Jamming Detection and Mitigation in Wireless Broadcast Networks

SAMULA ANNAPURNA¹ Dr.K.V.V.S.NARAYANA MURTHY ² Prof.M.VAMSI KRISHNA³

1. MTECH(CSE), Chaitanya Institute of Science & Technology
2. Prof & Head, Department of IT, Chaitanya Institute of Science & Technology, Kakinada
3. Prof & Head, Department of CSE, Chaitanya Institute of Science & Technology, Kakinada

Abstract—Wireless communication systems are often susceptible to the jamming attack where adversaries attempt to overpower transmitted signals by injecting a high level of noise. Jamming is difficult to mitigate in broadcast networks because transmitting and receiving are inherently symmetric operations: A user that possesses the key to decode a transmission can also use that key to jam the transmission. We describe a code tree system that provides input to the physical layer and helps the physical layer circumvent jammers. In our system, the transmitter has more information than any proper subset of receivers. Each receiver cooperates with the transmitter to detect any jamming that affects that receiver. In the resulting system, each benign user is guaranteed to eliminate the impact of the attacker after some finite number of losses with arbitrarily high probability. We show that any system that relies on only using spreading code, and no other physical factors, to mitigate jamming must use at least codes, where is the number of jammers. We then propose an optimized scheme that is power-efficient: Each transmission is sent on at most codes simultaneously. Finally, we demonstrate that our scheme approaches the best possible performance by performing an extensive analysis of the system using both event-driven ns-2 and chip-accurate MATLAB simulations.

Index Terms—Broadcast networks, jamming mitigation, spread spectrum.

I. INTRODUCTION

WIRELESS communication systems are often susceptible to the jamming attack in which adversaries attempt to overpower transmitted signals by injecting a high level of noise, thereby lowering the signal-to-noise ratio (SNR). Lowering the SNR, in turn, can significantly reduce the achievable rate of a communication system. An effective countermeasure to the jamming attack is increasing the bandwidth of the spectrum of the communication system and using spread spectrum as part of the modulation technique [3]. In spread-spectrum systems, a transmitter takes advantage of the increased bandwidth to redundantly encode information using a spreading code. To receive a message, a spread-spectrum receiver decodes the incoming signal by correlating the signal with the spreading code. Spread-spectrum codes are thus inherently symmetric; that is, the transmitter and the receiver use the same information for encoding and for decoding.
Without knowing the spreading code used by a pair of a transmitter and receiver, unintended signals such as jamming or self-interference will likely appear noise-like upon decoding, and most of the unintended signal power can then be rejected by filtering. However, if a jammer discovers the spreading code in use (for example, by compromising the receiver), all benefit of using spread spectrum against jamming is lost. While using spread spectrum as part of modulation can be highly effective against jamming in point-to-point wireless communication systems in which a single transmitter transmits to a single receiver, it is difficult to prevent jamming in a broadcast system that transmits information to multiple users at once. This is because if a group of receivers shares a single code, then a jammer can deny service to the entire group by compromising any one of the group members. However, a transmitter is interested in conserving the number of spreading codes used in a broadcast system since the total transmission power is divided between the set of spreading codes simultaneously used.

In this paper, we present a scheme that allows a receiver to detect jamming by observing that a secondary message is received without the primary message. We then present a keying scheme that allows the transmitter to cooperate with the receiver to isolate the set of jammers from the set of benign users. Finally, we develop a technique called tree remerging to optimize our keying scheme so that a transmitter can group benign receivers together and let that group share one spreading code, thereby providing satisfactory quality of service to the receivers without requiring higher total transmission power. Modern mobile networks commonly use broadcast messages to discover routing information. Cellular phone standards, such as IS-95, also use broadcast messages for synchronization and paging. It is therefore very important to defend broadcast from jamming. Previously proposed approaches to mitigate jamming, such as spread spectrum, reside entirely at the physical layer.

However, substantial previous work shows that upper layer feedback can improve lower layer performance in areas such as transmit power control [4]. Our keying scheme uses a binary tree structure implemented above the physical layer that takes advantage of the unique properties of spreading codes in order to mitigate jamming in any broadcast systems based on existing spread-spectrum techniques. Current commercial spread-spectrum systems, such as IS-95, are not suitable for use in an adversarial environment due to the use of fixed and published codes. We will assume the use of unpredictable and time-varying spreading codes, such as a code generated using Advanced Encryption Standard [5], to eliminate the security flaws inherent in using fixed spreading codes over an extended period of time. Our proposed protocol has broad applicability to a wide variety of existing wireless access technologies such as IEEE 802.11 [6], IS-95 [7], and CDMA2000 [8], which are already CDMA systems. To adopt our protocol, a CDMA system must be able to assign each user a different set of spreading codes that should change over time. Most current CDMA systems already require a client registration phase, where each client is given an identification number. For example, a client needs to provide some identification in order to obtain 3G service on a CDMA phone with a unique electronic serial number (ESN). The set of spreading codes can thus be distributed during the registration phase. The use of time-varying spreading code is not
necessary for running our protocol; however, our protocol adopts time-varying spreading codes in order to prevent attackers from learning a spreading code by correlating messages over time. Our protocol does not require regular feedback from receivers; however, our broadcast transmitter does need to be able to receive jamming report from receivers occasionally.

FFH-CDMA and DS-CDMA

FFH-CDMA and DS-CDMA are two distinct spread-spectrum implementations. In FFH-CDMA, a transmitter changes the frequency bands on which the signals are transmitted. In DS-CDMA, a transmitter maps each bit into a sequence of chips, which are then modulated and transmitted. In a FFH-CDMA system, the entire spectrum of the communication system is divided into a number of frequency bands, and time is divided into time slots, the duration of which is much shorter than the time it takes to send 1 bit of information. Each user is assigned a frequency-hopping pattern that serves as his spreading code. In each time slot, the transmitter occupies a particular set of frequency bands and changes, at each time slot, to another set of bands according to his frequency-hopping pattern. The transmission made in a single time slot is referred to as a chip. The receiver receives the signal by monitoring the waveforms on the set of frequencies specified by the hopping pattern in each time slot and combining the waveforms. In a DS-CDMA system, each bit is mapped to either 1 or 0, and each user is assigned a pseudorandom code of length .

Unintentional interference and jamming mitigation using CDMA has been studied at length [3]. Other physical-layer techniques, such as the use of multiple antennas and antenna nulling [10], have also been studied. Recently, researchers have also sought to avoid jamming by taking advantage of various properties of physical propagation. Bahn et al. proposed a particular coding scheme, the BBC code, such that when used with indelible marks, an energy-limited jammer cannot interfere with the message transmission indefinitely [11]. Strasser et al. proposed the uncoordinated frequency-hopping protocol [12], in which the transmitter seeks to finish its transmission before a jammer can find out on which frequency band the signal was transmitted. Follow-up studies have sought to extend the concept to other spreading techniques and to incorporate variable length of spreading code for faster decoding [13]. Our approach is different from these schemes in that any transmitter–receiver pair in our proposed jamming mitigation technique shares prior-agreed keys and spreading codes. We thus do not need to make any new assumptions about the computation ability of a jammer. For example, in the uncoordinated frequency-hopping scheme, the authors relied on the assumption that a jammer cannot timely detect the frequency band on which a packet of multiple bits is transmitted [12]. Asymmetric cryptography [14], such as RSA [15] and Diffie–Hellman [16], rely on the alleged asymmetry of certain computational functions to achieve public-key cryptography and digital signatures. Our work differs in that it overlays an inherently symmetric operation: wireless transmission. Other work has used time and delayed disclosure to provide asymmetry [17], [18]. If we wish to use digital signatures as spreading codes (as described by Kuhn [18]), we still need a jam-resistant way to provide receivers with a spreading code. Attacker and System Model

We make the standard assumption that any jammer is powerlimited, but not necessarily energy-limited. That is, we assume that a
jammer can transmit for as long as he wishes; however, the jammer cannot transmit with infinite power regardless of how short the time duration is. Specifically, we assume that a jammer is not powerful enough to saturate the analog-to-digital converter at the receiving end. We make no other assumptions on the physical ability of the jammer. We assume a jammer cannot calculate the spreading code based on a message within the time duration to transmit 1 bit. We make no other limitations on the computation power of a jammer. Since our broadcast transmitter does not publicly select any subset of spreading codes to use, the number of codes a jammer needs to test to find the set of spreading codes in use is exponential with respect to the length of the spreading code. However, the time duration to send a bit is only linear with respect to the length of the spreading code. Therefore, our assumption is reasonable since the computation time is of different order than the transmission time.

minimizing the number of codes simultaneously used, the transmitter wants to transmit on a set of spreading codes such that any user can decode using exactly one spreading code in the set. We call such a set of spreading codes a disjoint cover. Once jamming has been detected on some spreading codes (we will discuss jamming detection in Section III-C), the transmitter should avoid using such spreading codes in the future. To receive a message, each receiver simply decodes the signal using all the codes he knows. If a receiver does not have enough computation ability to decode using all codes he knows simultaneously, the receiver can sequentially try all codes, using only a subset of codes in each time instance.

C. Jamming Detection Algorithm and Response
In this section, we present our algorithm to detect jamming on a particular spreading code. We then show how a broadcast system using our code tree can respond to detected jamming.

1) Jamming Detection: When the transmitter sends a packet, it will do so on the current minimal safe cover, on which no jamming had been previously detected, so that all legitimate receivers can decode the packet. In order to detect further jamming activities, the transmitter additionally transmits on a test spreading code that is randomly chosen from among the descendants of the cover. This redundant test spreading code allows the transmitter and receivers to cooperatively detect jamming on any spreading code in the cover that is an ancestor of the test spreading code. We call this ancestor code the detectable spreading code.

Fig. 1. Example code tree.

In the initial phase of our protocol, a transmitter transmits to all receivers on a single spreading code; specifically, it would choose the spreading code corresponding to the root of the tree. Transmissions on this spreading code can be decoded by any legitimate (benign and compromised alike) receiver if the code is not jammed. In general, in order to ensure that every receiver can decode a packet while

www.ijrcct.org chiefeditor@ijrcct.org
1) Jamming is successful on a code only if a jammer knows that code (i.e., jamming cannot overcome the processing gain).
2) Each subset of the tree is a possible test set (i.e., each such subset is tested with nonzero probability).
3) When only benign receivers know a test code, and jamming is perpetrated on the corresponding detectable code, at least one benign receiver detects the jamming with probability at least (i.e., jamming detection sometimes works).

Fig. 2. Code tree is merged with the main tree. (a) Main tree and tree to be inserted. (b) and (c) show the right half of the tree in (a). (b) Code tree is merged by being inserted into the leftmost place that it would “fit.” (c) Resulting main tree after subtrees are swapped to keep all nonempty nodes flush to the left. Another approach is to disseminate the current cover using the testing mechanism. When the base station transmits on a test code, the message includes all ancestor codes of that particular test code. Thus, whenever a code known to a receiver is selected for testing, that receiver is able to update the ancestor codes to which he has access. This dissemination technique is desirable since some receivers might not know the current cover and would redundantly report jamming detection when tested. In this section, we describe the results of two simulation-based evaluations. In the high-level simulation, we assume the codes are completely orthogonal, and precisely model the received signal and noise levels after processing gain, using the resulting signal-to-noise ratio to select a bit error rate. In the low-level simulation, we model the use of random codes and tree remerging in order to ensure that the random codes provide sufficient interference cancellation, and that the tree remerging scheme does not substantially reduce the effectiveness of jammer detection.

A. High-Level Simulation Methodology
We simulate our basic jamming mitigation scheme without the remerging optimization in a high-level simulation that is based on the ns-2 discrete-event network simulator [22]. We implement the following features into ns-2: simultaneous sending of a single packet on multiple codes and simultaneous reception of multiple packets on multiple codes. We conduct our simulations on a 1500 300 m area with 50 receivers. For each incoming packet, we compute the maximum interference power experienced during the reception of the packet, including power contributed by any outgoing packets, the jammers, other incoming packets, and ambient noise (conservatively computed as half of the IEEE 802.11b carrier sense threshold from ns-2). We then compute the signal-to-noise ratio, including processing gain from the original packet, the energy cost of simultaneously sending on multiple codes, and any processing gain that the jammers receive as a result of transmitting on the same code.
CONCLUSION

Due to the symmetric nature of spread-spectrum codes and the inverse relationship between signal power and number of codes used simultaneously, it is difficult to extend the jamming resilience of spread-spectrum techniques from a point-to-point wireless communication system to a broadcast wireless communication system. In this paper, we provide a protocol that allows a broadcast communication system to dynamically change the spreading codes used by subsets of receivers so that some benign users can share a single spreading code, thereby conserving the number of spreading codes used simultaneously. We show a lower bound on the number of spreading codes used simultaneously in order to mitigate jamming by relying only on keying and not other physical characteristics. We optimize our protocol so that it can mitigate jamming by using twice as many spreading codes simultaneously as the lower bound. We present simulation results to support our theoretical results and show that jamming can be effectively mitigated in a broadcast wireless system.

REFERENCES