Coping with Spoofed PS-Poll Based DoS Attack in IEEE 802.11 Networks

Hocine Souilah
Laboratory of Modelling and Optimization of Systems
Faculty of exact science, University of Bejaia, Algeria
hocinesouilah@gmail.com

Abderrahmane Baadache
Laboratory of Modelling and Optimization of Systems
Faculty of exact science, University of Bejaia, Algeria
abderrahmane.baadache@gmail.com

Louiza Bouallouche-Medjkoune
Laboratory of Modelling and Optimization of Systems
Faculty of exact science, University of Bejaia, Algeria
louiza_medjkoune@yahoo.fr

IEEE 802.11 networks are particularly vulnerable to DoS (Denial of Service) attacks targeting the network availability. In this paper, we focus on the PS-Poll based DoS attack, where the attacker spoofs the polling frame on behalf of the client in order to discard the client's buffered packets at the access point level. To cope with this attack, we propose a security solution called APSP (Authenticated Power Save Poll) and based on the integer prime factorization to authenticate PS-Poll frames. Our solution is both detective and preventive one and generates low communication, computing and storage overheads. It did not require any additional hardware and can be implemented via firmware upgrade. Simulation results show that the proposed solution is effective and robust to defend against the considered attack.

IEEE 802.11 networks, DoS attacks, integer prime factorization, power save mode, PS-Poll frame

1. INTRODUCTION

IEEE 802.11 networks are extremely popular and used in several civilian and military applications to avoid the expenses and delays associated with installing wired networks. They are deployed in businesses, homes, communities, and open spaces to provide the connectivity to anyone with a receiver that is in radio range. IEEE 802.11 standards series are providing increasingly higher access speeds and offering some accommodations to users. However, several security issues need to be taken into deeper consideration in order to secure 802.11 wireless communications.

In this paper, we focus on vulnerabilities pronounced in the Power Save Mode (PSM), where the client is in sleep state and unaware to security threats. One of DoS attacks that can be launched in PSM is the spoofed PS-Poll attack, where the attacker spoofs the client PS-Poll frame and sends it, on behalf of the client, to the AP (Access Point). When this spoofed frame is received by the AP, the latter delivers the buffered packets (these packets are intended to be delivered to the legitimate sleepy client) to the attacker, then empties the buffer as soon it receives an acknowledgment from the attacker. This attack can be taken place because PS-Poll frames are neither protected nor authenticated. To cope with this attack, we propose an integer prime factorization based solution called APSP (Authenticated Power Save Poll). To successfully conduct its attack, the attacker should decompose large integer numbers into non-trivial prime divisors. No efficient integer prime factorization algorithm is known when considered numbers are very large, so, the attacker cannot never launch its attack. Performed simulations prove that the proposed solution is effective and robust to defend against the spoof PS-Poll based DoS attack. Furthermore, no important communication, computing or storage overheads are generated by our solution, and it can be easily implemented through a firmware upgrade, without requiring any additional hardware.

The remainder of this paper is organized as follows. Section 2 introduces IEEE 802.11 networks, Section 3 summarizes some related works and Section 4 describes how the spoofed PS-Poll based DoS attack is launched. The proposal is presented and discussed in Section 5. Simulation results are analyzed and interpreted in Section 6. In Section 7, we conclude the paper and highlight some future works.

2. BACKGROUND

The IEEE 802.11 standard defines the physical and MAC layers of OSI model for ad hoc and infrastructure modes. It uses three types of frames, namely, data frames, control frames and management frames. Data frames are used to send the upper layer data, control frames are used to arbitrate access to the medium and management frames are used for network management tasks. The PS-Poll frame considered in this paper is a control frame used by a client in power save mode to request pending frames buffered at the access point. Some control and management frames enumerated in Table 1 are usually exploited to launch DoS attacks in IEEE 802.11 networks (1).

Management frames	Control frames
Probe Request/Response	Request to Send
Authentication/Deauthentication	Clear to Send
Association /Disassociation	Acknowledgement
Reassociation	Power Save Poll

Table 1: *Control and management frames*

In order to identify APs within communication range, a client listen to beacon frames periodically transmitted by APs. After this, authentication request and response frames are exchanged between client and AP. Then, an association process takes place in which the client learns the AP's MAC address and the AP assigns an association identifier to the wireless client. An 802.11 client can be authenticated by multiple APs, however it should be associated with only one AP at a time. Once the authentication and the association processes are finished, the communication between the client and AP can take place.

3. RELATED WORK

Usually, DoS attacks launched in IEEE 802.11 networks exploit vulnerabilities related to unauthenticated management frames exchanged between clients and the AP. In (2; 3), authors present several denial of service attacks against 802.11-based networks, and examine the 802.11 MAC layer in order to identify a number of vulnerabilities that could be exploited to deny service to legitimate users. WEP (Wired Equivalent Privacy) (4) is the popular security protocol that ensures security services such as confidentiality, authentication and integrity. This protocol did not provide solutions to already discovered security weaknesses (5). To remedy to these security weaknesses, IEEE proposed Wi-Fi Protected Access (WPA) and 802.11i (6) as the security standards for WLANs. In (8), authors proposed an encryption based solution using pre-established keys, in order to detect and prevent the spoofed PS-Poll based DoS attacks. This solution does not require any additional hardware and can be implemented in both wireless clients and AP via firmware upgrade. Authors in (9) presented a solution to address vulnerabilities that exist in the exchange of management frames, and employ a modified Diffe-Hellman's algorithm to ensure the authentication and the integrity, and consequently prevent threats such as active eavesdropping and DoS attacks.

Some commercial softwares such as AirDefense Guard, Odyssey Server and SnifferWireless are available and considered as intrusion detection solutions that provide real-time network audits and monitoring, in order to identify and respond to hardware failures, network interferences and performance degradation (8). Authors of (10) proposed an intrusion detection system based on the relationship that can be exist between a node and the traffic it generates, in order to detect attacks that target the MAC layer of 802.11 networks. General approches (11; 12) for detecting MAC address spoofing attacks are also proposed. This detection can be achieved through the analysis of sequence number patterns of the captured wireless traffic.

4. ATTACK MODEL

The Power Save Mode (PSM) (7), defined in the 802.11 standard, allows stations to switch from active mode to sleep mode when there are no transmission in order to conserve their power. As depicted in Figure 1, to enter into PSM, a client sends a PS (Power Save) request to AP and a PS response should be sent back by AP to the client before it can enter into sleep mode. During the sleep period, the AP buffers all packets addressed to that client. The presence of buffered packets is periodically indicated in the Traffic Indication Map (TIM) contained in beacon frames. If there is an indication of pending packets, the client can choose to receive those frames at its convenience, otherwise, it sleeps immediately (8). To receive pending data, the client asks the AP through the Power Save Poll (PS-Poll) frame to get these packets. After successful reception of data frames, the client sends an acknowledgment (ACK) which allows the AP to empty data buffer.

The PS-Poll frame is neither protected nor authenticated. An attacker can easily spoof PS-Poll frame using tools such as SpoofMAC, Airsnarf and NetStumbler. Therefore, it can simply launch a DoS attack by sending spoofed PS-Poll frame on behalf of the asleep client, thereby causing the destruction of packets destined to the client. A generic PS-Poll DoS attack scenario is shown in Figure 2.

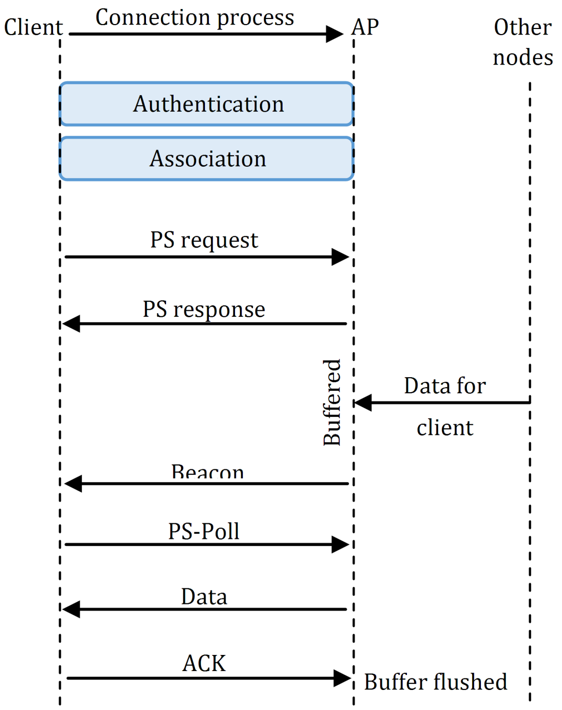

***Figure 1:** Power save mode*

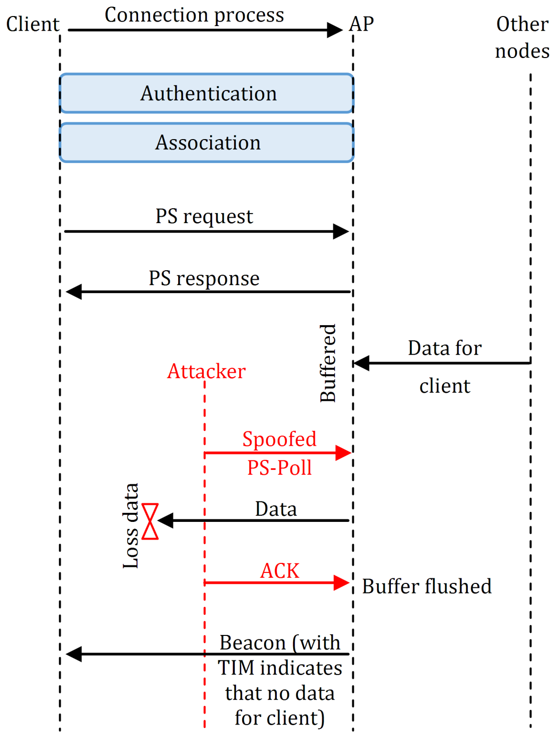

***Figure 2:** Spoofed PS-Poll based DoS attack*

5. OUR PROPOSAL

In order to cope with the spoofed PS-Poll based DoS attack, we have proposed APSP (Authenticated Power Save Poll). This solution exploits the principle of the integer prime factorization, that consists to decompose a large number $N = p * q$ (where p and q are two positive large prime numbers) into non-trivial prime divisors. When the number is very large, no efficient integer prime factorization algorithm is known (13). As depicted in Figure 3, APSP works as follows :

1. Initially, when the client wants to switch to PSM, it randomly generates two positive large prime numbers p and q then computes $N = p * q$.

2. During the PSM switching process, the client sends a PS request containing N to the AP. The AP stores N and sends a PS response to the client.

3. When the sleepy client receives a beacon frame from AP indicating that it has pending frames in buffer, it sends the PS-Poll frame to the AP, along with the p to get these frames. If this number p corresponds to the number N previously stored, i.e., p divides N, then the PS-Poll frame is authenticated and will be processed accordingly. Consequently, the AP delivers buffered frames to the client. Otherwise, the frame is rejected assuming that it is from the attacker.

4. After the reception of frames, the client renews the parameters p, q and N. For this, it sends an acknowledgment (ACK) containing the newly calculated N, which will be used to authenticate the PS-Poll subsequently exchanged with the recent generated p.

Since p and q are two large primes, even the attacker can obtain N, it is difficult for it to generate the same prime number p generated by the client due to the intractable factorization problem. Also, while the division N/p can be efficiently performed by the AP, the spoofed PS-Poll will be easily detected. Furthermore, the factorization of N is unique, so, only the client who generated the number N can prove that it is the legitimate owner of the challenge p, and thus it alone can send the legitimate PS-Poll frame.

6. PERFORMANCE EVALUATION

This section is devoted to evaluate the performance of our security protocol (APSP). We have performed series of simulations by implementing a prototype in Maple modeling and development environment (14). Our prototype has a modular design, which allows parallel programming. We have used one AP and one legitimate client operating in 802.11 PSM. Another client periodically sends packets to the legitimate client and one attacker to launch the spoofed PS-Poll based DoS attack. The source

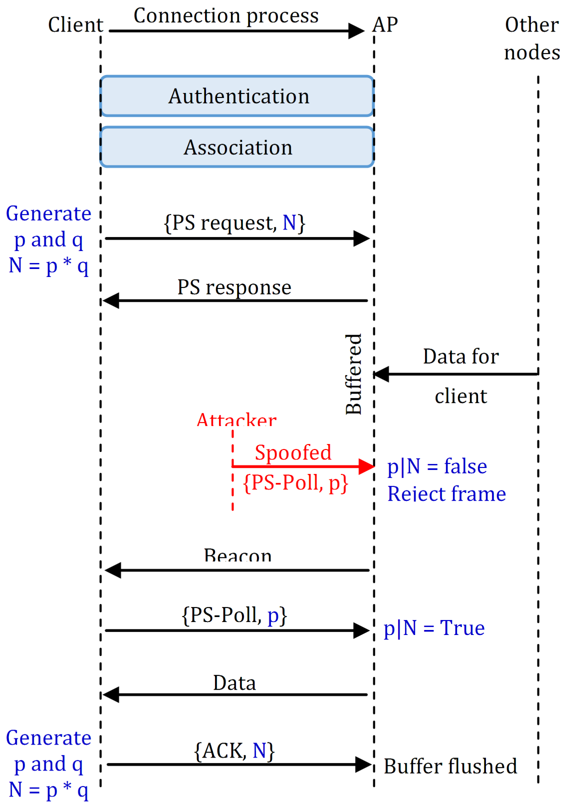

***Figure 3:** APSP, Authenticated Power Save Poll*

node periodically and randomly sends data packets to the client in PSM, while the AP sends beacon frames with an average of 10 beacons/second. The simulation duration is 3600 seconds. We use different values of primes p and q in order to determine the impact of the size of prime numbers in our solution performance. Furthermore, the simulation was performed without protection constraints (i.e., without WEP or WPA/WPA2). Additionally, we have ignored transmission errors that can be occurred in the wireless channel.

The main goal of our solution is to ensure the reliability of the buffering and subsequent delivery of packets by the AP. Thus, following metrics have been measured :

- Packet Delivery Ratio (PDR): denotes the ratio between the number of delivered packets by the AP that well received by the client in PSM and the total number of packets generated by the source node and buffered by in the AP.
- Packet Saving Ratio (PSR): is defined as the ratio between the number of maintained packets in the buffer during the client sleep period and the total number of packets buffered in the AP.
- Attack Success Ratio (ASR): represents the ratio between the number of buffered packets devastated because of the attack and the total number of packets buffered in the AP. We can consider this ratio as packets loss ratio.
- Attacker Efficiency: we define this metric as the ratio between the number of spoofed PS-Poll successfully treated by the AP and the total number of spoofed PS-Poll sent by the attacker.

Simulation results shown in Figure 4 represent PDR, PSR and ASR with N equal to 512 bits. From Figure 4, we observe that the PDR increases, while the PSR decreases. This means that the AP has kept the buffered packets while the client sinks into a deep sleep then buffered packets are well delivered to the client. In other words, the client and the AP have been fully mastered through our solution. Additionally, ASR is kept at 0% during the simulation. This means that all the spoofed PS-Poll sent by the attacker were detected and ignored by the AP, i.e., the adequate challenge p hasn't discovered by the attacker, hence the total failure of the attack. These simulation results shows that our solution is fully effective against the spoofed PS-Poll based DoS attack.

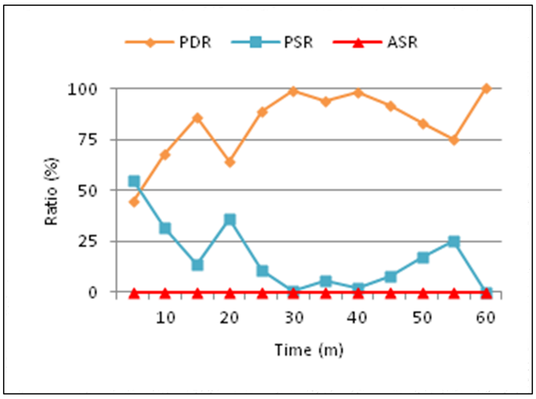

***Figure 4:** PDR, PSR and ASR, N=512 bits*

In order to determine the impact of the size of the challenge p (or the size of the number N) on PDR, ASR and attacker efficiency, we have used different sizes of N. Results are shown in Figure 5.

From Figure 5, we observe that the increasing of PDR is the direct consequence of the increasing of the size of N. More N is larger, more PDR becomes closer to 100% with sizes less than 64-bits. PDR reachs 100% with sizes equal to 64-bits and more. Moreover, we observe that the increasing of the size of N causes the decreasing of ASR and the attacker efficiency. In other words, more N is larger; more ASR and attacker efficiency become closer to 0% for

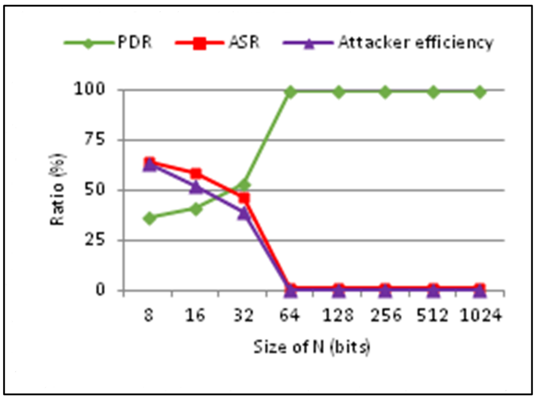

Figure 5: *Impact of N on performance metrics*

sizes less than 64-bits. These latter metrics reach 0% for sizes equal or more than 64-bits. We can conclude also that sizes of N equal or less than 32-bits are insufficient to prevent the attack, because it is relatively easy for the attacker to find the challenge p with small primes. On the contrary, with large sizes of N, the attacker has any chance to find the correct challenge p.

In order to check the robustness of our solution, we have modified the attack to launch a brute force PS-Poll DoS attack, this by testing a set of potential numbers p to find the correct one. In this experiment, N is equal to 512 bits. The obtained results are depicted in Figure 6. Note that similar results were obtained with N equal to 64, 128, 256 and 1024 bits.

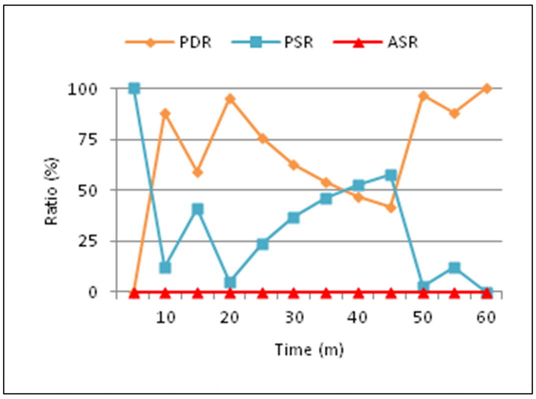

Figure 6: *Robustness of the proposed solution*

From Figure 6, we can say that the AP has mastered the legitimate trade in favor of the client, despite the existence of a brute force PS-Poll based DoS attack. Also, simulation results show that the brute force PS-Poll based DoS attack has totally failed where the ASR is kept at zero (0%) during the simulation. This is due to the total prevention and protection provided by our solution against the spoofed PS-Poll attack. All spoofed PS-Poll sent by the attacker was detected and crushed. So, it is very difficult for the attacker to find the correct number p within a reasonable time. This justifies the result of the attacker efficiency (0%).

Note that the solution we propose is not only detective but also preventive against the spoofed PS-Poll based DoS attack, with low communication, computing and storage overheads. Furthermore, it can be easily implemented in wireless clients and AP via firmware upgrade and without any additional hardware.

7. CONCLUSION

In this paper, we have focused on the spoofed PS-Poll based DoS attack, where the attacker spoofs the PS-Poll frame in the objective to destruct buffered packets intended to be delivered to sleepy clients. To cope with this attack, we have proposed APSP (Authenticated Power Save Poll) in order to authenticate PS-Poll frames. Our solution is based on the integer prime factorization known as an intractable problem to mitigate this DoS attack. The solution we propose is both detective and preventive one, with low communication, computing and storage overheads, and it can be easily implemented through a firmware upgrade without requiring any additional hardware. Simulation results show that the proposed solution is effective and robust to defend against the considered attack. In future work, we plan to compare our solution to other reference works in order to assess further its effectiveness and robustness, and extend it to consider other DoS attacks.

REFERENCES

[1] Farooq, T., Llewellyn-Jones, D. and Merabti, M. (2010) *MAC Layer DoS Attacks in IEEE 802.11 Networks*. The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK.

[2] Bellardo, J. and Savage, S. (2003) *802.11 denial-of-service attacks: real vulnerabilities and practical solutions*. Proceedings of the 12th conference on USENIX Security Symposium, vol. 12 of SSYM'03, Berkeley, CA, USA, USENIX Association, pp. 15-28.

[3] Bernaschi, M., Ferreri, F. and Valcamonici, L. (2008) *Access points vulnerabilities to DoS attacks in 802.11 networks*. Wireless Networks, Vol. 14, No. 2, pp. 159-169.

[4] (1999) *IEEE 802.11 Local and Metropolitan Area Networks: Wireless LAN Medium Acess Control (MAC) and Physical (PHY) Specifications*.

[5] Wong S. (2007) *The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards*. GSEC Practical v1.4b.

[6] Moffat, M. and Hunt, R. (2007) *Evolution of wireless LAN security architecture to IEEE 802.11i (WPA2)*. AsiaCSN'07 Proceedings of the Fourth IASTED Asian Conference on Communication Systems and Networks, pp. 292-297.

[7] Matthew G. (2002) *802.11 Wireless Networks: The Definitive Guide*. O'Reilly, pp. 122-133.

[8] Qureshi, Z. I., Aslam, B., Mohsin, A. and Javed, Y. (2008) *Using Randomized Association ID to Detect and Prevent Spoofed PS-Poll Based Denial of Service Attacks in IEEE 802.11 WLANs*. WSEAS Transactions on Communications, Vol. 7, No. 3, pp. 170-179.

[9] Samad, F., Mahmood, W. and Umar Kaleem, A. (2006) *Improved Security in IEEE802.11 Wireless LANs*. Proceedings of the 5th WSEAS International Conference on Data Networks, Communications and Computers (DNCOCO'06), Bucharest, Romania.

[10] LaRoche, P. and Zincir-Heywood, A. N. (2005) *802.11 Network Intrusion Detection using Genetic Programming*. Proceedings of the 2005 Workshops on Genetic and Evolutionary Computation, Washington, D.C, pp. 170 171.

[11] Guo, F. and Chiueh, T. C. (2005) *Sequence Number-Based MAC address spoof Detection*. Proceedings of 8th Recent Advances in Intrusion Detection Symposium (RAID 2005), Location, Seattle, Washington, USA, pp. 309-329.

[12] Toledo, A. L. and Xiaodong, W. (2008) *Robust Detection of MAC Layer Denial-of-Service Attacks in CSMA/CA Wireless Networks*. IEEE Transactions on Information Forensics and Security, vol. 3, No. 3, pp. 347-358.

[13] Hildebrand, A. (1987) *On the number of prime factors of integers without large prime divisors*. Journal of Number Theory. Vol. 25, No. 1, pp.81106.

[14] http://www.maplesoft.com/products/maple/