MAC Spoofing Attack Detection based on EVM in 802.11 WLAN

Gaeil An and Shin-hyo Kim
Cyber Security Research Laboratory
Electronics and Telecommunications Research Institute (ETRI)
Dajeon, Korea
{fogone, shykim}@etri.re.kr

***Abstract*— Wireless LAN is very vulnerable to MAC spoofing attack. This paper proposes an Error Vector Magnitude (EVM)-based MAC spoofing attack detection scheme. The proposed scheme identifies wireless devices by using EVM as feature for distinguishing them. The proposed scheme can detect MAC spoofing attacks in real-time by using a prototype hardware system which has been developed in this paper to capture radio signal of wireless devices and extract EVM. Through experiment, we have confirmed that our scheme is excellent in detecting MAC spoofing attacks that employ wireless devices with different Wi-Fi chipset from legitimate one.**

Keywords-MAC spoofing attack; EVM; Error Vector Magnitude; Wireless device; WLAN

I. INTRODUCTION

As mobile devices have increased explosively with appearance of smartphone and performance of Wireless Local Area Network (WLAN) has been highly enhanced with realization of new technology such as channel bonding and Multiple-Input Multiple-Output (MIMO) in 802.11n, the importance of WLAN in wireless communication network is growing bigger and bigger. Currently, one of the greatest barriers that obstruct development of WLAN is problems with security. In WLAN, there exist a lot of security vulnerabilities such as eavesdropping, wireless spoofing, DoS, session hijacking, man-in-the-middle attacks, data modification, and so on. In this paper, we focus on security attack that spoofs MAC address of wireless device among many security threats that occur in WLAN. In this paper, a wireless device indicates a computer device with 802.11 WLAN card such as smart phone and Access Point (AP).

IEEE 802.11 implicitly trusts the MAC address of L2 frame and does not basically provide any mechanism for verifying it, just like IEEE 802.3 Ethernet. So, WLAN is very vulnerable to MAC spoofing attack, which can raise de-authentication, dis-association, power-saving, rogue AP, and rogue client attacks[1][2].

To react against MAC spoofing attack, various kinds of schemes have been proposed such as authentication, sequence number analysis, Received Signal Strength (RSS) fingerprinting, Radio Frequency (RF) fingerprinting, and so on. Authentication scheme is a way to defeat the attack by authenticating wireless devices or frames through cryptography [3]. Even if it is excellent in defeating MAC spoofing attack, it is not perfect solution because it is not a scheme for device authentication, but for user and message authentication.

Sequence number analysis scheme [4] detects the attack by checking consistency between the sequence numbers of L2 frames with the same MAC address. Even if it works well, it is known to be vulnerable to impersonation attack because it is a kind of software-based scheme. RSS fingerprinting scheme [5][6] distinguishes wireless devices by using Received Signal Strength Indication (RSSI). RSS fingerprinting scheme is based on a fact that the RSS pattern of a legitimate node is different from that of the spoofed one because their transmission power or location is different from each other. RSS fingerprinting scheme can effectively detect rogue AP, but not good at detecting rogue mobile client. Finally, RF fingerprinting scheme [7-10] is a way to identify a wireless device by using distinctive physical layer characteristics exhibited by the device. Even if RF fingerprinting scheme need hardware equipment to extract physical layer characteristics, its performance is known to be better than any other existing schemes.

This paper proposes an Error Vector Magnitude (EVM)-based MAC spoofing attack detection scheme, which is a kind of RF fingerprint scheme. The proposed scheme identifies a wireless device by using EVM as feature for distinguishing wireless devices. EVM is related to digital modulation error and defined as vector magnitude difference between an ideal reference signal and measured signal. The existing RF fingerprinting schemes are not real-time in that they collect feature information with the help of wireless measurement instrument such as Agilent. Our scheme has a capability that can detect MAC spoofing attack in real-time. For this, we have developed a prototype hardware system which can capture radio signal of wireless devices and extract EVM.

The rest of this paper is organized as follows. Section 2 introduces MAC spoofing attack in WLAN and the existing detection schemes. Section 3 describes our scheme, EVM-based MAC spoofing detection scheme. The performance of the proposed scheme is measured and evaluated in Section 4. Finally, conclusion is given in Section 5.

II. RELATED STUDY

Generally, attacker spoofs MAC address of wireless device to hide his or her presence or to use network resource illegally. MAC spoofing attack can be used to raise other attacks such as de-authentication attack, dis-association

 ISBN: 978-1-61208-289-9

attack, power-saving attack, Rogue AP, and rogue mobile device.

First of all, in IEEE 802.11 a client uses authentication message to authenticate itself to AP to join. De-authentication message is used to release authentication relationship between the connected nodes. Similarly, a client uses association message to setup a L2 link with a wireless node. Disassociation message is used to release the link between the associated nodes. De-authentication attack and disassociation attack can illegally terminate connections between legitimate nodes by using a spoofed de-authentication and disassociation message with MAC of victim node.

Power-saving attack makes use of device power conservation function. The device power conservation function allows clients to enter sleep mode for the purpose of battery conservation. The data sent to the client by other nodes is temporally stored into its AP. To check whether the data for the client is buffered by its AP, the client periodically wakes up from sleep mode and receives a traffic indication map (TIM) from its AP. If through the TIM the client gets known that its AP buffers its data, it sends its AP a poll message to receive its data. Power-saving attack is used to prevent clients from communicating normally with their APs. For example, power-saving attacker can send a spoofed poll message to remove the buffered data or a spoofed TIM message to prevent a client from receiving its data from its AP.

Rogue AP attack is one that lures clients into connecting to a fake AP instead of a legitimate one by spoofing MAC and SSID of legitimate one. Finally, rogue client attack is one that spoofs the MAC of a legitimate mobile device to bypass an MAC address-based access control system. Through this attack, rogue client can gain illegally access to a WLAN.

To protect WLAN from such MAC spoofing-based security threat, various kinds of schemes have been proposed such as authentication scheme, sequence number analysis, RSS fingerprinting, and RF fingerprinting. First of all, authentication scheme provides IEEE 802.11i and 802.11w as a way that authenticates wireless devices or L2 frames. The standard IEEE 802.11i is designed to provide secure communication based on cryptography in WLAN. The standard 802.11w is designed to provide cryptographic protection to IEEE 802.11 management frames such as de-authentication and disassociation. Even if authentication scheme is very excellent in defeating MAC spoofing attack, it is not perfect solution because it is not a scheme for device authentication, but for user and message authentication.

Secondly, sequence number analysis scheme is based on a fact that there is no consistency between the sequence numbers of L2 frames from the legitimate device and those from the spoofed device with the MAC of the legitimate one. If sequence number analysis system finds that there is a jump in the sequence number of the received frame, it regards the transmitter of the frame as a MAC spoofing device. Even if sequence number analysis scheme works well, it is vulnerable to impersonation attack because it is a kind of software-based scheme.

RSS fingerprinting scheme distinguishes wireless device by using RSSI. RSSI is correlated with transmission power, distance between transmitter and receiver, and radio environment that raises multipath and absorption effects. RSS fingerprinting scheme detects MAC spoofing devices by making use of a fact that the RSS pattern of a legitimate node is different from that of a spoofed one because their transmission power or location is different from each other. RSS fingerprinting scheme has a merit that it can exactly detect MAC spoofing attack performed by fixed wireless devices such as AP. But, its performance is not good at detecting MAC spoofing attack performed by mobile devices.

Finally, RF fingerprint scheme is a way to identify a wireless device by using distinctive physical layer characteristics exhibited by the device, such as modulation error or radio signal pattern. Our scheme belongs to RF fingerprint scheme. RF fingerprint scheme is expensive because it requires hardware equipment that can capture radio signal and extract RF feature. However, RF fingerprint scheme has been known as one that can detect MAC spoofing attacks most accurately among the existing ones. According to [7] and [8], the accuracy of RF fingerprinting in wireless device identification is more than 99%.

III. EVM-BASED MAC SPOOFING ATTACK DETECTION

A. Background

To detect MAC spoofing attack, we should be able to identify a wireless device. The scheme proposed in this paper identifies a wireless device by using digital modulation error which is distinctive physical layer characteristics exhibited by the device.

To transfer messages over wireless network, a transmitter should perform digital modulation. Digital modulation is to transfer digital bit streams over analog channel. The number of data bits to encode is determined by each modulation scheme. For example, Quadrature Phase Shift Keying (QPSK) encodes two bits using a symbol, 8-state quadrature amplitude modulation (8-QAM) does three bits, and 16-QAM does four bits. When digital modulation is performed, there exists a slight error because of manufacturing imperfections.

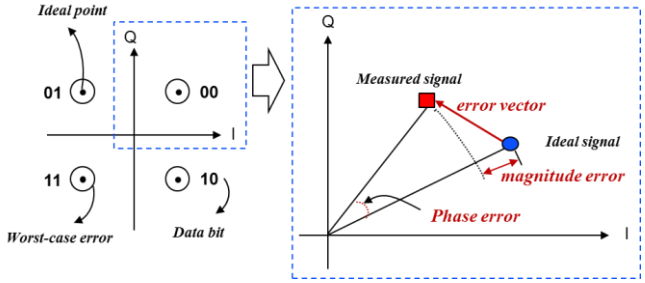


Figure 1. Modulation Error in QPSK.

Fig. 1 shows digital modulation error in QPSK. QPSK can send two bits of digital information at a time. In QPSK, data is encoded using two independent carrier components, in-phase (I) and quadrature phase (Q). The carrier

components are separated in phase by π /2. If data is sent by transmitter using digital modulation, the signal measured in the receiver should be mapped to the ideal point as shown in Fig. 1. However, the measured signal does not match with ideal point because of various reasons such as hardware impairments, channel characteristics, and noise at the receiver. Modulation error becomes the most important element for identifying wireless devices because wireless transceivers made not only by different manufacturer, but also even by same manufacturer have different values. To quantify the performance of a digital radio transmitter or a receiver, it is can be used several metrics such as EVM, magnitude error, phase error, as shown in Fig. 1. In this paper, we use EVM as a feature for distinguishing wireless devices. EVM is vector magnitude difference between an ideal reference signal and measured signal.

B. *Architecture and Algorithm*

Fig. 2 shows architecture for MAC spoofing attack detection proposed in this paper. The architecture includes four components: signal acquisition, EVM extraction, training, and MAC spoofing detection.

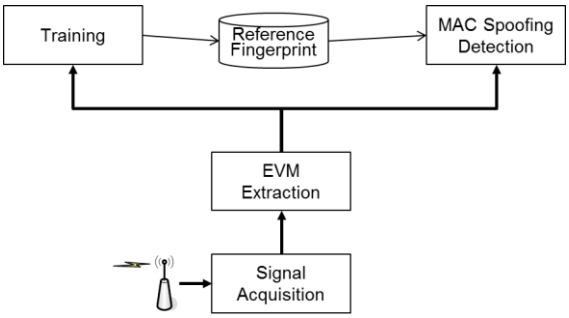


Figure 2. Architecture for MAC spoofing attack detection.

The signal acquisition is a hardware component. It monitors WLAN and captures the radio signal of wireless devices. The EVM extraction component has a responsibility for extracting EVM and MAC address from the radio signal. The training component is performed before the MAC spoofing detection module starts. It measures EVM values for authorized wireless devices and stores them into the reference fingerprint DB. Finally, MAC spoofing detection component accepts or rejects newly detected devices by comparing the measured EVM and the reference EVM.

$$d_1(x) = \sum_{i=1}^{k_1} \frac{ed\left(x - NN_i(x)\right)}{k_1} \quad (1)$$

$$d_2(x) = \sum_{i=1}^{k_1} \sum_{j=1}^{k_2} \frac{ed\left(NN_i(x) - NN_j(NN_i(x))\right)}{k_1 \cdot k_2} \quad (2)$$

In this paper, we employ K-NNDD (K-Nearest Neighbor Data Description) [11] as an algorithm for training EVM for authorized wireless devices and for comparing the measured EVM and the reference EVM. K-NNDD has been proposed to solve one-class classification. In this paper, K-NNDD is used to decide whether a new device is authorized one or attacking one with spoofed MAC address because it can calculate distance between the measured fingerprint and the reference fingerprint.

K-NNDD is explained through (1) and (2). The distance between the measured fingerprint and the reference fingerprint is calculated by (1). The distance between the reference fingerprints is calculated by (2). If the distance calculated by (1) is less than the distance calculated by (2), the measured fingerprint is regarded as the same one as the reference fingerprint. In (1) and (2), *ed* means Euclidean distance. $NN_i(x)$ is the i^{th} nearest reference EVM value to the measured one, x. K_1 indicates the number of reference EVM values to be compared with the measured EVM value. K_2 indicates the number of reference EVM values to be compared with each of K_1-number of reference EVM values. In (1), $d_1(x)$ means average distance between the measured EVM and its nearest reference EVM fingerprints. In (2), $d_2(x)$ means average distance between the reference EVM fingerprints selected in (1) and their nearest reference EVM fingerprints. If ($d_1(x)$ / $d_2(x)$) is greater than a threshold, then our scheme regards the wireless device with the EVM value x as one with a spoofed MAC address because the distance between the measured EVM and the reference EVM is farther than the distance between the reference EVM values. Typically, the value of the threshold in K-NNDD is set to 1.

IV. PERFORMANCE EVALUATION

A. *Experimental environment*

We have implemented a prototype system called a MAC spoofing detection sensor which provides EVM-based MAC spoofing attack detection.

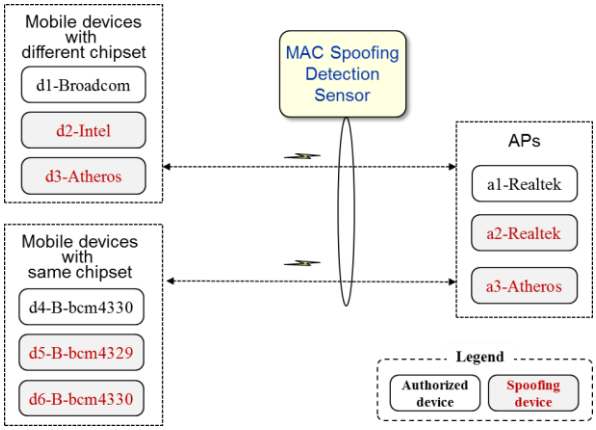


Figure 3. Experimental network.

The sensor consists of Athoros 9380 wireless LAN chipset, Intel atom CPU, 4GB memory, PoE, and so on. The Athoros chipset in the proposed sensor monitors WLAN and captures the radio signal of wireless devices. To extract EVM and MAC address from the radio signal, we have

modified a WLAN device driver called compat-driver. In our scheme, the training and the MAC spoofing detection components have been implemented as application software. The extracted EVM values include abnormal ones. So, the training and the MAC spoofing detection components choose the best 15 EVM values among the received 20 ones.

Fig. 3 shows an experimental network for measuring and evaluating the performance of the proposed scheme. The experimental network consists of a MAC spoofing detection sensor, mobile devices with different Wi-Fi chipset, mobile devices with same Wi-Fi chipset, and APs. As mobile devices with different chipset, d1-Broadcom, d2-Intel, d3-Atheros each indicates a smart-phone with Broadcom chipset, a laptop computer with Intel chipset, and a laptop computer with Atheros chipset, respectively. As mobile devices with same chipset, d4-B-bcm4330 and d6-B-bcm4330 are smart-phone (iphone-4s) with Broadcom's BCM 4330 chipset. The d5-B-bcm4329 means smart-phone (iphone-4) with Broadcom's BCM 4329 chipset. As AP, a1-Realtec and a2-Realtec both are ipTIME AP with Realtek RTL8198. The a3-Atherros means Netgear AP with Atheros AR7161. The APs stay away from each other about 1m. In Fig. 3, white box and gray box mean authorized wireless device and MAC spoofing device, respectively.

B. *Experiment Results*

The experiment results of the proposed scheme are described in Fig. 4, 5, and 6. In Fig. 4 and 5, x axis indicates a device identification execution number and y axis indicate distance/dissimilarity between the measured EVM for a device and its reference EVM.

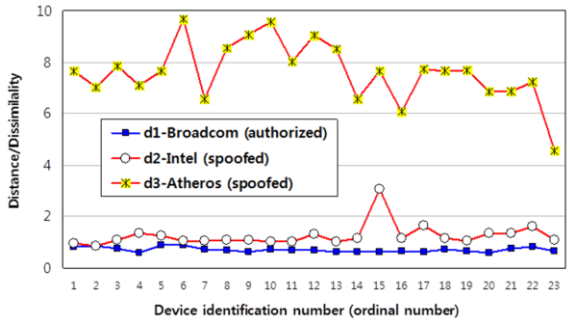


Figure 4. Performance of MAC spoofing attack detection against mobile devices with different Wi-Fi chipset.

Fig. 4 shows the performance of MAC spoofing attack detection against mobile devices with different Wi-Fi chipset. In Fig. 4, d1-Broadcom (device with Broadcom chipset) is an authorized device and its EVM fingerprint is trained and stored into DB before the MAC spoofing detection operation is started. The d2-Intel and the d3-Atheros both are attacking devices that spoof the MAC address of d1-Broadcom.

In the average distance ($d_1(x)$ / $d_2(x)$) between the measured EVM and the reference EVM, d1-Broadcom, d2-Intel, and d3-Atheros are about 0.7, 1.3 and 7.6, respectively, as shown in Fig. 4. This indicates that the wireless devices with different Wi-Fi chipset have different values in EVM. When we set the threshold for deciding between the authorized device and the spoofed device to 1, our scheme decides d1-Broadcom as authorized one, and d2-Intel and d3-Atheros as attacking one with spoofed MAC. Therefore, Fig. 4 means that the proposed scheme can almost perfectly detect MAC spoofing attack in case that attacker employs wireless devices with different Wi-Fi chipset from that of the authorized device. In Fig. 4, False Accept Rate (FAR) is 4.35% and False Reject Rate (FRR) is 0.0%. EER (Equal Error Rate) is 1.09 % (when threshold = 0.93). The 'false accept' means that the system mistakes device with spoofed MAC as authorized one. On the contrary, the 'false reject' means that mistakes authorized device as one with spoofed MAC. EER indicates the value where FAR and FRR are equal.

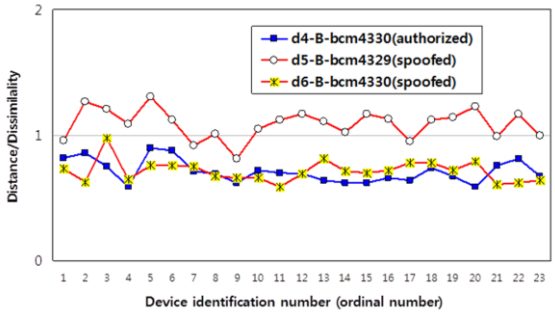


Figure 5. Performance of MAC spoofing attack detection against mobile devices with same Wi-Fi chipset.

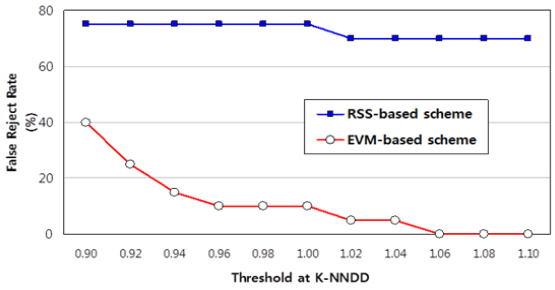
Fig. 5 shows the performance of our MAC spoofing attack detection against mobile devices with same Wi-Fi chipset. In Figure 5, d4-B-bcm4330 is authorized device. D5-B-bcm4329 and d6-B-bcm4330 both are ones with spoofed MAC address. The average distances in d4-B-bcm4330, d5-B-bcm4329, and d6-B-bcm4330 are about 0.7, 1.1 and 0.7, respectively, as shown Fig. 5. Fig. 5 indicates that even if our scheme is not bad in case that attacker employs device with same chipset but different model (i.e., d5-B-bcm4329), it has great difficulty in detecting attack devices with same chipset and same model (i.e., d6-B-bcm4330). In Fig. 5, FAR is 63.04% and FRR is 0.0%. EER is 31.52% (when threshold = 0.74).

Fig. 6 shows the performance of our detection scheme against rogue AP that spoofs MAC address. In this experiment, our scheme (i.e., EVM-based scheme) is compared with RSS-based scheme. RSS-based scheme is commonly used to detect rogue APs because it is comparatively easy to measure RSSI on WLAN and APs that are located in different place have different RSSI values. In Fig. 6, x axis indicates threshold value at K-NNDD algorithm and y axis indicates the error rate of MAC spoofing detection schemes.

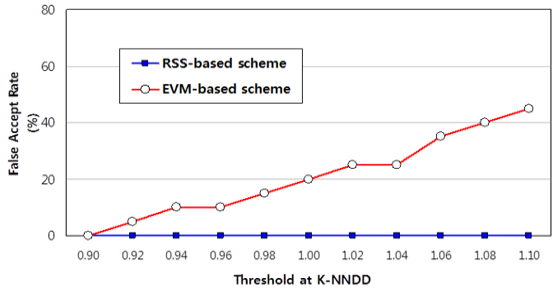
Fig. 6-(a), (b), and (c) shows FRR of two detection schemes against the authorized AP (a1-Realtec), FAR of them against the spoofed AP with same Wi-Fi chipset (a2-Realtec), and FAR of them against the spoofed AP with different Wi-Fi chipset (a3-atheros), respectively. In Fig. 6-(a), our scheme is much better than RSS-based scheme in terms of FRR. When the threshold is set to 1.0, FAR of our

 ISBN: 978-1-61208-289-9

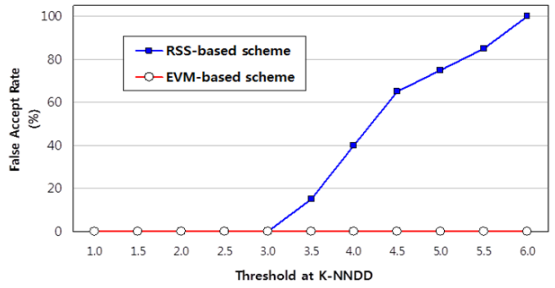
scheme is 10% while that of RSS-based scheme is 75%. We think that this happens because RSSI is more sensitive to radio frequency interference than EVM.



(a) Against the authorized AP (a1-Realtec)



(b) Against the spoofing AP with same Wi-Fi chipset (a2-Realtec)



(c) Against the spoofing AP with different Wi-Fi chipset (a3-atheros)

Figure 6. Performance of the spoofing AP detection by RSS-based and EVM-based scheme.

In case of FAR of the detection schemes against the spoofing AP with same Wi-Fi chipset, RSS-based scheme is better than our scheme, as shown in Fig. 6-(b). As mentioned above, our scheme is not good in detecting device that spoofs MAC address using same Wi-Fi chipset. However, the performance between our scheme and RSS-based scheme does not make big difference. When the threshold is set to 1.0, FAR of our scheme is 20% while that of RSS-based scheme is 0%. In Fig. 6-(c), our scheme is better than RSS-based scheme in terms of FAR against spoofing AP with different Wi-Fi chipset. As mentioned above, this is because our scheme is very good in detecting device that spoofs MAC address using different Wi-Fi chipset.

V. CONCULSION AND FUTURE WORK

In this paper, we have proposed an EVM-based MAC spoofing attack detection scheme. The proposed scheme belongs to RF fingerprinting one. To measure and evaluate the performance of the proposed scheme, we have developed a prototype hardware system. The experiment results prove that our scheme is excellent in detecting MAC spoofing attack that employs a wireless device with different Wi-Fi chipset from that of legitimate one. However our scheme is not good in case that attacker employs a wireless device with same Wi-Fi chipset as that of legitimate one.

Our future work is to add new other features besides EVM to enhance the performance of the proposed scheme as highly as it can detect the sophisticated attacks using a wireless device with same Wi-Fi chipset from that of legitimate one. Another future work is to construct a large-scale of experiment environment that consists of lots of and various kinds of wireless devices to verify and refine the proposed scheme.

ACKNOWLEDGMENT

This research was funded by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013.

REFERENCES

[1] G. Lackner, U. Payer, and P. Teufl, "Combating Wireless LAN MAC-layer Address Spoofing with Fingerprinting Methods," International Journal of Network Security,Vol.9, No.2,pp.164-172, Sept. 2009.

[2] B. Danev, D. Zanetti, and S. Capkun, "On Physical-Layer Identification of Wireless Devices," ACM Computing Surveys, Vol. 45, No. 1, Nov. 2012.

[3] Z. Yang, A. C. Champion, B. Gu, X. Bai, and D. Xuan, "Link-Layer Protection in 802.11i WLANs with Dummy Authentication," ACM WiSec, pp. 131-138, March 2009.

[4] F. Guo and T. Chiueh, "Sequence number-based MAC address spoof detection, " Lecture Notes in Computer Science Volume 3858, pp 309-329, 2006.

[5] D. Madory, "New Methods of Spoof Detection in 802.11b Wireless Networking," A Thesis Submitted to the Faculty in partial fulfillment of the requirements for the degree of Master of Science, Darmouth College, June 2006.

[6] Y. Sheng, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," INFOCOM 2008, pp. 1768-1776, April 2008.

[7] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," International Conference on Information Processing in Sensor Networks (IPSN), pp. 25-36, April 2009.

[8] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," ACM MobiCom, pp. 116-127, Sept. 2008.

[9] Y. Shi and M. A. Jensen, "Improved Radiometric Identification of Wireless Devices Using MIMO Transmission," IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 4, pp. 1346-1354, Dec. 2011.

[10] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on Physical-layer Identification," 10th ACM Conference on wireless network security (WiSec), pp. 89-98, March 2010.

[11] J. Son and S. Kim, "kNNDD-based One-Class Classification by Nonparametric Density Estimation," Journal of the Korean Institute of Industrial Engineers, Vol. 38, No. 3, pp. 191-197, Sep. 2012.

 ISBN: 978-1-61208-289-9