New Approach in Detection MAC Spoofing in a WiFi LAN

Asst. Prof. Hamid Mohamed Ali
Department of Computer Engineering
College of Engineering
Baghdad University
Email: habdul_hussain@yahoo.com

M.Sc. Student Ammna Mohamed Abbas
Department of Computer Engineering
College of Engineering
Baghdad University
Email: ammna_maa@yahoo.com

ABSTRACT

Medium Access Control (MAC) spoofing attacks relate to an attacker altering the manufacturer assigned MAC address to any other value. MAC spoofing attacks in Wireless Fidelity (WiFi) network are simple because of the ease of access to the tools of the MAC fraud on the Internet like MAC Makeup, and in addition to that the MAC address can be changed manually without software. MAC spoofing attacks are considered one of the most intensive attacks in the WiFi network; as result for that, many MAC spoofing detection systems were built, each of which comes with its strength and weak points. This paper logically identifies and recognizes the weak points and masquerading paths that penetrate the up-to-date existing detection systems. Then the most effective features of the existing detection systems are extracted, modified and combined together to develop more powerful detection system called Sequence Number with Rate and Signal Strength detection method (SN-R-SS).

SN-R-SS consists from three phases. First phase is Window Sequence Numbers; to detect suspicious spoofed frames in the network. Second phase is Transmission Rate Analysis; to reduce the amount of the suspicious spoofed frames that are generated from the first phase. Finally, the third phase is Received Signal Strength; this phase is decisive phase because it decides whether the suspicious spoofed frames are spoofed or not. Commview for WiFi network monitor and analyzer is used to capturing frames from the radio channals. Matlab software has been used to implement various computational and mathematical relations in SN-R-SS. This detection method does not work in a real time because it needs a lot of computation.

Keywords: Sequence Number with Rate and Signal Strength detection method, detection, frame, spoof.

طريقة جديدة في اكتشاف تزوير المتحكم بالوصول للوسط في شبكة الواي فاي المحلية

أ.م. حامد محمد علي
قسم هندسة الحاسبات
كلية الهندسة/جامعة بغداد

طالبة ماجستير آمنة محمد عباس
قسم هندسة الحاسبات
كلية الهندسة/جامعة بغداد

الخلاصة

الهجمات عن طريق تزوير المتحكم بالوصول الى الوسط تشمل تغيير المهاجم العنوان المصنعي للمتحكم بالوصول الى الوسط الى اي قيمة اخرى. هجمات التزوير للمتحكم بالوصول الى الوسط في شبكات الواي فاي بسيطة بسبب سهولة الوصول الى الادوات التي تزور المتحكم بالوصول الى الوسط على الانترنتوبالاضافة الى ذلك نستطيع تبديل عنوان المتحكم بالوصول الى الوسط يدويا بدون ادوات. هجمات تزوير المتحكم بالوصول الى الوسط تعتبر من اخطر الهجمات في الشبكات الواي فاي; ونتيجة لذلك, عدة انظمة لاكتشاف التزوير بنيت, جميعها لها نقاط قوة ونقاط ضعف. هذه المقالة تعرف وتميز نقاط الضعف

ومسارات الاختراق لانظمة الاكتشاف الموجودة. بعد ذلك يتم استخلاص المميزات المؤثرة لانظمة الاكتشاف الموجودة, تعديلها ودمجها مع بعض لتطوير نظام الاكتشاف اكثر قوة.

طريقة الاكتشافرقم التسلسل مع السرعة وقوة الاشارة يتضمن ثلاثة اطوار. الطور الاول هو نافذة تسلسل الارقام; هذا الطور يكشف عن الرسائل المشكوك بتزويرها في الشبكة. الطور الثاني هو تحليل سرعة الارسال; هذا الطور يقلل من عدد الرسائل المشكوك بها في الشبكة. الطور الاخير هو قوة الاشارة المستلمة; هذا الطور هو طور القرار وذلك لانه من خلاله يتم الكشف ما اذا كانت الرسالة المشكوك بها مزورة ام لا. تم استخدام برنامج ماتلاب لتطبيق العلاقات الرياضيةوالحسابية الموجودة في طريقة الاكتشاف رقم التسلسل مع السرعة وقوة الاشارة.هذه الطريقة لاتعمل في الزمن الحقيقي لانها تحتاج الى حسابات كثيرة.

الكلمات الرئيسية :طريقة الاكتشاف, رقم التسلسل مع السرعة وقوة الاشارة, إكتشاف, إطار, خداع.

1. INTRODUCTION

Existing Institute of Electrical and Electronics Engineers(IEEE) 802.11 security techniques, such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or IEEE 802.11i (WPA2), can only protect data frames **Bansal, R., etal., 2008**.

Detection of adversary presence avoids the launching of other wireless attacks **Goel, S., etal., 2009**. Guo and Chiueh **Guo, F., etal., 2006** proposed spoof detection scheme based on the SN field in IEEE 802.11 MAC header. The difference modulus 4096 between consecutive frames SN transmitted by a STA is calculated. This detection system generated many false positive and false negative alarms **Li, Q., etal., December 2007**.This method results in large amounts of false positives on wireless networks which experience even small amounts of frame loss **Madory,D., June 2006**, and caused in large amount of false positive in case both of the victim and attacker have QoS propriety in Wireless Local Area Network (WLAN) card, or one of them has this propriety **Chandrasekaran, G., etal., 2009**. Douglas Madory **Madory,D., June 2006** proposed detection system based on the same field of MAC header that is SN field. Instead of raising alarm simply on the basis of SN gap, Douglas Madory considers the transmission rate of the frames transmitted by a STA. By using this method the false alarm that was raised due to natural loss of frames will not be generated. The transmission rate is calculated by taking difference modulo 4096 of the SN of consecutive frames and dividing it by the difference of their arriving time. This method generates large amount of false positive alarms caused by the existence of Quality of Service (QoS) propriety **Chandrasekaran, G., etal., 2009**. Qing and W. Trappe **Li, Q., etal., December 2007** defined a relation to detect spoofing using the linear behavior of SN. Rather than operating strictly on two consecutive frames, the detection scheme operates on a window of frames coming from a specific STA. This method also results in large amounts of false positives on wireless networks which experience even small amounts of frame loss **Chandrasekaran, G., etal., 2009**. Also this method caused in large amount of false positive in case both of the victim and attacker have QoS propriety in WLAN card, or one of them has this propriety **Chandrasekaran, G., etal., 2009**. Yong Sheng and et al. **Sheng, Y., etal., April 2008** proposed an approach based on Gaussian mixture models, building received signal strength (RSS) profiles for spoofing detection. They proposed to use Gaussian Mixture Modeling (GMM) for RSS profiling. This approach cannot detect attackers who spoof the MAC addresses of mobile STAs. Shikha Goel and Sudesh Kumar **Goel, S., etal., 2009** proposed algorithm analyze the possible reasons for generating false positive and false negative in Forge Resistance Relationship (FRR) spoof detection method and proposed an improved method Forge Resistance Relationship Rate Analysis (FRR-RA) with reduced false alarms. This method caused in large amount of false positive in case both of the victim and attacker have QoS propriety in WLAN card, or one of them has this propriety **Chandrasekaran, G., etal., 2009**.T. Saelim, C. Sriklauy and P. Chumchu **Chumchu, P., etal., 2011** proposed new MAC Address Spoofing Detection Algorithm using Physical Layer Convergence Protocol (PLCP) Header. In this algorithm they are utilizing PLCP header of IEEE 802.11 frames to differentiate an attacker STA from a victim STA. PLCP header of IEEE 802.11 frames maybe changed for each frame. It depends on transmission rate adaptation algorithm which is designed by vendors of wireless interfaces driver. The rate adaptation of an attacker STA and a victim STA is different depending on adaptive algorithm and

environments; therefore it is much harder to spoof PLCP header. This algorithm performs by setting a number of monitoring STAs. Then STAs whose MAC addresses are the monitored MAC address will reply the special frame. If the monitoring STAs receive more than one response frames, they decide that spoofing occurs. The drawback of this approach is the attackers could avoid this detection algorithm by stopping to reply any frames. This is could be modified drivers of wireless adaptors. The rest of the paper is organized as follows; Section 2 describes variations of MAC spoofing attacks. Section 3 describes SN-R-SS method. Section 4 describes the evaluation. Finally, section 5 concludes the paper and gives further work.

2. MAC SPOOFING ATTACKS

The theory of the MAC spoofing attack is that the attacker masquerades as a legitimate client. Thereby the attacker gains access to the network. As the name implies the masquerading is done by spoofing the MAC address of the legitimate client. This information can easily be obtained through eavesdropping.

There exist several variations of this attack. They differ in the way the victim is treated, whether the attacker tries to avoid detection, and as a result the complexity of performing the attack. In the remaining of this section five different versions will be briefly explained without going into the practical details of performing each of the attacks.

MAC freeloader attack: This is the simplest variation of the attack. It does not require much skill, and it does not try to avoid any form of detection. The attack consists of spoofing the MAC address of a legitimate client and nothing more. In this case both the attacker and victim will be connected to the network at the same time, and as a result both STAs will receive each other's traffic. It is pointed out in [20] that this behavior should cause problems in the Transmission Control Protocol (TCP) layer. More specifically it should result in a termination of the ongoing TCP connections, thus making it very difficult for the attacker to use TCP.

QoS optimized MAC freeloader attack: In the QoS optimized version the attacker tries to avoid detection based on simple SN analysis. This is done by changing IEEE 802.11 QoS priorities to some priority not currently in use by the legitimate client. Each QoS class has its own sequence counter. By using a previous unused class the attacker will obtain his own counter and fool some systems based on plain SN analysis.

Wait-for-availability attack: This attack is very similar to the freeloader attack, but there is one important difference. In this case the attacker waits until there is no longer any traffic going to or from the victim's STA. Then, assuming the victim has left; the attacker spoofs the address and tries to connect. This is the most relevant version of the MAC spoofing attack as it is easy to perform and very hard to detect with existing methods based on two STAs transmitting at the same time.

Session hijacking deauthenticates attack: In this variation the attacker first spoofs the AP's MAC address in order to send fake deauthenticate messages to the victim. The victim's STA believes that the deauthenticate is legit, and as a result it terminates its association with the AP. The attacker can then spoof the victims MAC and have the session for himself. To prevent the victim from reconnecting the deauthenticate procedure will have to be repeated frequently.

Session hijacking channel switch attack: A recent variation of the session hijacking, called channel switch attack is described in [21]. In this version the attacker does not send fake deauthenticate messages; instead he sends a channel switch announcement element. A correctly crafted element would result in the victim changing channel (to an invalid one) immediately, and stay on that channel for up to 255 beacon intervals before switching back. The authors report that a denial of service (DoS) effect of up to one minute can be achieved with a single message **Idland, C., June 2011**.

3. SEQUENCE NUMBER WITH RATE AND SIGNAL STRENGTH DETECTION METHOD (SN-R-SS)

3.1 Window of Sequence Numbers Phase

This phase is used to analyze and inspect out of order frames for the intention of detecting spoofing activity. The proposed detection scheme should operate on a window of frames which are coming from a specific MAC address MAC(i). Suppose that an observation w(k) to be a collection of n states corresponding to the kth frame from MAC(i). For example, one choice for w(k) might be to take w(k)={S(k), S(k-1)}, which is simply two consecutive frame states. The window w(k)={S(k), S(k-1),….., S(k-n-1)}, where n consider as window size consisting of n consecutive SN of frames S(k) **Li, Q., etal., December 2007**. This phase consists of two stages:

First stage of this phase is carried out by checking for the presence of two frames with same SN in the window of certain STA MAC address [16]. The purpose of this stage is to discover the phenomenon of a retransmitted frame due lost Acknowdgement (ACK). This phenomenon occurs when the ACK frame sent by the receiver STA is lost and is not received by the sender STA. If the window contains two frames with same SN, then the contents of the two frames are compared. The second arrival frame is considered a retransmitted frame and thus has to have the same content as the first arrival frame. This means that the frame is not spoofed and cannot possibly do any harm as it is just a duplicate and it is dropped by the monitor STA from the window. Otherwise, if the contents of the two frames, with same SN, have not the same contents, then this window is marked as containing suspicious spoofed frame and is passed to the third phase for further analysis.

Second stage of this phase adopts the Window of SNs techniques. By using a window of frames, rather than only two consecutive frames, different degrees of detection accuracy can be used to enhance the detection system. The detection accuracy can be adjusted to increase or decrease the false positive and negative alarms generated by the detection system. In this stage, the detector calculates the n-1 SN differences {d1, d2, d3,…., dn-1}, where dn=[SN(k-n+1) - SN(k-n)] (mod 4096). The detector determines the occurrence of spoofed frames if Max (di) > T. Where ‘i’ varies from 1 to n and ‘T’ correspond to a threshold that governs the probability of false alarms and missed detection. Threshold value ‘T’ usually taken to be ‘3’ on considering frame loss, where frames are sent by the sender STA and are not received by the receiver STA. Usually the frame SN is incremented by one for each consecutive frame. The lost frame would cause the frames not to be received sequentially. A threshold value is used to reflect approximately the maximum number of acceptable loss of consecutive frames in IEEE 802.11 based wireless network **Goel, S., etal., 2009**. The threshold value can be adjusted according to the level of security required in a network. With the decrease in threshold value the number of false positive alarms will increase but there will be a decrease in false negatives. When the frame SN differences are greater than that threshold, then it is an indication of suspicious spoofed frame which is the purpose of the next phase.

3.2 Transmission Rate Analysis Phase

This phase adopts the Transmission Rate Analysis method to inspect the window of suspicious spoofed frame passed from previous phase. Transmission Rate Analysis considers the time difference between consecutive frames and permit for naturally occurring loss frames while still detecting invalid SNs. To avoid false positive situation due to heavy frame loss, the window of suspicious frames of the previous phase is passed to this phase. This phase works on the basis of measuring the transmission rate of each STA in the WLAN. To detect the spoofing in the window, Transmission Rate Analysis on the suspicious frame with its previous and next frame is performed. Transmission rate considers possibility of frame loss and do not raise false positive alarm for it. Transmission rate is calculated by taking difference modulo 4096 of SNs from consecutive frames and dividing by the difference of their respective arrival time. The function can be defined as **Goel, S., etal., 2009**:

$$\text{Transmission Rate} = ((S(i)-S(i-1)) \bmod 4096) / (T(i)-T(i-1)) \quad (1)$$

Where S (i) and S (i-1) is the SN and T(i) and T(i-1) are the arrival time of ith and (i-1)th frame respectively. By using this method, gaps from natural frame loss do not cause false alarms because they will not yield an abnormally large difference in transmission rate. It is necessary to show the relationship between the frame SN and its arrival time. For example, assume, the frame sequence numbers: { 1, 2, 3, 5, 6, 7}, are sent one millisecond apart, then the transmission rate between the first two frames would be (2-1) frames/0.001 second or 1000 frames/seconds as frame of SN 2 is arrived one millisecond after the arrival of frame of SN 1.

The rate between the third and fourth frames would be (5-3)/0.001 or 1000 frames/second as frame 5 arrived two millisecond later than frame 3 due lost frame 4. The rate between the four and fifth frames would be (6-5)/0.001 or 1000 frames/second.

3.3 Received Signal Strength Phase

This phase adopts RSS approach to inspect suspicious spoofed frames passed from previous phase. RSS is the signal strength of a received frame measured at the receiver's antenna. RSS is correlated to the transmission power. A wireless STA does not often changes its transmission power, so distribution pattern of a STA mostly remain same. Also the attacker has no idea what RSS looks like from the receiver perspective. Thus, a drastic change in RSS value of received frames from same MAC address indicates spoofing. Hence, two STAs at different places have two separate and distinct signal signatures (mean and variance of signal strength values).

In this phase, the monitor STA is placed in a monitor mode, while in monitor mode it can determine the RSS for all frames being transmitted within the range of the receiver. The monitor STA will compute mean value and variance value of captured RSS sample for each MAC address of the wireless STAs. Practical work shows, for stationary wireless STAs, the RSS does not deviate more than 5dBm, taking in account that the other affecting factors, like obstacles, temperature degree. are fixed. Hence, the RSS can be modeled as normal distribution with mean and variance values calculated as follows **Konings, B., etal., 2009**:

$$\text{Mean}=\sum_{i=1}^{n}\sum_{j=1}^{m} RSS(i,j) * P(i,j) \quad (2)$$

$$\text{Variance}=\sum_{i=1}^{n}\sum_{j=1}^{m} RSS^{2}(i,j) * P(i,j) - \text{Mean} \quad (3)$$

Where (j) is the numbers of frames for specific MAC address (i), (P) is the probability of the occurrence of specific RSS.

The false positive alarms, generated by previous phases, which is due to the wireless cards that have QoS extensions, where assumptions about monotonic of SNs in frames originating from a STA do not typically hold. In this phase, in addition to detecting spoofed frames in WLAN STAs that are not equipped with QoS interface, the QoS specification is one of the main metrics used to detect spoofing. Therefore, this phase will make extra test on the windows of suspicious frames and use the RSS as a final solution for detecting MAC spoofing. The steps performed by this phase are summarized as follows:

- For the suspicious window that contains duplicate frames of unequal contents, the type field of the frame is examined, a management frame indicates spoofed frame. A data frame leads to examine the subtype field of the duplicate frames, matched priority of the two frames indicates spoofed frame. Unmatched priority of the two suspicious frames leads to examining the RSS of the two frames. If the value of the RSS of the two frames in the range of the variance value, then there is no indication of spoofing. Otherwise, any RSS value deviated from the mean with a value greater than the variance then it is indication of spoofing.
- A challenge for the Transmission Rate Analysis, of the second phase technique is the handling the phenomenon of retransmitted frames due to the frame loss. This phenomenon occurs when a frame is sent and is not received by the receiver STA. In IEEE 802.11, every data frame transmitted is assumed lost if, in response, an acknowledgement frame is not received. When this loss is detected, a frame is

retransmitted with the same SN as was previously sent. In order to solve this problem, in this phase, the monitor STA checks the Retry bit of suspicious frames marked from the previous phase. The following steps are performed:

1. In case, the Retry bit is equal to one (which means a retransmitted frame), the RSS of the suspicious frame is examined. If the value of the RSS is the range of the variance value, then there is no indication of spoofing. Otherwise, the frame is spoofed.
2. IF the Retry bit is equal to zero, the monitor STA checks the type of the suspicious spoofed frame, a management frame indicates spoofing. Because management frame is associated with a single MAC sequence counter, it must be in linear progression. A data frame leads to examine the subtype field of the previous and next frames, matched priority of the two frames indicates spoofed frame. Unmatched Frame priority leads to examine the RSS of the suspicious frame. The RSS indicates either spoofing or not which depends on RSS deviation from the mean.

4. SIMULATION RESULTS

This section evaluates the performance of the SN-R-SS detection method by comparing it with two other well-known different methods; FRR and FRR-RA methods. FRR and FRR-RA methods are implemented separately in this work, and then the results obtained from these methods are used to evaluate the SN-R-SS detection method for MAC spoof detection. An attack view has one genuine STA, one attacker STA which spoofs the MAC address of the genuine STA; both of them are able to be connected to the internet as shown in **Fig. 1**. The distance between an attacker STA and Access Point (AP) is 7 meter, between a genuine STA and Ap is 3 meter, and between an attacker and genuine STAs is 10 meter. The practical works is conducted by changing the MAC address of the attacker STA to the address of the victim STA. Then around 80 frames are extracted from the file, produced in the capturing stage, to evaluate the performance of the SN-R-SS detection method compared to the FRR and FRR-RA detection methods. The window size for the implementation of the three methods mentioned above is taken to be ten.

Description and evaluation the performance of the system with two types of wireless IEEE 802.11 attacker models are studied. The two types of wireless IEEE 802.11 are:

- STAs without QoS property.
- STAs with QoS property.

Figure 1. an Attacker model.

4.1 STAs without QoS Property

In this case, victim STA and attacker STA do not have QoS Property. Figures (2, 3, and 4) illustrate the results performance of applying FRR, FRR-RA and the SN-R-SS detection methods, respectively. The raising edge lines of the three Figures indicate spoofing or false positive alarms. When there are no spoofed frames and no false positive alarms, the Figures show only straight line (the x-axis) shown in the Figures. The false negative alarms are not shown in the figures because they are passed through the detection system as they were genuine frames.

In terms of false positive alarms and spoof detection, it is observed from the figures that both the SN-R-SS detection method and FRR-RA methods give better performance than FRR method since FRR method generates large number of false positive alarms than the others. Also the SN-R-SS detection method gives better performance than FRR-RA method since FFR-RA generates larger number of false positives than the SN-R-SS detection method.

Fig. 2 shows the result performance which is obtained from FRR method. The FRR method produces 82.5% spoofing and false positive. The spoof and false positive alarms signs, shown in the figure, is very high compared to other methods. Actually, FRR method generates many false positive alarms mostly due to the following reasons:

- Frame loss.
- Out of order frames.
- One of duplicate frames is spoofed.
- Retransmitted frame due to the loss of an ACK frame.

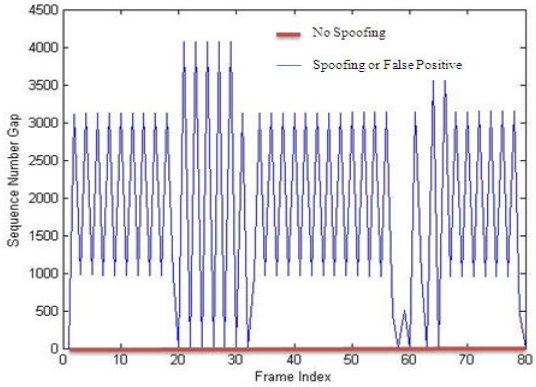

Figure 2. FRR method.

The results which are obtained from the FRR-RA method are shown in **Fig. 3.** The FRR-RA method produces 28.75% spoofing and false positive. The spoof and false positive alarms signs are less than the spoof and false positive alarms signs shown in **Fig. 2** of FRR method. This method decreases the false positive alarms which occur in FRR method because:

- It treats and overcomes the states of the frame loss.
- This method treats the spoofing in duplicate frames which are not treated in the FRR method.

But also this method suffers from generating false positive alarms for the following states:

- Out of order frames.
- Retransmitted frame due to the loss of an ACK frame

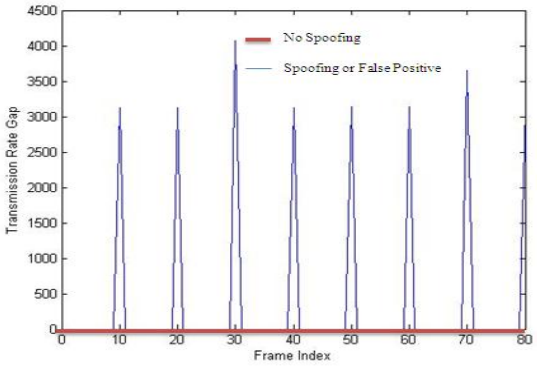

Figure 3. FRR-RA method.

Fig. 4 shows the results which are obtained from SN-R-SS detection method. The SN-R-SS detection method produces 25% spoofing and false positive. This Figure shows a better performance results than FRR-RA method. As shown in the Figure, the spoof and false positive signs are less than the spoof and false positive alarms signs shown in **Fig. 3**. This is because the SN-R-SS detection method can solve all of the following problems that are encountered in FRR and FRR-RA:

- Frame loss.

- Out of order frames.

- One of duplicate frames is spoofed.

- Retransmitted frames due to the loss of an ACK frame.

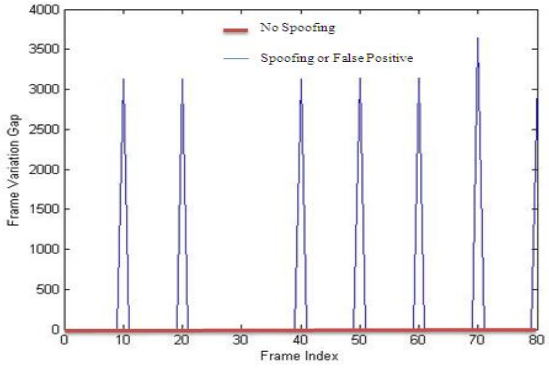

Figure 4. SN-R-SS detection method.

4.2 STAs with QoS Property

Three cases will be studied in this section:

- An attacker has QoS property while the victim does not have it.
- An attacker does not have QoS property while the victim has this property.
- Both of them (an attacker STA and the victim STA) have QoS property.

The results shown in Figures (5 to 13) illustrate the performance of FRR, FRR-RA and the SN-R-SS detection methods, respectively. In terms of false positive alarms and spoof detection, it is observed from the figures that the SN-R-SS detection method gives better performance than FRR and FRR-RA methods. FRR and FRR-RA generate large number of false positive alarms. The main reason of these alarms is the QoS property in the WLAN card of STAs.

- **attacker with QoS / victim without QoS**

In this case an attacker STA has QoS property in its WLAN card, but the victim does not have this property in its WLAN card. Figures (5, 6 and 7) illustrate the results performance of applying FRR, FRR-RA and the SN-R-SS detection methods, respectively.

Fig. 5 shows the result performance which is obtained from FRR method. The FRR method produces 22.5% spoofing and false positive.The spoof and false positive alarms signs, shown in the figure, is very high compared to other methods. The reasons for generating false positive alarms, in FRR method, are:

- Frame loss.
- Out of order frames.
- One of duplicate frames is spoofed.
- Retransmitted frame due to the loss of an ACK frame.
- The QoS property of an attacker STA.

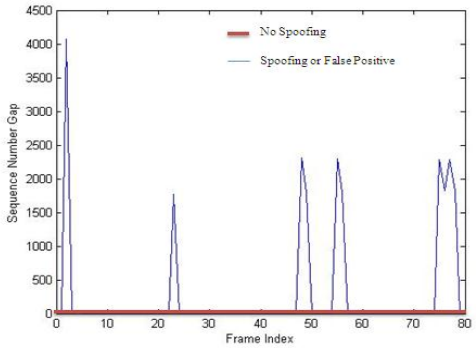

Figure 5. FRR method.

The results performance which are obtained from the FRR-RA method are shown in **Fig. 6**. The FRR-RA method produces 17.5% spoofing and false positive. The spoof and false positive signs are less than the spoof and false positive signs shown in **Fig. 5** of FRR method. FRR-RA method fails to overcome the false positive alarms generated due QoS property of WLAN card.

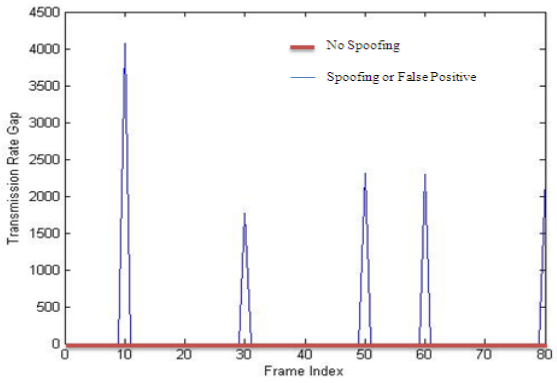

Figure 6. FRR-RA method.

Fig. 7 shows the result of the performance which is obtained from SN-R-SS detection method. The SN-R-SS detection method produces 13.75% spoofing and false positive. The SN-R-SS detection method gives better results than the other two methods (FRR and FRR-RA). As shown in the Figure, the spoof and false positive signs are less than the spoof and false positive signs shown in **Fig. 5** and **Fig. 6** respectively.

The following are the reasons for generating false positive alarms that are faced totally in FRR and partially in FRR-RA and solved by the SN-R-SS detection method:

- It treats the case of frame loss.
- It treats the problem of out of order frames.
- It treats the problem of spoofing existence in duplicate frames.
- It treats the problem of the retransmitted frame due to the loss of an ACK frame.
- It treats the problem of QoS property in an attacker STA WLAN card.

Although the SN-R-SS detection method has better spoof detection capability than FRR and FRR-RA, as indicated by the rising edge signs shown in **Fig. 7**, but also the rising edge signs could partially indicates false positive alarms. The false positive alarms signs shown in **Fig. 7** are generated due to the RSS environmental variation, calibration drift, and other factors that make it difficult to trace the RSS value as these disturbances make it unstable and noisy.

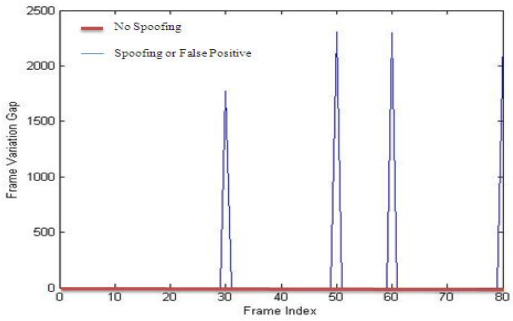

Figure 7. SN-R-SS detection method

- **Victim with QoS / Attacker without QoS**

In this case, an attacker STA has no QoS property and the victim STA has QoS property. Figures (8, 9 and 10) illustrate the results performance of applying FRR, FRR-RA and the SN-R-SS detection methods, respectively. The results show that the SN-R-SS detection method gives better result than

FRR and FRR-RA methods. The same analysis and performance results discussed in the previous case are applied for this case, for the three detection method FRR, FRR-RA and SN-R-SS detection method, are shown in Figures (8, 9 and 10) respectively.

Fig. 8 shows the results which are obtained from FRR method. The FRR method produces 90% spoofing and false positive.

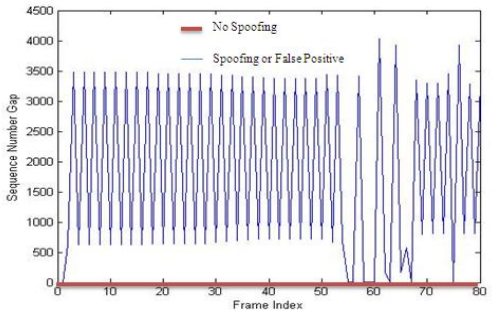

Figure 8. FRR method.

Fig. 9 shows the results which are obtained from applying FRR-RA method on the data file. The FRR-RA method produces 28.75% spoofing and false positive.

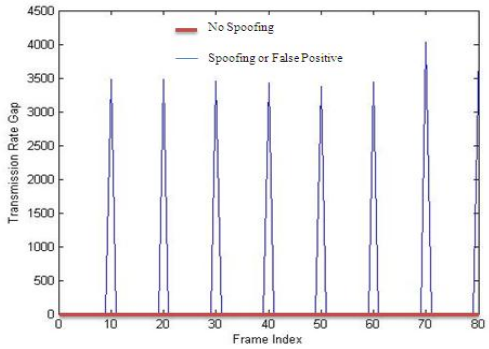

Figure 9.FRR-RA method.

Fig. 10 shows the results which are obtained from applying SN-R-SS detection method on the data file. The SN-R-SS detection method produces 25% spoofing and false positive.

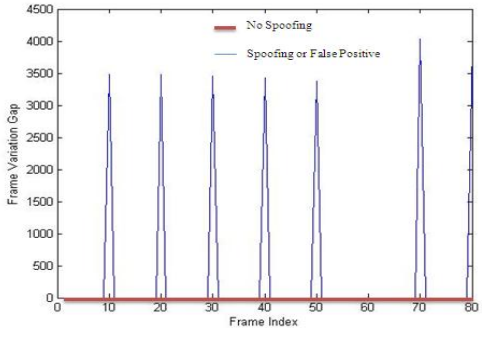

Figure 10. SN-R-SS detection method.

- **Victim and Attacker with QoS Property**

In this case both attacker and victim STAs have QoS property in their WLAN cards. Figures (11, 12 and 13) illustrate the results performance of applying FRR, FRR-RA and the SN-R-SS detection methods, respectively. By applying the three methods (FRR, FRR-RA and the SN-R-SS detection method) on the data file. The SN-R-SS detection method gives better results than the other methods (FRR and FRR-RA). All the analysis and performance results discussed in the first case are also applied to this case for the three detection method FRR, FRR-RA and SN-R-SS detection method, are shown in Figures (11, 12 and 13) respectively.

Fig. 11 shows the results which are obtained from FRR method. The FRR method produces 36.25% spoofing and false positive.

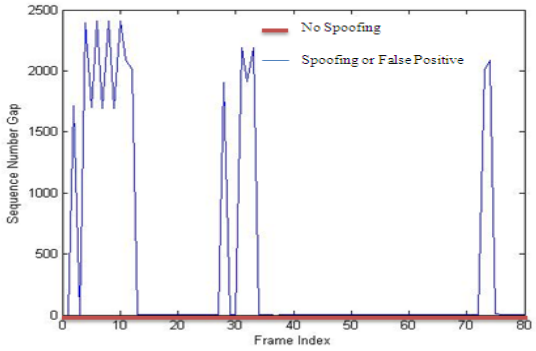

Figure 11. FRR method.

Fig. 12 shows the results which are obtained from FRR-RA method. The FRR-RA method produces 17.5% spoofing and false positive.

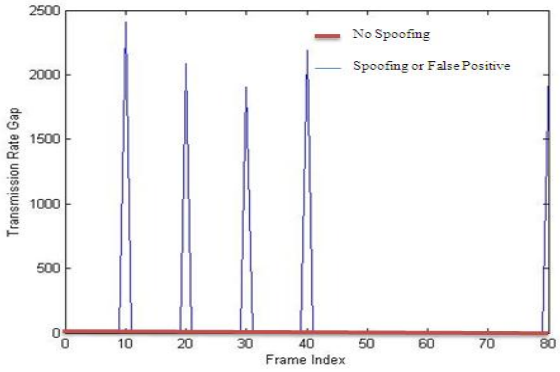

Figure 12. FRR-RA method.

The results which are obtained from applying SN-R-SS detection method on data file are shown in **Fig. 13**. The SN-R-SS detection method produces 13.75% spoofing and false positive.

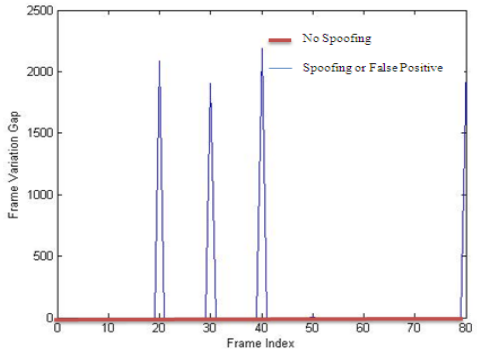

Figure 13.SN-R-SS detection method.

5. CONCLUSION

During the study and development of the proposed system, several points observed and noticed:

After deep analysis and inspection of the existing MAC spoof detection systems, it is found and realized that one mechanism such as FRR, FRR-RA or RSS alone is not sufficient to build efficient MAC spoof detection system. Each one of the mentioned detection system has its drawbacks in detecting MAC spoof. To enhance the MAC spoofing detection system, many factors has to be taken into account to design reliable detection system.

The results that have been obtained from SN-R-SS detection method after compared with two detection methods (FRR and FRR-RA) indicate that the SN-R-SS detection method gives better results performance than FRR and FRR-RA MAC spoof detection methods.

SN-R-SS detection method treats the problems when an attacker STA and victim STA have QoS property in the WLAN card, when attacker STA has QoS property while the victim STA does not have this property and the case when an attacker STA does not have QoS property while the victim STA has this property. The SN-R-SS detection method produced better results performance than FRR and FRR-RA when wireless station is equipped with Qos property WLAN interface card.

SN-R-SS detection method does not work well when the attacker and genuine STA are placed near enough to each other. This is because the final phase of SN-R-SS detection method depends on RSS value. In other satuation, when an attacker and the victim close to each other, the RSS value of an attacker STA is approximately equal to the RSS value of the victim STA. This statuation causes the RSS phase genrates false positives and negatives alarms.

SN-R-SS detection method does not work well when the victim STA is mobile. This is because the final phase of SN-R-SS detection method depends on RSS value. In case, when the victim STA is mobile STA, This causes oscilating of the RSS value received at the monitor STA that could generate false positives and negatives alarms.

SN-R-SS detection method unable to detect the attacker presence if victim not communicating. This results in false negative alarms.

Due the three phases of checking embedded in the SN-R-SS detection method which requires a lot of computation. The SN-R-SS detection method will not be able to conform in the real time spoof detection. But there is always tradeoff between security required and time consuming.

In this paper, the third phase is RSS phase; the researchers can use other fingerprinting tools in the STA to enhance the system. Other attributes can be used to uniquely identify WLAN station. Such attributes like wireless driver fingerprinting.

The researcher can use backpropagation neural network to obtain required values of threshold and window size which are used in first phase of SN-R-SS detection method algorithm instead of fixed values. In this case the system will be enhanced.

REFERENCES

- Bansal, R., etal., *2008, Non-Cryptographic Methods of MAC Spoof Detection in Wireless LAN*, Networks. ICON 2008.16th IEEE International Conference on, ISSN 1556-6463.

- Chandrasekaran, G., etal., *2009, Detecting Identity Spoofs in IEEE 802.11e Wireless Networks*, Global Telecommunications Conference,.Globecom 2009.IEEE , ISSN 1930-529X.

- Chumchu, P., etal., *2011, A new MAC Address Spoofing Detection Algorithm using PLCP Header*, Information Networking (ICOIN), 2011 International Conference on, ISSN 1976-7684.
- Goel, S., etal., *2009, An Improved Method of Detecting Spoofed Attack in Wireless LAN*, Networks and Communications. NETCOM '09.First International Conference on.

- Guo, F., etal., *2006, Sequence Number-Based MAC Address Spoof Detection*, Recent Advances in Intrusion DetectionLecture Notes in Computer Science, Vol 3858.

- Idland, C., *June 2011, Detecting MAC Spoofing Attacks in 802.11 Networks Through Fingerprinting on MAC Layer*, M.Sc. Thesis, Norwegian University of Science and Technology.

- Konings, B., etal., *2009, Channel Switch and Quiet Attack: New DoS Attacks Exploiting The 802.11 Standard*, Local Computer Networks. LCN 2009.IEEE 34th Conference on.

- Li, Q., etal., *December 2007, Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships*, Ieee Transection on Information Forensics and Security, VOL. 2, NO. 4.

- Madory,D., *June 2006, New Methods of Spoof Detection in 802.11b Wireless Networking*, M.Sc. thesis, Thayer School of Engineering.

- Sheng, Y., etal., *April 2008, Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength*, NFOCOM 2008. The 27th Conference on Computer Communications. IEEE,ISSN 0743-166X.