A Survey: Spoofing Attacks in Physical Layer Security

(Invited Paper)

Mustafa Harun Yılmaz[1], Hüseyin Arslan[1,2]
[1]Department of Electrical Engineering, University of South Florida, Tampa, Florida 33620
[2]School of Engineering and Natural Sciences, Istanbul Medipol University, Beykoz, İstanbul 34810
Email: myilmaz@mail.usf.edu, arslan@usf.edu

***Abstract*—Increasing demand on wireless communications also increases the issues related to communication security. Among different security solutions, physical layer security have recently been gaining many interests by the researchers. In this paper, a survey study is provided in one of the most critical attacks, namely spoofing attacks. When a legitimate transmitter stops sending a signal to a legitimate receiver, the spoofer starts to transmit a deceiving signal to the same legitimate receiver by acting as if it is the legitimate transmitter. The aim of the spoofer is to deceive the legitimate receiver. Within this concept, we first review the detection methods and countermeasures to spoofing attacks. To be able to evaluate the proposed techniques, we discuss different metrics provided in the literature. Then, we conclude the paper with the open issues.**

***Index Terms*—Spoofing attack, physical layer security.**

I. Introduction

Wireless devices have acquired an important place in human life due to providing numerous conveniences. Besides the benefits of these devices, their broadcast nature brings various wireless communication challenges in terms of security. To tackle the security issues, different solutions were provided in the literature. Most of the proposed techniques are based on cryptology which is performed in upper layers of the wireless communication systems. Since the encryption techniques increase the complexity with increasing the overhead of the systems [1], current trend shifts the researchers towards the security in physical layer.

Physical layer security studies can mainly be classified under three groups [2]. The first group of studies focuses on passive attacks such as eavesdropping. It refers to receiving/listening to the legitimate transmitted signal illegally. Since the eavesdropper is passive, i.e., not propagating a signal, the legitimate transmitter or receiver [1] cannot detect the eavesdropper. The second group of the studies is about the active attacks such as jamming. When a transmitter sends a signal to a receiver, a jammer transmits a jamming signal towards the receiver with the aim of disrupting the communication. Because of the jamming attack, the receiver cannot decode the legitimate transmitted signal. The third group of the studies is another active attack, spoofing. Spoofer transmits a signal to the receivers. The aim is to deceive the receivers. As seen in Fig.1, there can be two types of cases where the spoofing can be performed; a) when the transmitter stops transmitting the signal, the spoofer can start to transmit a deceiving signal to the receiver, and b) in the case of transmission phase between transceiver, the spoofer can transmit the deceiving signal with higher power to the receiver. So, the receiver would accept the spoofing signal as legitimate signal while it rejects the legitimate signal coming from the transmitter.

[1]The words 'transmitter and receiver' refer to legitimate transmitter and receiver throughout the paper.

In the literature, a few survey papers are written about physical layer security [3]–[5]. These studies examine the security for a specific application such as cognitive networks, smart grids. In this paper, we investigate the spoofing attacks studies for all application areas in physical layer. Thus, it is aimed to provide more comprehensive knowledge about the spoofing attacks. Additionally, we also explain the metrics utilized in the literature.

The remainder of the paper is organized as follows. In Section II, we mention what the security requirements are. We provide the literature survey and metrics used in studies in Section III and IV, respectively. In Section V, we draw the conclusion and present the open issues in spoofing attacks.

II. Security Requirements

Security in communication systems is a critical task to be fulfilled by the technology providers. In order to achieve a secure communication, the systems should satisfy some requirements [6] as listed below. It should be noted that these requirements are not necessary for only physical layer security, but security in communication systems in general.

1) Confidentiality: When a data is sent, it needs to be prevented from being disclosed to unauthorized users. Confidentiality is especially important against passive attackers such as eavesdroppers.

2) Integrity: The data is desired to be received by authorized users as it is transmitted. Any alteration should not be allowed to be performed by unauthorized users.

3) Availability: Availability refers to two things: 1) The data should be accessible and available to all authorized users when it is needed, and 2) The communication should be held continuously.

4) Authentication: When a data is sent, it needs to be confirmed that the data is coming from the legitimate user. Especially, when a receiver is aimed to be deceived by the attacker, this data should not be processed by the receiver.

978-1-4673-6773-8/15/$31.00 ©2015 IEEE

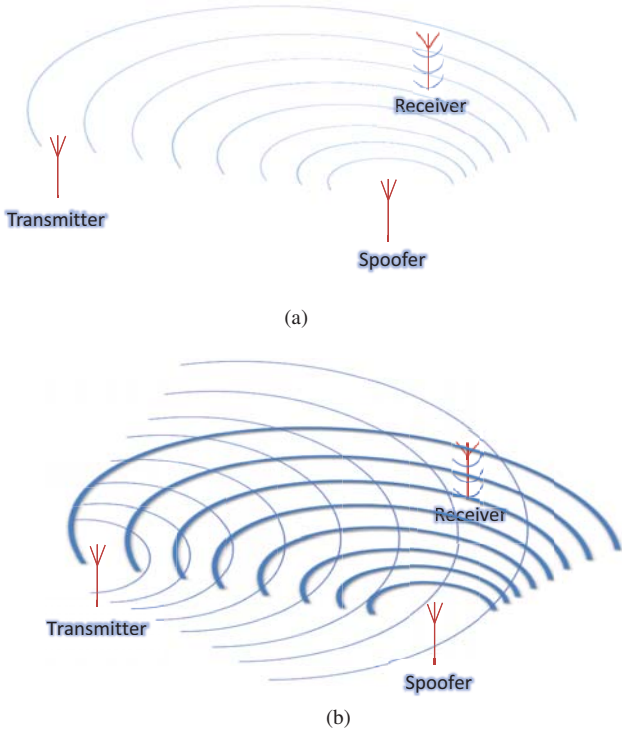

Fig. 1. In 1a, spoofer does not transmit a signal at the beginning. It only listens the legitimate transmitter. When the legitimate transmitter stops sending a signal to the legitimate receiver, spoofer starts sending the deceiving signal. Also, in the second type of spoofing attack (1b), when the legitimate transmitter is transmitting a signal to the legitimate receiver, the spoofer is also transmitting the deceiving signal with higher transmission power.

5) Non-repudiation: When the data is authenticated, it should be transmitted or received without being denied by legitimate users.

III. Studies in Physical Layer Security

Spoofing attack studies can be classified into two main categories; detection methods and countermeasures.

A. Detection Methods

1) Localization of Spoofing Attacks: In spoofing attacks, estimating the location of the attacker has received a lot of attention from researchers. In the literature, numerous localization techniques were proposed. Mainly, a few techniques are utilized to provide security against spoofers. Such techniques can be given as received signal strength (RSS), angle of arrival (AoA) and time difference of arrival (TDoA) based localization techniques.

(a) Received Signal Strength Based Localization: The open nature of wireless signals leads to transmitted signals being available at each receiver in the environment. The RSS of the transmitted signals is widely used in wireless communication systems for various purposes. By looking at the RSS of the transmitted signal, the receiver can obtain (or extract) some information about the transmitter. One critical information is said to be the location of the transmitter [7]. In physical layer security studies, spoofing attacks can also be detected or localized by utilizing the RSS measurements [1], [8], [9]. To locate the spoofers (or transmitters in general), multiple receivers (or anchors) work collaboratively, and measure the RSSs of the transmitted signals. Based on these RSS measurements, transmitters' locations can be estimated by utilizing the fingerprinting or propagation based schemes [9].

While RSS is utilized to locate the transmitters, it has some weaknesses. As given in [9], if the spoofer uses smart antenna to create beams with various beam widths and peak power in different directions, multiple receivers in different locations will measure the RSS of the spoofer wrongly. For instance, if a receiver which is close to the spoofer stands in the null of the spoofer beams, measured RSS level would be low. So, it will be assumed that the spoofer is far from this relevant receiver. With all RSS reports taken from all receivers, the spoofers' location would be estimated wrong. If there is a legitimate transmitter in the estimated location, the legitimate receiver will reject the signals coming from the legitimate transmitter and accept the ones coming from the spoofer.

There are many impairments which have an effect on RSS. Such effects can be given as path loss, transmit power level, antenna gain, shadowing etc. Mathematically, RSS is defined as

$$RSS(dB) = P_{\text{tx}} + \rho - PL \tag{1}$$

where P_{tx} is the transmit power, ρ is the antenna gain and PL is the path loss. As seen in (1), dependency on P_{tx} can weaken the RSS based spoofing localization. Since the spoofer can easily adjust the P_{tx}, it can manipulate the RSS readings on the receiver, which would cause the wrong location estimation [10].

(b) Angle of Arrival Based Localization: As the name implies, the angles of arriving signals are calculated to estimate the location of the transmitters in the AoA technique. When compared to RSS based localization, the AoA technique provides more accurate positioning [11]. In [12], this technique is utilized to locate the spoofers. Applicability of this technique depends on the number of antennas in the receiver which necessitates at least two antennas which increase the complexity and the cost of the receiver in terms of detection of the spoofing attacks [13]. When it is employed in an indoor environment, because of the intensive multipath components and non-line of sight (NLOS) communication, its accuracy degrades [14].

(c) Time Difference of Arrival Based Localization: When a transmitter sends a message, the arrival time difference of two consecutive pulses is utilized to find the location of the transmitter. When multiple receivers whose locations are known receive the pulses, they measure the time differences of the pulses. While the time synchronization is not needed in transmitter, it is important to have synchronization in the receivers to be able to measure the time difference correctly. Based on this measurement, transmitter's location can be estimated. When TDoA is calculated and the location is determined, a source-ID is assigned to this location estimation

[15]. If another message arrives at the receivers with different source-ID, the message is considered to be transmitted by a spoofer. Since the TDoA technique needs multiple receivers to compute the location of the transmitter, it will increase the complexity and the cost of the system as in AoA technique [16].

2) Channel Based Prevention Methods Against Spoofing Attacks: The channel is an important component in wireless communication systems. Since the channel has a uniqueness feature, it can be utilized to provide secure communication. In the literature, many studies consider the unique channel between legitimate transceiver to prevent the spoofing attacks [2], [17].

In channel based solutions, fingerprints or link signatures are utilized against the spoofing attacks. Such examples to link signatures can be given as amplitude, phase, multipath delay of the signals. Since the link signatures are obtained from the channel impulse response (CIR), the change on the transmitter's place would lead to the change on CIR, hence, also in the link signatures [18]. When the legitimate transmitter sends a message, the receiver performs the link estimation and assigns it as a reference link signature. Because of being in different location, the link signature of the spoofer would differ from the legitimate transmitter's one. When the spoofer's link signature is compared with reference, the receiver would decide that the signal is not transmitted from legitimate transmitter, and reject it. In [2], power delay profile (PDP) of the channel is derived to perform the spoofing attack identification. Since, the method is distance dependent, this dependency limits the applicability of the algorithm to certain areas. For instance, in health care domain, legitimate transmitter is usually closer to receiver than the attacker. If the attacker is closer to receiver or at the same place with the legitimate transmitter, the receiver might make a wrong decision or not be able to distinguish whether the message is coming from the attacker or legitimate transmitter. So, the algorithm might fail.

Most of the channel dependent security solutions are proposed when a transceiver is assumed to be static, i.e., mobility is not considered. If any of the transceivers is mobile, the proposed techniques would fail. To overcome this issue, in [19], authors provide a spoofing detection algorithm based on channel frequency response (CFR) statistics by considering the time variations which stems from the mobility of the transceiver. But, these studies are performed according to pedestrian speed, i.e., for the slowly varying channels. This solution might also fail when a high speed vehicle is in question.

It is worth mentioning that to be able to determine if the signal is coming from the legitimate transmitter or spoofer, the receiver performs the hypothesis testing in channel based solutions. The detailed explanation of the hypothesis testing in general can be seen in Section IV-A.

3) Game Theoretical Methods Against Spoofing Attacks: Game theory (GT) is a mathematical tool to manage selfish users who interact with each other. Players, strategies and utility function are three fundamental components required to be defined. Based on the utility function, each user (player) acts with its own strategy. The aim is to reach the Nash equilibrium (NE). When NE is reached, no player will intend to do unilateral deviation.

In physical layer security studies, GT is used to detect the spoofing attacks. In [20], Bayesian games are utilized to detect the spoofers probabilistically in the environment. It is assumed that there are two players in the game. Player 1 might be either a licensed user or spoofer (or emulator) and player 2 is a secondary user (SU). The utility (u(i)) of player *i* is based on the revenue *r* gained and cost *c* paid, i.e., $u(i) = r(i) - c(i)$. By utilizing the payoff matrix, the pure and mixed strategy equilibrium can be obtained with the dominance solvability method. When the NE is reached, the attacker would be detected. Similar to [21], in [22], a multistage game is proposed to detect the emulator. The players are defined as SU and the attacker (emulator). Attacker in this game does not transmit the spoofing signal continuously, instead, it acts intelligently and performs primary user emulation attack (PUEA) with some probability. As shown in the paper, mixed strategy NE is attained by the SU. However, in these solutions, when a mobility is considered, since it is difficult to reach the NE, proposed techniques might fail.

B. Countermeasures to Spoofing Attacks

Physical layer security studies against spoofing attacks are basically investigated in terms of detectability of such attacks as explained above. In a few papers, prevention methods are also studied. Providing a countermeasure to spoofing attacks is another critical step. Otherwise, as mentioned in Section III-A, the spoofer can utilize the drawbacks or weaknesses of the detection algorithms and continue deceiving the receiver. In the literature, countermeasures are mainly proposed based on encryption methods [23]. In terms of providing the security in physical layer, jamming and GT based prevention methods are proposed. In [24], authors protect the implantable medical devices (IMD) from the spoofing attacks. To fulfill this aim, they designed the new device called shield. Shield acts as a relay between the programmer and the IMD. One of the most important duties of shield is to protect the tranceived data against the attackers. It provides two types of security. When an IMD sends a report to the programmer about a patient, the shield jams this data to prevent it from being captured by eavesdroppers. Since, the shield knows the jamming signal, it can decode the transmitted data and forward it to the programmer. Secondly, when a spoofer sends a deceiving data to the IMD, the shield again jams this signal to preclude the IMD to be able to decode this deceiving data.

Another prevention method is proposed in wireless sensor networks (WSN). The power consumption is important to increase the sensors' life in WSN. Therefore, any proposed security techniques for the WSNs should not increase the battery usage. Security becomes more critical nowadays since WSN applications are deployed with an immense growth. In [25], a security technique against spoofing attacks is proposed in WSNs. Security is provided by the base station (BS) of the

WSN. Since the BS is the transmitter rather than the receiver as the case in most current solutions in the literature, and the sensors act as receivers all the time, the BS is assumed to have a capability of estimating the spoofing signals. When a spoofer is attacking, the BS will detect this attack and transmit a jamming signal to the environment. The aim of the BS is to disrupt the deceiving signal to make it undecodable by the sensors.

A GT based countermeasure is proposed in [26]. In cognitive radio networks, there are primary users (PU)s and SUs who are licensed and unlicensed users, respectively. When a SU is willing to employ the PU's band, it needs to perform spectrum sensing to determine the unoccupied or idle bands. If there is/are available band(s), then the SU can use it to transmit a signal. Since the PU has a priority to use the spectrum, SU should avoid the bands utilized by the PU. In terms of physical layer security, this naive cognitive structure can be exploited by the attackers. In the literature, there is a type of attack called PUEA. An attacker acts as PU to cause other SUs not to use the idle bands. In [26], PUEA is investigated in terms of corrupting the communication of SU. When a SU determines an unoccupied band by a PU, an attacker will act as a PU and prevent the communication of SU. For SU to get rid of this attack, it needs to jump to another channel to communicate. Authors utilize the random frequency hopping scheme to find available channels with some probability. They assume that, in this case, an attacker also needs to hop randomly. They do this study with known and unknown channel statistics in [26] and [27], respectively. However, as indicated in the paper, this solution method can only be applied when there are multiple available channels in the environment. For single channel case, this method would fail. In [28], similar method is used to defend the SU against PUEA.

IV. Metrics to Evaluate the Applicability of Solution Methods

In this section, we will provide the metrics used in the spoofing attack studies.

A. False Alarm & Miss Detection Rates

Hypothesis testing is a measure of the probability for a given hypothesis (or claim). This hypothesis may or may not be true. There are two types of hypotheses.

1) $\mathcal{H}_0$: Null hypothesis
2) $\mathcal{H}_1$: Alternative hypothesis

Two types of errors are defined to find the false alarm and miss detection.

1) *Type I Error*: $\mathcal{H}_1$ is decided, when in fact $\mathcal{H}_0$ is true. It can be named as false alarm, too.
2) *Type II Error*: $\mathcal{H}_0$ is decided, when in fact $\mathcal{H}_1$ is true. It can be named as miss detection,too.

The probability of false alarm, $P(\mathcal{H}_1|\mathcal{H}_0)$, and the probability of miss detection, $P(\mathcal{H}_0|\mathcal{H}_1)$, can be denoted as $\mathcal{P}_{FA}$ and $\mathcal{P}_{MD}$, respectively in detection theory. $\mathcal{P}_{FA}$ and $\mathcal{P}_{MD}$ are aimed to be reduced. If the system has high, for instance, $\mathcal{P}_{FA}$, this can lead to a vital mistake in the decision-making phase. In such a critical example, if a troop aims at estimating whether or not there is an enemy in a given field, the system can warn about the existence of enemy mistakenly, i.e., while there is no enemy, the system can respond as an enemy existence. Therefore, the troop can unintentionally reveal his place by means of surviving himself against the virtual enemy. While decreasing $\mathcal{P}_{FA}$ and $\mathcal{P}_{MD}$, on the contrary, another aim is to increase the probability of detection, $1 - P(\mathcal{H}_0|\mathcal{H}_1)$, which is denoted as $\mathcal{P}_D$.

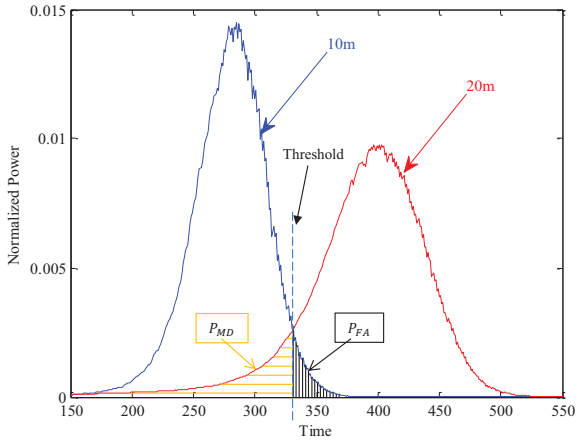

Fig. 2. Pictorial definition of $\mathcal{P}_{FA}$ and $\mathcal{P}_{MD}$ [2]

Pictorially, $\mathcal{P}_{FA}$ and $\mathcal{P}_{MD}$ can be seen in Fig. 2. The figure shows the power delay profile of a spoofer and a transmitter obtained in the receiver when they are 20m and 10m away from the receiver, respectively. If the aim is to detect the spoofer, the red curve shows the spoofer's detection probability, $\mathcal{P}_D$, which is the clear part of the red curve.

When the analysis is performed with unknown parameters, as introduced in [19], generalized likelihood ratio test which deals with the estimation of the parameters achieved by utilizing the maximum likelihood estimator type of equalizers can be employed in the system.

B. Receiver Operating Characteristics

Receiver operating characteristics (ROC) curves show the accuracy of the detected signal against false alarms according to some threshold shown in Fig. 2. ROC curves can sit to two different regions diminished by a diagonal dashed line as depicted in Fig. 3. When the ROC curve bows up towards 'good region', the receiver is said to have good detection performance. Contrarily, when the ROC curve bows up towards 'bad region', the receiver is said to have bad detection performance, i.e., the detection is failed.

It is important to have more bowed-up curve. That's, if the curve is more bowed up, then the accuracy of $\mathcal{P}_D$ increases. In other words, false alarm can occur in the higher $\mathcal{P}_D$. This can be obtained by measuring the area under the curve, $0 \leqslant area \leqslant 1$. For instance, as seen in Fig. 3, $\mathcal{P}_D$ would

be achieved with a higher accuracy for the transmitter who is 10m away from the receiver when compared to a spoofer who is 20m away from the receiver. In this case, the transmitter's signal will be separated from the spoofer's signal which will increase the detection performance.

C. Precision, Recall and F-Measure

The metrics defined above provide the relevant results when there is only one attacker in the environment. These metrics may not give sufficient enough information in the detection phase of the existence of multiple attackers. In order to estimate the multiple attackers, precision and recall metrics can be utilized. In information retrieval field, precision is defined as the ratio of the relevant data to data subset which is extracted from the whole data set. On the other hand, recall is the ratio of the relevant data in the data subset to relevant data in the whole data set. For instance, let's assume there are 7 red, 5 black balls in a box. When 4 balls are picked, if 3 balls are red, then the precision is said to be 3/4 while the recall is 3/7.

Mathematically, precision and recall measures can be defined with the false positive (FP), false negative (FN), and true positive (TP) parameters.

$$Precision = \frac{TP}{TP + FP}$$
$$Recall = \frac{TP}{TP + FN}$$

In these parameters, while true and false show the observation, positive and negative show the expectation. For instance, when the spoofer is attacking the receiver, if the receiver estimates that the signal is coming from the spoofer, it is said that the estimation is TP.

F-measure, or F-score, gives the accuracy of the measured (or estimated) data and defined as

$$F = 2\frac{Precision.Recall}{Precision + Recall}$$

V. Conclusion and Open Issues

Security in physical layer is a critical concept in wireless communications. Since the wireless signals are open and accessible in nature, it encourages the attackers in terms of eavesdropping, jamming or spoofing the legitimate communication. In this paper, we surveyed and reviewed one of the most significant attacks, the spoofing attack. Since the aim is to deceive the receiver, it becomes highly critical to detect these attacks. Otherwise, if the receiver does not detect the spoofers, the result might be vital or fatal such as in health care or military domain. On the other hand, as mentioned in Section III-A, each detection method has weaknesses. To overcome these weaknesses, countermeasures should be improved against spoofing attacks. So, detection and countermeasures together will provide very high level protection.

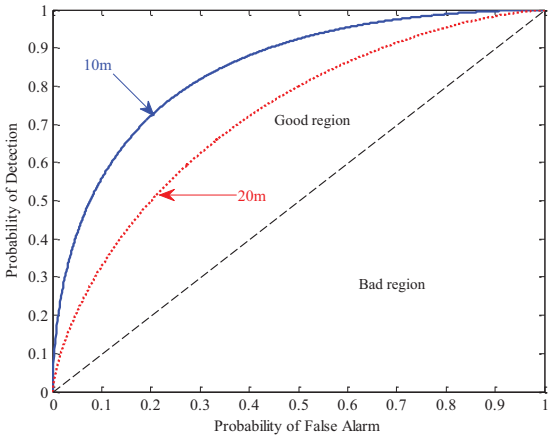

Fig. 3. Sample ROC curve based on the power delay profile of the legitimate transmitter and spoofer [2]

In the literature, some location algorithms are employed to detect the spoofing attacks. There are numerous localization techniques as seen in [29]. When multiple spoofers exist in the same environment, how to determine the number of attackers and their locations is an important further study. How accurate are the proposed localizations techniques in this case?

Multiple antennas are mainly used to increase the data rate in the wireless communication systems. In security studies, they are utilized to provide security. When the spoofing attacks are in question, they are primarily used to find the direction of the received signal for the positioning purpose. There are still more opportunities in multiple antenna usage. Countermeasure methods are open for the improvement as further study. Such an example can be given from health care domain. Since the frequency bands are very limited in medical services [30], to jam the spoofer with the aim of preventing such attacks can disrupt the other legitimate transceiver in the environment. To overcome this issue, the transmitter can create a beam to jam the spoofer while not harming the communication of other transceivers.

Studies about spoofing attacks are performed from the receiver side, i.e., the receiver spoofing is considered in general. To the best of authors' knowledge, no study considers the transmitter spoofing. For instance, one way of spoofing the transmitter is to send repeat request. If the spoofer aims to harm the communication without jamming, it can easily keep sending repeat request to the transmitter. Since, the transmitter would transmit the same signal, the communication would be disrupted. Especially, in military domain, if the eavesdropping of the military is not possible because of an implemented physical layer security method, the troops can be directed to the intended place of enemies in the battling area by causing that the same command is sent by the legitimate transmitter. Transmitter spoofing is another area for the future research.

In channel based approaches, solutions were mainly proposed with the assumption of the static users. Very few studies

consider the mobility which is for pedestrian speed. Since the channel has uniqueness feature, it is important to exploit this feature. In reality, while, for some cases, the users would be static, in some other cases, users would be mobile such as the users in aircraft or high speed vehicles. So, the security should also be provided in these fast varying channel conditions. This also needs further investigation.

REFERENCES

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

[2] M. Yilmaz and H. Arslan, "Impersonation attack identification for secure communication," in *IEEE Globecom Workshops (GC Wkshps)*, Dec 2013, pp. 1275–1279.

[3] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey," *Journal of Network and Computer Applications*, vol. 35, no. 6, p. 1691 Ű 1708, 2012.

[4] E.-K. Lee, M. Gerla, and S. Oh, "Physical layer security in wireless smart grid," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 46–52, August 2012.

[5] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2011.

[6] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, April 2011.

[7] E. Elnahrawy, X. Li, and R. Martin, "The limits of localization using signal strength: a comparative study," in *First Annual IEEE Sensor and Ad Hoc Communications and Networks Conf. (SECON)*, Oct 2004, pp. 406–414.

[8] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, pp. 44–58, Jan 2013.

[9] T. Wang and Y. Yang, "Analysis on perfect location spoofing attacks using beamforming," in *IEEE INFOCOM*, April 2013, pp. 2778–2786.

[10] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proceedings of the 2006 International Symp. on on World of Wireless, Mobile and Multimedia Networks*, ser. WOWMOM '06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 564–570.

[11] H.-C. Chen, T.-H. Lin, H. Kung, C.-K. Lin, and Y. Gwon, "Determining RF angle of arrival using COTS antenna arrays: A field evaluation," in *IEEE Military Communications Conf. (MILCOM)*, Oct 2012, pp. 1–6.

[12] J. Xiong and K. Jamieson, "Secureangle: Improving wireless security using angle-of-arrival information," in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, ser. Hotnets-IX, 2010, pp. 11:1–11:6.

[13] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *3rd IEEE Symp. on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Oct 2008, pp. 1–6.

[14] R. N. Zahid Farid and M. Ismail, "Recent advances in wireless indoor localization techniques and system," *Journal of Computer Networks and Communications*, vol. 2013, 2013.

[15] M. Wen, H. Li, Y.-f. Zheng, and K.-f. Chen, "TDOA-based sybil attack detection scheme for wireless sensor networks," *Journal of Shanghai University (English Edition)*, vol. 12, no. 1, pp. 66–70, 2008.

[16] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, pp. 25–37, Jan 2008.

[17] F. Liu, X. Wang, and S. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *IEEE International Conf. on Communications (ICC)*, June 2013, pp. 4724–4728.

[18] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *Proceedings of the 14th ACM International Conf. on Mobile Computing and Networking*, ser. MobiCom '08, 2008, pp. 26–37.

[19] L. Xiao, L. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 5948–5956, December 2009.

[20] R. Thomas, B. Borghetti, R. Komali, and P. Mahonen, "Understanding conditions that lead to emulation attacks in dynamic spectrum access," *IEEE Communications Magazine*, vol. 49, no. 3, pp. 32–37, March 2011.

[21] R. Thomas, R. Komali, B. Borghetti, and P. Mahonen, "A bayesian game analysis of emulation attacks in dynamic spectrum access networks," in *IEEE Symp. on New Frontiers in Dynamic Spectrum*, April 2010, pp. 1–11.

[22] Y. Tan, S. Sengupta, and K. Subbalakshmi, "Primary user emulation attack in dynamic spectrum access networks: a game-theoretic approach," *IET Communications*, vol. 6, no. 8, pp. 964–973, May 2012.

[23] K. Wang, M. Wu, P. Xia, S. Xie, W. Lu, and S. Shen, "A secure authentication scheme for integration of cellular networks and MANETs," in *International Conf. on Neural Networks and Signal Processing*, June 2008, pp. 315–319.

[24] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2–13, Aug. 2011.

[25] A. Bachorek, I. Martinovic, and J. Schmitt, "Enabling authentic transmissions in WSNs turning jamming against the attacker," in *4th Workshop on Secure Network Protocols (NPSec)*, Oct 2008, pp. 21–26.

[26] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics," *IEEE Trans. Wireless Commun.*, vol. 9, pp. 3566–3577, November 2010.

[27] ——, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems-part ii: Unknown channel statistics," *IEEE Trans. Wireless Commun.*, pp. 274–283, January 2011.

[28] D. Hao and K. Sakurai, "A differential game approach to mitigating primary user emulation attacks in cognitive radio networks," in *IEEE 26th International Conf. on Advanced Information Networking and Applications (AINA)*, March 2012, pp. 495–502.

[29] G. Sun, J. Chen, W. Guo, and K. Liu, "Signal processing techniques in network-aided positioning: A survey of state-of-the-art positioning designs," *IEEE Signal Processing Mag.*, vol. 22, no. 4, pp. 12–23, July 2005.

[30] [Online]. Available: http://www.fcc.gov/encyclopedia/medical-device-radiocommunications-service-medradio