DENIAL OF SERVICE ATTACKS AGAINST 802.11 DCF

Bo Chen, Vallipuram Muthukkumarasamy
School of Information and Communication Technology, Griffith University, Australia
Gold Coast Campus, PMB 50, GCMC Queensland 9726, Australia
b.chen@student.griffith.edu.au, v.muthu@griffith.edu.aul

ABSTRACT

This paper investigates the vulnerabilities in the 802.11 Distributed Coordination Function (DCF) mechanisms. We have conducted a series of Denial of Service (DoS) attack experiments targeting at the 802.11 DCF and evaluated the effectiveness of such attacks on different configurations. The results show that any current or upcoming 802.11 standards would not provide adequate help to mitigate the risk of DoS attacks. Therefore, the 802.11-based wireless LANs should not be used in any environments where the requirement of network availability is essential. We have also analysed some countermeasures against such attacks.

KEYWORDS

Denial of Service attacks, Distributed Coordination Function, WLAN Security.

1. INTRODUCTION

The widespread deployment of Wireless LANs has led to a number of security challenges, which were not present in traditional wired LANs. Denial of service attack was largely ignored earlier because it appeared that the attackers would not gain anything from such an exercise. Obviously this is not the case today. The widely publicized DOS attacks have now proved that it can have devastating effects. The vulnerabilities in 802.11 DCF mechanism should attract more attention because they allow the adversary to launch the DoS attacks using commonly available hardware and free software with low power consumption. This research will practically analyze the key features posed by the DoS attacks against 802.11 Distributed Coordinated Function (DCF) in both PHY and MAC layers. The effect from such DoS attacks on different 802.11 wireless configurations and different network modes is also investigated. The rest of this paper is structured as follows: the next section discusses the related work in this area. DCF mechanism is briefly described in Section 3. Section 4 explains the experimental set up. Results and analysis are given in Section 5. Section 6 concludes the paper.

2. RELATED WORK

A great deal of research has been done related to 802.11 network security. These works mainly focus on the confidentiality and integrity of wireless LANs or the availability of the wireless LANs. A number of attacks against the Wired Equivalent Privacy (WEP), which was employed by 802.11 to provide network confidentiality, have been demonstrated. Fluhrer et al. [2001] and Stubblefield et al. [2002] demonstrated how the secret key can be recovered by using recurring weak keys in WEP and passive monitoring. Furthermore, Borisov et al. [2001] identified some vulnerability, which can be used by attackers to modify and spoof WEP-protected frames without knowing the shared secret key.

Significant DoS attacks against the 802.11 networks' availability have also been identified. For example, a misbehaving station can keep accessing the medium by modifying the back-off process. Gupta et al. [2002] examined such DoS attacks in 802.11 ad hoc networks and indicated that traditional wireline-based detection and prevention approaches do not work in wireless LANs. Bellardo et al. [2003] have identified some identity-based DoS attacks which exploit the vulnerability that the management frames in 802.11 are

unauthenticated. They also demonstrated the DoS attack against the 802.11 DCF through a simulation study [Bellardo et al., 2003]. Chen et al. [2003] considered the DoS attack against the 802.11 DCF in MAC layer by virtual jamming through injecting control frames. They also suggested a possible countermeasure in the form of NAV validation, which resets the NAV to zero if the expected data frame exchange does not commence within the appropriate time. Recently, Wullems et al. [2004] identified a new attack based on commonly available IEEE 802.11 hardware and freely available software. This attack targets at the Direct Sequence Spread Spectrum (DSSS) Wireless LANs. However, very limited work has been done on investigating the vulnerabilities of 802.11 DCF mechanism using actual practical set ups.

3. 802.11 DCF

The 802.11Distributed Coordination Function (DCF) is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol, which regulates every node such that it must check the availability of the channel before transmitting data. The function of PHY layer in 802.11 standard is to provide information for the MAC layer about the availability of the transmission medium (carrier sense function) and is involved with the transmission and reception of data. To determine if the channel is clear for transmitting data, the physical carrier sense mechanism performs the Clear Channel Assessment (CCA) procedure and provides the results to MAC layer via the PHY-CCA indicate service primitive.

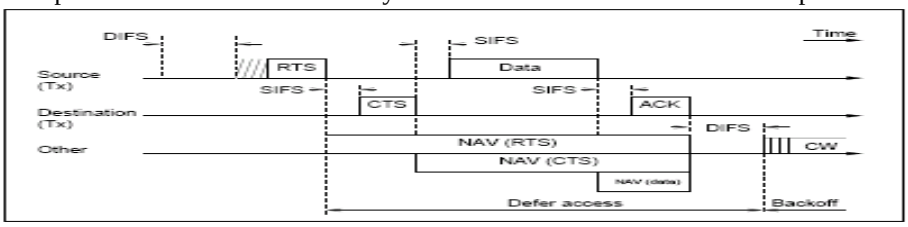

Figure 1. DCF operating procedure in RTS/CTS mode [LAN/MAN, 1999]

To address hidden terminal problem, virtual carrier-sense mechanism is employed by the IEEE 802.11 standard, as depicted in Figure 1. Under this mechanism, each 802.11 frame carries a duration field indicating the time that the channel is reserved for. This time is then used to program the Network Allocation Vector (NAV) on each node. The NAV can be thought of as a timer indicating the amount of time for which the medium has been reserved. Transmitting nodes set the value of NAV to the time for which they expect to use the medium, other nodes set up a process to count down the NAV. Only when the NAV on a node reaches zero, is it allowed to transmit. The above principle is used by the Request To Send (RTS)/ Clear To Send (CTS) handshake to synchronize access to the channel and prevent hidden terminal problem.

From what has been discussed above, the 802.11 DCF is apparently vulnerable to DoS attacks in both PHY layer and MAC layer as follows: (i) In the PHY layer, it is possible to subvert Clear Channel Assessment (CCA) using a continuous jamming signal, hence making the result of channel assessment always BUSY to permanently defer the legitimate transmission. (ii) In the MAC layer, an attacker can send the control frames with large duration at an appropriate frequency to ensure the value of NAV on each node greater than zero to permanently defer the legitimate transmission.

4. EXPERIMENTS

4.1 Physical layer attack

A laptop equipped with an 802.11b Prism based wireless network interface card was chosen to work as an attacker. The laptop was installed with Debian Linux operating system and used Host AP as the driver for the wireless network interface. We modified the Host AP driver to add a private configuration command to add a continuous transmit firmware test mode. If the test mode is enabled, the wireless network interface repeatedly transmits a specified sixteen-bit pattern until the test mode is disabled. When attacking, the laptop with the modified Host AP driver and the 802.11b wireless network interface continuously generates the jamming

signal. To enlarge the attack range, this particular interface was equipped with a high power (200mW) wireless network interface coupled to an external 8dB gain directional antenna.

4.2 MAC layer attack

Implementation of the MAC layer attack requires the ability to generate arbitrary frames directly. For these experiments the PC with Atheros AR5212 wireless network card is chosen to work as the attacker. The PC running Debian Linux used the MADWiFi-bsd driver for the wireless network interface, which supported the MAC frame injection directly.

It is possible to use almost any frame types to control the NAV. We selected the RTS, CTS and ACK frames as the attacking frames since there will not be ACK frames sent from the stations in respond to these control frames. Using RTS frames to attack has some advantages. If the RTS frames are configured to reach the access point, the access point will propagate the attack with the CTS frames, hence it will extend the attack range. In our experiments, we generated four types of frames for the attacking as listed below: (i) RTS addressed to the AP (CTS from AP). (ii) RTS addressed to a non-existent station (hence no CTS). (iii) CTS addressed to a non-existent station. (iv) ACK addressed to a non-existent station.

Each type of frame carries a maximum 32767 μ s duration field and they are injected repeatedly at an appropriate frequency, which ensures the value of NAV on each test station is greater than zero.

5. RESULTS AND ANALYSIS

5.1 Results

5.1.1 Physical layer results

The whole 802.11b mode network was blocked when the PHY layer attack was on as can be seen from Figure 2 (the vertical axis shows the network traffic in packets and the horizontal axis shows the time in seconds). There was no network traffic when the attack was conducted from 18 sec. to 38 sec., during the attack, our laptop using Ethereal to monitor the network traffic was also blocked and cannot sniff any packets.

As expected the narrowband jamming signal generated by our 802.11b card had no effect on the 802.11g configuration. However, when test network was in 802.11b/g multi-mode configuration, the interfaces configured to use either 802.11b or 802.11g as appropriate mode were also blocked and unable to transmit during the PHY layer attack as shown in Figure 3. The attack started at 28 sec. and finished at 37 sec. During the attack, there was no network traffic in the test network. This occurred even when the 802.11g was suggested as the data rates in use.

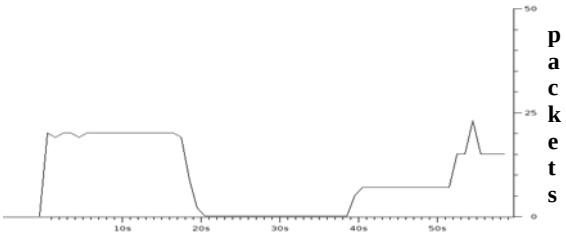

Figure 2. 802.11b network traffic during physical layer attack

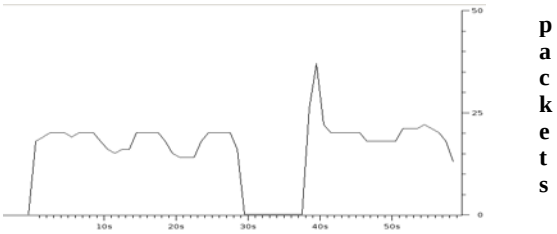

Figure 3. 802.11 b/g network traffic during physical attack

5.1.2 MAC layer results

In the MAC layer attack, all stations receiving the RTS frame addressed to a non-existent station were silenced even though it should be possible to reset the NAV after the expected arrival of a CTS has elapsed as

shown in Figure 4. When the RTS frames were sent between second 28 and second 38, the network traffic reduced to zero. We launched CTS and ACK attacks and obtained similar results. Therefore, the MAC layer attacks worked across all 802.11 configurations and network types when the RTS/CTS/ACK frames were injected to a non-existent address.

When RTS frames were sent directed to AP, it is expected that either the RTS frames or the CTS frames from the AP in respond to the RTS would block the network. However, to our surprise, we found that such attack cannot block the network while it can only delay the transmission as shown in Figure 5.

We repeated the test using three APs and all the wireless network interfaces we had and got the same results. After careful examination of the traces obtained during the attack, we found that the interfaces emitted packet within one millisecond after receiving the CTS frame from the AP which should keep the channel idle for 32.453ms. Such activities should be impossible under the 802.11 standards since nodes receiving the CTS should assume the channel is busy because the transmitter may be a hidden terminal. In this case we draw the conclusion that the wireless devices we had do not properly implement the 802.11 specifications.

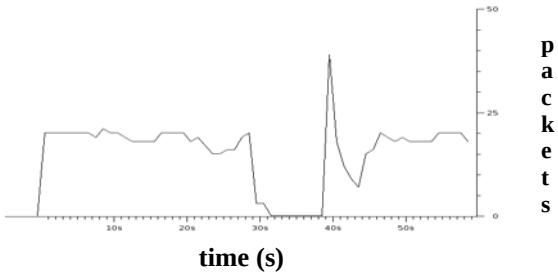

Figure 4. Network traffic during RTS frames addressed to a non-exist station injection

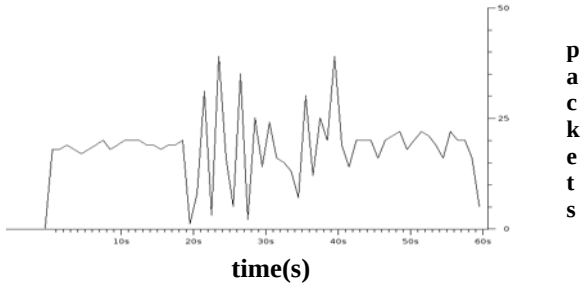

Figure 5. Network traffic during RTS frames addressed to a AP injection

5.2 Analysis

5.2.1 Physical layer attack analysis

In the above experiments we successfully demonstrated that the PHY layer attack can stop our test network in 802.11b mode. While the narrow band jamming signal generated by our 802.11b attacker was unable to affect the pure 802.11g and 802.11a configurations operating based on OFDM. It was somewhat surprising that the 802.11b/g multi-mode was affected by such PHY layer attacks. This was mainly because 802.11g are designed to be full backward compatible with 802.11b. When the wireless network interface is set to 802.11b/g multi-mode, it uses a combination of OFDM and DSSS transmission to support a large set of data rates.

It is worth noting that the 802.11i protocol would not mitigate the risk of the PHY layer attack because the efforts of 802.11i are made only at the MAC layer. To defend such type of attacks, Wullems et al. [2004] suggested the use of dynamically negotiated spreading functions or hop sequences, hence the attacker has to jam each channel independently or jam an entire frequency range, increasing the power requirement to conduct this attack and the risk of being detected and localized. However, this approach introduces more problems than it solves. For example: (i) how to inform all stations to change to a specific channel during the DoS attacking and, (ii) how to maintain the synchronization of transmission in all stations after changing to a new channel. Our experiments have proved that the jamming signal generated by our 802.11b network interface based on the DSSS had no effect on 802.11g and 802.11a configurations based on OFDM. Therefore, for the physical layer attack, it is more appropriate to use modulation changing as a possible countermeasure.

5.2.2 MAC layer attack analysis

The MAC layer denial of service attack against the 802.11 DCF mechanism offers the attacker several potential advantages:

- Medium independence – The same attack works against 802.11b, 802.11g and 802.11a configurations in the same channel.

- Low energy consumption – The attack does not require special device with high power to inject the control frames, an adversary can use battery powered equipments to conduct the attack

In our experiments, we demonstrated that the virtual jamming signal had successfully stopped our test networks completely in all 802.11configurations and different network modes when the control frames are sent to non-existent address. Detection of the MAC layer DoS attack targeting at the DCF is a difficult problem. Although it is possible to use network sniffer such as Ethereal to track the station sending the control frames in high frequency, it is difficult to judge if it is a legitimate busy network neighborhood or it is an attacker. On the other hand, the attacker may spoof the transmitter address or the receiver address by modifying the injecting frames, making the tracking almost impossible to achieve.

Unfortunately the upcoming 802.11i standard can not reduce the risk of MAC layer attacks as well as the PHY layer attacks. This is due to the fact that 802.11i only provides authentication for the management frames which will address the problems of the documented DoS attacks. The control frames such as RTS, CTS, ACK frames are not authenticated in any current or upcoming 802.11 standards. Even if they are authenticated, it won't help to prevent the attack because there is no trust relationship to begin with. This would only provide evidence for identifying the attacker since the virtual-carrier sense mechanism will affect all nodes on the same channel by design.

6. CONCLUSION

The findings presented in this paper aimed at identifying the vulnerabilities posed by the 802.11 DCF mechanism and investigating the effectiveness of DoS attacks targeting at the 802.11 DCF. Our experiments have proved that the jamming signal generated by the 802.11b network card based on DSSS physical layer will stop the 802.11b mode and 802.11b/g multi-mode networks. We have demonstrated that the MAC attacks also can stop network functions. Any current or upcoming 802.11 standards would not provide any help to mitigate the risk of DoS attacks against the 802.11 DCF. Even cryptographic techniques are unlikely to be effective countermeasures, as by design, the 802.11 DCF must coordinate the access to the open shared medium with untrusted parties. As a counter measure for the physical layer attack, we have suggested modulation change technique. Future work will investigate in detail the PHY layer vulnerabilities of OFDM-based 802.11a and 802.11g products.

REFERENCES

Bellardo, J. and Savage, S., 2003. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. *In Proceedings of the 12th USENIX Security Symposium* , Washington D.C., USA.

Borisov, N. et al, 2001. Intercepting mobile communications: the insecurity of 802.11. *In Proceedings of the 7th annual international conference on Mobile computing and networking* , New York, NY, USA, pages 180–189.

Chen, D. et al, 2003. Protecting wireless networks against a denial of service attack based on virtual jamming. *In The Ninth ACM Annual International Conference on Mobile Computing and Networking*, San Diego, CA, USA.

Fluhrer, S. et al, 2001. Weaknesses in the key scheduling algorithm of RC4. *In Selected Areas in Cryptography: 8th Annual International Workshop*, SAC 2001 Toronto, Ontario, Canada, volume 2259 of Lecture Notes in Computer Science.

Gupta, V. et al, 2002. Denial of service attacks at the MAC layer in wireless ad hoc networks. *In Military Communications Conference*, Anaheim, CA, USA, pages 1118–1123.

LAN/MAN Standards Committee, 1999. "*ANSI/IEEE Std 802.11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*", IEEE Computer Society.

Stubblefield, A. et al, 2002. Using the Fluhrer, Mantin and Shamir attack to break WEP. *In Ninth Annual Symposium on Network and Distributed System Security*, Internet Society, pages 17–22.

Wullems, C. et al, 2004. A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs. *In 2004 Wireless Telecommunications Symposium*, Pomona, CA, USA pages 129–136.