Poster: Low-Power DoS Attacks in Data Wireless LANs and Countermeasures

Guevara Noubir
College of Computer Science
Northeastern University, Boston, MA, USA
noubir@ccs.neu.edu

Guolong Lin
College of Computer Science
Northeastern University Boston, MA, USA
lingl@ccs.neu.edu

ABSTRACT

In this paper we investigate the resiliency to jamming of data protocols, such as IP, over WLAN. We show that, on existing WLAN, an adversary can successfully jam data packets at a very low energy cost. Such attacks allow a set of adversary nodes disseminated over an area to prevent communication, partition an ad hoc network, or force packets to be routed over adversary chosen paths. The ratio of the jamming pulses duration to the transmission duration can be as low as 10^{-4}. We investigate and analyze the performance of using various coding schemes to improve the robustness of wireless LANs for IP packets transmission. A concatenated code that is simple to decode and can maintain a low Frame Error Rate (FER) under a jamming effort ratio of 15%. We argue that LDPC codes will be very suitable to prevent this type of jamming. We investigate the theoretical limits by analyzing the performance derived from upper bounds on binary error-control codes. We also propose an efficient anti-jamming technique for IEEE802.11b.

Categories and Subject Descriptors

D.3.3 [**Computer-Communications Networks**]: Network Protocols.

General Terms

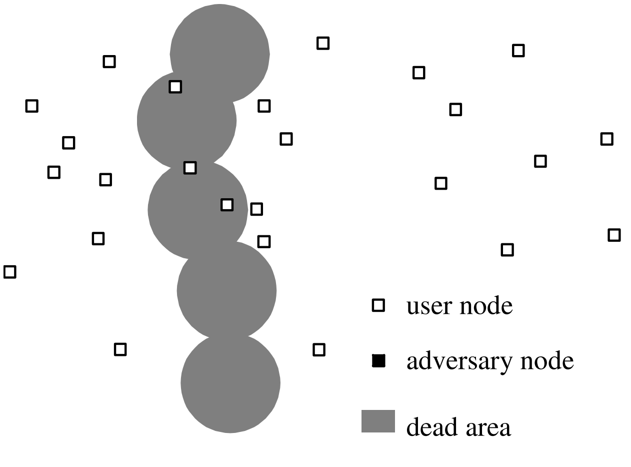
Reliability, Security.

Keywords

Jamming, Wireless, WLAN, DoS.

1. INTRODUCTION

Current standards for wireless data communications such as IEEE802.11 and Bluetooth are easy targets of denial of service attacks. For example, the physical layers of IEEE802.11 and IEEE802.11b do not have any error-correction scheme. If an attacker sends a strong jamming signal of duration ***one*** bit/symbol it will make the CRC computation wrong. Therefore the whole packet will be lost. If we assume that this wireless link is used to transmit an IP data packet (usually 12000 bits long), the energy ratio between a jammer and user can be of the order of 1/10000 (which is equivalent to 40 dB gain for the jammer). Other wireless data standards that make use of error-correction codes can also be easily defeated. The reason is that current systems are designed to resist to non-malicious interference and noise. Even robust wireless links designed to resist jamming do not fully take into account the data aspect of the communication. Existing anti-jamming systems rely on an extensive use of spread-spectrum techniques. These techniques *separately* protect *bits* against jammers. They are adequate for voice communication where the jammer has to keep jamming the channel to prevent a communication. In voice communication, when the communicating nodes use a high-gain spreading sequence, the energy of a jammer can be easily exhausted for a continuous jamming of the voice communication. Non-continuous jamming only results in a graceful degradation of the voice quality. In the context of data communication, spread-spectrum techniques are not sufficient because the jammer does not need to jam a data packet for a long period of time to be able to destroy it. In a "non error-correction" encoded data packet a single bit error generates a CRC error, leading to the loss of the entire packet. Our work aims at building on top of traditional anti-jamming techniques, used at the bit level (such as spread spectrum), to protect data packets.



In the context of a multihop ad hoc network a small number of smart jammers disseminated across a geographical area can last for a long period of time with limited energy resource. Since they only need short jamming durations, the remaining time and energy can also be used to jam other communication channels. They can even be coordinated to create an attack network targeting traffic between specific nodes. They can achieve several goals such as preventing all communication, partitioning

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

MobiHoc'03, June 1-3, 2003, Annapolis, Maryland, USA.

Copyright 2003 ACM 1-58113-684-6/03/0006…$5.00.

a network at low energy cost, or forcing all packets to be routed over chosen areas. In the last case, the traffic will be forced over an area where the adversary has powerful nodes that do better channel decoding and traffic analysis. The adversary nodes can stay in sleep mode most of the time and be triggered to jam some communication between specific nodes. In this case, the attackers would only wake-up to detect some MAC/IP address and, if needed, jam only few bits of the packet to destroy. The attacking nodes receivers can be designed to consume very little energy because the goal is not to demodulate/decode correctly a packet but only to detect (or carrier sense), with a reasonable probability, ongoing communication. These low-power jammers will be referred to as *cyber-mines.* Even if anti-jamming techniques, such as spread-spectrum, are used, the substantial gain achieved by having to jam only few bits out of 1500 bytes IP packets can be invested in a higher signal power (for direct-sequence spread spectrum) or multi-channel jamming (for frequency hopping spread spectrum). This gain in jamming effort can be invested by the attacker to circumvent the processing gain (usually 20 to 30 dB in the context of military communications) achieved by spread spectrum techniques.

2. JAMMER EFFICIENCY AGAINST WLAN

In the following tables we show that a jammer can prevent data packet communication of existing WLANs with very high jamming efficiency (i.e., ratio of communication effort to jammer effort).

Mod/coding 802.11 & 802.11b	Packet Length	Bits to Jam	Jammer Efficiency
BPSK	1500*8	1	12000
QPSK	1500*8	2	6000
CCK (5.5Mbps)	1500*8	4	3000
CCK (11Mbps)	1500*8	8	1500

Table 1. Jamming efficiency against IEEE802.11b.

Rate Mbps	Mod	Code Rate	Bits Jam	Encoded length	Jammer Efficiency
6	BPSK	½	48	1500*8*2	500
9	BPSK	¾	48	1500*8*4/3	333
12	QPSK	½	96	1500*8*2	250
18	QPSK	¾	96	1500*8*4/3	167
24	16QAM	½	192	1500*8*2	125
36	16QAM	¾	192	1500*8*4/3	83
48	64QAM	½	288	1500*8*2	62.5
54	64QAM	¾	288	1500*8*4/3	55.5

Table 1. Jamming efficiency against IEEE802.11a.

Packet Type	Number of bits	Bits to Jam	Jammer Efficiency
DH1 (no ECC)	28*8 = 224	1	224
DM3 (15, 10, 4)	123*8 = 984	2	984/2 = 492
DH3 (no ECC)	185*8 = 1480	1	1480
DM5 (15, 10, 4)	226*8 = 1808	2	1808/2 = 904
DH5 (no ECC)	341 * 8 = 2728	1	2728
DV (15, 10, 4)	150	2	75

Table 2. Jamming efficiency against Bluetooth data packets.

3. PROPOSED TECHNIQUES AND BOUNDS

The proposed technique is based on the combination of error-correction codes and cryptographically strong interleavers (i.e., adversaries cannot guess the interleaving function). The underlying assumption to our work is that jamming a single bit has a constant cost. We investigate how this cost scales to destroying a complete packet. All existing techniques, such as spread spectrum, can be transparently combined with our approach for an increased resiliency. An error control code C is characterized by $(n, k, d)_q$. n denotes the codeword length, $k = \log_q|C|$ the uncoded word length, d the code minimum distance, and q the code alphabet size. The encoding of a packet starts by appending a CRC (s bits), dividing the packet into l blocks of k bits. Each block is encoded into n bits. Finally the encoded packet bits are interleaved in a non-guessable way for the jammer. If the aggregate jamming duration is e, the jamming effort is denote as $\tau=e/nl$ and the achievable throughput is $T=(lk-s)(1-FER)/nl$ where FER is the frame error rate under the considered jamming effort.

First we considered using a single block of best-known short binary code (upto 95 bits and not taking into account the checksum overhead) a throughput of 0.25 can be achieved against jamming effort 15% and 0.18 against 20% jamming effort. When using a cryptographically strong interleaver the upper bound on throughput can be computed from Shannon channel capacity for a binary symmetric channel $1+\tau*\log(\tau)+(1-\tau)*\log(1-\tau)$. We have shown that dividing a packet into l blocks encoded using best-known short codes leads to extremely poor performance when l increases. For binary modulation schemes we constructed simple concatenated coding schemes (e.g., Preparata code and Reed-Solomon codes) that achieve reasonable performance for reasonably long packets (e.g., throughput 15% against 14% jamming effort for packets of length 400 bits). Our conclusion is that the most suitable codes for binary modulation would be the Low Density Parity Codes (LDPC) because in addition to being close to Shannon's bound, they can be long enough for IP packets (thousands of bits) and still have reasonably low decoding complexity. Although an LDPC can act on the whole packet they would still need a cryptographic interleaver because there still exists some low weight uncorrectable errors. In the case of non-binary modulation schemes such as IEEE802.11b CCK (11 Mbps), we propose to use a Reed-Solomon code of symbol length 8 that achieves a throughput that is a linear function of the jamming effort. This is possible because data is transmitted as a sequence of symbols of 8 bits each.

In the full paper (www.ccs.neu.edu/home/noubir/publications) we describe the communication system model, packet encoding, and the adversarial model. We show why traditional jamming techniques are not adequate for data packet communication. Then we describe in detail efficient jamming techniques against existing WLANs. We investigate upper bounds on the throughput and the use of single codeword binary codes, multiple codeword binary codes, some concatenated codes, and LDPC codes. Finally we propose an efficient non-binary RS code for IEEE802.11b.