A Solution to Spoofed PS-Poll Based Denial of Service Attacks in IEEE 802.11 WLANs

ZAFFAR I. QURESHI[1],BABER ASLAM[1], ATHAR MOHSIN[2], YONUS JAVED[3]
Information Security Department, College of Signals[1]
Computer Science Department, College of Signals[2]
Computer Engineering Department, College of Electrical &Mechanical Engineering[3]
National University of Science & Technology
Tamizuddin Road, Rawalpindi
PAKISTAN

Abstract: - Wireless Local Area Networks (WLAN) provide connectivity along with flexibility at low cost. Appreciating the exponential growth in this area, Institute of Electrical and Electronics Engineers (IEEE) ratified IEEE standard 802.11 in 1999 which was widely accepted as the defacto industry standard for interconnection of portable devices. Due to the scarcity of battery power in portable devices operating in WLANs, 802.11 directly addresses the issue of Power Saving (PS) and defines a whole mechanism to allow stations (STA) to go into sleep mode without losing information, as access point (AP) keeps buffering the messages directed to the sleeping STA. Growing use of 802.11 lead to the identification of flaws in security specifications of the standard known as Wired Equivalent Privacy (WEP). These flaws were addressed by the introduction of amendments/enhancements. However, IEEE's security enhancements failed to achieve the desired objectives especially availability, which is the main concern of any network administrator. Identity theft due to unauthenticated management and control frames left a window open for hackers to launch successful Denial of Service (DoS) attacks. The PS functions of 802.11 present several identity based vulnerabilities, exploiting which, an attacker can spoof the polling message on behalf of the STA and cause the AP to discard the buffered packets of the client while it is asleep. As a result, an attacker can block the victim STA from receiving frames from the AP, thus launching a successful DoS attack. In this paper we have explained the spoofed PS-Poll based DoS attack and proposed a robust solution to this problem.

Key-Words: - Wireless security, Denial of service DoS, 802.11, Power Saving PS, PS-Poll, Association ID.

1. Introduction

The proliferation of networking across the world continues to grow at an astounding rate. Devices connected over wireless networks provide an opportunity to the communicating world to free itself from the restrictive, inflexible and expensive web of network cables and wires. After ratification of IEEE standard 802.11 in 1999 [1], it was widely accepted as the defacto wireless standard. Nevertheless, the rapid growth in the use of WLANs can be attributed to the prolific innovatively in portable mobile devices. The complete range of devices like laptops, Personal Digital Assistants (PDA), pervasive computing devices, mobile phones and sensors show a propensity towards miniaturization. With miniaturization came the issues of computing and power efficiency.

The key concern with 802.11 WLANs has always been security. WLANs add an extra level of security complexity compared to their wired counterparts. Security risks in WLAN are sum of the risks of operating a wired network, new risks introduced due to portability of wireless devices and risks due to the unrestrictive nature of wireless transmission. The security specifications of 802.11 known as WEP, failed to address the issues of confidentiality, availability and integrity. The security holes are well known [2, 3]. To address the security concerns new standards were introduced. The related standards are IEEE Standard 802.1x [4] and IEEE Standard 802.11i [5]. The IEEE 802.1x, a port-level access control protocol provides a security framework for networks, including wired and wireless both. The IEEE 802.11i standard is created for wireless specific security functions that operate with IEEE 802.1x. With these standards IEEE proposed a secure architecture called Robust Security Network Architecture (RSNA). RSNA addressed the issues of data confidentiality and integrity but failed to resolve the compromise of availability, which is the first causality in a DoS attack.

WLANs are typically related to a system that is pervasively and unobtrusively embedded in the environment, completely connected, intuitive,

effortlessly portable and constantly available. In such systems, battery power is a scarce resource. Current wireless devices do not manage their energy usage well and as such quickly drain their batteries. As the authors of [6] show, a large part of power drain can be attributed to the wireless LAN card. This is the reason why IEEE 802.11 directly addresses the issue of PS and defines a whole mechanism to allow STAs to go into sleep mode for long periods of time without losing information.

Different modes in which devices operate within a network, present different vulnerabilities, exploiting which, the confidentiality; availability and integrity of information in a network can be compromised. Identity theft due to unprotected management and control frames, which is a persistent flaw in WEP and 802.11i, leaves a window open for hackers to launch successful DoS attacks. High rate of success of these attacks in PS mode is mainly due to two reasons. Firstly, portable mobile devices recurrently operate in PS mode to conserve their scarcest recourse i.e. battery power and secondly, at the time when the attack is being perpetrated, the legitimate user is sleeping and thus oblivious of this malicious activity on the network. Therefore, an attacker can easily spoof the polling message on behalf of the client and cause the AP to discard the client's packets while it is asleep, thus blocking the victim STA from receiving frames from the AP. In this paper we have explained the spoofed PS-Poll DoS attack and have proposed a robust solution to this problem.

The rest of the paper is organized in following sections; section 2 discusses related previous work, section 3 describes the communication setup procedure and power management in IEEE 802.11 standard, section 4 analyzes the DoS attacks in PS mode, section 5 presents our proposed solution and sections 6 concludes the paper.

2. Related Work

Techniques to detect spoofing of MAC addresses have been presented in [7]. Authors of [8] studied usage patterns in university networks using information from packet capturing tools and syslog files. However, techniques studied in their work focus on detection and not prevention.

E. D. Cardenas [9] uses Reverse Address Resolution Protocol (RARP) to detect spoofing. If MAC address is spoofed then we will get two IP addresses in response to RARP indicating multiple NICs with same MAC address. However, the solution is not applicable to our research, since the victim node will be in PS mode and RARP will fetch only one response i.e. from the attacker node.

Many researchers for e.g. F. Anjum et al. [10], F. Guo et al. [11], D. Dasgupta et al. [12] and H. Xia et al. [13] have proposed sequence number based solutions to different DoS attacks. However, as the PS-Poll frames do not include the sequence number field, therefore these solutions cannot be applied to PS-Poll based DoS attacks.

LaRoche et al. [14] proposed a genetic programming based network intrusion detection. There exists a relationship between a node and the traffic it generates, if spoofing is in progress then traffic statistics will change. This solution can detect spoofing but cannot prevent it; further the solution needs a separate monitoring device.

Several commercial softwares are available providing 802.11 WLAN intrusion detection and security solutions that identify security risks and attacks. They provide real-time network audits and monitor the health of the WLAN. These solutions require special hardware / software and are expensive to install and maintain.

The solutions using separate hardware monitoring devices cannot be implemented easily at each node. The sequence number based approaches discussed above can be useful against some DoS attacks, but will fail in PS-Poll based DoS attacks because of the absence of sequence number field in PS-Poll frame. Most of these solutions are hardware intensive, requiring special hardware. However, our proposed solutions can easily be implemented on individual nodes by firmware upgrade only. As it uses a pseudo randomized Association ID (AID) frame, encrypted using pre established keys, so it cannot be spoofed or predicted by the attacker.

3. Communication Setup and Power Management in IEEE 802.11

3.1 Overview of Communication Setup

The communication setup takes place in four stages which are maintained by state machines running both at AP and STA. When a STA powers up it is in state 1 as it starts probing for AP or receives a beacon. Following the discovery of an appropriate AP, open system authentication takes place. On successful authentication, state machines of both AP and STA transit to state 2. While in state 2, wireless client initiates association request to AP and on successful association, both transit to state 3. This is where AID, a 16 bit number, is assigned sequentially by AP to each associating STA. While in state 3, 802.1x authentication is initiated to generate Master Session Key (MSK). On successful completion of

authentication, a Pair wise Master key (PMK) will be established. This step may be skipped if Pre-Shared Key (PSK) is used as PMK. A 4-way handshake between AP and STA follows to generate Pair-wise Transient Key (PTK) from PMK or PSK. Both the AP and client, now being in state 4, can initiate data encryption using PTK along with selected data confidentiality algorithm.

3.2 Power States

IEEE 802.11 has two power management modes i.e. the active mode and the PS mode. In the active mode, a STA is fully powered and can send and receive frames. In the PS mode, STA can be in one of two states, the sleep state and the awake state. Most of the time, a STA in the PS mode remains in the sleep state, it only gets into the awake state to listen to management frames called beacons transmitted by AP. In this mode, a STA consumes very low power [15]. When a STA is in PS mode, the AP buffers all the frames that are directed to that STA. By reading the beacon frames, a STA in PS mode can determine if there are data frames stored for it and decide if it wants to change to the awake state to receive pending frames from AP.

3.3 Power Saving Mode

To enter PS mode, a STA must first inform the AP. A frame with a PS request is sent from STA to AP following the basic medium access procedure [1]. A reply should be sent by AP and received by STA before it can enter PS mode. Once the request reply exchange is successful, the STA goes in sleep state of PS mode and operates with very little power consumption. AP buffers all the frames addressed to this STA. In case of unsuccessful exchange of request / reply message, the STA will remain in active mode and retransmit the request to the AP.

The interval, at which a STA in PS mode wakes up to listen for beacon frames, is defined by the value in "Beacon Interval" field

Contained in beacon frames is information, coded in partial virtual bitmap called Traffic Indication Map (TIM). TIM is composed of 2,008 bits. Each bit corresponds to a particular AID, if set, it indicates whether any frames directed to the indicated STA are pending in the AP. If there is an indication of pending unicast frames, the STA can choose to receive those frames at its convenience.

To receive a unicast frame, the STA sends out a PS-Poll to the AP, this signals that the STA is ready to receive a frame. After the reception of PS-Poll, the AP forwards a pending frame to the STA. The "More Data" field can be set in the data frame to indicate further pending frames buffered at AP. Broadcast / multicast frames are sent without any PS-Poll message so STAs in PS mode cannot choose when to receive them, but can choose to ignore these frames. After successful reception of data frames, the STA can either go back to sleep state or choose to receive more frames by sending out another PS-Poll. If no more frames are buffered in the AP, then the STA will go back to the sleep state.

If a mobile STA switches to the active mode from a sleeping state, frames can be transmitted without waiting for a PS-Poll. PS-Poll frames indicate that a STA in PS mode has temporarily switched to an active mode and is ready to receive buffered frames, even without receiving explicit notification to that effect.

3.4 PS-Poll Message

The format of PS-Poll message frame is shown in (Fig. 1). The Control Frame field and Frame Check Sequence (FCS) field have standard settings, as defined in [1]. The AID field is a 16 bit value assigned by an AP during association. The Basic Service Set Identifier (BSSID) is a 48-bit field of the same format as an IEEE 802 MAC address. This field uniquely identifies each BSS. The value of this field is the MAC address currently in use by the STA, stored in the AP of the BSS. The Transmitter Address (TA) field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the Wireless Medium (WM).

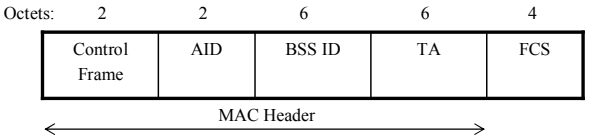

Figure 1: PS-Poll Frame

4. DoS Attack in PS Mode

A malicious user could sniff transmitting MAC addresses in a network and change its own MAC address to pose as a legitimate user to gain entry into the network. With packet-sniffers for wireless networks available for free, coupled with the fact that MAC addresses are sent in the clear, it takes little effort for an adventurous attacker to sniff out legitimate MAC addresses (most softwares provide this facility) and subsequently use them in spoofing. Many MAC spoofing tools and techniques (such as *SpoofMAC* [16], *SMAC* [17]) are available. Changing the MAC address of a wireless card is also a very trivial task that can be performed even by novice attackers, using softwares (such as

Technitium MAC Address Changer [18], *MAC-Changer* [19]). With a spoofed MAC address a malicious user could exploit the network and launch DoS attacks.

4.1 PS-Poll Based DoS Attack

An attacker could initiate a DoS attack by sending spoofed PS-Poll frames, pretending to be a legitimate client, operating in PS mode. The PS-Poll frame can easily be spoofed since it is neither encrypted nor authenticated. An attacker within range, running *NetStumbler* [20], *Airsnarf* [21], *dsniff* [22] or similar type of sniffing software, can sniff the management frames and easily extract the AID and BSSID being sent in clear. Using these tools, the attacker can also spoof the transmission at the time of association and subsequently send counterfeited PS-Poll frames thus forcing AP to transmit the buffered data which will be lost because the legitimate recipient is still asleep (Fig. 2).

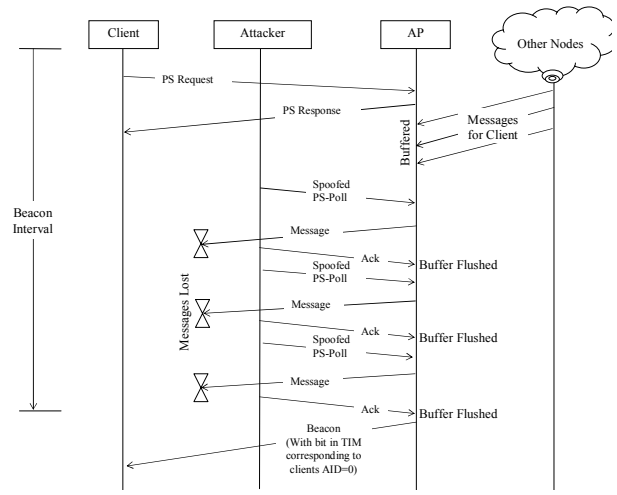

Figure 2: PS-Poll DoS Attack

5. Solution to Ps-Poll DoS Attack

5.1 Basic Assumptions

The basic assumptions in our proposed solution are that the state machines of AP and client are in state 4, so the STA is in possession of PTK distributed by AP. The initiation of PS-Poll message by the client will be from state 4.

5.2 Proposed Solution

The basic idea of proposed solution is to encrypt the AID field in PS-Poll frame. The encryption will be done by using a simple Exclusive OR (XOR) operation between AID and Key Stream (KS). For generation of KS a Pseudo Random Function (PRF) defined in [5] can be used as suggested in [23]. The KS generation function is defined as (1).

$$KS_{160} \leftarrow \{PRF_{160}\ (PSK, \text{“Power Save Protection”}, APA, SA)\}. \quad (1)$$

Where KS_{160} : 160 bit Key stream, generated for encryption of AID.
PRF_{160}: Pseudorandom function producing 160 bits of output, (defined in 8.5.1.1 of [5]).
APA : MAC Address of AP.
SA : MAC Address of STA.

The encryption defined in (2) is a simple bitwise XOR between 16 bit AID assigned to STA at the time of association and 16 bits taken out of generated KS_{160}. For each PS-Poll message, the STA will pickup bits from KS_{160}, starting from 0^{th} bit at LSB of KS_{160} to 15^{th} bit for the first PS-Poll, 16^{th} bit to 31^{st} bit for the second and so on.

$$AID_E \leftarrow AID_{16}\ \text{XOR}\ KS_L^M \quad (2)$$

Where KS_L^M : 16 bit partial key stream to encrypt AID_{16}, taken from KS_{160} starting from LSB side bit L till the MSB side bit M.
AID_E : Association ID after encryption.
AID_{16} : 16 bit AID assigned to the STA by AP at the time of association.
ctr : Counter maintained both at AP and STA for synchronization of partial key stream bits taken from KS_{160}.
L : {(ctr -1) * 16}.
M : (ctr * 16) – 1.

The decryption at AP to authenticate the PS-Poll is again a simple bitwise XOR operation to verify the AID assigned to STA at the time of association.

5.3 Analysis of Proposed Solution

The solution not only detects but also prevents the PS-Poll based DoS attack. To save the processing overhead during communication, KS_{160} can be pre computed during communication setup phase and XOR operation carried out only when a STA in PS mode wants to retrieve frames buffered at AP by sending PS-Poll frame. As the XOR operation is carried out with lowest computing resources, so

during communication the processing overhead is very low.

Each time a STA in PS mode has to send a PS-Poll frame, it picks up a fresh 16 bit partial key stream using the ctr value maintained at the STA as well as at AP. Along with the cryptographic strength of the one-time-key; this method also ensures synchronization of key stream bits at both ends. Moreover, after ten successful PS-Poll messages by a STA, the used 160 bits of KS_{160} will be cleared from memory and new 160 bits KS will be generated for subsequent communication, so we will have fresh KS after every ten PS-Poll frames.

The wireless client can use the proposed solution without need of any special hardware. The solution can be implemented by just a firmware upgrade.

6. Conclusion

IEEE 802.11 standard suffers from basic security flaws. The measures introduced via IEEE standard 802.11i did tackle a number of concerns but failed to address the vulnerabilities exposing the network to DoS attacks. These vulnerabilities linger because of unauthenticated and unencrypted management and control frames. This vulnerability is much pronounced in PS mode due to the fact that clients are inactive in order to conserve battery power and thus oblivious to the attack being perpetrated. This weakness is exploited by attackers to launch spoofed PS-Poll based DoS attacks. A robust solution based on encryption of AID field in PS-Poll message using pre established PTK is proposed. The strength of the solution lies in its simplicity, the use of a new key for encryption of each message and the fact that the solution does not require any additional hardware and can be implemented in both wireless clients and AP via firmware upgrade.

References:

[1] IEEE Standard 802.11-1999, "Wireless LAN Medium Access Control and Physical Layer Specifications", 1999, reaffirmed in June 2003.

[2] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications - The insecurity of 802.11". In *Proc. of the 7th Annual ACM/IEEE International Conf. on Mobile Computing and Networking - Mobicom'01*, Rome, Italy, pp. 180-189, July 2001.

[3] W. A. Arbaugh, N. Shankar, and J. Wang, "Your 802.11 Network has no Clothes". In *Proc. of the First IEEE International Conf. on Wireless LANs and Home Networks*, pp.131-144, December, 2001.

[4] IEEE Standard 802.1X-2004, "Port-Based Network Access Control". December, 2004.

[5] IEEE P802.11i – 2004. "Medium Access Control (MAC) Security Enhancements", July 2004.

[6] Mark Stemm and Randy H. Katz, "Measuring and Reducing Energy Consumption of Network Interfaces in Handheld Devices". In *IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Science*, August 1997.

[7] Wright J., "Detecting Wireless LAN MAC Address spoofing":*http://www.linuxsecurity.com/articles/documentation_article-6585.html*.

[8] Kotz, D., Essien, K., "Analysis of a campus-wide wireless network". In *Proc. of MOBICOM,* 2002.

[9] E. D Cardenas, "MAC Spoofing - An Introduction": *http://www.giac.org/practical/GSEC/*

[10] F. Anjum, S. Das, P. Gopalakrishnan, L. Kant, K. Byungsuk, "Security in an Insecure WLAN Network". In *Proc. of the International Conf. on Wireless Networks, Communications and Mobile Computing,* 2005, pp. 292-297.

[11] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection". In *Proc. of 8th International Symposium on Recent Advances in Intrusion Detection. 2005*.

[12] D. Dasgupta, F. Gonzalez, K. Yallapu and M. Kaniganti, "Multilevel Monitoring and Detection Systems (MMDS)". In *Proc. of the 15th Annual Computer Security Incident Handling Conf. (FIRST)*, Canada, June , 2003.

[13] H. Xia, and J. Brustoloni, "Detecting and Blocking Unauthorized Access in Wi-Fi Networks". In *Proc. of Networking.* 2004.

[14] P. LaRoche, A. N. Zincir-Heywood, "802.11 Network Intrusion Detection using Genetic Programming". In *Proc. of the 2005 workshops on Genetic and evolutionary computation***,** Washington, D.C, 2005, pp. 170 –171

[15] P. J. Havinga and G. J. Smit, "Energy-Efficient TDMA Medium Access Control Protocol Scheduling". In *Proc. Asian International Mobile Computing Conference (AMOC 2000)*. Nov, 2000.

[16] "SpoofMAC": *http://www.klcconsulting.net/smac/*

[17] "SMAC": For Windows VISTA, 2003, XP, and 2000 systems: *http://www.klcconsulting.net/smac/*

[18] "Technitium": MAC address Changer: *www.technitium.com/tmac/index.html*

[19] "MAC Changer": *http://www.alobbs.com/*

[20] "Netstumbler": *http://www.netstumbler.com/*

[21] "Airsnarf": *http://airsnarf.shmoo.com*

[22] "Dsniff": Collection of tools for network penetration: *http://packages.debian.org/stable/net/dsniff* interfaces): *http://www.alobbs.com*.

[23] B. Aslam, M. H. Islam, S. A. Khan, Pseudo randomized sequence number based solution to 802.11 Disassociation DoS Attack. In *Proc. Of the first international; conference on Mobile Computing and Wireless Communications (MCWC 2006),* Amman, Jordan, September 17 – 20, 2006.