International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 5, Number 1 (2013), pp. 19-29

http://www.irphouse.com

Non-Cryptography Authentication for Wireless Communications based on two Uncorrelated Attributes

Ahmed Refaey[1], Khaled Loukhaoukha[2] and Mohamed Haj-taieb[2]

[1]Dept. of Electrical and Computer Engineering, University of Western Ontario, London, ON, N6G5B9 Canada
e-mail: ahusse7@uwo.ca
[2]Dept. of Electrical and Computer Engineering, Université Laval, Québec, Canada
e-mail: khaled.loukhaoukha.1, mohamed.haj-taieb.1@ulaval.ca

Abstract

Recently in modern wireless systems, the physical-layer authentication has been proved to be a viable technique that can be combined with the higher-layer cryptographic to enhance the communication security. The existing physical-layer authentication schemes are single-variable based to verify transmitter's identity. In fact, these kind of techniques are not quite reliable as the obtained information based on one characteristic is relatively more vulnerable to various interferences. Herein, a novel two-variable cross-layer authentication scheme is proposed. In particular, the proposed scheme provides a novel solution to detect spoofing attacks based on the time of arrival (TOA) as well as the received channel power indicator (RCPI). The TOA and RCPI are considered as two featured sample variables. Consequently, the legality of the both variables are also validated and a decision rule is provided to accurately authenticate the transmitter's identity according to the two observed characteristics' information. Eventually, the proposed scheme shows an improved spoofing detection capability than the single-variable authentication can provide for the IEEE 802.11 WLANs. It is noteworthy that the proposed technique can be applied to any other wireless system standards.

1 Introduction

Due to the broadcast and open nature of the wireless communication systems

environment, more and more concern is focused on the security features of modern technology As a matter of fact, most of the existing wireless security techniques are mainly focused on processing techniques in the data or protocol domains to prevent potential security threats. It is noteworthy that, the existing higher-layer wireless security mechanisms are vulnerability to spoofing attacks [1]. Therefore, recently a new wireless security techniques exploiting the physical link properties provide additional protection for the communication process have been investigated exploiting physical-layer attributes in order to identify the transmitters.

Shannon in [8], discussed the definition of perfect secrecy in a pessimistic model without noise and verified that the physical-layer can provide secure wireless communications according to the information-theoretic security, following, Wyner in [15] introduced the concept of wiretap channel with noise which is used till the date. In addition, Csiszar in [16] explored that the existence of channel codes can guarantee a secure communication on a broadcast channel.

Recently many authentication schemes are proposed by exploitation of the properties of physical communication links to detect spoofing transmitters employing of hypothesis testing to formulate physical layer authentication [2, 3, 4]. In particular, most of these authentication schemes are based on single physical-layer related variable/attribute such as the properties of channel differences between two consecutive channel frequency responses (CFRs) in a time-variant channel [5, 6, 7]. In addition, the channel impulse response (CIR) is proposed to identify the transmitter identity in [9].Furthermore, in [11] and [12], two authentication schemes based on RSSI have been investigated, while the cooperation of additional nodes is required in order to extract the corresponding RSSI. Unfortunately, due to the mobility of channel the attributes will change in a dynamic range which leads to the single-variable based authentication is not reliable all the time. It is worth mentioning that, in the WLAN standards, the RSSI has been replaced with Received Channel Power Indicator (RCPI), which is the measurement of the received radio frequency (RF power) in a selected channel over the preamble and the entire received frame and it has defined absolute levels of accuracy and resolution.

Herein, we present a cross-layer authentication scheme in order to improve the the spoofing detection performance by means of the TOA and the RCPI. The leading superiority of these attribute that they are readily available or at least could be simply extracted in most of IEEE 802.11 based platforms.

On one hand, the RCPI is measured by the physical sublayer of the received RF power in the channel measured over the entire received frame of the IEEE 802.11 platform. On the other hand, TOA is a statistical quantity which can be obtained from the MAC layer. In fact, the two attributes can be easily accessed at the receiver. It is noteworthy that the proposed scheme requires no additional cooperated nodes compared with [11] and [12] although they offer enough information to uniquely identify the transmitter, and consequently introduce a better performance in detecting spoofing attacks over the single-variable based schemes. The main advantages of employing these two attributes together in the proposed authentication scheme is that the TOA and RCPI can be easily determined at receiver involved, in addition, the proposed scheme offers an enhanced reliability as it is beyond the bounds of

possibility for the adversary to emulate two uncorrelated and environment dependent attributes synchronically [17].

The rest of this paper is organized as follows: In Section II, the system model is provided whereas the TOA and RCPI are investigated as well as the decision rule. The validity of these attributes to be used in the authentication is discussed in Section III. The experiment setup and simulation results are shown in Section IV. Finally, in conclusions, the main results and contributions are summarized.

2 System Modeling

For theoretical analysis and numerical simulations in the proposed authentication scheme, an OFDM system is employed and the TOA as well as the RCPI are used for decision-making based on the likelihood ratio test under a binary hypothesis testing. In addition, the ubiquitous "Alice-Bob-Eve" scenario is used to explain the concept of authentication, where Alice, Bob and Eve are at different locations in space. Alice and Bob as the legitimate users, require secure communications, while the intruder Eve intends spoofing Bob. The objective of the proposed authentication is to detect the presence of spoofing attack. At the receiver side, the received packets, which in our scenario are transmitted by Alice, should be firstly analyzed to extract the corresponding information of TOA and RCPI respectively. The following subsections provide the detailed description on observing the TOA and the RCPI. Figure 1 shows the receiver side (Bob) which is periodically sample from the received packets transmitted by Alice or Eve. As described in the figure, the receiver process samples to obtain the information of corresponding variables then the authentication is conducted based on the acquired information.

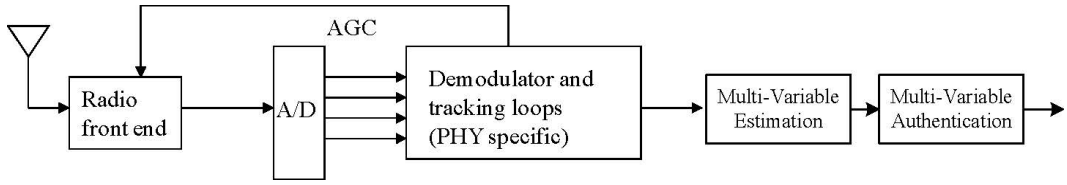

Figure 1: The system model of physical/lower layer authentication based on multiple variables associated with transmitter-receiver pair.

2.1 Time of Arrival-TOA

The time of arrival (TOA) estimations based on upper layer information is desired to make the implementation of WLANs more feasible with commercial WLAN devices in order to avoid the incompatibility issues of the PHY layer TOA estimations. The round trip time (RTT) based on the TOA techniques are usually employed for the upper layer TOA estimations. This is because the RTT based on TOA estimation does not require strict synchronization and it takes advantages of existing frame exchange sequences in IEEE 802.11 standards to perform the TOA estimations. Such frame exchanges are standard compatible and have been implemented by commercially

available WLAN devices. In some applications, nanosecond time resolution is needed to limit the distance measurement error to the scale of a few meters. However, neither the current IEEE 802.11 standards nor the existing WLAN network interface card chip-sets provide time stamps with the sufficient time resolution. In fact, the IEEE 802.11 standard only specifies the timing synchronization function with a resolution of $1\mu s$ that can be accessed for stamping frame transmissions and receptions $1\mu s$ corresponds to a distance of approximately 200 m, which usually exceeds the range of WLANs coverage and that will be appropriate for our scheme.

Now, denote τ as the true TOA value at which the frame arrives at the network interface card. Let τ_m signify the frame arrival time measured by WLAN network interface cards in the continuous time domain. The measured frame arrival time τ_{m} by network interface card is distributed as a Gaussian distribution with the width σ_τ and the mean τ. Therefore, the probability density function (PDF) of TOA measurement τ_m in the continuous time domain is

$$p\tau_m(\tau_m) = \frac{1}{\sqrt{2\pi}\sigma_\tau}\exp^{-}\frac{1}{2\sigma_\tau^2}(\tau_m - \tau)^2. \quad (1)$$

The continuous frame arrival time τ_m is then quantized with a quantization step $\Delta\tau = 1\mu s$ by assigning the closest discrete time stamp, t_i, to the frame arrival time. Whereas the t_i is the discrete time represented by the i^th time stamp bin of a finite set of discrete timestamps. Since there is no preference for frame arrival time, it is assumed to be uniformly distributed in the i^th discrete arrival time bin, $\left(t_i - \frac{\Delta\tau}{2}, t_i + \frac{\Delta\tau}{2}\right)$. As a consequence, the quantization error is uniformly distributed in the interval $\left(-\frac{\Delta\tau}{2}, \frac{\Delta\tau}{2}\right)$. As a result, the PDF of quantization error is a rectangular with a width of $\Delta\tau$ and height of $\frac{1}{\Delta\tau}$, centered at the origin.

2.2 received channel power indicator -RCPI

The RSSI is facing hard demands such as the high dynamic range of the signal due to the fast channel variation and the high detection speed required to settle the automatic gain control loops during short time window. As a matter of fact, for either the localization or the authentication problems, the RSSI method offers lower complexity and is widely used, however, it is highly influenced by multipath fading in indoor environments. In [13] and [14], the PDF of RSSI values have been precisely modeled by Gaussian PDF. Recently in the new 802.11 releases, the RSSI has been replaced with Received Channel Power Indicator (RCPI). The RCPI is an indication of the total channel power (signal, noise, and interference) of a received frame measured on the channel and at the antenna connector used to receive the frame. In particular, it is the measurement of the received radio frequency (RF) power in a selected channel over the preamble and the entire received frame and it has defined absolute levels of accuracy and resolution. This parameter is measured at the antenna connecter, particularly, is measured by the physical sublayer of the received RF power in the channel measured over the physical-layer convergence procedure preamble and over the entire received frame. The RCPI values fall into the range from 0 through 334

(octal) with indicated values rounded to the nearest 0.5 dB and accuracy of measurement of $+/-5$dB across the defined range, equivalent to accuracy specified by the TGH mechanism for RPI histogram [18].

2.3 Hypothesis Testing Model

The hypothesis testing is commonly used in physical-layer authentications. In the proposed scheme, the received packets which are transmitted by Alice should are analyzed to extract the corresponding information of each variable. Assuming that all variables are interfered by different white Gaussian noises; consequently, each variable the mean (μ_a) and the variance (σ_a) is estimated to determine the distribution of the Gaussian probability density function (PDF). The receiver calculate the corresponding mean (μ_e) and variance (σ_e) separately for each attribute [19]. In practice, Alice and Eve have different positions in the space and consequently the receiver will receive different values of TOA and RCPI from each of them. Also, even if both of Alice and Eve have the same position, which is consider as the worst case scenario, they still have different received RCPI values, following the fact that this attribute is channel dependent and therefore it will be defiantly different for each of them. Therefore, the corresponding offset is calculated as $\Delta\mu = \mu_a - \mu_e$.

The $\Delta\mu$, reï¬ecting the discrepancy of physical characteristics, is utilizable for further comparison in the multi-variable hypothesis testing to identify different transmitters. The hypothesis testing model can be summarized as follows:

$$\begin{cases} \mathcal{H}_0: & \mathbf{X}_{[i][j]} = \mathbf{W}_{[i][j]} \\ \mathcal{H}_1: & \mathbf{X}_{[i][j]} = \Delta\mu + \mathbf{W}'_{[i][j]} \end{cases}, \tag{2}$$

where,

$$\mathbf{X}_{[i][j]} = \begin{bmatrix} X_{[0][0]} & \cdots & X_{[0][N-1]} \\ X_{[1][0]} & \cdots & X_{[1][N-1]} \\ \vdots & \ddots & \vdots \\ X_{[n][0]} & \cdots & X_{[n][N-1]} \end{bmatrix}$$

indicates the information of n variables and each variable has N sampling data;

$$\mathbf{W}_{[i][j]} = \begin{bmatrix} W_{[0][0]} & \cdots & W_{[0][N-1]} \\ \vdots & \ddots & \vdots \\ W_{[n][0]} & \cdots & W_{[n][N-1]} \end{bmatrix}$$

and

$$\mathbf{W}'_{[i][j]} = \begin{bmatrix} W'_{[0][0]} & \cdots & W'_{[0][N-1]} \\ \vdots & \ddots & \vdots \\ W'_{[n][0]} & \cdots & W'_{[n][N-1]} \end{bmatrix}$$

are white Gaussian noises with zero mean and variance $\sigma_0^2 = [\sigma_{01}^2, \sigma_{02}^2, \cdots, \sigma_{0n}^2]^T$ and

$\sigma_1^2 = [\sigma_{11}^2, \sigma_{12}^2, \cdots, \sigma_{1n}^2]^T$ respectively. In addition, $\Delta\mu = [\Delta\mu_1, \Delta\mu_2, \cdots, \Delta\mu_n]^T$ implies the offset of each variable between Alice and Eve. Particularly, if the absolute value of $\Delta\mu$ is less than a predetermined threshold, then $\mathcal{H}_0$ is accepted, which claims the received data is sent from the legitimate transmitter (Alice); other than, is considered as received from the intruder (Eve).] The general likelihood ratio test (GLRT) is used to fulfill the authentication. In particular, under $\mathcal{H}_0$, the joint PDF for the m^{th} variable can be defined as

$$p_m(\mathbf{X}; \mathcal{H}_0) = \frac{1}{(2\pi\sigma_{0m}^2)^{\frac{N}{2}}} \exp[-\frac{1}{2\sigma_{0m}^2} \sum_{i=0}^{N-1} x_{[i]}^2], \quad (3)$$

where $x_{[i]}$ indicates the m^{th} row of $\mathbf{X}_{[i][j]}$. Additionally, under $\mathcal{H}_1$, the joint PDF for the m^{th} dimension is

$$p_m(\mathbf{X}; \boldsymbol{\Theta}_1, \mathcal{H}_1) = \frac{1}{(2\pi\sigma_{1m}^2)^{\frac{N}{2}}} \exp[-\frac{1}{2\sigma_{1m}^2} \sum_{i=0}^{N-1} (x_{[i]} - \Delta A_m)^2], \quad (4)$$

where $\boldsymbol{\Theta_1} = [\Delta\mu_m, \sigma_{1m}^2]$ is the unknown parameters in $\mathcal{H}_1$.

In general, the standard likelihood test is able to decide $\mathcal{H}_1$ if

$$L_{m(x)} = \frac{p_m(\mathbf{X}; \widehat{\boldsymbol{\Theta}}_1, \mathcal{H}_1)}{p_m(\mathbf{X}; \mathcal{H}_0)} > \gamma, \quad (5)$$

where $\widehat{\boldsymbol{\Theta}}_1 = [\Delta\hat{\mu}_m, \hat{\sigma}_{1m}^2]$, is the maximum likelihood estimation of $\boldsymbol{\Theta_1}$; and γ is the predetermined threshold.

3 decision rule

In this section the decision rule based on hypothesis testing is provided to accomplish the authentication based on the two proposed attributes, TOA and RCPI. Firstly, each attribute will take its decision separately [10]. Secondly, the decisions are combined together to form the final decision. That can be summarized as follows:

According to (3), (4), and (5), the specific GLRT for the m^{th} variable can be executed as

$$L_{m(x)} = \frac{\frac{1}{(2\pi\hat{\sigma}_{1m}^2)^{\frac{N}{2}}} \exp[-\frac{1}{2\hat{\sigma}_{1m}^2} \sum_{i=0}^{N-1} (x_{[i]} - \Delta\hat{\mu}_m)^2]}{\frac{1}{(2\pi\hat{\sigma}_{0m}^2)^{\frac{N}{2}}} \exp[-\frac{1}{2\hat{\sigma}_{0m}^2} \sum_{i=0}^{N-1} x_{[i]}^2]} > \gamma.$$

Substituting $\hat{\sigma}_{0m}^2 = \frac{1}{N} \sum_{i=0}^{N-1} x_{[i]}^2$ and $\hat{\sigma}_{1m}^2 = \sum_{i=0}^{N-1} (x_{[i]} - \Delta\hat{\mu}_m)^2$ and taking the logarithms to produce

$$\Delta\hat{\mu}_m^2 > \hat{\sigma}_{1m}^2 (\gamma^{\frac{2}{N}} - 1). \quad (6)$$

Correspondingly, the threshold $T_{[m]}, m = 1, 2$ is set as

$$T_{[m]} = \hat{\sigma}_{1m} \sqrt{|\gamma^{\frac{2}{N}} - 1|}, \quad (7)$$

Then the authentication is executed by comparing $|\Delta\hat{\mu}_m|$ with the corresponding threshold.

Hence, the probability of false alarm $P_{fa[m]}$, where $m = 1, 2$ for one of the two variables is calculated based on the corresponding threshold $T_{[m]}$ as

$$P_{fa[m]} = P(|\Delta\hat{\mu}_m| > T_{[m]}; \mathcal{H}_0)$$
$$= P(\Delta\hat{\mu}_m > T_{[m]}; \mathcal{H}_0) + P(\Delta\hat{\mu}_m < -T_{[m]}; \mathcal{H}_0). \quad (8)$$

Given that $\Delta\hat{\mu}_m \sim \mathcal{N}(0, \sigma_{0m}^2/N)$ under $\mathcal{H}_0$, the equation (8) will be expressed by the Q-function [1] to produce

$$P_{fa[m]} = 2\,Q\left(\frac{T_{[m]}\sqrt{N}}{\hat{\sigma}_{0m}}\right). \quad (9)$$

Therefore, the threshold $T_{[m]}$ is determined from $P_{fa[m]}$ by

$$T_{[m]} = \frac{\hat{\sigma}_{0m}}{\sqrt{N}} Q^{-1}\left(\frac{P_{fa[m]}}{2}\right), \quad (10)$$

where $Q^{-1}(x)$ is the inverse of the Q-function.

Additionally, (10) implies that the threshold $T_{[m]}$ is artificially adjusted by changing the value of $P_{fa[m]}$ when $\hat{\sigma}_{0m}$ and N is predetermined. In this case, considering that $\Delta\hat{\mu}_m \sim \mathcal{N}(\Delta\mu_m, \sigma_{1m}^2/N)$ under $\mathcal{H}_1$, the probability of detection $P_{d[m]}, m = 1, 2$ for each variable is

$$P_{d[m]} = P(|\Delta\hat{\mu}_m| > T_{[m]}; \mathcal{H}_1)$$
$$= Q\left(\frac{T_{[m]} - \Delta\hat{\mu}_m}{\sqrt{\hat{\sigma}_{1m}^2/N}}\right) + Q\left(\frac{T_{[m]} + \Delta\hat{\mu}_m}{\sqrt{\hat{\sigma}_{1m}^2/N}}\right)$$
$$= Q\left(\frac{\hat{\sigma}_{0m}}{\hat{\sigma}_{1m}} Q^{-1}\left(\frac{P_{fa[m]}}{2}\right) - \sqrt{\frac{N\Delta\hat{\mu}_m^2}{\hat{\sigma}_{1m}^2}}\right)$$
$$+ Q\left(\frac{\hat{\sigma}_{0m}}{\hat{\sigma}_{1m}} Q^{-1}\left(\frac{P_{fa[m]}}{2}\right) + \sqrt{\frac{N\Delta\hat{\mu}_m^2}{\hat{\sigma}_{1m}^2}}\right). \quad (11)$$

Consequently, the corresponding probability of miss detection $P_{m[m]}, m = 1, 2$ under $\mathcal{H}_1$ can be written as

$$P_{m[m]} = 1 - P_{d[m]}. \quad (12)$$

It is noteworthy that, in the decision rule the final decision is depend on the majority variables' judgment. Given that the two variables may make opposite decisions in the authentication scheme, the decision rule should take this condition into consideration. Particularly, if the number of variables who claim Alice (n_A) is larger than that who claim Eve (n_E), the final decision will treat Alice as the

---

[1] $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt.$

transmitter; otherwise, Eve will be claimed. Herein, if $n_A = n_E$, a conservative decision is taken that received data is transmitted by Eve. The probability of detection P_d is defined as

$$P_d = P_{d1}P_{d2} + (1 - P_{d1})P_{d2} + P_{d1}(1 - P_{d2}), \quad (13)$$

where P_{d1} and P_{d2} are the probability of detection for each variable.

Figure 2 shows the hypothesis testing theory for various number of N samples.

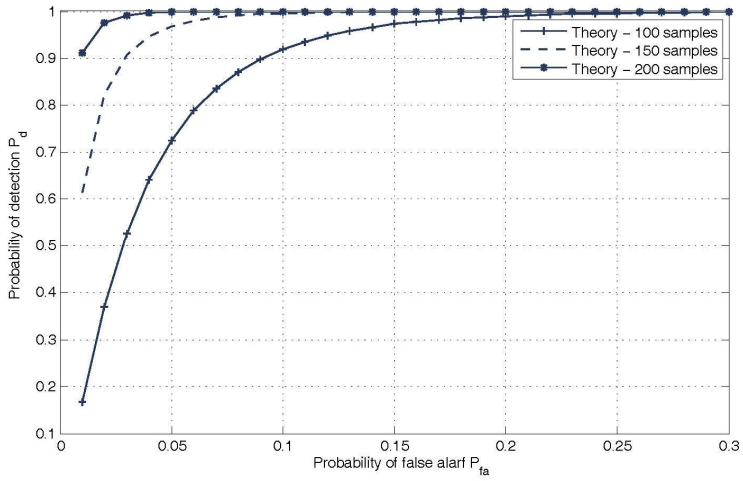

Figure 2: Probability of detection vs. effective probability of false alarm for various number of samples.

4 Experiment and Simulation Results

In this work, a basic system model is proposed to simulate the practical multi-variable authentication scheme. The proposed communication scenario consists of three nodes which are set as Alice, Bob and Eve. The node Bob, working as a receiver, which is periodically observe sample from the received packets transmitted by either Alice or Eve. After that, the receiver start to process the observed samples to obtain the information of corresponding variables. Eventually, the authentication is conduced at the receiver side based on the acquired information. Herein, an experiment is conducted in order to verify the validity of using the attributes TOA and PER in the proposed multi-variable authentication. The TX/RX nodes used in this experiment are IEEE 802.11b platforms working on 2.4 GHz. Note that, the TX power can be adjusted up to approximately 100 mW, while the data rate has the range of 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s.

In the conducted experiment, the intruder Eve is located in a different distance in the space than Alice, and this considered as the best case scenario to detect the intrusion as in this case both attribute the TOA as well as the RCPI would be different than the legitimate transmitter Alice. The worst scenario is also examined, where Eve is trying to establish a connection with BoB within the same distance as Alice located. In this case, the TOA will be almost the same, however, the RCPI will be still

different due to the variation in the channel conditions. For both cases, the TX power is set to be 23 mW and 45 mW, also the data rate is set to be 36 Mbit/s and 53 Mbit/s respectively.

4.1 Simulation and Results

In this subsection, we mainly present the processed simulation results of the obtained experimental data in order to verify the theoretical analysis presented in Section III. There are three considered aspects in order to better assess the performances; the probability of detection P_d, the probability of false alarm P_{fa}, and the number of samples N.

Among these aspects, the P_d implies the capability of detecting the intruder; the P_{fa} is a criterion to evaluate whether this kind of authentication is overly sensitive to result in making overmuch false alarm mistakes or not; N directly determines the time consuming aspect which affects the authentication's real-time performance and the practicability in future applications. Following are the simulation results of our proposed authentication scheme. It is noteworthy that all of the data used for simulation are derived from the conducted experiment using IEEE 802.11b platforms.

In Figure 3, the proposed authentication scheme is examined in terms of P_d vs P_{fa} with $N = 100, 150, 200$. A comparison is provided between the obtained experimental data and the theoretical simulations. The results confirm the effective of the proposed authentication scheme of considering the TOA as well as RCPI as two possible attributes to authenticate the legitimate transmitter. Also, as shown in the figure, increasing the number of samples leads to more accuracy in the detection capability. However, increasing the number of samples is time-consuming and consequently affect the latency of the decision operation. In is noteworthy that, the appropriate N should be selected according to the different application requirements in the authentications.

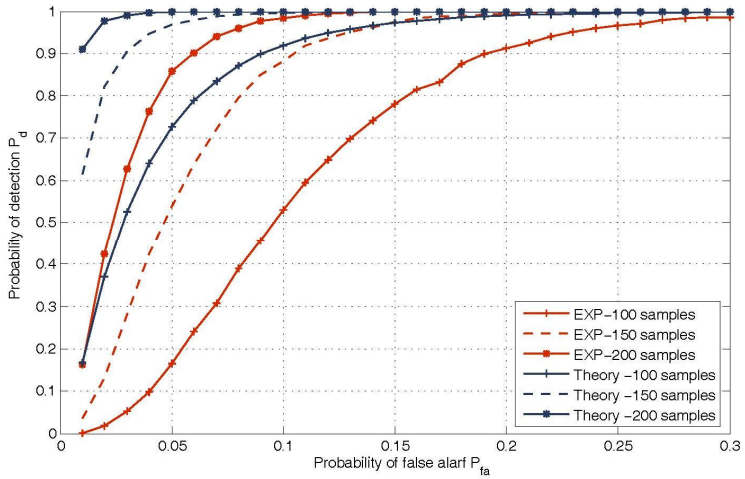

Figure 3: Probability of detection vs. probability of false alarm for $N = 100, 150, 200$.

5 Conclusions

In this paper, an enhanced cross-layer authentication scheme using two attributes, which are TOA and RCPI, is proposed. The TOA and RCPI are easy to obtain during the communication at the receiver side which makes the proposed authentication is desired in practice. In the decision rule, by comparing the differences of the different transmitters in each variable with the corresponding false alarm rate dependent threshold, each variable could roughly draw a conclusion that whether the received packets are from a legal transmitter or not. Then the accuracy of the final decision is significantly improved by combining the two variables together. The effectiveness of the proposed two-variable authentication is demonstrated by simulation with the experiment. All the data used in the simulation are derived from IEEE 802.11b platform, and the results show that it is more robust and efficient than the single-variable authentication in detecting spoofing attacks. Indeed the proposed scheme is examined on the IEEE 802.11 platforms, however, it can be employed for different wireless communication systems.

References

[1] M. Shin, J. Ma, A. Mishra, and W.A. Arbaugh "Wireless network security and interworking," *Proc. IEEE*, vol.94, pp. 455-466, Feb. 2006.

[2] P. Yu, J.S. Baras, B.M. Sadler, "Physical layer authentication," *IEEE Trans. on Inf. Forensics and Security*, vol.3, no. 1, pp. 38-51, Mar. 2008.

[3] P. Yu, J.S. Baras, B.M. Sadler, "Multicarrier authentication at the physical layer," *World of Wireless, Mobile and Multimedia Networks*, pp. 1-6, Aug. 2008.

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

[5] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, "Fingerprints in the ether: using the physical layer for wireless authentication," *Proc. IEEE Internationa Conference on Communications (ICC)*, pp. 4646-4651, Jul. 2007.

[6] F. He, H. Man, D. Kivanc and B. McNair, "EPSON: enhanced physical security in OFDM networks," *Proc. IEEE International Conference on Communications (ICC)*, pp. 1-5, Jun. 2009.

[7] S. Haykin, *Neural Networks and Learning Machines (Third Edition)*. Prentice Hall, 2008, ch. 3.

[8] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, 1949.

[9] J. K. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proc. IEEE International Conference on Communication systems and networks (COMSNETS)*, Mar. 2010, pp. 1-9.

[10] A. Mood, A. G. Franklin and C. B. Duane, *Introduction to the Theory of Statistics (Third Edition)*. McGraw-Hill, 1974.

[11] M. Demirbas, S. Youngwhan, "An RSSI-based scheme for sybil attack detection in wireless sensor networks, " *World of Wireless, Mobile and Multimedia Networks 2006*, pp. 43-52, Sept. 2006.

[12] S. Misra, A. Ghosh, A.P. Sagar, M.S. Obaidat, "Detection of Identity-Based Attacks in Wireless Sensor Networks Using Signalprints, " *Green Computing and Communications (GreenCom), 2010*, pp. 35-41, Dec. 2010.

[13] V. Seshadri, G.V. Zaruba, M. Huber, "A Bayesian sampling approach to in-door localization of wireless devices using received signal strength indication, " *Pervasive Computing and Communications, 2005*, pp. 75-84, Mar. 2005.

[14] K. Kaemarungsi, "Distribution of WLAN received signal strength indication for indoor location determination, " *Wireless Pervasive Computing, 2006*, pp. 6-11, Jan. 2006.

[15] A. Wyner, "The wire-tap channel, " *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[16] I. Csiszar and J. Korner, "Broadcast channels with confidential messages, " *IEEE Trans. Inf. Theory*, vol. 24, 1978.

[17] S. Rosati, G. E. Corazza and A. V. – Coralli, "OFDM channel estimation with optimal threshold-based selection of CIR samples, " in *Proc. IEEE Global Telecommunication Conference (GLOBECOM)*, 2009, pp. 1-7.

[18] N. Patwari, and S. K. Kasera, "Temporal link signature measurements for location distinction, " *IEEE Trans. on Mobile Computing*, vol. 10, no. 3, Mar. 2011.

[19] A. Papulis, *Probability, Random Variables, and Stochastic Processes (Third Edition)*. McGraw-Hill, 1991.