Journal of Advances in Computer Research
Quarterly ISSN: 2008-6148
Sari Branch, Islamic Azad University, Sari, I.R.Iran
(Vol. 4, No. 1, February 2013), Pages: 65-80
www.jacr.iausari.ac.ir

RSSAT: A Wireless Intrusion Detection System Based on Received Signal Strength Acceptance Test

S.Mobarakeh Moosavirad [1], Peyman Kabiri [2]✉, Hamidreza Mahini [3]

(1) Iran University of Science and Technology (IUST), Center for ELearning, Tehran, Iran
(2) Iran University of Science and Technology (IUST), School of Computer Engineering, Tehran , Iran
(3) Islamic Azad University (IAU) , Science and Research Branch, Department of Computer Engineering, Tehran, Iran

moosavirad@vu.iust.ac.ir; peyman.kabiri@iust.ac.ir; hamidreza.mahini@srbiau.ac.ir

Received: 2012/11/03; Accepted: 2012/12/14

Abstract

Intrusion detection in wireless networks has been a challenging research problem in network security for more than half a century. This paper presents a novel intrusion detection method based on Received Signal Strength Acceptance Test (RSSAT) to improve the IDS capabilities in anomaly-based Host-based Intrusion Detection Systems (HIDS). The new system can identify suspicious behaviors detecting anomalies in the received signal strength from the access points. Several scenarios are implemented in Omnet++ environment to evaluate the performance of the proposed scheme. A test criterion is used to improve accuracy in detecting forged signal powers and at the same time to reduce number of the false positives i.e. number of false attack alerts resulted from the legitimate signal powers.

Keywords: *Intrusion Detection System, Wireless, WIDS, Security*

1. Introduction

Due to the widespread use of the internet, increasing the internet application and consequently the internet users and also increase in ubiquitous services as one of the main objectives in the development of web services in recent years, wireless computer networks became a great concern. The communication world is moving from the personal computer age to the pervasive age where each user can easily access all necessary information that is scattered around the world in various operating systems. The comprehensive feature of wireless networks makes this kind of networks the easiest solution for the wireless users to do their interconnections [1]. Some statistics conducted in 2007 show that about 34% of the internet users have used the internet via a wireless connection in US [2]. This suggests that almost one third of the users benefit from the internet facilities using means such as a laptop computer, a Personal Digital Assistant (PDA) or cell phones (smart phones). On the other hand, as the severity and number of computer attacks and intrusions are increasing, necessity for strong security measures and advanced Intrusion Detection Systems (IDS) is a fundamental requirement.

Intrusion detection is considered as a key solution in today's network security. Using IDS has grown considerably in the last few years to complement network firewalls and improve the security management capabilities of system administrators, e.g. monitoring, attack recognition, and response.IDS has an important role to provide security in wireless networks. To improve defense capabilities of the protected network, it is possible to combine IPS and IDS together [3]. An IPS destroys the security holes of the network before the attack occurs.

There are two types of IDS: Host-based IDS (HIDS) and Network-based IDS (NIDS) [4]. From yet other aspect, IDSs are further classified as two distinct categories: pattern-based IDS that is capable of detecting all the known intrusions and anomaly-based IDS with the ability to detect unknown intrusions. Some HIDS is anomaly-based and its operation is based on detecting any anomalous behavior and to raise an alert [1]. This paper proposes an approach to improve intrusion detection in anomaly-based HIDS. Some common IDSs operate at layers above the physical layer such as data link and cannot make difference between packets from an intruder and packets from legitimate wireless users [5]. The proposed architecture is based on physical layer.

Different parts of this paper are as following: In section 2, the background of using the IDSs to detect intrusions in computer networks is presented. Section 3 focuses on scrutinizing the details of the proposed architecture. In section 4, the performance evaluation of Received Signal Strength Acceptance Test (RSSAT) architecture is considered. Experimental results after implementing the proposed intrusion detection method is presented in section 5. Eventually, the conclusion and future works will be presented in section 6.

2. Background

In recent years, many efforts have been made to produce and improve wired and wireless IDSs. Some of these efforts use multi-agent techniques, some are based on neural networks solutions, and some are host-based or network-based approaches. Some of these reported approaches are briefly explained in this section. Kannadiga and Zulkernine [6] used Mobile Agents (MA) to propose a Distributed Intrusion Detection System (DIDMA). DIDMA maintains a list of attacked hosts in the Victim Host List (VHL) component. An MA moves from one host to the other as they are listed in the VHL. In each step, due to the type of the attack MA performs alert aggregation and/or correlation analysis. At the end a final decision is made and sent to the IDS console. Advantages of DIDMA compared with a centralized based analysis distributed IDS is that DIDMA makes better use of the total bandwidth to transmit collected data from one host to another one and reduces the network usage. On the other hand, the authors suggested encryption and authentication mechanisms to provide the required security to guarantee the integrity and confidentiality of data during transferring from one host to another. Chan and Wei [7] proposed a network based preemptive Distributed Intrusion Detection System (DIDS). Static Agents (SA) perform required researches to acquire evidence data at the host. MAs move from one host to the other host with the least load to collect evidence data and perform detection analysis. The gateway agent receives packets from the external network and delivers them to an appropriate controller agent. The detection agent performs the analysis and notifies the controller agent with the result. Then the result will be also sent to the policy agent to implement. At each host, the home agents control the traffic of packets. Once a packet arrives at a host, the home agent consulting with the policy agent decides whether to block or allow the packet to pass. The reported work proposes an approach where the analysis is performed on a host that is operating within its minimum load. This is a major advantage for the proposed method. Mukkamala and Sung [8] used Support Vector Machines (SVMs) and Artificial Neural Networks (ANNs) that are two classes of artificial intelligent techniques, for intrusion detection based on recognition of the attack patterns. The SVM approach transfers data into a feature space with huge dimensions. The ANN is a multi-layer feedforward network. These types of ANNs are capable of making multi-class classifications. In the reported work ANN was used to perform the intrusion detection. Han-Pang Huang and Chia-Ming Chang [9] proposed a scalable intrusion detection system based on active network technology for detecting both known and unknown intrusion behaviors. The proposed system consists of three basic parts: IDS, Management Center (MC) and Intrusion Detection Center (IDC). When confronted with a suspicious activity, the relevant responses of IDS are sent to IDC for further analysis. MC is responsible for subnets and it can dispatch service agents. IDC is also responsible for updating the detection model. Timothy R.Schmoyet et al. [10] examined an architecture which integrates an intrusion detection engine with an active countermeasure capability. They used a classic man in the middle attack as a case study to specify the integrated wireless intrusion detection capability with the active countermeasure response. In the architecture every node uses an IDS agent to monitor local activity and responds to intrusions. In order to collect adequate data to detect or determine the type of an attack, local agents are able to communicate safety once an intrusion is suspected. The performance of wireless IDS and response systems can be increased using a distributed and cooperative system. In the MITM attack, the first frame received at the client is a deauthentication frame. Since the sequence number is controlled by the operating system in MAC implementation, it is clear that the sequence number of the frame will not match the sequence number used by the AP. This sign can raise the suspicion about an anomalous behavior. The response engine performs a response strategy based on the alarm confidence, attack frequency, assessed risks and estimated response costs. Tomko et al. [5] propose a method to detect intrusions in wireless local area networks which uses the radio frequency waveform of each network packet to extract some physical layer features. These features are related to the wireless user node which is the packet source and the propagation path between an access point and the wireless node. In wireless propagation environment the packet delivery mechanism is independent from the packet source. Therefore, it is possible for rouge transmitters to forge the source identification such as Medium Access Control (MAC) address. The authors proposed a wireless IDS called WIND to identify whether the received packet is sent by an adversary or a legitimate wireless node. WIND measures a set of RF features of each propagated packet and using the statistics of the feature set to deduce a fingerprint which can exclusively identify the source of the packet. It will be laborious for an intruder to imitate a legitimate node by using the physical layer features. Some intrinsic features used in the proposed method are turn-on transients, frequency error and the received signal power. The architecture is made of several sensors with multiple different antennas to extract the RF features to generate the feature vectors. An intrusion detector which processes the received feature vector to derive a fingerprint for each source identifier found in the packets and when anomalies are detected in any fingerprint, an intrusion alert will be issued. Fragkiadakis et al. [11] proposed a novel intrusion detection algorithm that uses some progressions in Compressed Sensing (CS) theory with a cumulative-sum anomaly-based algorithm to detect physical layer intrusions. CS is a new method [11] to capture and represent compressible signals at a rate below the Nyquist rate. This method is already used in positioning, routing, video streaming, signal reconstruction and other wireless communication areas. Effective energy consumption is an important issue in communication networks and fewer SINR measurements lead to energy efficiency of the IDSs. The algorithm is based on the Signal-to-Interference-plus-Noise-Ratio (SINR) metric. To make effective intrusion detection, compressed sensing theory uses far fewer SINR measurements than other existing techniques. Let N to be the original number of SINR values that is used for intrusion detection, here performance of the intrusion detection algorithm is investigated using only M measurements (M << N).

On the other hand, existence a rogue access point in the configuration of the network is another threat when using IEEE 802.11x networks. A rogue AP feigns to be a legitimate access point to deceive the targeted clients. In first step, a rogue AP intercepts the connection between legitimate AP and the victim and spoofs the critical transferred information. Later on, it forges legitimate AP using its SSID to attract the victims [12] [13] [14]. In [15] an intrusion detection method is proposed to detect such forged APs. The authors introduced a timing-based client-centric scheme to help the users eschew connecting spurious APs. The proposed detection method analyses the round trip time between the DNS server and the client to determine the real identity of the connected access point.

3. RSSAT in details

RSSAT is a host-based wireless intrusion detection system which identifies suspicious behaviors according to the received signal strength anomaly. The main idea of RSSAT is that the current received signal strength after a short time interval dt, for example, should not have a significant variance from the average of the N previous received signal powers. In the other words, if the current received signal strength compared with the average of the N last signal powers is greater than a threshold, it would indicate a potential anomaly. Consequently, the detected anomaly suggests that the signal source will be probably bogus.

3.1 RSSAT Architecture

Generally, in a host machine, a wireless network interface card (NIC) has the three levels of abstraction which are depicted in figure 1. The radio unit is the lowest level of abstraction which transfers the signals in radio channels. The next higher level is the Media Access Control (MAC) unit that is responsible for implementing the IEEE 802.11x protocol. Finally, the highest level of abstraction describes the management unit that is used to interpret and generate the management packets.

RSSAT is an acceptance test subsystem added to the radio layer to empower the radio unit to detect the shady received signals. In fact, there is no need to change the layers of the access point to implement the proposed scheme. Equipping the radio layer of the wireless hosts with the appropriate tools to implement this idea will do the job. Therefore, the proposed plan is a HIDS.

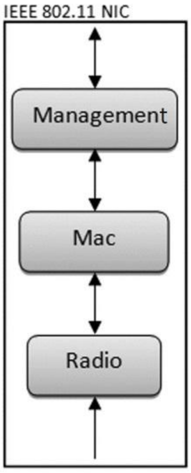

Figure 1. The three levels of layer abstraction in a wireless NIC

3.2 RSSAT Implementation

To implement the acceptance test subsystem, we need to design a new data structure called Circular-Averaging to collect the received signal powers and to calculate the mean of N last stored items. Since the number of the signals is large, this data structure is derived from a circular queue class.

Let N to be a discrete uniform random variable on the consecutive integers α, α+ 1, α+ 2, …, β, for α ≤ β. Mean and variance of the data is calculated using the following equations.

$$\mu = E(N) = \frac{\alpha+\beta}{2} \tag{1}$$

$$\sigma^2 = \frac{(\beta-\alpha+1)^2-1}{12} \tag{2}$$

It is clear that if m items are stored in Circular-Averaging and the current N is greater than m (N > m), then N can be replaced with m (Equation 3). URG in equation 3 stands for *Uniform Random Generator (URG)* and the value of α and β can be set diversely in different situations, but the default values are considered 10 and 30, respectively.

$$N = \min(URG(\alpha,\beta), CircularAveraging.getSize()) \tag{3}$$

After receiving a new signal, the Current Signal Power (CSP) and N will be calculated. Later on, the Mean of N Last Signal Powers (MNLSP) will be compared against CSP. If the difference (dif) is less than or equal to the predefined threshold (δ), then CPS will be queued by calling EnQueue procedure from Circular-Averaging and the signal is sent to the higher layer. Otherwise, a warning is generated to alert the occurrence of an attack. Figure 2 depicts an activity diagram which shows the sequence of this process.

4. Performance Evaluation

Although the main goal of IDS is to detect suspicious activities in a network we have to take into account the occurrence rate of the false positives play an important role in IDS performance evaluation.

In order to improve performance evaluation for RSSAT following assumptions are considered:

- T → The maximum accepted difference between the received signal power and the MNLSP
- n → The number of the received signal powers
- A → An event to indicate the occurrence of an attack
- f → The probability of an attack (equation 4)

$$f = p(A) = \frac{number\ of\ received\ \ forged\ \ signals}{number\ of\ received\ \ signals} \tag{4}$$

$f = p(A)$

- $(f = p(A))$D → an event where the RSSAT reports that the received signal is suspicious.
- s → The RSSAT sensitivity i.e. probability of an attack based on the detection by means of RSSAT (equation 5).

$$s = p(A|\ D) = \frac{p(A \cap D)}{p(D)} = \frac{number\ of\ \det ected\ \ forged\ \ signals}{number\ of\ received\ \ suspicious\ \ signals} \tag{5}$$

$(s = p(A|D) = \frac{p(A\cap D)}{p(D)})s = p(A|D) = \frac{p(A\cap D)}{p(D)}$

- δ → The RSSAT specificity i.e. the suspicious signal detected is really a malicious signal.

$$\delta = p(D|\ A) = \frac{p(D \cap A)}{p(A)} = \frac{number\ of\ \det ected\ \ forged\ \ signals}{number\ of\ \ forged\ \ signals} \tag{6}$$

δ has direct relationship with T value and inverse relationship with s. This relationship is observed in table 1.

Table 1. Relationship between T, δ and s

T	δ	s
↑	↑	↓
↓	↓	↑

Large s means that most attacks can be detected by RSSAT but it should be noted that in this case the probability of false positive occurrence will also increase. On the other hand, increasing δ means that probability of false positive occurrence is reduced but probability of an unrecognized attack by RSSAT will be increased.

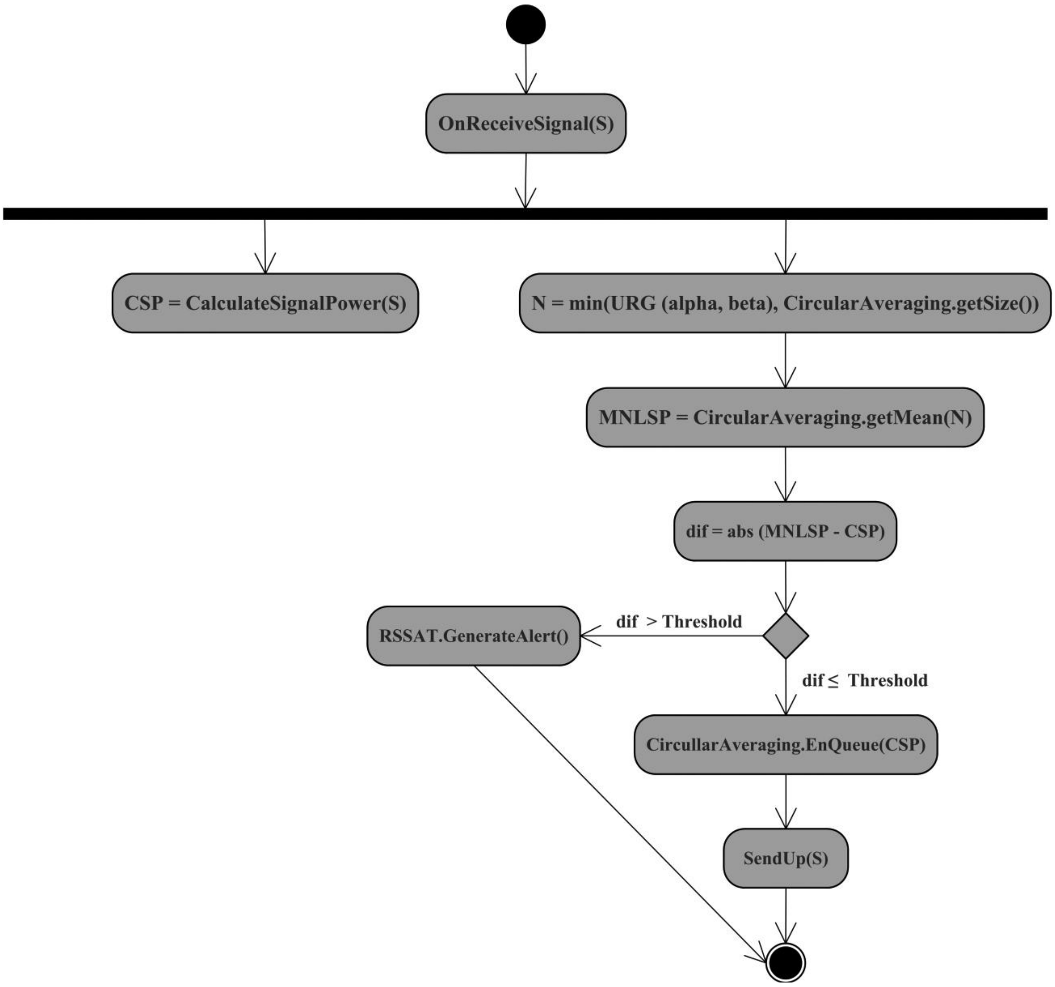
OnReceiveSignal(S)
CSP = CalculateSignalPower(S)
N = min(URG (alpha, beta), CircularAveraging.getSize())
MNLSP = CircularAveraging.getMean(N)
dif = abs (MNLSP - CSP)
dif > Threshold
RSSAT.GenerateAlert()
dif ≤ Threshold
CircullarAveraging.EnQueue(CSP)
SendUp(S)

Figure 2. Activity diagram for RSSAT implementation

5. Experimental Results

After implementing the idea in Omnet++ simulator, some scenarios are developed to evaluate performance of the proposed intrusion detection scheme. Several statistical graphs are presented to show performance of the proposed plan.

5.1 Scenario1

This scenario is the simplest scenario tested to verify the proposed approach. In this scenario a wireless host and two access points are considered. One of the access points is the legitimate AP and the other one is a forged AP. Selected mobility model for the host is linear mobility. The forged AP sends fake signals containing FORGED tags within the period time of 300ms. In this scenario, the goal is to prove that whether the difference between the legitimate and the forged signal power is good enough to distinguish between these two received signal groups or not. The reported results and the reported graphs verify the effectiveness of the approach.

Ratio (in percent) of the received legitimate signals divided by the received forged signals can be obtained using the following equation:

$$PercentDiff = 100 \times \frac{|MNLSP - CS|}{MNLSP} \tag{7}$$

Diagram of received legitimate and forged signals are represented in figures 3 and 4, respectively. Diagram reported from figures 3 and 4 are depicted alongside the difference vector between the received legitimate and forged signals, in figure 5. Figure 6 shows the ratio of the received legitimate divided by the received forged signals.

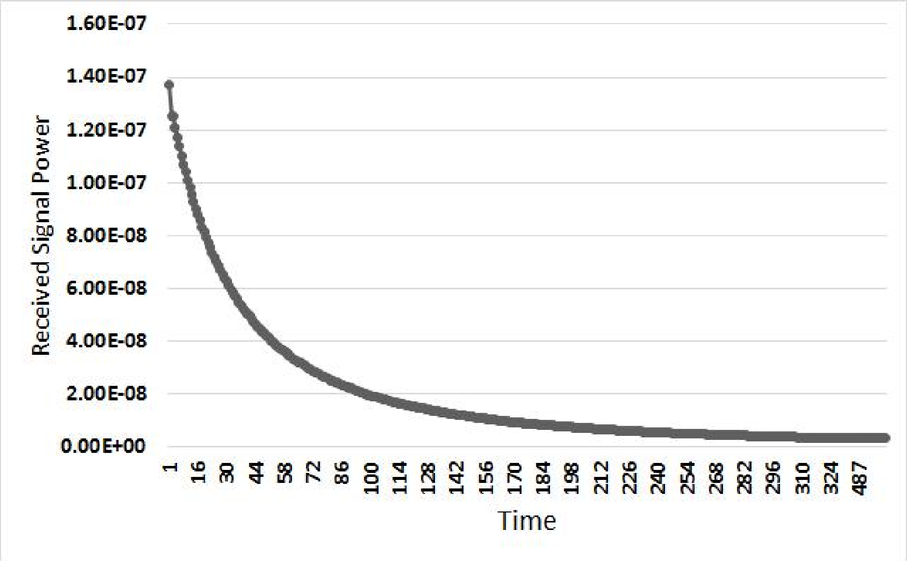

Figure 3. Scenario 1: Diagram of the received legitimate signal power

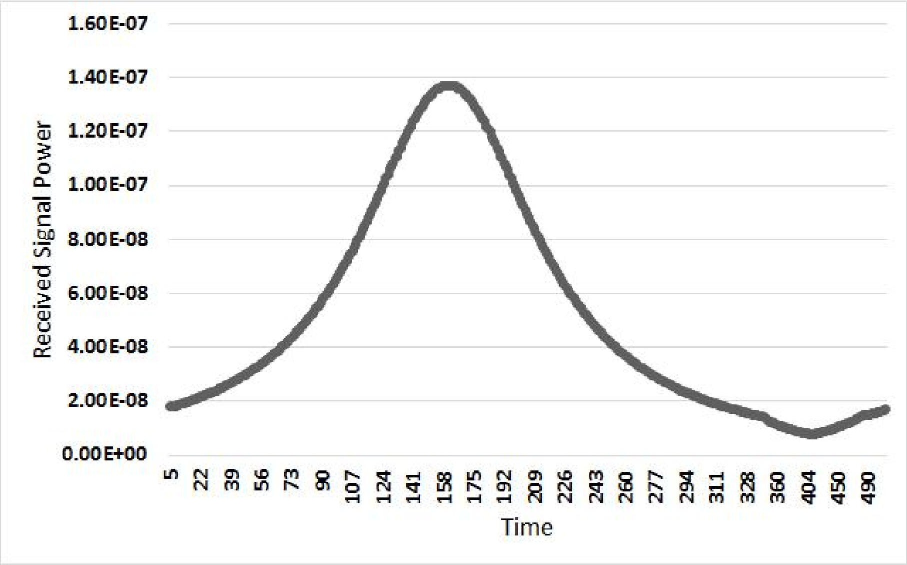

Figure 4. Scenario 1: Diagram of the received forged signal power

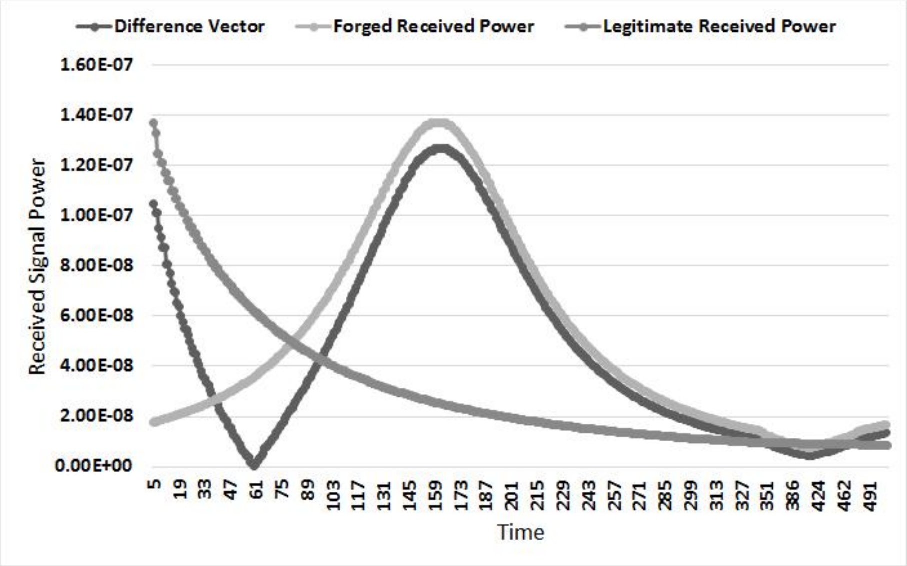

Figure 5. Scenario 1: Diagram of the received legitimate signal power, the received forged signal power and the difference vector between the received legitimate and forged signals

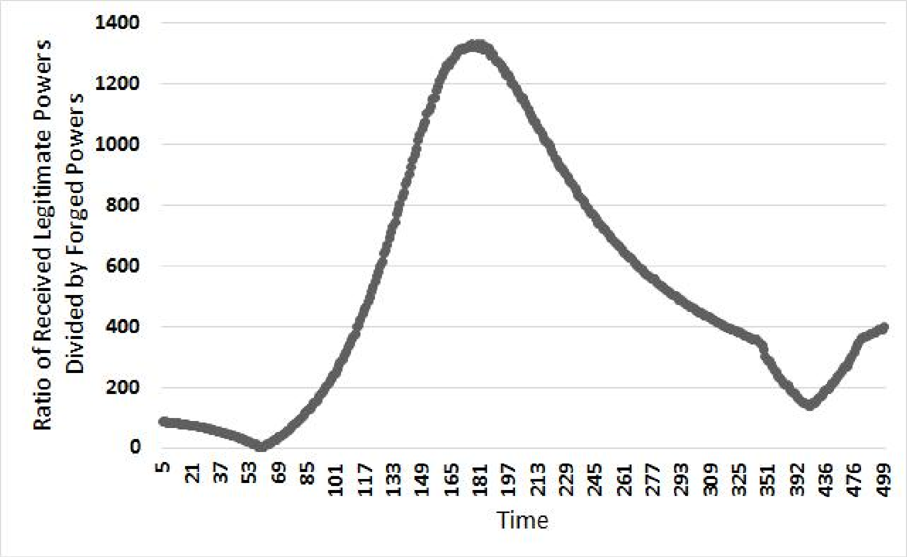

Figure 6. Scenario 1: Diagram for the ratio of the received legitimate divided by the received forged signals

Results reported in figures 3 through 6 represented validity of the proposed method. However, sometimes the conditions of the receiving signal from the APs are the same. For example, the wireless host may have equal distance from both APs where all the other conditions including obstacles and the signal powers are the same. In these situations, making the distinction between the legitimate and the fake signal strength of the received signal can be a bit risky. In figures 5 and 6, this issue is depicted in 50s and 80s time intervals. In some attacks this small delay can be problematic. This challenge is left for the future work.

Table 2 presents statistical scalar values resulted from the simulation of scenario1.

Table 2. Scenario1: Statistical scalar values.

Duration (Simulation Time)	500s
A	10
β	30
Threshold (T)	20
Total number of the received forged AP signals	1216
Total number of the received legitimate AP signals	2317
Total number of the received signals	3533
Total number of alerts after receiving the forged signals	1166
Total number of alerts after receiving the legitimate signals	0
Total number of alerts	1166

Considering Table 2, f, s and δ can be calculated using following equations.

$$f = p(A) = \frac{1216}{3533} \cong 0.34 \tag{8}$$

$$s = p(A|D) = \frac{1166}{1166} = 1 \tag{9}$$

$$\delta = p(D|A) = \frac{1166}{1216} \cong 0.96 \tag{10}$$

5.2 Scenario2

The only difference between this scenario and Scenario 1 is just mobility model for the host. In this scenario, instead of linear mobility, random movement (turtle mobility) is used. Here, wireless host travels half of the space with uniform probability distribution. Figures 7 and 8 present diagram of the received legitimate and forged signals, respectively. Difference between the received legitimate and forged signals is shown in figure 9. Diagram for the ratio between the received legitimate divided by the received forged signals is depicted in figure 10.

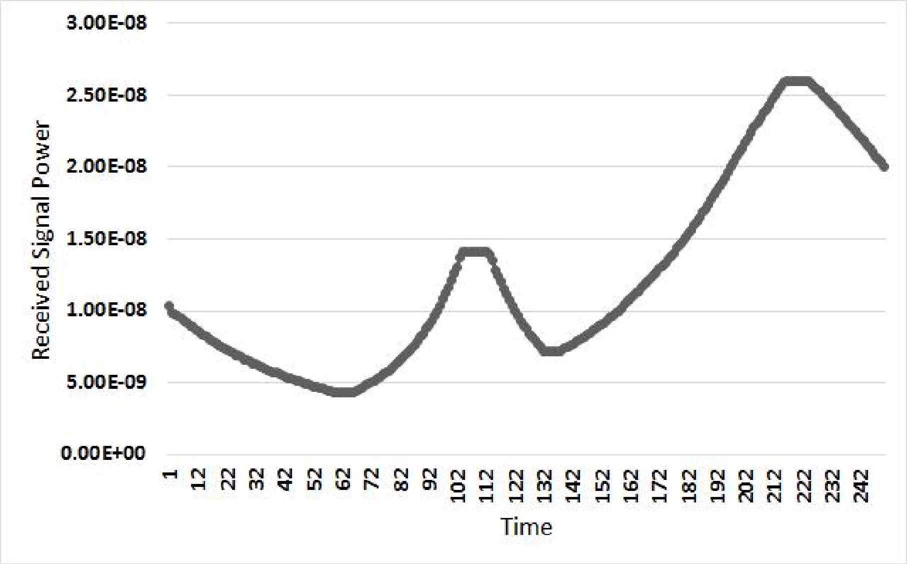

Figure 7. Scenario2: Diagram of the received legitimate signal power

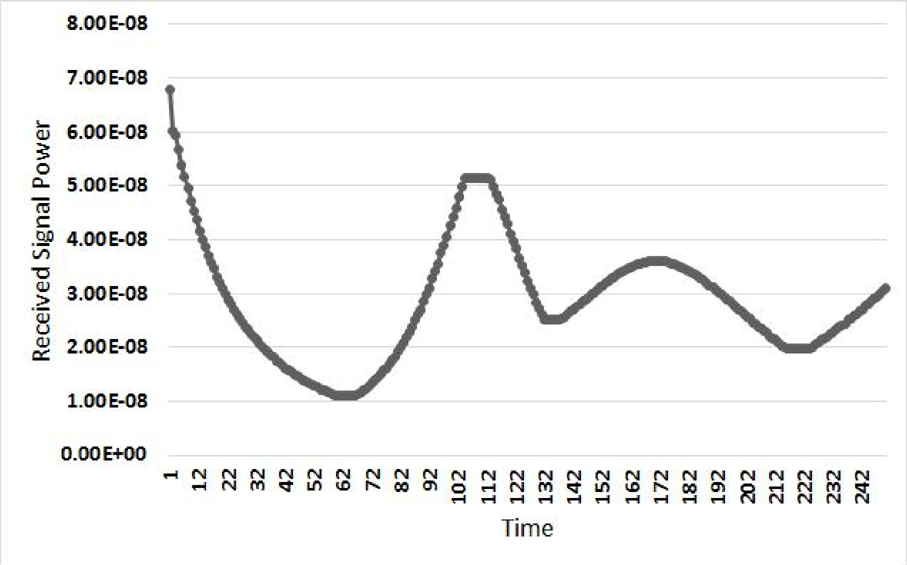

Figure 8. Scenario2: Diagram of the received forged signal power vector

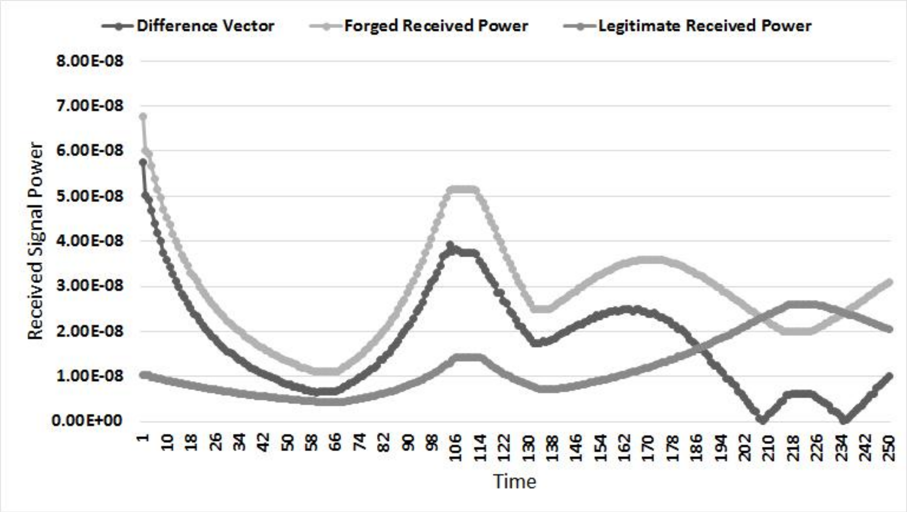

Figure 9. Scenario2: Diagram of the received legitimate signal power, the received forged signal power, the difference between the received legitimate and forged signals

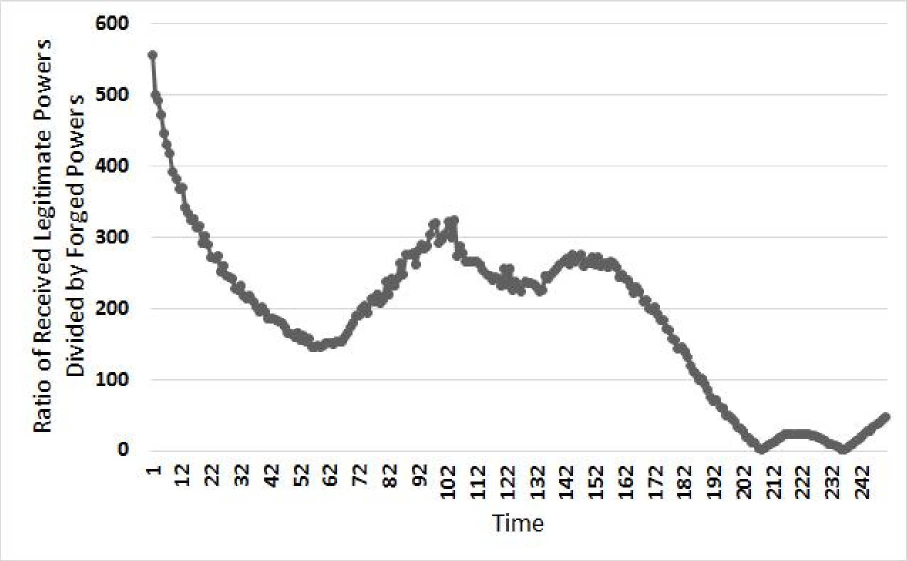

Figure 10. Scenario2: Diagram for the ratio between the received legitimate divided by the received forged signals

Results from simulation scenario2 that are presented in figures 7 through 10 prove validity of the proposed method. As mentioned in scenario1, the only remaining problem is when that the access points are physically close to each other. This challenge can be noticed in figure 10 during 200s to 240s time intervals. In this situation, making the distinction between the legitimate and the fake signal strength of the received signal can be a bit risky.

The statistical scalar values obtained from the simulation of scenario 2 are presented in Table 3.

Table 3. Scenario2: Statistical scalar values

Duration (Simulation Time)	603s
α	10
β	30
Threshold (T)	20
Total number of the received forged AP signals	1994
Total number of the received legitimate AP signals	2026
Total number of the received signals	4020
Total number of alerts after receiving the forged signals	1777
Total number of alerts after receiving the legitimate signals	20
Total number of alerts	1797

Considering Table 3, f, s and δ can be calculated using the following equations.

$$f = p(A) = \frac{1994}{4020} \cong 0.50 \qquad (11)$$

$$s = p(A|D) = \frac{1777}{1797} \cong 0.99 \qquad (12)$$

$$\delta = p(D|A) = \frac{1777}{1994} \cong 0.89 \qquad (13)$$

5.3 Scenario3

This scenario is quite similar to Scenario2, with the difference that both legal and forged APs are very close together at the beginning of the simulation. Indeed, the goal of this scenario is to simulate the worst possible case and to improve the aforementioned challenge. Figures 11 and 12 present diagram of the received legitimate and forged signals, respectively. Difference between the received legitimate and the forged signals are shown in figure 13. Diagram for the ratio between the received legitimate signals divided by the received forged signals is presented in figure 14.

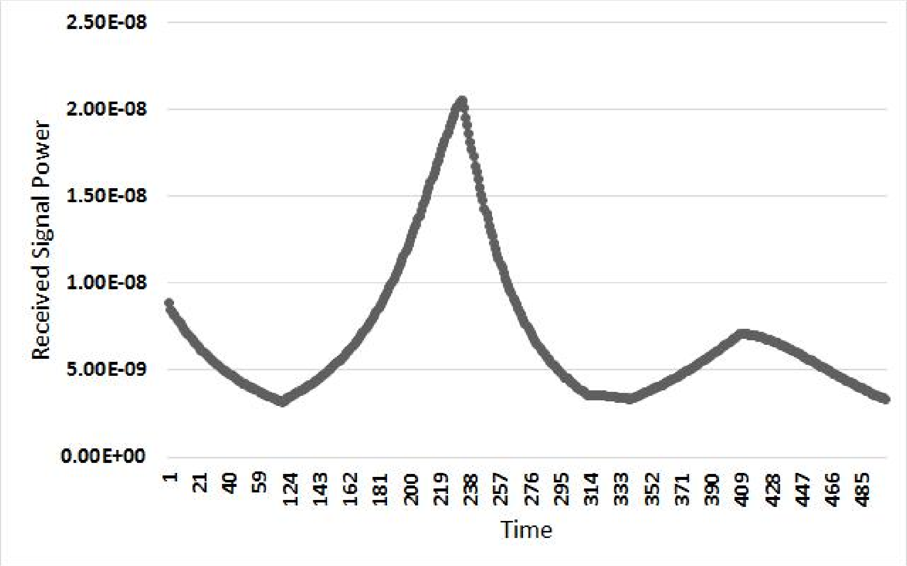

Figure 11. Scenario3: Diagram of the received legitimate signal power vector

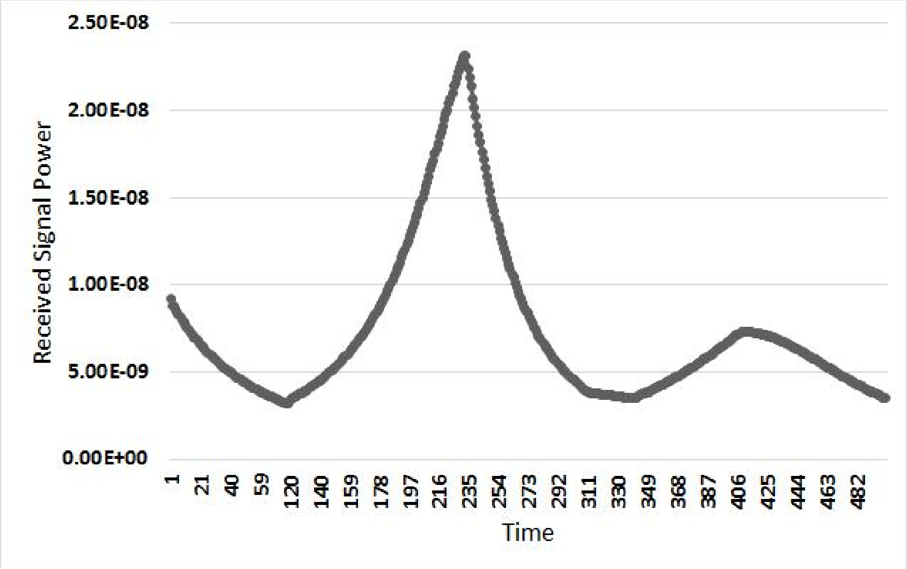

Figure 12. Scenario3: Diagram of the received forged signal power vector

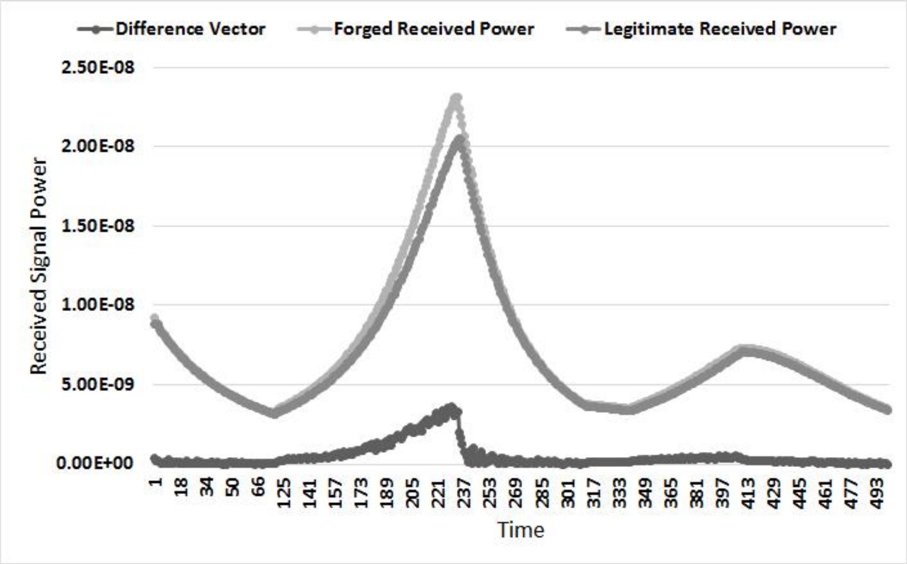

Figure 13. Scenario3: Diagram of the received legitimate signal power vector, the received forged signal power vector, the difference vector between the received legitimate and forged signals

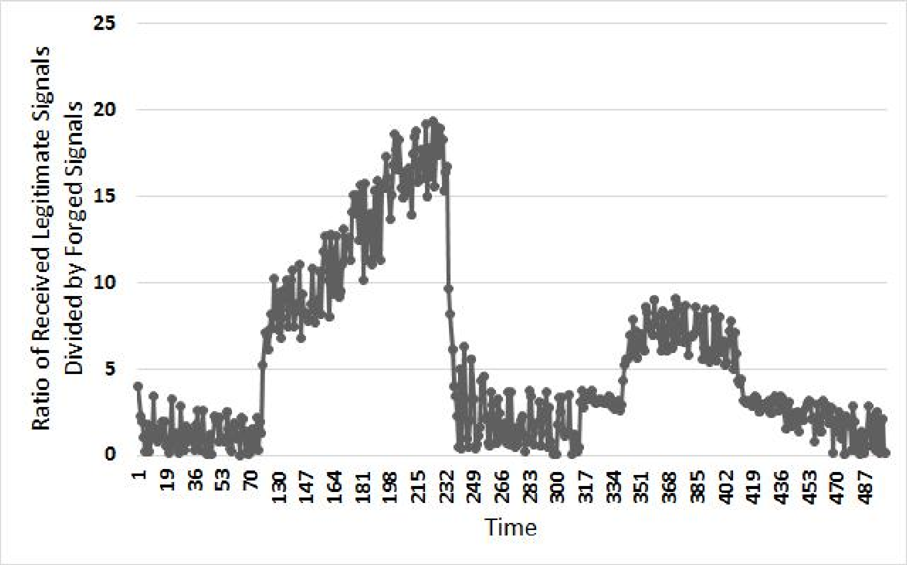

Figure 14. Scenario3: Diagram of ratio for the received legitimate divide by the received forged signals

Figure 14 depicts the maximum difference case, where, received legitimate and forged signals are about %20 different. However, results in the previous scenarios represent that these two ratios differ approximately by more than 5.6 times in figure 10 and more than 13 times in figure 6. Consequently, as an important result we can say that considering the threshold below 20mW seems to be an appropriate criterion. Although after testing different values of threshold we found that the best result will be obtained with a value of 6mW which is specified in the following table.

Table 4 shows statistical scalar values of scenario3 simulation.

Table 4. Scenario3: Statistical scalar values.

Duration (Simulation Time)	500s
α	10
β	30
Threshold (T)	6
Total number of the received forged AP signals	535
Total number of the received legitimate AP signals	1411
Total number of the received signals	1946
Total number of alerts after receiving the forged signals	165
Total number of alerts after receiving the legitimate signals	851
Total number of alerts	1016

Considering Table 4, f, s and δ can be calculated using the following equations.

$$f = p(A) = \frac{535}{1946} \cong 0.27 \tag{14}$$

$$s = p(A \mid D) = \frac{165}{1016} \cong 0.16 \tag{15}$$

$$\delta = p(D \mid A) = \frac{165}{535} \cong 0.31 \tag{16}$$

In this scenario, access points are close together, therefore, we are forced to set the threshold parameter equal to 20mW to gain good efficiency. In this case, as mentioned earlier, number of false positives will also increase.

6. Conclusions

This paper reports a new approach to design and implement a Wireless IDS (WIDS) called RSSAT based on received signals on the physical layer. The proposed approach is based on anomaly detection in host entities, so RSSAT is a host-based WIDS. Detecting the suspicious traffic depends on the threshold set for the difference between the current signal power and the mean of the N last signal powers. Results of simulation demonstrate that RSSAT can detect around 96% of the received forged signal powers. Meanwhile, the number of false positives can be significantly low. Scenario3 shows that the location of forged AP is an important issue. When the forged AP is physically close to the legitimate one, this situation may lead to a false detection. Therefore, one of the valuable results of this investigation is that the legitimate AP must be far from other existing access points. Since multi-layer defense is a principle in security, the proposed approach can be combined with other existing methods to present new approaches.

7. References

[1] M. Kumar, M. Hanumanthappa, T. V. Suresh Kumar, "Intrusion Detection Systems Challenges for Wireless Network", *International Journal of Engineering Research and Applications (IJERA)*, Vol. 2, pp. 274-280, 2012.

[2] J. Horrigan, " Wireless Internet Access", *Report: PEW Internet and American Life Project*, 2007.

[3] Zheng Wu, Debao Xiao, Hui Xu, Xi Peng and Xin Zhuang, "Virtual Inline: A Technique of Combining IDS and IPS Together in Response Intrusion", IEEE First International Workshop on Education Technology and Computer Science, pp. 1118-1121, 2009.

[4] Karen Scarfone and Peter Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", Recommendations of the National Institute of Standards and Technology, 2012.

[5] A. A. Tomko, C. J. Rieser and L. H. Buell, "Physical-Layer Intrusion Detection in Wireless Networks", *IEEE Military Communications Conference (MILCON)*, pp. 1-7, 2006.

[6] P. Kannadiga and M. Zulkernine, "DIDMA: a distributed intrusion detection system using mobile agent", *Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks*, pp. 238-245, 2005.

[7] P. C. Chan and V. K. Wei, "Preemptive distributed intrusion detection using mobile agents", *Proceedings of Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2002)*, pp. 103-108, 2002.

[8] S. Mukkamala, A. H. Sung, "Artificial Intelligent Techniques for Intrusion Detection", *Proceedings of IEEE International Conference Systems, Man, and Cybernetics, IEEE Computer Society Press*, pp. 1266-1271, 2003.

[9] Han-Pang Hung, Chia-Ming Chang, "An Active Network-Based Intrusion Detection and Response Systems", *Proceedings of the IEEE International Conference on Networking, Sensing & Control*, pp. 1317-1322, 2004.

[10] Timothy R. Schmoyer, Yu Xi Lim and Henry L. Owen, "Wireless Intrusion Detection and Response, A case study using the classic man-in-the-middle attack", *IEEE Communications Society*, pp. 883-888, 2004.

[11] Alexandros Fragkiadakis, Sofia Nikitaki and Panagiotis Tsakalide, "Physical-Layer Intrusion Detection for Wireless Networks using Compressed Sensing", *In Proceeding of the 5th International Workshop on Selected Topics in Mobile and Wireless Computing*, 2012.

[12] Yimin Song, Chao Yang, and Guofei Gu, "Who Is Peeping at Your Passwords at Starbucks? – To Catch an Evil Twin Access Point", Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 323-332, 2010.

[13] H. Han, B. Sheng, C.C. Tan, Q. Li, and S. Lu, “A Measurement Based Rogue AP Detection Scheme,” Proc. IEEE INFOCOM, 2009.

[14] S. Shetty, M. Song, and L. Ma, “Rogue Access Point Detection by Analyzing Network Traffic Characteristics,” Proc. IEEE Military Comm. Conf. (MILCOM ’07), 2007.

[15] Hao Han, Bo Sheng, Chiu C. Tan, Qun Li and Sanglu Lu, "A Timing-Based Scheme for Rogue AP Detection", IEEE Transactions on Parallel and Distributed Systems, pp. 1913-1925, 2011.