**

I. Introduction

Over the past decade, due to the ubiquity of wireless devices, security has become a significant concern as increasing amounts of sensitive user and enterprise data is exchanged through the wireless medium. Due to the inherent shared nature of the wireless medium, it is challenging to detect and counteract intrusions in wireless networks. Although conventional security measures based on cryptography are essential to secure wireless network, tasks like authentication may not always be possible as they require additional key management infrastructure which may not be always available. Moreover, cryptographic security mechanisms do not exploit the unique properties of the wireless medium to address security attacks. In recent years, cross-layer authentication schemes, especially those which employ channel information available at the physical layer have been proposed. They have been shown to either cooperate with high-layer security protocols or provide some level of protection for infrastructure-less networks such as ad hoc networks or sensor networks.

Some of the previously proposed channel-based authentication schemes such as those in [1], [2], [3] are based on comparing the channel response for each new message from a user with past channel responses. These schemes are setup as a hypothesis test using a metric derived from the channel. In [1], the hypothesis test is based on the distance between the reference channel created from channel estimates from the messages in the past and the channel from the message that needs to be authenticated. In [2], the authors employ a hypothesis test based on the covariance matrix of the time samples of a single link wireless channel to differentiate between transmitters. Further, in [3], authors consider a MIMO system model to improve the channel resolution by using M independent channel responses from M equally spaced (in frequency) pilot tones. They assume that the minimum frequency spacing is greater than the channel coherence bandwidth for perfect decorrealtion between channel samples. They further assess the performance of a channel-based authentication schemes in the presence of channel estimation error and terminal mobility and propose a generalized likelihood test (GLRT) for detection. Besides the schemes based on channel response, RSS based schemes have also been proposed in the past [4], [5]. In [5], authors use N-dimensional feature vector corresponding to RSS frames measured at N access points to cluster the M frames received from a given MAC address using k-means clustering. Their results are further improved by authors in [6] by using Gaussian Mixture Models(GMM) to model transmitter profile which consists of multi-modal RSS distribution as an effect of antenna diversity.

Though many of the proposed channel-based authentication schemes show promising results, they rely on selecting a test threshold value for achieving acceptable detection or false alarm rates for a given system and wireless environment. It has been shown that the selection of this test threshold significantly impacts the system performance [3]. Moreover, as the value of test threshold highly depends on factors such as, underlying channel statistics, channel estimation errors, terminal mobility and physical environment where devices are located, selection of the test threshold is challenging. In [3], authors propose two methods to select a test threshold. First, a very common method of selecting a pre-assigned threshold requiring a large number of field measurements, which can be prohibitively expensive. Secondly, an adaptive threshold method where transmitter and receiver exchange training messages and receiver selects the o-th percentile value of collected test statistics during the training phase as the test threshold value. However, the authors mention that the performance of this method is sensitive to value of o and

978-1-4673-6187-3/13/$31.00 ©2013 IEEE

the amount of training required. On the other hand we base our approach on the notion that the statistical model for the intruder and legitimate user can be built via semi-supervised learning where we do not require intruder samples before and require a very low number of samples for legitimate users without requiring extensive training data from the field measurements. We further modify our learning technique to update the learned model in an online fashion.

There has been significant research in using machine learning techniques for network intrusion detection by modeling network traffic and extracting information from higher layers. The data available for intrusion detection systems can have different levels of granularity and may consist of packet level traces, CISCO net-flows, or other information from higher layers of network stack [7], [8]. In [9] authors provide an exhaustive survey of anomaly detection techniques, including many techniques used in network intrusion detection.

In this paper, we propose a detection scheme based on semi-supervised learning through the use of Gaussian Mixture Model (GMM) and a classification technique to leverage the information available at the physical layer. In order to build a model of the wireless users' channel information, we use a family of Gaussian Mixture Model and update the model parameters online. We provide a feature selection technique by using the diversity of the wireless channel and show the performance improvement as the dimensions of the feature set increases. In that context we use the diversity technique proposed in [10], [11] where authors make use of the channel decorrelation obtained by the use of pattern reconfigurable antennas. They show that using a reconfigurable antenna, decorrelated channel realizations can be obtained by selecting the different modes of the antenna which are expected to have different statistics. This pattern diversity offered by reconfigurable antennas is exploited to enhance the performance of the channel based detection scheme. We note that other diversity techniques such as antenna diversity, frequency diversity and MIMO technique can also be used to create feature set for our proposed learning method and it is not a requirement to have reconfigurable antennas to implement the learning technique. We explain how we utilize pattern diversity in Sec II-C and for more information on reconfigurable antennas and their applications, we direct the reader to these references [12], [13].

II. System Model & Channel Fingerprint

A. Threat Model

We consider a model consisting of at least three players; a legitimate transmitter Alice, an intended receiver Bob and a spoofing intruder Eve. Alice and Bob have established a connection and are in the process of exchanging information. Intruder Eve tries to inject messages using Alice's identity, for example her MAC address, in an attempt to gain same level of access as Alice.

Our spoofing detection technique assumes that Alice and Bob are in a process of establishing a connection and at least t messages have been exchanged where $t \geq 1$. After the first t messages, Bob receives subsequent messages from Alice and his goal is to now detect whether each subsequent message is indeed sent by Alice or a spoofing intruder.

B. System Model with Reconfigurable Antennas

Consider a point to point SISO link with the transmitter equipped with a single dipole antenna and the receiver equipped with a single pattern reconfigurable antenna. We assume that reconfigurable antenna at the receiver has $\mathcal{M}$ such unique modes and is capable of switching between $\mathcal{M}$ such modes. The degree of correlation between $\mathcal{M}$ channel realizations is governed by the physical structure of the reconfigurable antenna. For stationary terminals, the temporal channel variations are primarily caused due to shadowing and scattering by the moving scatterers in the vicinity of the link [14], [15], [16]. Under a narrow-band flat-fading setting, the channel $\hat{h}_i$ can be given as:

$$\hat{h}_i = X h_i + \epsilon + n \tag{1}$$

where i is the index of the mode of the reconfigurable antenna, X denotes the shadowing gain on the time invariant component h_i, ϵ is the additional small scale fading gain induced by the scatterers and n denotes receiver noise. ϵ and n can be modeled as a complex Gaussian process with 0 means and variances σ_ϵ^2 and σ_N^2 respectively. X is modeled as a random variable with a log-normal distribution with 0 mean and variance σ_S^2.

C. Channel Fingerprint & Feature Selection

To detect a spoofing attack, Bob monitors the channel fingerprint, which is a function of the estimated wireless channel encountered by each received message. The injection of messages by an unwanted intruder Eve posing as Alice will correspond to a shift in the channel statistics which will lead to an abrupt change in channel fingerprint. The collected channel fingerprints can be then used to make a decision about the true origin of the received message. We create a channel fingerprint by using the channel response corresponding to different modes of the receiver antenna at Bob. Using multiple channel responses, we create a channel fingerprint $\hat{h}$ given as:

$$\hat{h} = \left[|\hat{h}_1| \quad |\hat{h}_2| \quad .... \quad |\hat{h}_M| \right] \tag{2}$$

where $|\hat{h}_i|$ is the magnitude of the channel estimate of the ith mode of the antenna, $i = 1, .., M$ and M is the total number of available receiver antenna modes. Due to a rich multipath environment typically seen in indoor environments, the channel response for each transmit-receive path has a different distribution. Thus, augmenting the channel signature with multiple channel responses enhances the signature quality and makes it more challenging for an adversary to manipulate the channel between itself and the intended receiver. For GMM, the channel estimates for different modes create a rich M-dimensional feature set which allows the data to be separated in an higher dimensional space. We note that the features for the channel fingerprint can be chosen via other means such as channel estimates from different antennas in

MIMO setting or using frequency diversity by estimating channel using equally spaced pilot tones in frequency. For this work, we choose the pattern diversity offered by reconfigurable antennas to build our feature set for the channel fingerprint.

III. Detection Scheme and Gaussian Mixture Model

A. Spoofing Detection via Clustering

In order to motivate and explain the method of spoofing detection based on clustering achieved via GMM, we first provide some assumptions about the data consisting of channel fingerprints. Many signature based network intrusion detection schemes [9] work by building models of normal data and anomalous data using existing labeled data sets of both normal or anomalous behavior. Once the model is built offline, the detection process is run either offline or online to detect anomalies in the observed data. On the other hand, in anomaly detection techniques, only a model of normal data is created and deviation from the normal data in the observed data is detected. However, more often, we either do not have any labeled normal and anomalous training data or have access to only a small amount of purely normal data before the detection process can be applied to the observed data. In the case of our proposed physical layer authentication technique, we assume that we have access to only a few messages from the legitimate transmitter Alice to begin with and we have no messages from the intruder. We start by building a model based on the true messages from Alice and then detect deviations from it online as subsequent messages are received. After the initial t true message exchanges, detection schemes decides the true origin of the subsequent messages. Once the decision is made, the message is stored to update the learned model. Due to this online update, we can improve the accuracy of the learned model as more messages are received. Also, we later show that by reducing the number initial t messages, we can reduce the chances of spoofing during the establishment of the connection.

B. Gaussian Mixture Model for Model Learning

We use a Gaussian Mixture Model [17] to perform probability density estimation and calculate the posterior probability of each data point in the unlabeled data set. The data set consists of N data points and each data point is an M dimensional vector. M is the number of modes of the receiver antenna used to create the feature vector given by (2). We assume that the data is a mixture of k components and each component k generates data from a Gaussian distribution with mean μ_k and covariance Σ_k. The density of a single component k is then given as:

$$f_k(x) = \phi(x|\mu_k, \Sigma_k) \tag{3}$$

$$= \frac{1}{\sqrt{(2\pi)|\Sigma_k|}} exp\left(\frac{-(x-\mu_k)^t \Sigma_k^{-1}(x-\mu_k)}{2}\right) \tag{4}$$

The mixture density is given as the weighted sum of K component Gaussian densities where weight a_k for a component k is the prior probability of component k. Therefore, using (4) mixture density is given as:

$$f(x) = \sum_{k=1}^{K} a_k f_k(x) = \sum_{k=1}^{K} a_k \phi(x|\mu_k, \Sigma_k) \tag{5}$$

The parameters μ_k, Σ_k and a_k for the Gaussian Mixture Model are estimated by the maximum likelihood (ML) [18] criterion using the Expectation Maximization (EM) algorithm. The EM algorithm provides an iterative computation of the maximum likelihood estimation when the observed data is incomplete. During the expectation step, the posterior probabilities for each data point for all K components are computed as:

$$p_{i,k}^{(j)} = \frac{a_k^{(j)} \phi(x_i|\mu_k^{(j)}, \Sigma_k^{(j)})}{\Sigma_{k=1}^{K} a_k^{(j)} \phi(x_i|\mu_k^{(j)}, \Sigma_k^{(j)})} \tag{6}$$

Then, in the maximization step parameter values are updated as given below:

$$a_k^{(j+1)} = \frac{\sum_{i=1}^{n} p_{i,k}^{(j)}}{n} \quad , \quad \mu_k^{(j+1)} = \frac{\sum_{i=1}^{n} p_{i,k}^{(j)} x_i}{\sum_{i=1}^{n} p_{i,k}^{(j)}} \tag{7}$$

$$\Sigma_k^{(j+1)} = \frac{\sum_{i=1}^{n} p_{i,k}^{(j)} \left(x_i - \mu_k^{(j)}\right)\left(x_i - \mu_k^{(j)}\right)^T}{\Sigma_{i=1}^{n} p_{i,k}^{(j)}} \tag{8}$$

where j represent the j-th iteration. This iterative process is performed until the algorithm converges. Now, using the above method, data points are assigned to a cluster by selecting the component that maximizes the posterior probability. For the proposed spoofing detection scheme, Alice and Bob exchange initial training messages t and Bob stores the channel fingerprint vector $\hat{h}$ corresponding to each training message. We add the channel fingerprint of the incoming message into the dataset initialized by training messages and then the spoofing detector uses the mixture model to cluster the data into separate clusters corresponding to Alice and Eve respectively. The experiments use a GMM with mixture components $(K = 2)$ with the idea that one of the mixture components is associated with Alice, while other is associated with Eve.

Labeling Clusters: Since we are dealing with purely unlabeled data or have labeled data only from the initial training messages, it is necessary to find some way to determine which clusters obtained from mixture model contain normal instances and which contain attacks. Past research in unsupervised clustering techniques for intrusion or anomaly detection make some assumptions about the data in order to classify clusters. In [19], authors assume that normal instances constitute overwhelmingly large portion ($> 98\%$) of the data and therefore, the cluster containing the largest number of data points associated with it, is classfied as normal cluster. For a single link scenario, where data corresponding to each

transmitter is stored and treated separately this technique might be suitable. Instead, we rely on the training messages that we collected during initial training to classify the clusters. We note that for the purpose of GMM model learning, only unlabeled data is used. After the clusters are created using mixture model, we identify the cluster to which most data points from the training phase are associated and classify that cluster as normal. The other cluster is then classified as associated with the intruder.

IV. Experimental Setup

A. Indoor Channel Measurements

Channel measurements were conducted to evaluate the performance of the proposed scheme using a four port vector network analyzer (VNA) (Agilent N5230A) by measuring S_{21} between the transmitter and receivers [11]. Measurements were conducted in the Drexel Wireless Systems Laboratory (DWSL), a medium-sized lab with typical office and lab furniture. Transmitter, receiver, and intruder positions were chosen to accommodate LOS and NLOS links as shown in Fig. 3. Nodes at transmitter and intruder positions were equipped with omni-directional whip antennas and placed at desk level of approximately 0.75m.

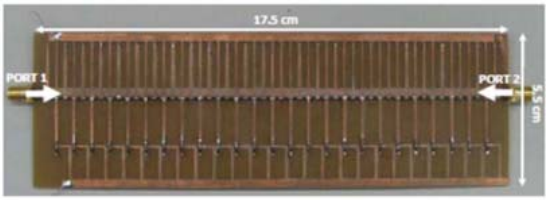

Fig. 1. Two port reconfigurable leaky wave antenna [20]

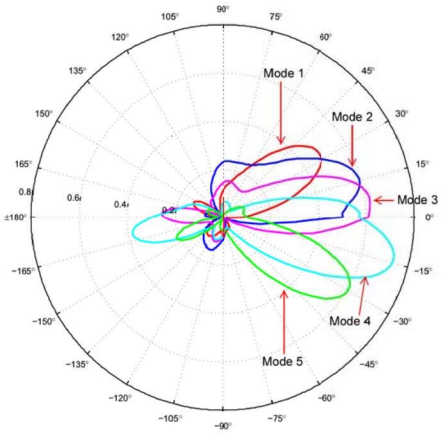

Fig. 2. Measured radiation patterns

A total of eight links were considered between the transmitter and receiver locations. Furthermore, for each of these links, ten distinct intruder locations were considered. Each receiver was equipped with a Reconfigurable Leaky Wave Antenna (RLWA) capable of electrically steering its beam pattern in different directions by applying varying levels of bias voltages to the varactor diodes on the antenna. Initially proposed by the authors in [20], the prototype shown in Fig. 1 is a two-port, composite right/left-handed leaky wave antenna composed of 25 cascaded metamaterial unit cells. Since, we are considering only a SISO link, we used channel measurements from only one of the ports. The five antenna modes chosen to steer the radiation pattern over an angular range from -45° to 45° in the elevation plane as shown in Fig. 2.

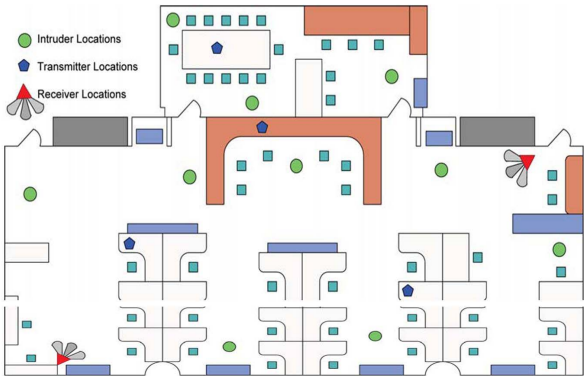

Fig. 3. 2D CAD model of test environment showing locations of receivers, transmitters and intruders

Frequency was swept over a 22 MHz bandwidth equally spaced into 64 frequency samples centered at 2.484GHz which corresponds to channel 14 of the 802.11 standard. For each receiver location, a pair of transmitter and intruder locations was selected to simultaneously transmit 200 samples for each of the five antenna modes for a total of 1000 samples.

V. Performance Analysis

To evaluate the performance of the proposed detection scheme, we use the receiver operating characteristics (ROC) curves. A point on the ROC curve is a pair of false alarm rate (FAR) and miss detection rate (MDR) calculated by applying the detection algorithm with a certain threshold. Even though our scheme does not rely on applying a threshold during operation, we can characterize the performance using the posterior probability $p_{i,k}$ given by (6) as our metric. At each step, when a new message i is received at the receiver, the posterior probability $p_{i,k}$ is compared against a threshold value and FAR and MDR are calculated. We perform this test for varying dimensions of the feature set used to create the channel fingerprint $\hat{h}$ and analyze the impact of using diversity to increase the fingerprint dimensions thereby analyzing detection performance. This procedure is repeated for all combinations of receiver, transmitter and intruder locations at a given frequency point from the channel measurements.

A. Feature Set Dimensions & Diversity

In Fig. 4, we show the ROC curve for the best performing combination of antenna modes for varying dimensions of the

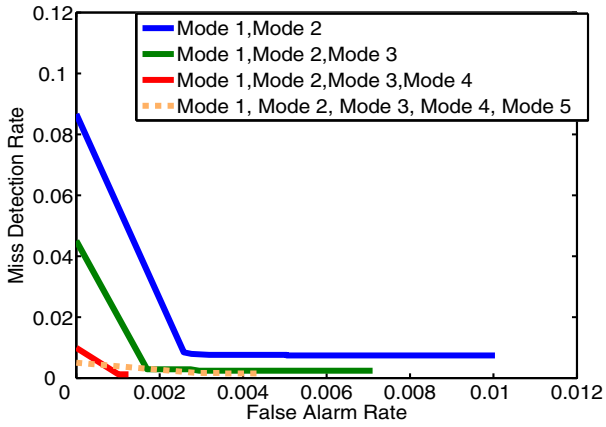

Fig. 4. ROC results for independent antenna modes at frequency 2.484 GHz averaged across all locations

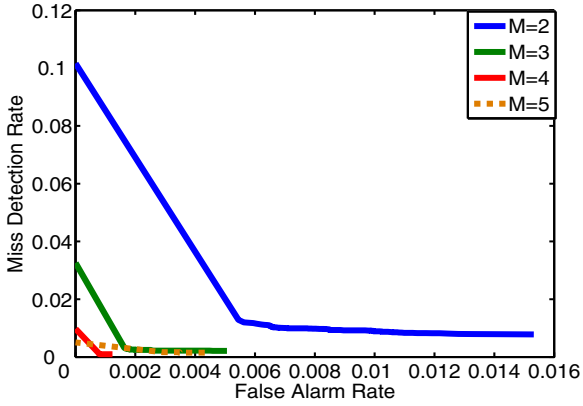

Fig. 5. ROC results for combination of independent antenna modes at frequency 2.484 GHz averaged across all locations

feature set used to create the channel fingerprint. As we increase the dimensions of the feature set, overall detection performance increases for a given false alarm rate. Using all five features (corresponding to five antennas modes), algorithm achieved MDR of 0.1% and FAR of 0.4%. It can also be observed that percentage improvement in performance, reduces as more modes are added. Moreover, using only two modes, mode 1 and mode 2 respectively, we acheived MDR of 0.8% and FAR of 0.3%. It is not required that adjacent modes are selected and system designer can select different modes base on pattern correlation properties [11]. Since we are exploting pattern diversity provided by reconfigurable antennas, it is essential that as we add more modes to create channel fingerprint, the inter-element correlation should be as low as possible. Since, the correlation between the selected features can impact on overall performance, we also show ROC curve for the average performance for all combinations of mode pairs in Fig. 5.

B. Transmission Frequency

We also analyze the effect of transmission frequency on the performance of the proposed detection scheme. As mentioned in section IV-A, the channel response corresponding to each antenna mode was measured over 64 evenly spaced frequency samples. The choice of transmission frequency in the 802.11 band can possibly effect the channel estimates due to relative interference in certain bands which can effect the performance of the detection scheme. In Fig. 6, we show the ROC curve for best performing combination of antenna modes averaged over all sampled frequencies over a bandwidth of 22MHz. We observe that using more than 3 antenna modes provides consistent performance for all frequencies with MDR$\leq 0.4\%$ and FAR of 0.9%.

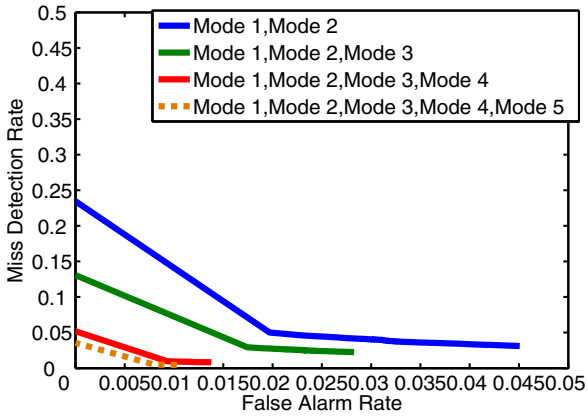

Fig. 6. ROC results for independent antenna modes averaged over bandwidth of 22MHz centered at 2.484 GHz

C. Attack Percentage

In Fig. 7, we analyze the impact of number of attack attempts on the performance of our detection scheme. The attack percentage is an important criteria as that highlights the strength of the model learning technique.

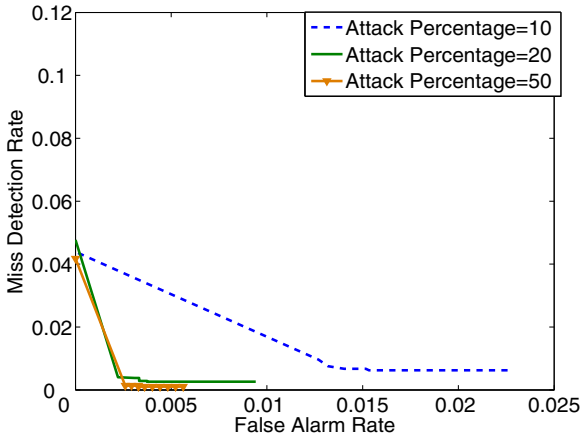

Fig. 7. ROC results for various size of test set containing observed samples from legitimate transmitter and intruder

In the scenario, where you have access to only a fraction of data from anomalous source, the model learning technique should be robust to still maintain required performance. We observe that as the attack percentage increases, the performance of the detection scheme improves. Also, with attack percentage of 20% and using three antenna modes, we acheived MDR of 0.4% for a false alarm rate of 0.2%.

D. Number of Training Messages

Finally, in Fig. 8, we analyze the impact of number of training messages t between the Alice and Bob used to initialize the GMM, on the detection performance.

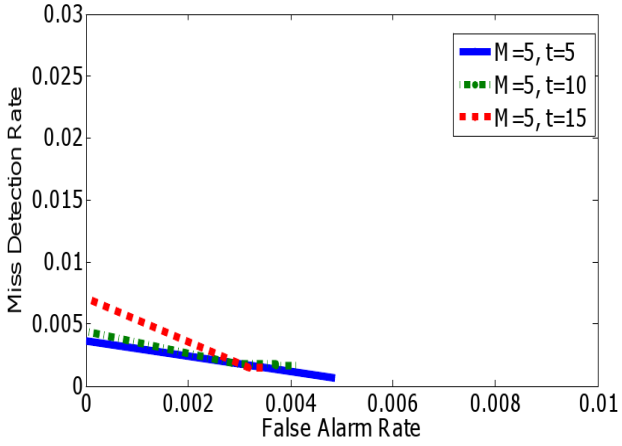

Fig. 8. Detection Performance with Minimum Training Messages

From implementation perspective, the number of samples in the dataset, required to initiate GMM, is lower bounded by the dimensionality of the feature set. For instance, for $M = 2$, $t \geq 2$. From Fig. 8, it can be seen that even with minimum training messages ($t = 5$ for $M = 5$), the proposed scheme achieved MDR of $.06\%$ and FDR of $.4\%$. Interestingly in this case, as t is increased, there is a marginal decrease in performance. This is primarily because the attack percentage is kept low at 10%.

VI. Conclusion and Future Work

In this paper, we proposed a semi-supervised clustering based approach using Gaussian Mixture Modeling (GMM) for physical layer authentication. We have shown that by using unlabeled data and only a few samples from the normal data our scheme can achieve very low false alarm rates and miss detection rates. Our results from measured channel responses from field tests in an indoor environment show that using pattern diversity coupled with proposed reduced training, detection scheme is feasible for real-world scenarios. We envision adapting this technique for mobile nodes and integration with higher layer security protocols as future work.

Acknowledgment

The authors wish to acknowledge Dr. Prathaban Mookiah for his valuable suggestions and feedback. This material is based upon work supported by the National Science Foundation under Grant No. 1028608.

References

[1] N. Patwari and S. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, 2007, pp. 111–122.

[2] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 7, pp. 2571–2579, 2008.

[3] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 12, pp. 5948–5956, 2009.

[4] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM Workshop on Wireless Security*, 2006, pp. 43–52.

[5] Y. Chen, W. Trappe, and R. Martin, "Detecting and localizing wireless spoofing attacks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, 2007, pp. 193–202.

[6] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 1768–1776.

[7] K. Sequeira and M. Zaki, "ADMIT: anomaly-based data mining for intrusions," in *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*, 2002, pp. 386–395.

[8] M. Otey, S. Parthasarathy, A. Ghoting, G. Li, S. Narravula, and D. Panda, "Towards NIC-based intrusion detection," in *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, 2003, pp. 723–728.

[9] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.

[10] P. Mookiah and K. Dandekar, "Enhancing wireless security through reconfigurable antennas," in *Radio and Wireless Symposium (RWS), 2010 IEEE*, 2010, pp. 593–596.

[11] P. Mookiah and K. R. Dandekar, "A reconfigurable antenna-based solution for stationary device authentication in wireless networks," 2012.

[12] A. Grau, H. Jafarkhani, and F. De Flaviis, "A reconfigurable multiple-input multiple-output communication system," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 5, pp. 1719–1733, 2008.

[13] R. Bahl, N. Gulati, K. R. Dandekar, and D. Jaggard, "Impact of pattern reconfigurable antennas on interference alignment over measured channels," in *Globecom Workshops (GC Wkshps), 2012 IEEE*. IEEE, 2012, pp. 557–562.

[14] J. Medbo, J. Berg, and F. Harrysson, "Temporal radio channel variations with stationary terminal," in *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, vol. 1, 2004, pp. 91–95.

[15] P. Pagani and P. Pajusco, "Characterization and modeling of temporal variations on an ultrawideband radio link," *Antennas and Propagation, IEEE Transactions on*, vol. 54, no. 11, pp. 3198–3206, 2006.

[16] C. Oestges, D. Vanhoenacker-Janvier, and B. Clerckx, "Channel characterization of indoor wireless personal area networks," *Antennas and Propagation, IEEE Transactions on*, vol. 54, no. 11, pp. 3143–3150, 2006.

[17] C. Bishop, *Pattern recognition and machine learning*, 2006, vol. 4.

[18] R. Redner and H. Walker, "Mixture densities, maximum likelihood and the em algorithm," *SIAM review*, pp. 195–239, 1984.

[19] L. Portnoy, E. Eskin, and S. Stolfo, "Intrusion detection with unlabeled data using clustering," in *In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001*. Citeseer, 2001.

[20] D. Piazza, D. Michele, and K. Dandekar, "Two port reconfigurable CRLH leaky wave antenna with improved impedance matching and beam tuning," in *Antennas and Propagation, 2009. EuCAP 2009. 3rd European Conference on*. IEEE, 2009, pp. 2046–2049.