International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Study an Improvisation Method for Detecting Spoofed Attack in Wireless LAN

R R. Agale[1], S V. Athawale[2]
Department of Computer Engineering, AISSMS COE, Savitribai Phule Pune University

Abstract— In terms of network security, spoofing is gaining illegitimate advantage by falsifying data. Spoofing can be done by a person or a program. Popularity of spoofing is increasing because of less precautions taken by application while verifying identity. In case of wireless security, spoofing threats are increasing. If MAC address act as only identification of the wireless devices, the adversary can pretend as any wireless device by changing MAC address using various free available tools over the internet. Therefore detection of presence of the adversary can avoid the launching of other wireless attacks. After lots of research on anomaly detection, still some wireless attacks are undetected. The analysis of possible reasons for generating false positive and false negative in Forge Resistance Relationship (FRR) spoof detection method is explained in this paper. Also on the basis of anomaly detection, the FRR rate analysis (FRR-RA) is compared with parent FRR method of different network scenarios FRR-RA method fails to identify all the spoofing attacks of scenario where attacker is sending the forged sequence numbered spoofed packets of higher signal rate than genuine packet sender. We are proposing a solution to this attack scenario. The proposed algorithm is combination of FRR-RA and Received Signal Strength (RSS), considering there is no change in environmental condition and no multipath effect.

Keywords— MAC address, false positive, false negative, anomaly detection, Forge resistance relationship.

I. INTRODUCTION

Free availability of MAC address changing tools publicly, gives chance to an attacker to masquerade the network identifiers. The various attacks like denial of service, man in the middle, session hijacking, and synchronization are generated due to spoofing attack. Spoofing is gaining illegitimate advantage by falsifying data. Hackers are using Kismet or Ethereal tool to capture packets on an encrypted network, decode it as well as can get the valid MAC address of a network. SMAC is easy and powerful MAC addresses changer, regardless the permission of manufacture. MAC address changed by these tools sustains from reboots. Not only a hacker but anyone can generate random MAC address, validate MAC address and view Mac addresses using freely available tools over the internet. Therefore it is necessary to identify the presence of anomaly of having spoofed MAC address and discard them from the network. In operating systems like windows, through network control panel MAC address can be changed. And it can facilitate a hacker to connect to wireless network, bypassing MAC address filtering. Also in Linux operating system, command like 'ifconfig' and ioctl() function can be used to achieve the same result. Existing encryption methods like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or 802.11i (WPA2), can give protection for data frames only. WPA and WPA2 security can be bypassed and broken in many situation. Unfortunately, they cannot protect the control frames. Maintenance of communication in the networks is done by management frames. Authenticating of management frames can prevent them from spoofing, however authentication of Beacon frames and probe response frames may not be possible always.

Beacon frames, sent out at regular intervals to publicize the presence of an Access Point in wireless network, broadcasting SSID to connect to the network. Any change in beacon frames may lead to Power Saving Mode attacks, Denial of service attack [8]. Various MAC spoofing detection techniques generate large number of false positives, but they do not detect the beacon frames spoofing. The false alarm raised by Forge Resistance Relationship (FRR) Method can be reduced by analysing the reasons for false negative and false. By analysing transmission rate of each detected spoofed packets by FRR method can reduce false alarm. After FRR method, detected spoofed packets will be analysed. And if result is positive then spoofing alarm is raised and spoofed packet is dropped from analysis window. The rest of the paper is organized as follows. The various spoofing detection methods described in Section II. Section III describes parent Forge Resistance Relationship method, reasons for false positive and false negative. Section IV describes the improved method FRR. The proposed solution which is a combination of FRA-RA and RSS method is described in section V. The proposed algorithm is given in Section VI. Finally, Section VII concludes the paper.

II. RELATED WORK

This section illustrates the pros and cons of different MAC address spoof detection methods. For securing a network from attack like

identity fraud, a traditional cryptographic authentication as well as hop-by-hop authentication framework can be used. But various cryptographic authentications as well as hop-by-hop authentication protocol requires infrastructural operating cost and computational cost for distributing, and maintaining the cryptographic keys. Since wireless devices are constrained in case of power and accessibility of resources, hence cryptographic authentication methods are not considered. A method proposed by Guo and Chiueh [3], is based on incremental behaviour of 12 bit sequence number fields of the frame. It creates irregularity in the behaviour of sequence number pointing spoofing attack. A threshold value is set to check the probability of false alarm and missed detection. If threshold is smaller than gap, then spoof detection alarm is raised. MacSpoof [7] uses the same approach.

A proposed method [4] is based on analysis of transmission rate of the frames transmitted by a wireless device along with sequence number field. Due to this, the problem of generating false positive alarms in case of normal loss of packets is reduced. Transmission rate is calculated by taking difference between modulo 4095 of sequence numbers from consecutive frames and dividing by the difference between arrival times of respective frame. This method introduces a theoretical limit of number of frames sent by wireless device in 1 second. If this gap exceeds than theoretical limit then spoof detection alarm will be raised. Qing Li. And Wade Trappe [4] [1] introduced Forge Resistance Relationship method for anomaly detection of spoofed packets. Authors considered changing behaviour of sequence number field relation to spoof detection. If the adversary transmits data first then the detection rules will follow sequence numbers, and when the legitimate device finally transmit data, the discontinuity will be detected. If legitimate device remains silent and does not transmitting the data then FRR spoof detection method results in non-recognition of the adversary.

Authors [5], used concept of Received Signal Strength. Signal strength of a received frame is measured at the receiver's antenna gives output as power, transmission loss, etc. The transmission powers and frame distribution patterns of the wireless device do not change frequently, and therefore this technique is used in detecting spoofing. A radical change in RSS values of frames received from same MAC address alarms as spoofing. Short term Fourier Transform (STFT) can also be used to detect spoofing behaviour by analysing frequency instead power of received packet. Also RSS values are used to derive the location of the attacker node in wireless network. The method proposed by Martinez [6] identifies the masquerading of the beacon frames. It helps to reduce the number of false positives in sequence number analysis detection method in case of MAC address spoofing. In, 802.11 beacon frames are sent out at regular intervals to publicize the presence of an Access Point in wireless network, broadcasting SSID to connect to the network. The beacon frames must be transmitted after beacon intervals, mentioned in the header. The method analyses the time gap between the beacons frame, called as Delta. If Delta is smaller than threshold then packets are considered as anomalous.

III. FRR METHOD

All Forge Resistance Relationship (FRR) Method lowers the false positives and increases the number of spoofed frames detected. A lot of computation power is required such that each frame is analysed for so many numbers of time. If both an attacker and legitimate station are sending data simultaneously then FRR method generates false positives. If the adversary transmits data first then the detection rules will follow sequence numbers, and when the legitimate device finally transmit data, the discontinuity will be detected. If legitimate device remains silent and does not transmitting the data then FRR spoof detection method results in non-recognition of adversary. It does not support in case of victim silent problem. Analysis of the reason for false negative and false positive may result into improvements in FRR method.

A. Reasons For False Positive

1) FRR operates on a window which consists of n consecutive sequence numbered frames. Detection of the one spoofed packet raises alarm for previous n consecutive frames. Therefore FRR method raises n number of alarms.
2) The victim is transmitting very few packets and adversary transmitting continuous stream of packet resulting flood in the network.
3) In this situation adversary act as the only transmitter, the FRR method considers adversary packet to be genuine and raises spoofing alarm for victim packets.
4) The Frame loss is more than threshold value, then it results as false positive because spoofing is detected on the basis of difference inconsecutive sequence numbers of frame in window.
5) Out of order retransmitted frames results as false positive because sequence number of frames varies more than threshold value.

B. Reasons for False Negative

1) The victim is silent and only an attacker is transmitting data then FRR method cannot find the sequence number of legitimate device.
2) An attacker is sending spoofed packets of higher rate than the victim then it may result in receiving continuous frames of an attacker greater than window size.
3) An attacker transmits the forged sequence number spoofed frame and finally the victim transmits original frame of this sequence number which get lost.

IV. FRR- RA METHOD

Forge Detection of spoofed packet can prevent the launching of others attack. FRR-RA operates on a window which consists of n consecutive sequence numbered frames and calculates 'n-1' sequence number differences like FRR method. Differences in transmission rate and consecutive sequence numbered 'n' frames are considered for reducing false negative and false positive in FRR-RA method. Transmission rates considers possibility of packet loss resulting in not raising false positive alarm for packet loss. Transmission rate is calculated by taking difference between modulo 4095 of sequence numbers from consecutive frames and dividing by the difference between arrival times of respective frame. In case of retransmission and out of order frame, the current sequence number of frame equals or smaller than last sequence number of received frame is given to the received frame. If current packet is retransmitted, then there must be a copy of it at monitor node in same analysing window of packets. For verification, contents of both packets are matched such that current sequence number frame is not spoofed but a retransmitted packet of legitimate device.

In case the contents of the packets do not match, then originality of packet is checked by calculating transmission rate of first same sequence number packet. If first same sequence number packet fails in rate analysis then it proves that the second same sequence number packet is original. Then mark the spoofed packet and drop it from analysing window of packets. In FRR-RA method, spoofed packets dropped by FRR method are further analysed by transmission rate method. Packet which is detected as spoofed by both the methods is dropped from analysing window of packets to avoid raising false positive alarms. This prevents false positive alarming for previous 'n' consecutive packets. To avoid false negative alarming in FRR-RA method, the strategy used is after receiving every 9th packet monitor node sends periodic probing. The Sequence number of probing response should be less than threshold gap between last or previous last received packet sequence number. All packets of window will be dropped if packets are not in threshold gap, considering packets are received from attacker and victim is silent.

V. PROPOSED SOLUTION

The FRR-RA method unable to perform spoof detection of frames having higher signal rate due to some false positive and false negative alarms. Due to higher signal rate of an attacker, the analysis window may not contain genuine packets resulting the whole analysis window contains forged sequence numbered spoofed packets. FRR-RA method fails here because it cannot detect all the spoofed frames because all frames of legitimate device are forged. Authors [5], used concept of Received Signal Strength. Signal strength of a received frame is measured at the receiver's antenna gives output as power, transmission loss, etc. The transmission powers and frame distribution patterns of the wireless device do not change frequently, and therefore this technique is used in detecting spoofing. A radical change in RSS values of frames received from same MAC address alarms as spoofing.

The proposed solution is combination of FRR-RA and Received Signal Strength (RSS). As there is no change in environmental condition and no multipath effect, each station has a signal strength which does not change frequently so change in RSS values of frames received from same MAC address indicates spoofing. At the stage of analysis window we can check uniqueness of received signal strength. Adversary can't detect the unique received signal strength of legitimate device, hence an attacker not able to a spoof.

VI. PROPOSED ALGORITHM

A. Check presence of two packets of same sequence number in the window of frames. It avoids false positive situation.
B. If two packets of same sequence number are present then match the contents of both packets. Check contents of saved packet and duplicate or retransmitted packet of original station. Drop the duplicate packet and add next packet to the window. Dropping of packet avoids false positive situation. If contents are not matched then one of the packet is spoofed.
C. Raise Alarm for all spoofed packets.
D. To determine the spoofed packet among these two of the window, perform rate analysis of first same sequence numbered packet with its previous & next packet. If rate analysis raises no spoofing alarm, then second packet is spoofed. Drop the

spoofed packet of the window to avoid the false positive situation. Raise alarm for the dropped spoofed packet.

E. In analysis window, spoofed packets having same sequence number and are received from same MAC address then check uniqueness of received signal strength. The RSS of an attacker will have radical change in RSS values than RSS value of legitimate device. Drop the packet which has radical changes in RSS.

F. Transmission rate is calculated for all spoofed packet detected by FRR method. The spoofed packets dropped by FRR method are further analysed by transmission rate method. Packet which is detected as spoofed by both the methods is dropped from analysing window of packets to avoid raising false positive alarms. This prevents false positive alarming for previous 'n' consecutive packets.

G. After every 9th received packet monitor node sends periodic. The Sequence number of probing response should be less than threshold gap between last or previous last received packet sequence number. All packets of window will be dropped if packets are not in threshold gap, considering packets are received from an attacker and victim is silent.

VII. CONCLUSIONS

The MAC address spoofing detection techniques are generation of too many false positives. Spoofing also makes possible other attacks in Wireless LAN. In wireless networks, both management and control frames are sent unencrypted and unauthenticated which results in risk of various attacks. FRR RA is an improved method than the parent FRR method. It also detects spoofing in case of victim silent problem. It is very complex method and require a lot of computation power because each frame is analysed for so many numbers of times. Improved FRR method is more suitable for high security level requirement. The FRR-RA method unable to perform spoof detection of frames having higher signal rate than legitimate device. The proposed solution gives better spoof detection results than FRR-RA method provided no environmental change and multipath effect. For future scope we can find another method to do improvisations in FRR- RA method.

VIII. ACKNOWLEDGMENT

This paper involves number of respected helping hands. I am grateful to Prof. S. V. Athawale for his dedication and valuable guidance. I would like to thank the Department of Computer Engineering, AISSMS COE, Pune for their uninterrupted help and support.

REFERENCES

[1] Shikha Goel and Sudesh Kumar, "An Improved Method of Detecting Spoofed Attack in Wireless LAN", IEEE, 2009.
[2] Shikha Goel, Vijender Kaushik, Dr. Suruchi Gautam, "Spoofing Detection Methods in Wireless LAN(WLAN) - A Study with pros and cons", AETS, 2013.
[3] F. Guo and T. cker Chiueh, "Sequence number- based MAC address spoof detection", Advances in Intrusion Detection Seattle, Sept. 2005.
[4] Qing Li and Wade Trappe, "Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships", IEEE, 2007.
[5] Yingying Chen, Wade Trappe, Richard P. Martin, "Detecting and Localizing Wireless Spoofing Attacks", IEEE, 2007.
[6] Asier Mart´ınez, Urko Zurutuzayz, et.al, "Beacon Frame Spoofing Attack Detection in IEEE 802.11 Networks", IEEE, 2008.
[7] Yingying Chen, Wade Trappe, Richard P. Martin, "Detecting and Localizing Wireless Spoofing Attacks", IEEE, 2007.
[8] W. A. Arbaugh, N. Shankar, and Y. J. Wan, "Your 802.11 wireless network has no clothes", IEEE- Wireless Communications, vol. 9, pp. 44–51, 2002.
[9] Sangram Goyal and Dr. S. A. Vetha Manickam, "Wireless LAN Security", Center for Information and Network Security, Pune University.
[10] F. Guo and T. cker Chiueh, "Sequence number- based MAC address spoof detection", Advances in Intrusion Detection Seattle, Sept. 2005.
[11] Shikha, Vijender Kaushik, Suruchi Gautam "Wireless LAN (WLAN) Spoofing Detection Methods - Analysis and the victim Silent case" ,IEEE, 2013.