Using Randomized Association ID to Detect and Prevent 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 E&M Engineering[3]
National University of Science & Technology
Tamizuddin Road, Rawalpindi
PAKISTAN
{zaffar, baber, athar}@mcs.edu.pk, myjaved@ceme.edu.pk

Abstract: - Wireless Local Area Networks (WLAN) provide connectivity along with flexibility at low cost. Appreciating the exponential growth in this area, the 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, IEEE 802.11 directly addressed the issue of Power Saving (PS) and defined 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 IEEE 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 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 a polling message on behalf of STA and cause AP to discard buffered packets of the client while it is asleep. As a result, an attacker can block victim STA from receiving frames from AP, thus launching a successful DoS attack. The mechanism proposed in [1] addresses the issue of spoofed PS-Poll based DoS attack and proposes a robust solution to this problem. Although the proposed solution was a novel idea; however it was only a mathematical analysis, not verified or tested by implementation on hardware or through simulation. In this extended version of the paper, an endeavor has been made to implement the theoretical idea and validate the mathematical calculations through simulation.

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 networking 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 [2], it was widely accepted as the defacto wireless standard. Nevertheless, the rapid growth in the use of WLANs can be attributed to the prolific innovation 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 IEEE 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 IEEE 802.11 known as WEP, failed to address the issues of confidentiality, availability and integrity. The security vulnerabilities are well known [3, 4]. Researchers investigated the security aspects of 802.11 networks, specifically the security threats by providing an overview of the existing security architectures, the WEP security flaws and the progress made towards replacing WEP [5]. To address these security concerns new standards were introduced. The related standards are IEEE Standard 802.1x [6] and IEEE Standard 802.11i [7]. 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 was 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). It was noted in a security analysis [8], that this framework too does not provide solutions to many DOS attacks. RSNA did address the issues of data confidentiality and integrity but failed to resolve the compromise of availability, which is the first causality in a DoS attack. This is mainly because management and control frames are not encrypted so DOS attacks are very easy to perpetrate. A malicious user can construct a de-authentication or a disassociation request and send it to a client whom it wants to disconnect from the network. Recognizing these shortfalls in RSNA, researchers elucidated these security vulnerabilities and proposed individual solutions [9, 10, 11]. However the niche of DoS attacks in PS mode had not been explored in due significance.

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. The authors of [12] show, a large part of power drain can be attributed to the wireless LAN card. Powering down the transceiver can lead to great power savings in wireless networks. Power conservation in IEEE 802.11 is achieved by minimizing the time spent in active state and maximizing the time in sleep state. However, IEEE 802.11 accomplishes this without sacrificing connectivity. It defines a whole mechanism to allow STAs to go into sleep mode for long periods of time without losing information [13]. As the use of battery operated mobile devices grew, extensive research was also being carried out to propose even more efficient battery power conservation mechanisms [14, 15, 16].

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 IEEE 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 a polling message on behalf of the client and cause the AP to discard 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 communication setup procedure and power management in IEEE 802.11 standard, section 4 analyzes different DoS attacks possible in PS mode, section 5 presents our proposed solution, sections 6 presents the design, conduct and results of simulation, section 7 gives a detailed analysis of the proposed solution and section 8 concludes the paper.

2. Related Work

Techniques to detect spoofing of MAC addresses have been presented in [17]. Authors of [18] 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 [19] 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. [20], F. Guo et al. [21], D. Dasgupta et al. [22] and H. Xia et al. [23] 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. [24] 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. We are presenting a few examples here:-

- *AirDefense Guard* by AirDefense, Inc [25]. Consists of distributed sensors and server appliances. It detects all rogue WLANs, secures a WLAN by recognizing and responding to intrusion and attacks, performs real-time network audits and tracks all WLAN activity. The remote sensors sit near IEEE 802.11 AP to monitor all WLAN activities and report back to the server appliance, which analyzes the traffic in real time.

- *Odyssey Server* by Funk Software, Inc [26]. It is a WLAN access control solution that provides strong security. It includes client and server softwares which secure the authentication and connection of WLAN users. Thus the connection credentials will not be compromised and data privacy will be maintained. Odyssey is based on the IEEE security standard 802.1x, and supports a wide variety of 802.1x security methods.

- *SnifferWireless* by Network General Corporation [27]. Spots security risks in real time, identifies network problems and helps to maximize network investments. It provides WLAN troubleshooting with a wireless specific expert analysis system that enhances visibility into network anomalies and facilitates automatic problem solving.

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.

Limited research work has been done in the area of developing practical or theoretical frameworks handling IEEE 802.11 availability issues or analyzing the security of IEEE 802.11 from this viewpoint. Most of the research focuses on confidentiality and authentication by explaining the problems related to native 802.11 security (WEP and shared-key authentication) and showing how inadequate such mechanisms are. The same effort hasn't been put into analyzing a wireless network's availability and robustness. Despite the fact that many DoS attacks against WLANs are known [8, 10, 11, 28], so far very few research efforts describe the actual implementation of de-authentication and virtual carrier-sense DoS attacks and possible countermeasures [29]. Authors of [30] presented a solution to secure management frames by employing a modified Diffe-Hellman's algorithm for authentication and integrity checks. In that the disassociation and de-authentication frames are checked for authenticity before processing. Ying-Sung Lee et al. proposed random bits placing into unused fields of management frames as an authentication mechanism [31]. Both of these solutions concentrate on de-authentication and association flooding attacks but ignore DoS attacks possible in PS mode. DoS attacks in PS mode have been identified and discussed in all the research work on availability issues [29] but practical solution proposed to counter this vulnerability are very few.

These proposed solutions do add a certain level of security and prevent some DoS attacks, but these solutions are hardware intensive, requiring special hardware. However, our proposed solutions can easily be implemented on individual nodes by just a firmware upgrade. 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, 802.1 x 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 [13]. 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 PS mode remains in sleep state, it only gets into awake state to listen to management frames called beacons transmitted by AP at predefined intervals. In this mode, a STA consumes very low power [32]. When a STA is in PS mode, the AP buffers all the frames that are directed to that STA. The STA periodically changes its state to awake on predefined intervals to read beacon frames. By doing so, a STA in PS mode can determine if there are data frames stored for it and decide if it wants to receive the pending frames from AP by sending periodic PS-Poll messages.

3.3 Power Saving Mode

In a wired environment all one has to do to connect is to plug the wire to the socket in the wall, but in wireless environment it's not that simple. Special frames have to be exchanged at appropriate time. Time brings in the need for synchronization. In PS mode, proper synchronization is of ought most importance. To enter the PS mode, a STA must first inform AP. A frame with a PS request is sent from STA to AP following the basic medium access procedure [2]. 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 (Fig. 1). In case of unsuccessful exchange of request / reply message, the STA will remain in active mode and retransmit the request to the AP.

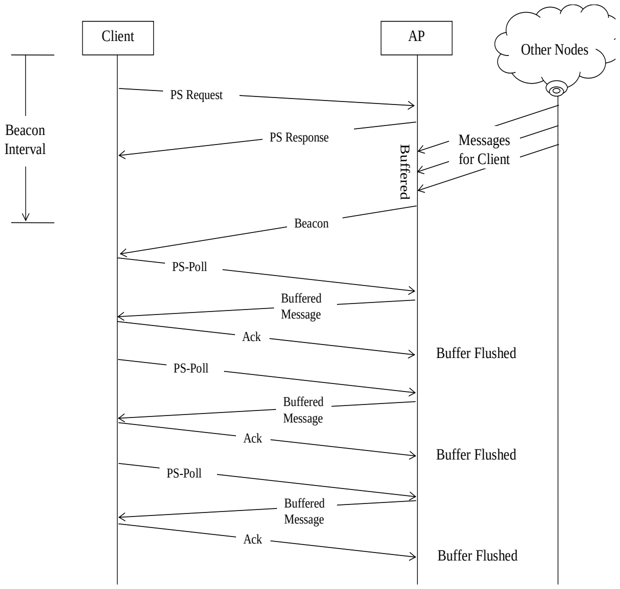
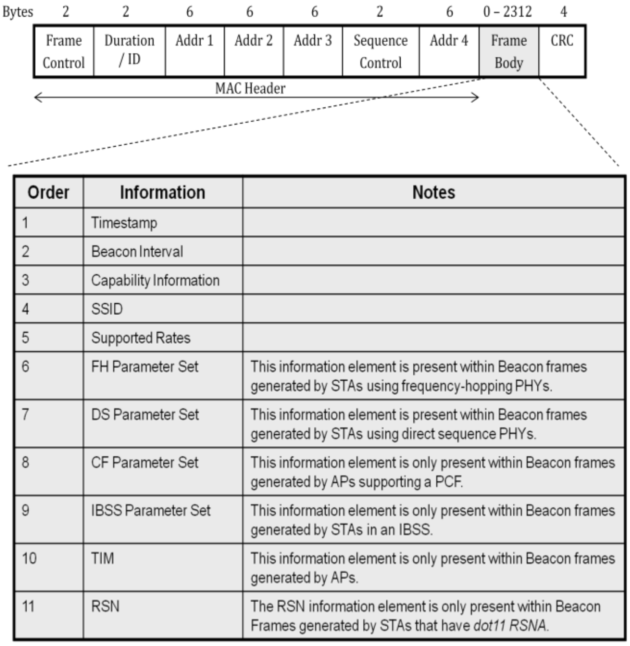


Figure 1: PS Mode

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 (Fig. 2).



Order	Information	Notes
1	Timestamp	
2	Beacon Interval	
3	Capability Information	
4	SSID	
5	Supported Rates	
6	FH Parameter Set	This information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	This information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	This information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	This information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	This information element is only present within Beacon frames generated by APs.
11	RSN	The RSN information element is only present within Beacon Frames generated by STAs that have *dot11 RSNA*.

Figure 2: Management Frame (Beacon)

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.

3.4 PS-Poll Message

The format of PS-Poll message frame is shown in (Fig. 3). The Control Frame field and Frame Check Sequence (FCS) field have standard settings, as defined in [2]. 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).

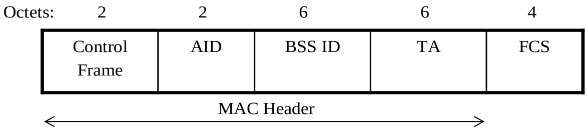


Figure 3: PS-Poll Frame

3.5 AID Field in PS-Poll Frame

AID field (Fig. 4) represents the 16 bit ID of a STA allotted at the time of association. Its value is in the range 1–2007, placed in the 14 Least Significant Bits (LSB) of the AID field. Each of the two Most Significant Bit (MSB) is always set to 1. The remaining 14 bit number in LSB is a sequential counter, incremented by one for each AID generated for every associating STA.

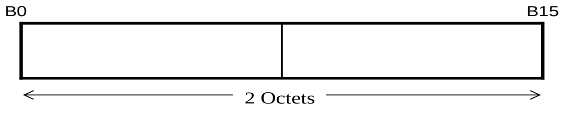


Figure 4: AID Field

4. DoS Attacks 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 enter the network. With packet-sniffers for wireless networks available for free, coupled with the fact that MAC addresses are sent in clear, it takes little effort from 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* [33], *SMAC* [34]) 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* [35], *MAC-Changer* [36]). With 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* [37], *Airsnarf* [38], *dsniff* [39] 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 monitor 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. 5).

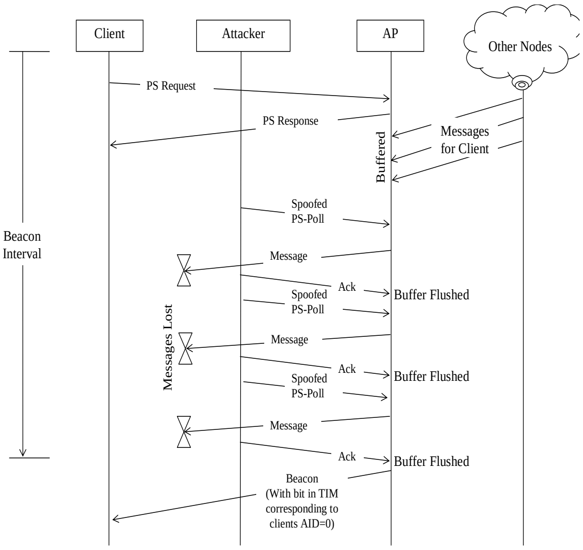


Figure 5: PS-Poll DoS Attack

4.2 Fake AP DoS Attack

Using appropriate hacking tools, an attacker could advertise as a legitimate AP by using the MAC address of an AP and could get clients to connect with it. If the beacon message itself is spoofed, an attacker may convince a STA that there is no pending data, by setting the bits in TIM corresponding to AID of STA in PS mode. So the clients will immediately revert back to sleep state. These attacks are particularly easy with programs and libraries such as *changeM* [40], *FakeAP* [41] and *SchiffmanM* [42].

4.3 TIM Based DoS Attack

The power conservation mechanism relies on time synchronization between the AP and its STAs. Synchronization information, such as the period of TIM packets and timestamp broadcast by the AP are neither authenticated nor encrypted. By forging these management packets an attacker can cause a STA to fall out of sync with the AP and fail to wake up at the appropriate intervals. Many DoS attack tools (such as *Airjack* [43], *KisMAC* [44], *Void11* [45]) can be used to launch these attacks.

In this paper we have focused on DoS attacks perpetrated by attackers exploiting the vulnerabilities in unauthenticated and unencrypted PS-Poll frames, which are exchanged in PS mode of IEEE 802.11 WLANs. We have focused only on the scenario in which communicating nodes are working in infrastructure based network architecture.

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 the 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 [7] can be used as suggested in [9]. The KS generation function is defined as (1).

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

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 [7])

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, the STA will pickup bits from KS_{160}, starting from 0th bit at LSB of KS_{160} to 15th bit for the first PS-Poll, 16th bit to 31st bit for the second and so on.

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

Where KS_L^M : Partial key stream to encrypt AID_{16}, taken from KS_{160}, starting from LSB side bit L till 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 (3) at AP to authenticate the PS-Poll is again a simple bitwise XOR to verify the AID assigned to STA at the time of association.

$$AID_{16} \leftarrow AID_E\ XOR\ KS_L^M \qquad (3)$$

On completion of communication setup, KS_{160} will be generated using PTK already available with AP and STA. Each time a PS-Poll message is sent, 16 bits out of KS_{160} will be used for encryption of the 16 bit AID. A counter (ctr) will be used on both ends to keep the partial KS synchronized. When the 160 bits of generated KS are used, these will be discarded and fresh 160 bits will be generated. To explain the process of key generation, the flow diagram is given (Fig. 6).

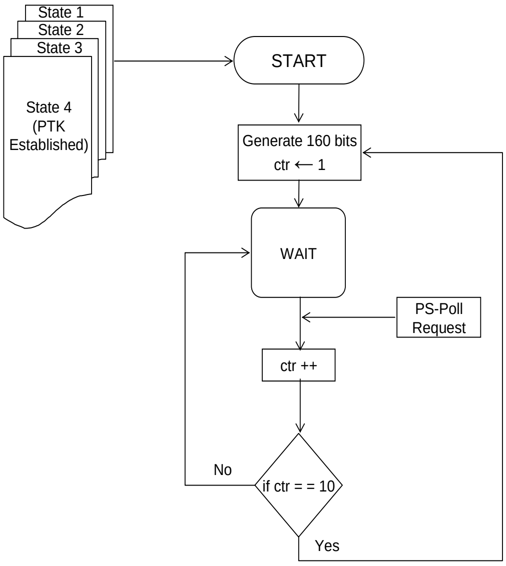


Figure 6: Flow Chart (Key Generation)

6. Implementation of Proposed Solution

The mechanism proposed in [1] addresses the issue of spoofed PS-Poll based DoS attack and proposes a robust solution to this problem. Although the proposed solution was a novel idea; however it was only a mathematical analysis, not verified or tested by implementation on hardware or through simulation. In this extended version of the paper, we have made an endeavor to implement the theoretical idea and validate the mathematical calculations through simulations.

The functionality and usability of a number of available simulators like OPNET, OMNET, NS2 and ModelSim was studied. Due to the possibility of implementation of proposed solution on hardware (wireless nodes and APs), ModelSim was selected. Verilog programming language with ModelSim as simulation tool formed the platform for the simulation and verification.

6.1 Simulator Design

The Verilog based IEEE WLAN simulator presented in [46] was used as a starting point. The simulator has a modular design and consists of media, carrier sense, receive, transmit, test-bench and log modules. Test-bench is the top level module which integrates all modules together and is also used to control the sequence of events. The simulation results are observed from the generated log. First of all the PS mode functionality was added to the simulator. This involved modifications to both the AP and wireless nodes. TIM and PS-Poll messages were defined and necessary logic was incorporated to ensure correct functioning as per IEEE 802.11 standard. Secondly, modifications were made to incorporate the proposed solution in the simulator. Both standard and modified protocols were implemented to get a fair comparison of performance. Two new types of wireless nodes were defined. The attacker node was defined to launch DoS attacks as described in section 4 and the modified node was defined to test the effectiveness of proposed solution. AP was also modified to incorporate the proposed solution.

6.2 Simulation Scenario

The simulation scenario comprises of a wireless network having two APs and three wireless nodes. One wireless node is a simple node without the modified protocol (Standard Node). The other has modified protocol incorporating the proposed solution (Modified Node). The third is attacker node without the modified protocol (Attacker Node) that launches PS-Poll based DoS attacks. Simple protocol is implemented on one AP (Standard AP) and the other (Modified AP) is with modified protocol incorporating proposed solution (Fig. 7).

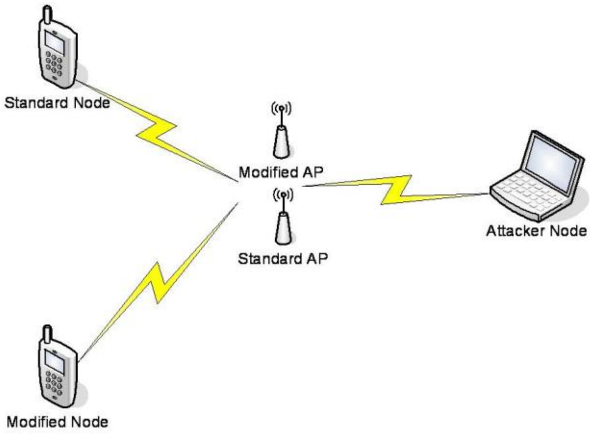


Figure 7: Simulation Scenario

6.3 Simulation Conducted

First of all standard network was simulated, this was necessary to confirm the correct functioning of standard protocol. The wireless network of standard AP and standard wireless nodes was simulated. After initial communication setup, several data transfer sessions between the wireless nodes were simulated. PS mode was repeatedly activated to check buffering and later delivery of frames by AP. The connections were initiated from different possible initial states.

Second simulation was conducted to check the effectiveness of DoS attack launched by attacker. For this the attacker node was added to the network. The standard node entered PS mode and the other node passed messages which were buffered at standard AP. A successful attack was launched by the attacker node by sending spoofed PS-Poll frames to the standard AP.

Third simulation was conducted to verify the proposed solution. For this a wireless network consisting of a standard node, a modified node, an attacker node and a modified AP was simulated. Modified node entered PS mode and DoS attack was launched by attacker node. Changing states of devices confirmed the validity of proposed solution. Successful processing of legitimate PS-Poll notification of modified node by the modified AP confirmed the normal PS mode process.

Finally, the attacker node was modified to continuously launch DoS attacks using new randomized AID each time. This was done to check the robustness of solution.

6.4 Simulation Results

The results were checked by both the waveform and log. The waveform shows the transition to states, sending / receiving of frames and updating of different variables / states graphically. The log is more concise and only provides the actions performed at various devices along with time and other important data.

The results clearly indicated that the standard AP fails to detect the spoofed PS-Poll based DoS attack, whereas the modified AP incorporating the proposed solution detects and effectively blocks this attack and allows successful processing of legitimate PS-Poll notification of modified node by modified AP.

Number of successful attempts of spoofed PS-Poll DoS attack by continuously randomizing the AID was very low; less than 10^{-5}. This showed the robustness of the proposed solution against a brute force search for key space.

7. Analysis of Proposed Solution

The strength of the proposed solution is that it not only detects but also prevents the spoofed PS-Poll based DoS attacks. 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 in 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 counter value maintained at the STA as well as at AP. The cryptographic strength of the KS against a cryptanalysis attempt is that of a One-Time-Pad (OTP) symmetric cipher. Along with the cryptographic strength, this method also ensures synchronization of key stream bits at both ends by maintaining a counter. 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 strength of PRF function is well established therefore the probability of attacker node generating same encrypted AID is given by equation (4).

$$P\,\{Spoofed\,AID = \,AID_E\} = \,{}^{1}\!/_{2^{16}} \qquad (4)$$

Fresh bits are used each time to encrypt AID; therefore the probability of success of the attack is independent of the number of tries made. The probability of at least one success in 'N' tries is given by equation (5). Similar results were observed from simulation.

$$P\,\{Atleast\,One\,Spoofed\,AID = \,AID_E\} \\ = 1 - (1 - P\,\{Spoofed\,AID = \,AID_E\})^N \qquad (5)$$

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

8. 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 in this paper. The strength of the solution lies in 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.

The proposed solution has been analyzed for its practicability and security. The effectiveness of the solution has also been verified through simulation. The proposed solution can be implemented in the APs and wireless nodes. The solution is effective against advanced attackers. The solution is fast and does not require heavy computation / storage. This property makes it robust against DoS attacks caused by repeated spoofed PS-Poll notifications that consume AP's resources.

The paper is mainly aimed at wireless networks in infrastructure mode in which all the traffic is directed through AP so wireless devices can communicate with each other only via an AP. Future research can be aimed at studying the DoS attacks in ad hoc networks and studying the effectiveness of proposed or a modified version of proposed solution in these networks.

Another possible future research is to confirm the effectiveness of proposed solution by implementing it on actual hardware and make any modification in existing solution if necessary.

References:

[1] Zaffar I. Qureshi, Baber Aslam, Athar Mohsin, Yonus Javed, "A solution to spoofed PS-poll based denial of service attacks in IEEE 802.11 WLANs*"*. In *Proceedings of the 11th WSEAS International Conference on Communications (ICCOM'07),* Vol. 11, Agios Nikolaos, Crete Island, Greece July 2007, pp. 7 –11.

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

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

[4] W. A. Arbaugh, N. Shankar, J. Wang and K. Zhang, "Your 802.11 Network has no Clothes". In *Proceedings of the 1st IEEE International Conference on Wireless LANs and Home Networks*, Singapore, December, 2001, pp.131-144.

[5] S.P. Ahuja and K. Dendukuri, "Security Problems in 802.11 based Wireless Networks". In *Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT 2004)* St. Thomas, US Virgin Islands, November 22-24, 2004.

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

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

[8] A. Mishra, , W. A. Arbaugh, "An initial security analysis of the IEEE 802.1X standard", *Technical Report CS-TR-4328, UMIACS-TR-2002-10,* University of Maryland, February 2002.

[9] B. Aslam, M. H. Islam, S. A. Khan, "Pseudo randomized sequence number based solution to 802.11 Disassociation DoS Attack". In *Proceedings of the 1st International Conference on Mobile Computing and Wireless Communications (MCWC 2006),* Amman, Jordan, September 17 – 20, 2006.

[10] Katerina Argyraki, David R. Cheriton, "Active Internet Traffic Filtering: Real-Time Response to Denial-of-Service Attacks". In *Proceedings of the USENIX Annual Technical Conference,* Anaheim, CA, April 2005.

[11] Daniel B. Faria, David R. Cheriton, "DoS and authentication in wireless public access networks". *Workshop on Wireless Security*. In *Proceedings of the 1st ACM workshop on Wireless security,* Atlanta, GA, USA, 2002, pp. 47 – 56.

[12] 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.

[13] Matthew Gast. "802.11 Wireless Networks: The Definitive Guide". O'Reilly, 0-596-00183-5, April 2002, pp. 122 – 133.

[14] Yoo-Jin Jeong, Soo-Young Shin, Soo-Hyun Park, Chang-Hwa Kim: "PBA: A New MAC Mechanism for efficient wireless communication in Underwater Acoustic Sensor Network", In *Proceedings of 2007 WSEAS International Conference on Circuits, Systems, Signal and Telecommunications*, Gold Coast, Australia, January 2007.

[15] Shun-Ping Chung and Vincent Chen, "Performance of Power Efficient Wake-Up Mechanisms for Mob Multimedia Communication with Bursty Traffic". In *Proceedings of the 5th WSEAS International Conference on Data Networks, Communications and Computers,* Bucharest, Romania, October 2006.

[16] Daji Qiao, Kang G. Shn, "Smart Power-Saving Mode for IEEE 802.11 Wireless LANs", In *Proceedings of 24th Annual IEEE Conference -- INFOCOM'05,* Miami, FL, USA, March 2005.

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

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

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

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

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

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

[23] H. Xia and J. Brustoloni. "Detecting and Blocking Unauthorized Access in Wi-Fi Networks". In *Proceedings of the Networking'2004 Conference, IFIP,* Athens, Greece, *Lecture Notes in Computer Science, 3042:795-806, Springer-Verlag,* May 2004.

[24] P. LaRoche, A. N. Zincir-Heywood, "802.11 Network Intrusion Detection using Genetic Programming". In *Proceedings of the 2005 Workshops on Genetic and Evolutionary*

*Computation***,** Washington, D.C, 2005, pp. 170 –171.

[25] “AirDefense Guard” by AirDefense, Inc: *http://www.airdefence.net*

[26] “Odyssey Client/Server” by Funk Software, Inc: *http://www.juniper.net*

[27] “Sniffer Wireless” by Network General Corporation: *http://www.networkgeneral.com/default.aspx*

[28] Daniel B. Faria, David R. Cheriton, “Detecting Identity-based Attacks in Wireless Networks Using Signalprints”, In *Proceedings of the 5th ACM Workshop on Wireless Security WiSe '06*, Los Angeles, California, USA, September 2006.

[29] John Bellardo and Stefan Savage “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions”. In *Proceedings of the USENIX Security Symposium,* Aug 2003: *http://www.cs.ucsd.edu/users/savage/papers/UsenixSec03.pdf*

[30] Fahad Samad, Waqar Mahmood, Arshad Ali Umar Kaleem. “Improved Security in IEEE802.11 Wireless LANs”. In *Proceedings of the 5th WSEAS International Conference on Data Networks, Communications and Computers (DNCOCO ’06),* Bucharest, Romania, October 2006.

[31] Ying-Sung Lee, Hsien-Te Chien, Wen-Nung Tsai. “Using Random Bit Authentication to Defend IEEE 802.11 DoS Attacks”, In *Proceedings of the 5th WSEAS International Conference on Data Networks, Communications and Computers,* Bucharest, Romania, October 2006.

[32] P. J. Havinga and G. J. Smit, “Energy-Efficient TDMA Medium Access Control Protocol Scheduling”. In *Proceedings of the Asian International Mobile Computing Conference (AMOC 2000)*. Nov, 2000.

[33] “SpoofMAC”: *http://www.klcconsulting.net/smac/*

[34] “SMAC”: For Windows VISTA, 2003, XP, and 2000 Systems: *http://www.klcconsulting.net/smac/*

[35] “Technitium”: MAC address Changer: *www.technitium.com/tmac/index.html*

[36] “MAC Changer”: *http://www.alobbs.com*

[37] “Netstumbler”: *http://www.netstumbler.com*

[38] “Airsnarf”: *http://airsnarf.shmoo.com*

[39] “Dsniff”: Collection of tools for network penetration: *http://packages.debian.org/stable/net/dsniff/*

[40] “ChangerM”: A GNU/Linux Utility for Viewing/Manipulating the MAC Address of Network Interfaces): *http://www.alobbs.com*

[41] “FakeAP”: Black Alchemy Weapons Lab: *http://www.blackalchemy.to/project/fakeap/*

[42] “SchiffmanM”: Radiate 802.11b frame handling: *http://www.packetfactory.net/projects/radiate/*

[43] “Airjack”: *http://sourceforge.net/projects/airjack/*

[44] “KisMAC”: *http://binaervarianz.de/projekte/*

[45] “Void11”: *http://www.wlsec.net/void11/*

[46] B. Aslam, M. Akhlaq, S. A. Khan, “IEEE 802.11 Wireless Network Simulator Using Verilog”, In *Proceedings of the 11th WSEAS International Conference on Communications 2007*, Agios Nikolaos, Crete Island, Greece, July 26-28, 2007.