Multi-channel Jamming Attacks using Cognitive Radios

Ashwin Sampath, Hui Dai, Haitao Zheng and Ben Y. Zhao
Computer Science Department, University of California at Santa Barbara
{ashwins,huidai,htzheng,ravenben}@cs.ucsb.edu

Abstract

To improve spectrum efficiency, future wireless devices will use cognitive radios to dynamically access spectrum. While offering great flexibility and software-reconfigurability, unsecured cognitive radios can be easily manipulated to attack legacy and future wireless networks. In this paper, we explore the feasibility and impact of cognitive radio based jamming attacks on 802.11 networks. We show that attackers can utilize cognitive radios' fast channel switching capability to amplify their jamming impact across multiple channels using a single radio. We also examine the impact of hardware channel switching delays and jamming duration on the impact of jamming.

1 Introduction

The advancement of wireless networks and technologies requires easily accessible spectrum where wireless devices can establish stable data communication. However, conventional spectrum management policies assign static spectrum to networks in long-term leases to prevent interference. Over time, this has led to the well-known *artificial spectrum scarcity* problem [13].

Dynamic spectrum access, enabled by next generation *cognitive radios* [9, 14], has been embraced by industry, academia, and regulatory agencies as the ideal and necessary solution to the spectrum scarcity problem. Without any statically assigned spectrum, cognitive radios identify locally available spectrum and reconfigure in real-time to utilize under-utilized spectrum, without affecting legacy spectrum owners. To utilize spectrum efficiently, cognitive radios supports the following features:

- *Real-time spectrum sensing*: Cognitive radios perform periodic spectrum sensing to identify unused spectrum.
- *Fast channel switching*: Being able to reconfigure in real-time, cognitive radios can switch among different spectrum channels with minimum delay.
- *Software-reconfigurable*: Radio operations are controlled by software, which can be updated regularly.

While providing tremendous flexibility, these radically new features also lead to a significant increase of control by end users. Without proper regulation and end device security, malicious users can take advantage of these features to attack both legacy networks and cognitive radio networks. Specifically, attackers can manipulate cognitive radios either by tampering a small set of radio devices physically or by infecting a large set of devices through malicious software update or botnets [3].

Previous work has demonstrated the feasibility of launching attacks on sensor and 802.11 networks using commodity radio devices [4, 17]. Malicious users can deviate from normal MAC behavior to maximize their own benefits or disrupt the operation of normal users. However, existing attacks, especially jamming attacks, are designed for single-channel wireless networks. Attacking a network with multiple channels in general requires multiple radios. The physical costs scale linearly with the number of channels, placing a fundamental limitation on the feasibility of large-scale attacks.

In this paper, we explore the feasibility and impact of launching jamming attacks on a multi-channel 802.11 network using a *single* cognitive radio. 802.11 networks are widely used to provide high-throughput connectivity for both small and city-wide areas. They are currently utilizing multiple channels to improve throughput and reduce user contention. Because commercial cognitive radio products are not yet available, we use Qualnet [1] based simulations to examine the impact of jamming attacks under different radio settings. We show that an attacker can manipulate a cognitive radio to switch frequently across channels and jam multiple channels simultaneously. With equal energy consumption, the effective number of channels jammed increases with the number of total channels in the system (to a limit). We also examine the difference between UDP and TCP traffic, the impact of packet size, and the channel switching delay.

The rest of the paper is organized as follows. In Section 2 we provide a brief background information on wire-

1-4244-1251-X/07/$25.00 2007 IEEE.

less security attacks, particularly jamming attacks and related work in this area. In Section 3 we describe in detail the single- and multi-channel jamming attacks using cognitive radios. We discuss experimental results and the feasibility of multi-channel jamming attacks using cognitive radios in Section 4. Finally, we summarize our findings and discuss future directions in Section 5.

2 Background and Related Work

In this section, we briefly discuss issues of wireless security in 802.11 networks, particularly single- and multi-channel jamming attacks, and existing works on securing cognitive radios.

2.1 802.11 Network Security

Security issues in 802.11 networks can be broadly classified into information security, network service security and infrastructure security. First, information security ensures data integrity and privacy between users. Existing proposals include WEP, WPA, 802.11i and 802.11x. Second, network service security protects the network from selfish users who deviate from normal behavior, and provides fair and efficient channel access to all users. Many have proposed extensions and modifications to the basic 802.11 MAC protocol to detect, mitigate and prevent selfish behaviors [7, 8, 10, 11, 12]. Finally, malicious users can attack network infrastructure to deny service to any legitimate user. For example, an adversary can use non-802.11 devices such as waveform generators, and transmit continuously on a wireless channel to jam the network completely. The goal of infrastructure security is to protect the underlying network infrastructure from such attacks.

2.2 Existing Work on Jamming Attacks

Prior work on wireless jamming attacks has focused on various attack models, detection mechanisms and simple solutions [4, 17, 18]. The work in [4] demonstrates the vulnerability of 802.11 MAC design to jamming attacks, and implements these attacks using off-the-shelf 802.11 hardware. In [17], the authors present four jamming attack models with varying levels of intelligence, and propose techniques to detect each attack by measuring signal strength, carrier sensing time and packet delivery ratio. Finally, the work in [18] proposes simple mechanisms to mitigate jamming attacks by hopping among channels and physically moving away from the adversary.

Existing work on jamming attacks mainly focuses on single channel networks. An adversary can attack a particular user by following the user as it hops across channels, but the goal is to jam a single channel (or a user). Our work is fundamentally different because we consider the possibility of attacking multiple channels (multiple users) simultaneously using a single cognitive radio.

2.3 Existing Work on Securing Cognitive Radios

Built on top of software defined radios (SDR), cognitive radios can dynamically reprogram their radio configurations through over-the-air software download [5]. Hence, one core security issue is to secure the over-the-air software download, verify the integrity of the radio configurations and authenticate the end points involved in the download process. In particular, a lightweight secure socket layer protocol is proposed in [6] to secure software update through low-bandwidth links. The work in [16] proposes mechanisms at authorized servers to verify radio configuration from open source developers before being downloaded onto client devices.

The above security mechanisms assume a trusted cognitive device and attempt to secure the device from malicious code update. In our work, however, we assume an adversary tampers a cognitive radio device to launch jamming attacks on multi-channel 802.11 networks.

3 Cognitive Radios based Jamming Attacks

In this section, we present mechanisms that use a single cognitive radio to jam a multi-channel 802.11 network. We assume an adversary has gained full control of a cognitive radio by tampering its radio reconfiguration software, and launches attacks on users who are communicating on multiple channels. We start from describing the basic jamming models on a single channel, and then present a simple attack to jam multiple channels simultaneously.

3.1 Single-channel Jamming Attacks

Malicious attackers use jamming attacks to disrupt network operations. The attacker transmits packets without adhering to the media access rules. Its jamming signals become noise/interference to communications between legitimate users, making the communication medium partially or completely unusable. Jamming has been widely used in battlefields where opposing parties try to disrupt each other's communication by detecting and jamming the corresponding wireless channels.

The simplest jamming attack on a single channel is to continuously transmit high-power signals on the channel,

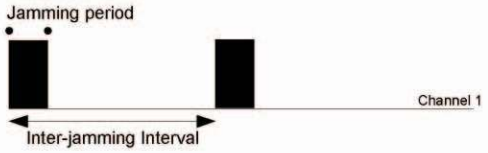


Figure 1: Periodic single channel jamming

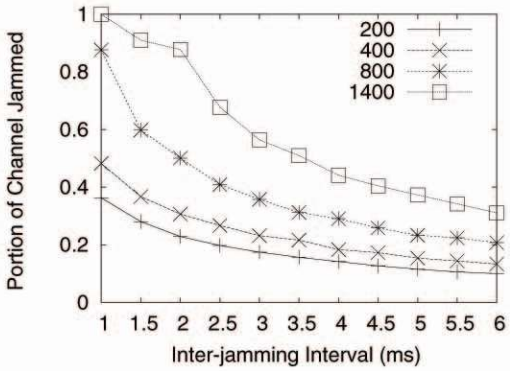


Figure 2: The portion of the channel jammed under different inter-jamming intervals, assuming 1 channel, 1 data link and 1 attacker. The attacker uses jamming packets of 50byte (≈0.2ms transmission time), and has a channel switching delay of 0.5ms. The user has different application packets of size 100, 500, 800 and 1400 byte, represented by each curve.

effectively interfering with any communication from legitimate users. However, this type of jamming is expensive in terms of energy cost, and can be easily detected [17]. An alternative is periodic jamming where the attacker transmits jamming packets at constant intervals, as shown in Figure 1. The impact of jamming depends on the length of inter-jamming interval, the size of jamming packets, and the size of data packets at the victim. In particular, previous work has shown that transmitting small jamming packets can corrupt normal data packets and effectively jam the channel.

To examine the impact of inter-jamming interval and the size of data packets, we show in Figure 2 the portion of channel jammed at various inter-jamming intervals for data packets of size 200, 400, 800 and 1400 byte. The attacker transmits jamming packets of 50byte (≈ 0.2ms jamming time) periodically to disrupt a data link. As expected, the impact of jamming degrades gracefully with the inter-jamming interval. Further, transmissions with larger data packets are more vulnerable to jamming attacks. Typical internet traffic with 1400byte packets can suffer from 100% to 40% degradation for small inter-jamming intervals. Apparently, reducing data packet size can effectively reduce the impact of jamming. However, previous study has shown that small packet sizes can significantly decrease transmission efficiency due to per-packet contention and protocol overhead [15]. Therefore, there is an inherent tradeoff between attack resistance and system efficiency.

Users can mitigate single-channel jamming attacks by switching to a different channel upon detecting large packet losses [18]. An alternative is to randomly hop across channels [2] and periodically synchronize to set up communication links. Next, we show that attackers can use a single cognitive radio to effectively jam multiple channels simultaneously, making channel-hopping based defense mechanisms less effective.

3.2 Multi-channel Jamming Attacks

To jam multiple channels simultaneously, attackers can make use of multiple radio devices, each dedicated to a channel. However, the cost of jamming scales linearly with the number of channels. An low-cost alternative is to use a *single* cognitive radio that switches across channels and disrupts operations of each channel on the fly.

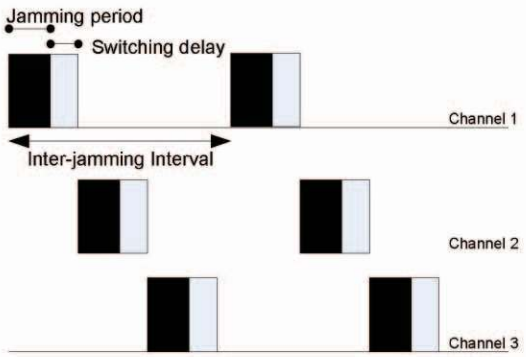


Figure 3: Multi-channel jamming

Figure 3 illustrates a multi-channel jamming attack on three channels. Initially the attacker corrupts data transmissions of legitimate nodes by transmitting on channel 1 for a fixed *jamming period*. At the end of the jamming period, the attacker switches to the next orthogonal channel (channel 2) with a minor switching delay, and starts the jamming operation. Similarly, it then switches to channel 3. After jamming channel 3, the attacker revisits channel 1 and repeats the jamming cycle.

This multi-channel jamming attack is simple to launch, even using a single 802.11 radio. However, the effectiveness of the attack can be limited by the slow channel switching of existing 802.11 radios. The switching delay varies from 5-100ms depending on the device manufacturer. Cognitive radios, on the other hand, can signifi-

cantly reduce channel switching delay by 10-100 times, making them more attractive to attackers.

In addition to fast channel switching, cognitive radios also have advanced channel sensing capabilities. This enables attackers using cognitive radios to build up channel usage patterns of network users, switch only among channels that are currently in use and launch highly intelligent and efficient jamming attacks. As reported by [17], it is very difficult to detect these intelligent attacks.

4 Experimental Results

In this section, we evaluate the effectiveness of jamming attacks. We simulate these attacks using Qualnet 3.8 [1], assuming the following two types of users:

- *Legitimate user* – We assume a group of legitimate users who share a set of channels using 802.11 MAC protocols. Each user has a 802.11 radio device and transmits at 2Mbits/sec. All the users have the same traffic model, either a UDP application with a fixed packet size (100, 512 or 1400 bytes), or a TCP application with a packet size of 512 bytes. Each user has backlogged traffic. We simulate both lightly- and heavily-loaded scenarios by varying the number of user pairs per channel, 1 per channel for lightly-loaded networks and 10 per channel for heavily-loaded networks.
- *Attacker* – We assume a single attacker with a single cognitive radio. The attacker is in range of all legitimate users and switches across channels to affect as many users as possible. By default, the attacker uses jamming packets of 50 bytes, and switches among channels with 0.5ms delay.

We measure the percentage of user traffic corrupted by the attacker on each single channel, and sum over all the channels. The result, referred to as the *equivalent number of channels jammed*, represents the impact of jamming in a multi-channel network using a single cognitive radio. Next, we examine the impact of jamming by exploring different radio settings, including the number of channels in the system, the size of jamming packets and the channel switching delay.

4.1 Impact of the Number of Channels

Figure 4 shows the result of jamming efficiency with different number of channels in the system. We observe that the impact of jamming converges as the number of channels increases. The impact of jamming is much more visible for networks with smaller number of channels. Hence, jamming attacks using cognitive radios pose a serious threat to 802.11 networks, especially 802.11b networks with only 3 orthogonal channels.

Comparing the results in Figure 4(a) and (b), we observe that the impact of jamming drops as the channel becomes more crowed. This is because each successful jamming attempt will lead to a subsequent backoff at the victim. In a heavily populated channel, while the victim backoffs, other users continue to use the channel and the extra impact from backoff becomes less visible. We note, however, this observation comes from the assumption of backlogged traffic at each user. When users have light traffic, the impact of jamming will scale with the number of users on each channel.

4.2 Impact of the Jamming Packet Size

Figure 5 examines the impact of jamming packet size (jamming period). We observe that jamming with 50byte packets leads to the highest impact – 7 out of 12 channels are jammed. This is because jamming with small packets not only effectively corrupts data packets, but also reduces the time of each jamming attempt. As a result, the jammer can switch frequently across channels and attack each channel at a smaller inter-jamming interval, leading to higher jamming impact.

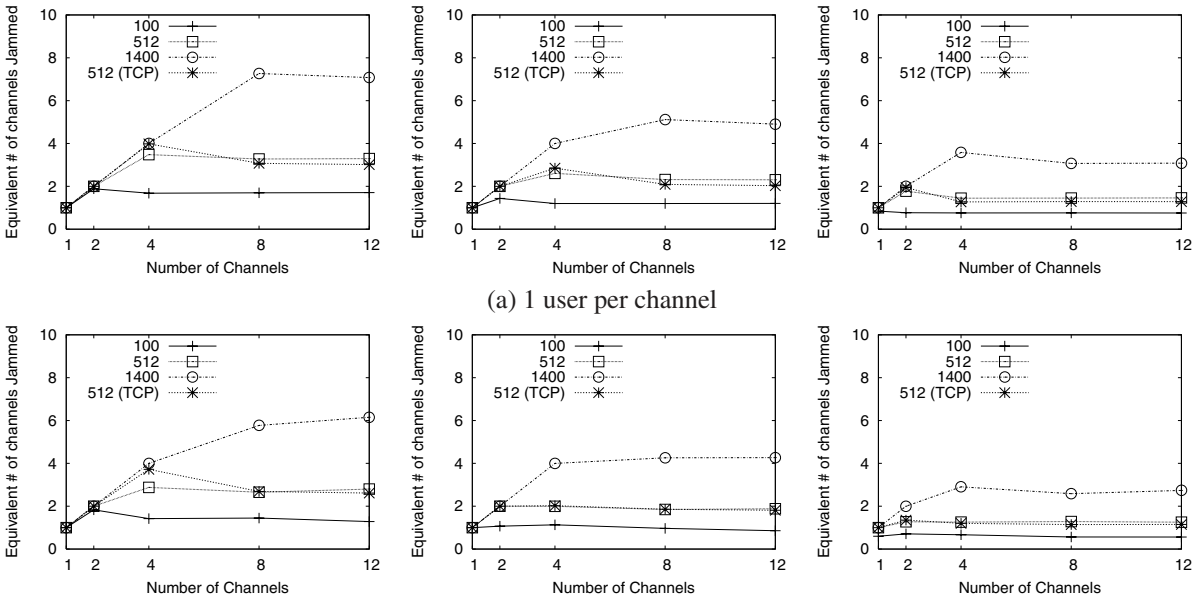
4.3 Impact of channel switching delay

Figure 6 shows the impact of channel switching delay on jamming efficiency. As expected, the impact of jamming is quite sensitive to switching delay, and increases as switching becomes faster. With a switching delay of 0.4ms and 1400byte data packets, the jammer can disrupt almost all the channels in a system with 4 channels and, 7 channels in a system with 8 and 12 channels. However, when the switching delay increases to 3.2ms, the impact of jamming drops to 2 channels.

This result is alarming since the maximum channel switching delay of cognitive radios can reduce to the order of a few hundred microseconds, making them perfect candidates for jamming attack devices.

5 Conclusion

In this paper, we take an initial look at the security threat posed by the flexibility of cognitive radios. We explore the feasibility of launching jamming attacks on multi-channel 802.11 networks using a single cognitive radio. Through extensive simulations, we show that an attacker using a single cognitive radio can jam up to 7 channels. Such jamming attacks pose a serious threat to existing multi-channel 802.11 networks and future cognitive networks.



(a) 1 user per channel

(b) 10 users per channel

Figure 4: The equivalent number of channels jammed for various number of channels in the system, assuming 1 user per channel (top 3 figures) and 10 users per channel (bottom 3 figures). Figures in each row represent channel switching delays of 0.4ms(left), 0.8ms(center) and 1.6ms(right).

References

[1] Qualnet. `http://www.scalable-networks.com`.

[2] BAHL, V., CHANDRA, R., AND DUNAGAN, J. Slotted seeded channel hopping for capacity improvement in ieee 802.11 ad-hoc wireless networks. In *Proc. of MobiCom* (Philadelphia, PA, Sept. 2004).

[3] BARFORD, P., AND YEGNESWARAN, V. An inside look at botnets. In *Special Workshop on Malware Detection* (August 2005).

[4] BELLARDO, J., AND SAVAGE, S. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *Proc. of USENIX Security Symposium* (Washington, DC, August 2003).

[5] BING, B. A fast and secure framework for over-the-air wireless software download using reconfigurable mobile devices. *IEEE Communications Magazine 44*, 6 (June 2006), 58–63.

[6] BRAWERMAN, A., BLOUGH, D., AND BING, B. Securing the download of radio configuration files for software defined radio devices. In *Proc. of MobiWac* (September 2004), ACM.

[7] GUANG, L., AND ASSI, C. A self-adaptive detection system for mac misbehavior in ad hoc networks. In *Proc. of IEEE International Conference on Communications* (June 2006).

[8] GUPTA, V., KRISHNAMURTHY, S., AND FALOUTSAS, M. Denial of service attacks at the mac layer in wireless ad hoc networks. In *MILCOM* (October 2002).

[9] HAYKIN, S. Cognitive radio: Brain-empowered wireless communications. *IEEE JSAC 23*, 2 (Feb. 2005), 201–220.

[10] KONORSKI, J. Multiple access in ad-hoc wireless lans with noncooperative stations. In *The Second International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols* (2002).

[11] KYASANUR, P., AND VAIDYA, N. H. Detection and handling of mac layer misbehavior in wireless networks. In *Proc. of IEEE International Conference on Dependable Systems and Networks* (June 2003).

[12] KYASANUR, P., AND VAIDYA, N. H. Selfish mac layer misbehavior in wireless networks. *IEEE Transactions on Mobile Computing 4*, 5 (2005), 502–516.

[13] MCHENRY, M. Spectrum white space measurements. *New America Foundation Broadband Forum* (June 2003).

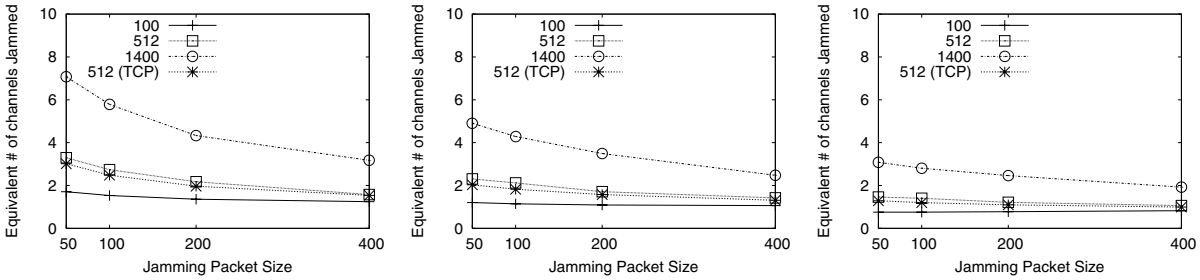
[14] MITOLA III, J. Wireless architectures for the 21st century. `http://ourworld.compuserve.com/homepages/jmitola`.

[15] RAGHAVENDRA, R., JARDOSH, A. P., BELDING, E. M., AND ZHENG., H. IPAC: IP-based adaptive packet concatenation for multihop wireless networks. In *Asilomar Conference on Systems, Signals and Computing* (Oct 2006).

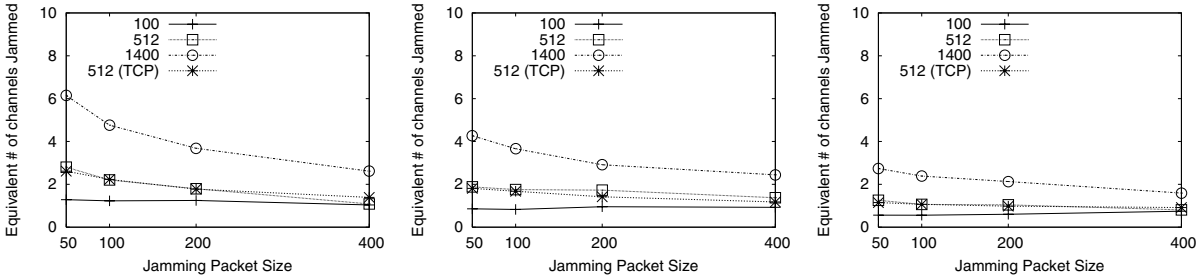
[16] RONDEAU, T. W., BIELAWA, T. M., MALDONADO, D., HSIAO, M., AND BOSTIAN, C. W. A methodology for a verifiable software platform to secure software defined and cognitive radios. In *Software Defined Radio Technical Conference and Product Exposition* (November 2005).

[17] XU, W., TRAPPE, W., ZHANG, Y., AND WOOD, T. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proc. of MobiHoc* (Urbana-Champaign, IL, May 2005).

[18] XU, W., WOOD, T., TRAPPE, W., AND ZHANG, Y. Channel surfing and spatial retreats: defenses against wireless denial of service. In *Proc. of Workshop on Wireless Security* (Philadelphia, PA, October 2004).

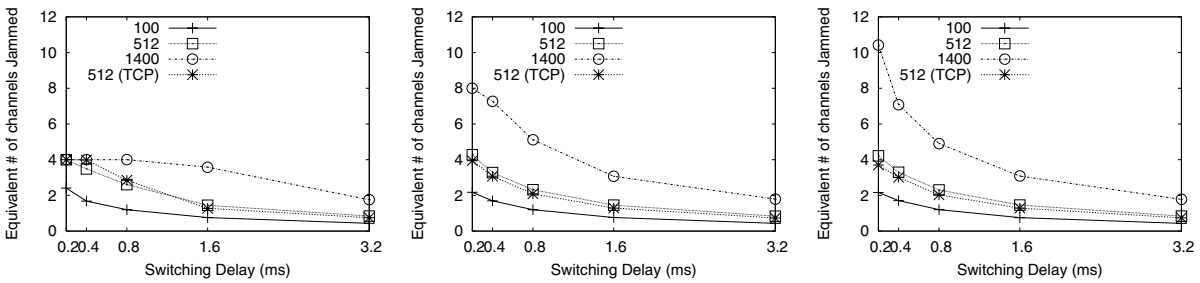


(a) 1 user per channel

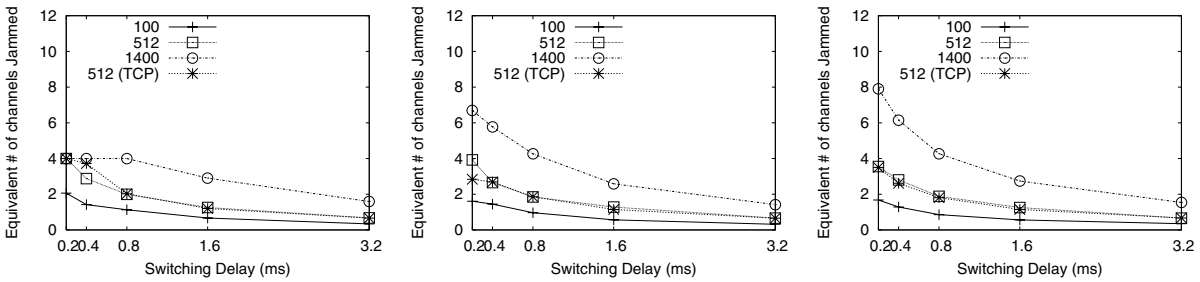


(b) 10 users per channel

Figure 5: The equivalent number of channels jammed for various the sizes of the jamming packet assuming 12 channels, 1 user per channel (top 3 figures) and 10 users per channel (bottom 3 figures). Figures in each row represent channel switching delays of 0.4ms(left), 0.8ms(center) and 1.6ms(right).



(a) 1 user per channel



(b) 10 users per channel

Figure 6: The equivalent number of channels jammed for different channel switching delays assuming 1 user per channel (top 3 figures) and 10 users per channel (bottom 3 figures). Figures in each row represent 4 channels(left), 8 channels(center) and 12 channels(right) as being attacked.