2010

Does the use of MIMO Technology used by 802.11n Reduce or Increase the Impact of Denial of Service Attacks?

William Pung
Edith Cowan University

Andrew Woodward
Edith Cowan University

DOI: 10.4225/75/57b2b2fb40ce1
Originally published in the Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November 30th 2010

Does the use of MIMO Technology used by 802.11n Reduce or Increase the Impact of Denial of Service Attacks?

William Pung and Andrew Woodward
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
a.woodward@ecu.edu.au

Abstract

This paper presents the results of a simulated wireless DoS attack against a 802.11g connection that uses Single Input Single Output (SISO), and an 802.11n device that utilizes MIMO. The aim of the experiment was to determine whether the impact of a denial of service attack against MIMO architecture is greater than SISO, since it is capable of receiving more(multiple) attack frames/packets within a given time frame. It was found that both devices were negatively impacted by such attacks, and that throughout was similarly affected. It was also observed that increasing the packet flood rate resulted in a corresponding and linear reduction in throughput for both 802.11n and 802.11g devices. Additionally, the 802.11g device appeared to reach a saturation point at 1000pps, with minimal reduction in throughout at 2000ps. Further observations were that although the overall throughput reduction in terms of percentage was greater for 802.11n than for 802.11g, the 802.11n device still achieved a higher throughput, despite a flooding rate of 2000 packets per second. Implications for network forensics are considered, given that wireless network devices are inherently difficult to identify. It was concluded that such an attack would be very difficult to tie to a particular attacking device, and to do so would require discovery of the attacker's computer by other means.

Keywords

Wireless network security, denial of service, MIMO, packet flooding

INTRODUCTION

Traditional 802.11a/b/g wireless network devices were built on Single-Input Single-Output (SISO) architecture, a half duplex radio system which is designed to reject multipath interference (IEEE, 1999). Wireless packets are sent and received between a wireless client and a wireless access point (infrastructure mode) in a single stream utilizing only one antenna on each end. While some devices utilised two antennas to reduce the effects of multipath interference, the lack of a second radio meant that only one antenna could be used to send or receive. The 802.11n protocol extension introduced a new class of wireless devices that takes advantage of a new architecture named Multiple-Input Multiple-Output (MIMO) (IEEE, 2009a). This new architecture utilizes multiple antennas on each end, effectively exploiting the spatial dimension, resulting in increased throughput and connection stability. This is achieved by not trying to avoid multipath, but in fact utilising the increase in bandwidth which results (Biglieri *et al*, 2007). Whilst the benefits of this new architecture are being widely advocated by manufacturers, there has been little exploration of any potential security flaws it presents.

Denial of service (DoS) attacks have been a threat to wireless networks since their inception (Gupta *et* al, 2002; Bellardo & Savage, 2003). Denial of service attacks are theoretically impossible to prevent in a wireless network due to the broadcast nature of the medium. These so called physical attacks are possible because you cannot easily control the propagation of radio waves. The Layer-2 class of attacks, which rely on lack of authentication of control and management frames, can be mitigated to some extent, and the 802.11w extension aims to reduce this attack even further (IEEE, 2009b). As such, this paper did not aim to determine whether a denial of service attack is any more or less likely, but whether the impact of such an attack is greater than those using current technologies, namely 802.11g.

In this paper, we examined one type of attack to compare 802.11n's resilience against the more commonly deployed 802.11g. The greatest strength of 802.11n is its capability to reach high data rates (AirTight Networks, 2010), but hypothetically, this could also mean that it will be more susceptible to flood attacks, as its enhanced capability to receive and read many more packets than 802.11g at any given time may be its downfall. Additionally, post incident implications of such an attack are also considered.

MATERIALS AND METHODS

This test focused on monitoring the effective throughput and stability of 802.11n and 802.11g when under a DoS attack directed at the wireless client. The DoS attack being used for this experiment is packet flooding, an effective form of Layer 1 jamming. It cannot be classified as a Layer 2 attack because there is no exploitation of control or management frames. Although this is a less-intrusive DoS attack method, it does examine the research question stated in the introduction – Does a denial of service attack against MIMO architecture have a greater or lesser impact on throughput for 802.11n devices as compared to 802.11g?

Experimental design

A standard testing environment was prepared in order to test the research question as follows. The role of each device in the experiment can be observed in Figure 2.

Hardware used

- 2 Laptops equipped with Linksys Wireless-N USB Network Adapter with Dual-Band (WUSB600N)
- 1 Linksys Simultaneous Dual-N Band Wireless Router (WRT610N)
- 1 Desktop PC

Software used

- Performance Monitor (Microsoft visualization and recording tool)
- Tera Copy (file transfer tool with throughput visualization)
- Aireplay-ng (packet injection tool)
- Kismet (wireless mapping and packet observation tool)

Performance monitor will be primarily set to observe the following counter:

- Bytes/second of wireless adapter

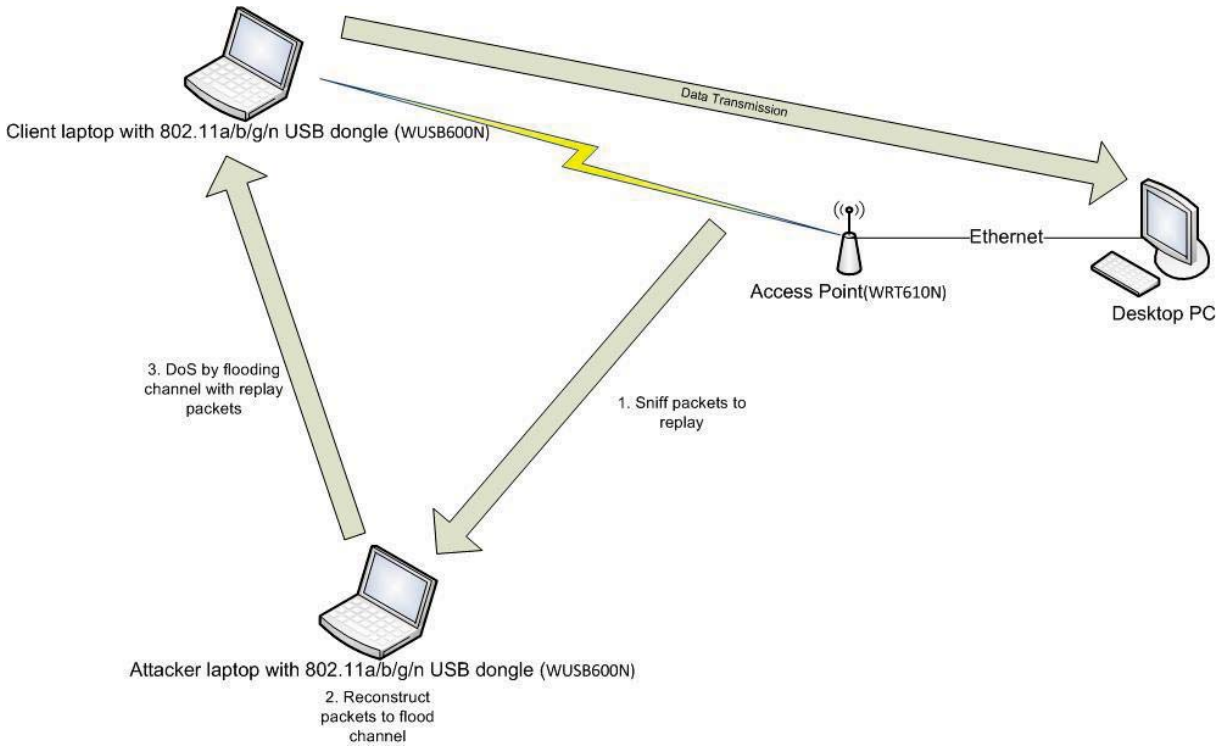


Figure 2: Experimental design for examination of the impact of packet flooding on 802.11n and 802.11g wireless network devices

Procedure

This experiment is held in a controlled environment where there are no other wireless networks interfering with the selected channel and bandwidth. The access point is connected to a desktop PC via ethernet. This is to maintain a 1 to 1 wireless communication channel in the surrounding. The client laptop was then associated with the access point and a file transfer session was established with the desktop PC.

A large file (2 GB) was then transferred from the Client laptop to the Desktop PC, using its wireless setup as the mode of transportation.

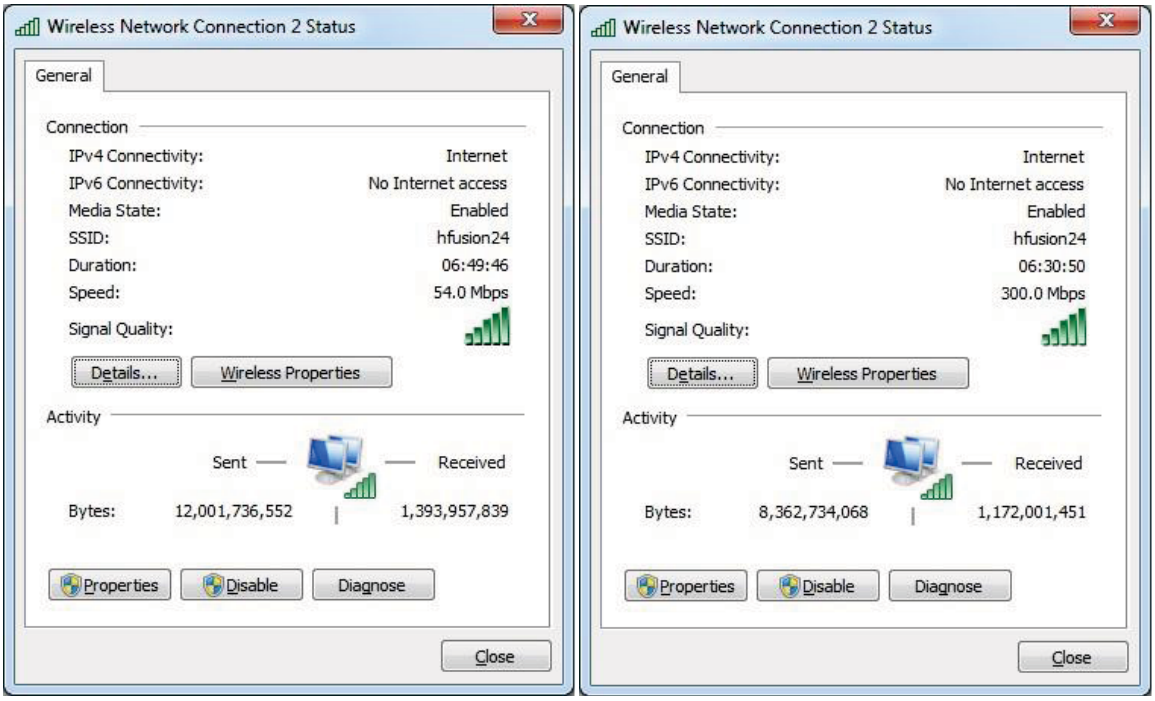
Next, Kismet was used on the attacker laptop to sniff the traffic for suitable packets for replaying and reconstructed them in a .cap file. This cap file was then used by Aireplay to conduct a 500/1000/2000 packet per second flood into the channel to induce a DoS attack.

This entire experiment is to be performed 2 times, in 802.11n(2.4ghz - 40mhz wide channels) and 802.11g(2.4ghz - 20mhz wide channels) modes.

Results will be collected from observing the effective throughput of the wireless network after 3 waves of progressively aggressive attacks, and monitors wireless network connectivity in the process.

Before the experiment starts, connectivity is checked for performance as seen in figure 3 below.

- 802.11n to operate under 300Mbps
- 802.11g to operate under 54Mbps



(a) (b)

Figure 3: Throughput report for 802.11g (a) and 802.11n (b) devices under control conditions

RESULTS

Results for both devices, and for all packet flooding levels tested are shown in figures 5 and 6. The observed throughput, as captured throughout the three stages of attack, where attack frame has been highlighted by an addition of a blue frame over the time frame of the attack. The 3 stages of attack are, 500 packets per second (PPS), 1000 PPS and 2000 PPS.

Figure 4: Impact of packet flooding on throughput for an 802.11g network device. The blue overlay represents the time period during which the flooding attacks were conducted.

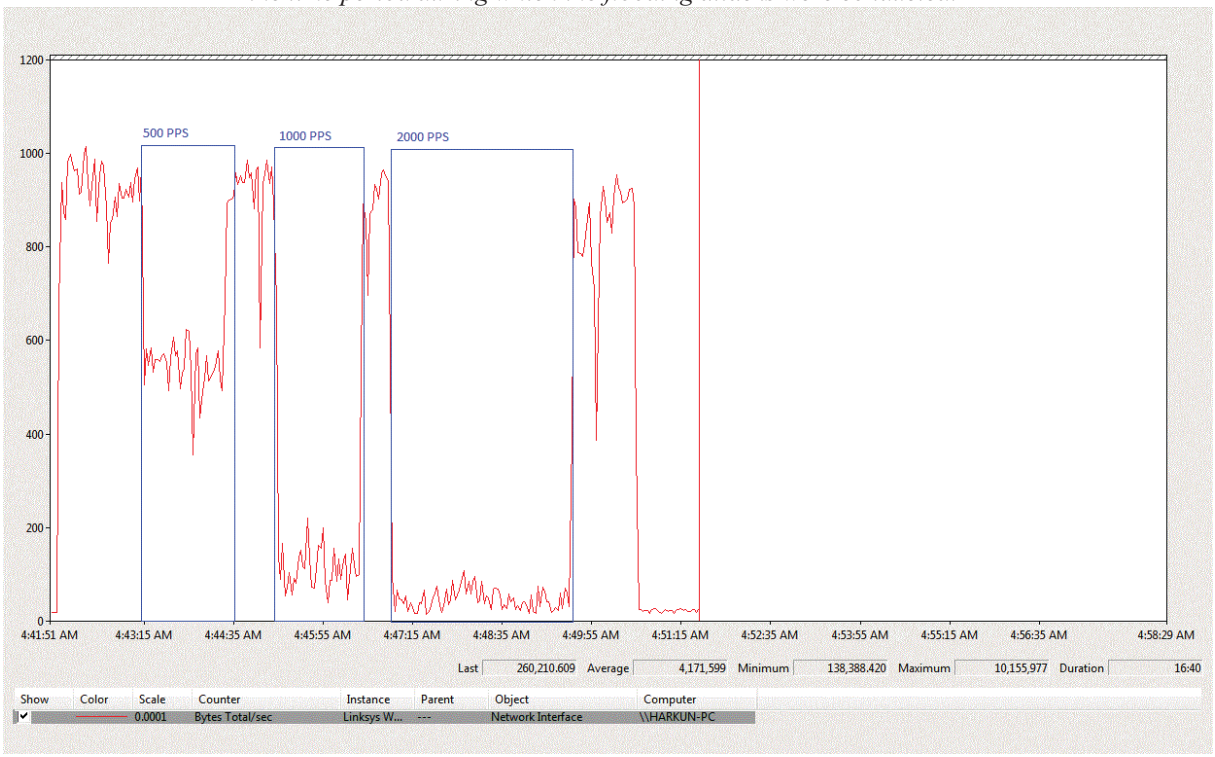


Figure 5: The impact of packet flooding on throughput for an 802.11n network device. The blue overlay represents the time period during which the flooding attacks were conducted.

The first observation was that both G and N standards were prone to the same attack, and both configurations saw a significant drop in data rates when hit by the attack. The second observation was that, based on the percentage reduction in throughput, 802.11n is slightly more resilient against the attack than 802.11g. However, at 2000PPS, the connection was throttled to 500kBps, a mere 5% of the original throughput.

A third observation was that the point at which throughput suffered a significant reduction for both 802.11g and 802.11n standards are approximately at 1000PPS and 2000PPS respectively.

- 802.11g suffered a 92% decrease at both 1000PPS and this persisted through 2000PPS.
- 802.11n suffered a 90% decrease at 1000PPS and a further 95% decrease at 2000PPS.

A fourth observation was that neither device dropped their connection (either association or authentication) as a result of the packet flooding attack. That is, connectivity persisted throughout the spam attack and recovered after the spam was stopped.

Table 1: The Impact of increasing packet flooding on throughout for both 802.11g and 802.11n based wireless network devices

Packet flood rate	0 PPS	500 PPS	1000 PPS	2000 PPS
802.11g				
Throughput (kilobytes/sec)	2500	1000	200	200
Throughput%	100%	40%	8%	8%
802.11n				
Throughput (kilobytes/sec)	10000	5500	1000	500
Throughput%	100%	55%	10%	5%

DISCUSSION

This experiment demonstrated that 802.11n devices are as susceptible to a packet flooding based denial of service attack as previous 802.11 protocol extension based devices. This is not really an unexpected result, as packet flooding is basically a form of jamming, and regardless of whether the protocol extension is b, g or n, packet flooding is always going to be a security issue in terms of availability. There are additional security mechanisms in the 802.11w extension to the protocol, and it is designed to increase the security of management frames, a significant source of many of the vulnerabilities present in wireless networks (IEEE, 2009b). More specifically, it is designed to protect against replay attacks. What this experiment shows is that the attack is successful in many ways, by controlling the volume of packets injected, a varying decrease in throughput may be observed. At certain points, throughput dropped to 0. Time sensitive applications such as VOIP or video conferencing will be severely impacted while the attack showed little symptoms, unlike a deauthentication attack, where users are forcefully disconnected from the wireless network. The implication for this lack of disconnection and the use of packets rather than noise as the source of jamming is that such traffic may not be detected by some intrusion detection systems. Additionally, the packet flood is effectively a high volume of traffic, and as such, it would be difficult to configure the rules of an IDS to alert to such an attack. It is likely that a high percentage of false positives would be generated in the normal course of wireless network usage, making the efficacy of an IDS questionable in this context. Such an attack may be mitigated through the use of QoS or other bandwidth allocation schemes.

Throughput and Availability

This experiment also showed that both MIMO and SIMO architectures are similarly vulnerable to this same attack. Throughput meters from results show that the resistance of 802.11g may even be lower than 1000PPS, as the advanced case of 2000PPS did not lower the throughput further, unlike the case of 802.11n.

The observation that the greater bandwidth available to 802.11n allowed In fact, what was also observed, is that the greater bandwidth available to 802.11n allows it to be more tolerant to these spam packets. 802.11g on the other hand, had lesser bandwidth to deal with such an attack that devastates bandwidth.

Even at 10% throughput, 802.11n's higher capacity allows less bandwidth intensive activities to continue without too much impact. The difference between 802.11g and 802.11n's bandwidth capacity is so great that 10% of 802.11n is roughly equivalent to 50% of 802.11g. This alone gives 802.11n more allowance to work with, before coming down to a complete halt due to a much more aggressive attack.

Digital Forensics and Incident Response

Aside from the implications for availability and throughput that have been reported and discussed here, there is another implication of such an attack: incident response. In the event that such an attack was conducted against a corporate wireless network of a critical infrastructure provider or other large enterprise, the victim of such an attack would likely want to determine who had carried out such an attack. The problem is that unless the attacker was naive enough to have conducted the attack using their own traffic, marked with their own MAC address, then it is an almost impossible task to forensically establish an attacking device based on nothing other than a wireless fingerprint. The main reason is that the commonly used MAC address can very easily be cloned, or spoofed, in a wireless network card. As such, the only remaining identifier would be the spectral characteristics of the wireless transmitter. There has been some research which has attempted to establish that such identification is possible (Franklin et al, 2006), but in real-world applications, it simply is not possible (Golygowski & Woodward, 2009).

However, in the event that a likely suspect is identified, confiscation of the attacking device may yield sufficient information to successfully prosecute or terminate the employment of that individual. Given that the attackers device would need to have a range of software loaded in order to carry out such an attack, it is likely that sufficient evidence would exist to identify the device as being that which carried out the denial of service attack.

Future Research

It would be interesting to conduct a further experiment to determine whether some of the newer security enhancements would be able to prevent such a replay attack from being perpetrated. The four-way handshake used by 802.11i as part of WPA authentication is designed to prevent a rogue client from connecting to an access point (He & Mitchell, 2004; IEEE 200x). However, given that the captured traffic is from that of an authenticated client, such a protection mechanism may not prevent this type of packet-flood jamming attack. It would also be valuable to determine what impact the new protective measures provided by the recently ratified 802.11w extension have on the type of attack used in this research.

CONCLUSION

The initial question and reason behind this experiment was to determine whether overcome by the naturally high bandwidth capacity MIMO provides. The increased data rates of MIMO are not detrimental to its stability during a packet flood attack. Conversely, it is shown that 802.11n exhibits higher tolerance to such attacks, possibly due to the MIMO architecture which is used to achieve this higher bandwidth. A 50% drop of performance will deal as much impact as an 802.11g running at 50%; mostly attributed by corporate needs. In both occasions, the attack is highly dangerous in that it will reduce operating capacity of a wireless network in an environment where there are a large number of users and high demands on throughput.

Given the software and tools required in order to perpetrate this type of attack, it does create more traces which may lead to identifying the perpetrator of a denial of service attack. It does not necessarily make it any easier to find the attacker, but it does make a stronger case for establishing whether they were responsible.

It is likely that implementation of both WPA encryption in combination with an IDS may mitigate such an attack. However, this would need to be determined by further research to determine whether the 802.11i security mechanisms would prevent such a jamming attack.

REFERENCES

AirTight Networks (2010). *802.11n frequently asked questions.* Retrieved Oct 1, 2010, from http://www.airtightnetworks.com/home/solutions/80211n/80211n-faqs.html

Bellardo, J. & Savage, S. (2003). *802.11 denial-of-service attacks: real vulnerabilities and practical solutions*. In Proceedings of the 12th conference on USENIX Security Symposium - Volume 12

Biglieri, E., Calderbank, R., & Constantinides, A. (2007). *MIMO wireless communications*: Cambridge University Press.

Franklin, J. McCoy, D., Tabriz, P., Neagoe, V., Van Randwyk, J. & Sicker, D. (2006). Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting . In Proceedings of the 15th USENIX Security Symposium

Golygowski, L. & Woodward, A. (2009). Wireless device identification for forensic purposes. *Journal of Network Forensics*. **1(1):** pp 1-15

Gupta, V., Krishnamurthy, S. & Faloutsos, M. (2002). Denial of service attacks at the MAC layer in wireless ad hoc networks. Proceedings of the Military Communications Conference, 2002

He, C. & Mitchell J.C. (2004). Analysis of the 802.11i 4-way handshake. Proceedings of the 3rd ACM workshop on wireless security

IEEE (1999). 802.11-1999 - IEEE Standard for Local and Metropolitan Area Networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE: New York

IEEE (2004). 802.11i-2004 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE: New York

IEEE (2009a). 802.11n-2009 - IEEE Standard for Local and Metropolitan Area Networks - Telecommunications and Information Ixchange between Systems -- Local and Metropolitan Area Networks -- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. IEEE: New York

IEEE (2009b). IEEE Ratifies 802.11w, WLAN Specification to Enhance Signalling Security Mechanisms. Retrieved October 3rd from http://standards.ieee.org/announcements/2009/pr_802.11w.html