ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

Wireless LAN (WLAN) Spoofing Attack- A Proposed Detection Method in Victim Silent Case

Shikha Goel

Deptt. of CSE, Mewar University, Mewar

Abstract: Spoofing makes the task of identification and tracking back of the perpetrator / initiator in Cyber Crimes very difficult, e.g. those relating to denial of service, session hijacking, and address masquerading attacks by changing its network identifiers in WLANs. In such a scenario, spoof detection methods have gain wide attention. One way to prevent from spoofing is to authenticate the frames. However, in 802.11 WLANs, authentication and encryption for management and control frames is not provided. Further, present MAC spoofing detection techniques bring out large number of false positives. This paper presents the proposed method of WLAN MAC spoofing attack in Victim Silent Case. One way hash function method is used along with an extra field named claimed identity field. The proposed method can detect the MAC spoofed packet having arrival time close to genuine packet. The method is analysed in false positive and false negative situation. By way of analysis of results, an outline of future work is also suggested in the concluding remarks.

Keywords: 802.11 Wireless LAN, SNRA, Sequence number, MAC address, spoofing, false positives / negatives, transmission rate analysis, FRR, forge resistance relationship (FRR-RA) rate analysis.

I. INTRODUCTION

This Wireless LANs are widely deployed in places such as corporate office conference rooms, industrial warehouses, Internet-ready classrooms, and even coffeehouses. By their very nature, wireless networks are difficult to roll out, secure and manage, even for the most savvy network administrators. Wireless networks offer great potential for exploitation for two reasons; they use the airwaves for communication, and wireless-enabled laptops are ubiquitous. To make the most of their security planning, enterprises need to focus on threats that pose the greatest risk and MAC spoofing is one of the most serious threat, in which an anomaly hide its presence in the network to impersonate as genuine node using various tools [4][5] freely available on the internet. Anyone within the geographical network range of an open, unencrypted wireless network can sniff on all the traffic using tools like WireShark, OmniView, CommView available on internet, gain unauthorized access to network resources, possibly sending spam or doing other illegal actions using the victim's MAC address. The various attack performing tools like Airjack, Void 11, KisMac, FakeAP, Dsniff, AirSnaf are freely available on the internet.

Spoofing makes the task of identification and tracking back of the perpetrator / initiator in Cyber Crimes very difficult. It is further facilitate many other forms of attacks [1][6][7] on the network like Denial of Service attack [8][14][15], de-authentication/disassociation, power saving attack [11][12], session hijacking[2][3], AP spoofing, man in the middle attack. It is thus necessary to identify the presence of anomaly of having spoofed MAC address and eliminate them from the network. Anomaly hides its presence to impersonate as genuine node.

Presently known anomaly detection algorithm works only if legitimate device also communicating. They do not work in victim silence problem. This paper discusses the victim silence problem along with its solution and increase in overhead with it. We consider the possibility that adversary not only changes the MAC address, but also forges the sequences number field value as used by legitimate device. Our strategy uses an extra field which is claimed identity field along with the sequence number field. Adversary presence can be detected by using extra field. This field uses a one way hash function [9] and make adversary difficult to predict the value.

The paper is organized as follows. Literature survey is described in Section II. The solution to legitimate device silence problem is described in Section III. Section IV describes the method we used to identify anomalous traffic. Extra field which claims identity is used with one way hash function. Evaluation of method is done in Section V describing Test bed setup and various scenarios of false positive, false negative and overhead involved. Finally, Section V concludes the paper and gives further work.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

II. LITERATURE SURVEY- MAC SPOOF DETECTION METHOD

Guo and Chiueh [10] [13] proposed a method for MAC spoof detection based on the gap in sequence number field of the two successive frames. In case, gap finds out to be more than the threshold value, spoofing alarm is created. Madory [14] proposed the method based on sequence number rate analysis. This method considers the probability of packet loss in the network. This technique considers both the arrival time and sequence number of the frame to conquer the difficulty of false positive due to loss of frame. Qing Li. and Wade Trappe [15] [16] defined a relation to detect spoofing based on varying activities of sequence number field. It examines windows of packets instead of two consequent packets as in previous methods. Windows having packets more than two is analyzed. The setting of window size is done as per security level of application. Higher window size means more security and more computation for spoof detection. Yingying Chen [17] gives a spoof detection method based on Signal strength of a receiver frame. The transmission power and frame distribution pattern of the station does not change frequently, and this property is used in detecting spoofing. A radical change in RSS value of frames received from same MAC address indicates spoofing. S. Goel [19] proposes a method which combines both the transmission rate method and FRR method to bring down false positives and false negatives in FRR method. The Problems in the existing MAC spoof detection methods [18] are generation of false positive/negative.

III. VICTIM SILENT CASE –AN ILLUSTRATION WITH PROPOSED SOLUTION

Legitimate device not communicating make detection algorithms difficult to detect anomaly. Adversary presence can be detected by discontinuity if legitimate device is communicating. Sequence number based detection algorithm keep track adversary sequence number and unable to identify anomaly. Sequence number rate analysis method found only adversary transmission rate and no change in transmission rate. Received signal strength based detection algorithm also not detects any anomaly as no change in signal strength.

To detect the anomaly in this situation, we propose two solutions. Firstly, it is required for the legitimate device to transmit periodically some packets to announce its presence like access point send beacon frame and showing its presence. Control frame has frame control type field value 01 and their subtype fields which are reserve are 0000 to 1001. Rest control subtype fields can be used to send periodic presence of the legitimate device. Secondly, silence problem can also be solved by sending ARP request by monitor node periodically. ARP response sequence number field used by detection algorithm for anomaly detection. ARP response sequence number should be in threshold gap with last received packet sequence number. This solution increases the probing overhead. But there is always a trade-off between overhead and anomaly detection rate. In some scenarios it requires to use both control frames periodic transmission and ARP request sending. There may be scenario that adversary sending data using claim field and then periodic control frame arrives. To check whether control frame is spoofed or not, ARP request is send. ARP response sequence number will detect whether data or control frames are spoofed.

IV. CLAIMED IDENTITY FIELD- USING ONE WAY HASH FUNCTION

Suppose two packets arrive at approximate same time (i.e. arrival time gap is very less) having same sequence number and signal strength. It is possible to forge the sequence number field as send in clear. Also arrival time of next packet can be guessed by adversary. And signal strength can be same if adversary is close to the real source. Hence sequence numbers of received packets are {45, 46, 47, 48, 48, 49….}. This indicates that either the first or second packet having sequence number 48 is spoofed. The packet is not duplicate sequence number, as content of both packets are not same. In this case all spoof detection algorithms usually consider first packet to be original and the second one to be spoofed and may give false negative.

To solve this problem we use the claimed identity field for each transmitted packets. This field used for taking decision in anomaly detection which uses one way hash function. Suppose source has to send n packets during communication. Source chooses a number m greater than value n. Source first chooses the final packet claimed identity value. Then calculate the previous packet identity value using hash function. The function can be represented as

S(i-1)=Hash(S(i)) where 1<=i<=m

S(i) and S(i-1) are claimed identity field of packet having sequence number I and i-1 respectively.

Monitoring node will detect the next packet to be anomalous if claimed identity field value of received packet can't derive the previous received packet field value. The first identification value can be send during authentication phase. Considering the adversary side, brute force will not work to find inverse relationship. One way hash functions are used, it is unable to predict the value of claimed identify field of next packet.

Considering the overhead associated include storage and authentication. More the number of packets send during a session, the more storage space needed. Efficient one way

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

hash function with reduced storage requirements is given in [9]. Finally, For packet loss, the function used is

S(l)=hash(hash(hash…..S(x)))

S(l) is the claimed identity field value of previous packet having sequence number l.

S(x) is the claimed identity field value of received packet having sequence number x.

Threshold value for packet loss is 3. Also whenever there is gap due to packet lost, previous packet saved in the buffer to solve the problem of out of order delivery. Suppose the sequence number of packets arrived are { 44, 47, 46, 48…}. Monitor node put the 44th sequence number packet in buffer and 47th sequence number packet is checked with packet loss function. When 46th sequence number packet reach it again checked with packet loss function with 47th and 44th packet sequence number. This gives no false positive alert.

V. TEST BED SETUP AND RESULT ANALYSIS

In spoofing scenario, there are more than two devices on the network with same network identity. To validate our proposed algorithm, we use network simulator NS2 to provide simulation environment. The simulator allows us to add an additional extra field to the packet in the end which is claimed identity field. The size of the field taken is 1 bye. But can be increase as per requirement of the security. In the environment both adversary and genuine station uses the linksys WUSB11 Network Adapter providing 802.11b interface. False alarm may occur with the increase in packet loss rate. We consider threshold value to be 3. So, we increase the packet loss from 3%, 5%, to 8%. More the packet loss more the false alarm occurs which shown in fig 1. Various false positive and false negative situations are presented by S. Goel [19].

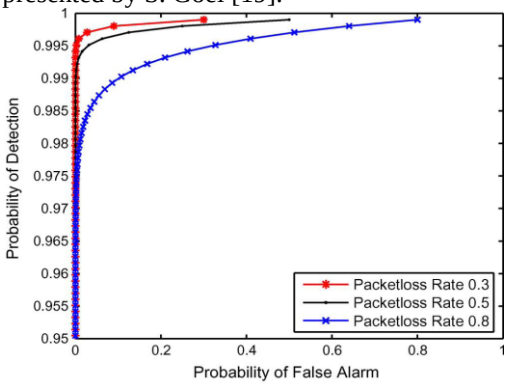


Fig. 1. Claimed identifier field value is of 1 byte. Curve plotted between detection and false alarm rate in different packet loss

False Positive test

False positive may occur in the following in these scenarios

- When out of order packet arrives. Threshold set for out of order delivery is 3. when this packet arrives, it is saved in buffer along with the previous packet. With the next arrived packet, we calculate the hash value for both the out of order and previous packet. Suppose the sequence numbers of arrived packets are {45, 47, 46, 48…}. 46th sequence number packet is put in buffer for verification. Next packet having 48th sequence number arrives. We check S(47)=Hash(S(48)) and S(46)=Hash(Hash(S(48))).
- When packet loss is more. If packet loss is more, it will give lot of false positives.
- When periodic control frame send by adversary. In this case monitor node send ARP request to source. ARP response sequence number field detects the spoofed control frame.

False Negative Test

False negative may occur in the following in these scenarios

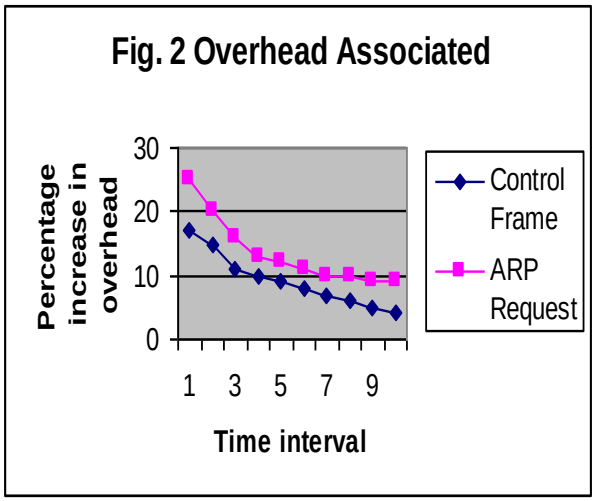
- When adversary guesses the same the identity field as that of real source. Possibility of guessing can be decreased with increase in the size of field. Also probability of guessing to be successful is very low.
- When real source is silent and adversary uses claimed identity field after analysis. Real source sends the control packets periodically. It announces its sequence number. Also, it is not possible as authentication required for sending first identity field value. Also, monitor node stores the last sequence number of the real source.

Overhead involves

- Storage overhead increase with increase in number of packets sends during session. Efficient one way hash function with reduced storage requirements is used.
- ARP request sending overhead. Send the ARP request if there was a lot of change in the sequence number field.
- Control frames periodically send by source to announce its presence when not transmitting data. If the time interval after which control frame is send increases, overhead decreases. Fig 2 indicates the time interval and overhead associated.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013



VI. CONCLUSION

In this paper, we present the use of claimed identity field along with sequence number to detect Wireless LAN MAC address spoofing. This additional field uses the one way hash function, which make adversary difficult to forge the value. This method able to detect which packet is spoofed if same sequence number packets arrive at the same time. Solution to the legitimate device silence problem is also presented. Presently available spoof detection methods unable to detect the adversary presence if victim not communicating. Various false positive and false negative scenarios are discussed with solution. This method gives only large false positive alerts if packet loss is very large. This method also require storage overhead, authentication overhead. But there is always trade-off between security required and overheads. Beacon frame spoofing may result in synchronization and power saving mode attack possible. These frames cannot be authenticated. It is required to develop an efficient approach, which can detect the management frame spoofing as well. Efficient methods required to reduce overhead associated with this method.

REFERENCES

1. A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1x standard," uMIACS-TR, Feb,2002,[Online Available]-citeseer.ist.psu.edu/566520 .html
2. G. R. Anbd Smith J., L. M., and A. . Clark, "Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks," AusCERT, 2005, pp. 26–38.
3. R. Gill, J. Smith, and A. Clark, "Experiences in passively detecting session hijacking attacks in IEEE 802.11 networks," ACS, AISW 2006, vol. 54. , pp. 221–230.
4. SMAC: MAC-address Changer, http://www.softpedia.com/get/Network-Tools/Misc-Networking-Tools/SMAC-MAC-Address-Changer.shtml.
5. MACMakeUp: MAC Address Spoofing Tools.
6. F.Robinson,"802.11i and WPA up Close" . Network Computing, 2004.
7. Sangram Goyal and Dr. S. A. Vetha Manickam, "Wireless LAN Security", Center for Information and Network Security, Pune University.
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. Y.C. Hu, M. Jakobsson, and A. Perrig, "Efficient constructions for one-way hash chains," in Applied Cryptography and Network Security (ACNS), 2005
10. F. Guo and T. cker Chiueh, "Sequence number- based MAC address spoof detection", Advances in Intrusion Detection Seattle, Sept. 2005.
11. J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," USENIX, Aug 2003, pp. 15–28. [Online Available]: http://www.cs.ucsd.edu/_savage/papers /UsenixSec03.pdf
12. IEEE, "1999 edition (r2003) part 11: Wireless LAN medium access control (MAC) and physical layer phy) specifications," IEEE, Tech. Rep., 1999 (R2003)
13. F. Guo and T. cker Chiueh, "Sequence number-based MAC address spoof detection", RAID, 2005, pp. 309–329.
14. D.C. Madory, "New Methods of Spoof detection in 802.11b wireless networks", M.Eng. Thesis, Dartmouth College, 2006.
15. Qing Li and Wade Trappe, "Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships", IEEE, 2007.
16. Qing Li and Wade Trappe, "Light-weight Detection of Spoofing Attacks in Wireless Networks", IEEE, 2006.
17. Yingying Chen, Wade Trappe, Richard P. Martin, "Detecting and Localizing Wireless Spoofing Attacks", IEEE, 2007.
18. Bansal, R. Tiwari, S. Bansal, D., "Non-cryptographic methods of MAC spoof detection in wireless LAN", IEEE ICON, 2008.
19. Goel, S. Kumar, S. "An Improved Method of Detecting Spoofed attack in Wireless LAN", IEEE Netcom, 2009.