THESIS OR DISSERTATION TITLE
TITLE LINE 2

by

Travis F. Collins

A Thesis
Submitted to the Faculty
of the
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements for the
Degree of Master of Science
in
Electrical and Computer Engineering
by

December 2012

APPROVED:

Professor Alexander Wyglinski, Major Advisor

Professor Y

Professor Z

Abstract

Put your abstract here.

Acknowledgements

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Since the advent of modern digital communications in the 20th century there has been an explosion in the demand for wireless spectrum. As a result spectrum is becoming an increasingly scare resource(Insert citation). This demand is a direct result of the availability and relatively inexpensive cost of such wireless device. Therefore in such envirorments as militaristic theatres the probability of interfering transmissions has steadily grown to a point where techniques need to be consider to combat such occurrences. More directly, in such situations when interfering signals are partially or completely understood measures can be taken to overcome such difficulties.

In military theatres it is extremely common to observe friendly operated high-power broadband jamming signals(citation). Such devices exists as part of group convoys in several branches of the military and in many other forms in contested territories or war-zones. Unfortunately such devices block both friendly and hostile communications, and current anti-jamming techniques haven't provided a viable solution to this problem. Therefore new avenues should be considered, utilizing more flexible radio technologies.

Understanding how to overcome such challenges is a complex task; with vastly different

transmission envirorments and differing operating devices and operating standards. A new system that could combat such downfalls should rely on all friendly information, or be able to construct solutions of its own from a set of tools given to the radio. Such tools should be flexible and easily modified, changed, or improved. This ability to easily change or adapt is a key feature as the technical requirements can change from day to day, or between branches of the military itself. As such a solution should have the following attributes:

- **Flexible:**
- **Resilient:**
- **Hardened:** in changing enviroments

1.2 State of the Art

Current implementations in anti-jamming technology lies on the strateling point of hardware and software in the communications world. This is true because hardware provides the speed and performance needed for digital data transmission, while software provides higher level intelligence and flexibility in such layers as the media access control layer and the network layer of the OSI model (insert citation of OSI model.) For anti-jamming applications, high intelligence allows for mobility again the jammer. Therefore a large implementation in software must be considered when investigating anti-jamming technics.

Insert figure of OSI model

Current anti-jamming technics include channel hopping, spatial retreat, jammed area mapping, node escape, retreat restoration, frame masking, and many more[5]. All of these techniques use mechanisms of evasion or despection. These can be quite effective when attacked by generally narrowband, non-dynamic/learning jammers. In the case of wide and ultra-wide band jammers, they fail miserably. This wide-band enviorment is the primary situation of interest, and it generally considered a hopeless scenario. These anti-jam technics are design for specific situations and jammers.

Let us first examine these anti-jamming technics which are broken down into three primary categories: Proactive countermeasures, Reactive countermeasures, and Mobile agent-base countermeasures[5]. Reactive countermeasures relies on a varying array of detection mechanisms first to determine if that node is being jammed. These detection methods must be coupled with a countermeasure or the scheme is in operable. Examples of these detection methods include a transmitter-based approach and a receiver-based detection. In a transmitter-based approach, such as ad-hoc networks, a decision algorithm is used based on four metrics: PDR (Packet Delivery Ratio), RSSI (Received Signal Strength Indicator), Physical rate, and Noise levels[3]. In the receiver-based detection additional information must be injected into frames to help the receiver determine the number of frames lost. Since frames can be easily lost in wireless transmissions, the receiver is handicapped when determining the number of retransmissions that have occurred. In the transmitter the PDR is deterministicly determined by the data-link layer, sequence numbers must be added to frames for the receiver to accurately calculate the PDR[3]. Several other detection methods exist including using a detected detector, cooperative detection among nodes in a wireless network, and more sophisticated methods of RF fingerprinting[3].

Once the jammer has been detected the reactive countermeasures come into play. Many evasion techniques exists to combat narrowband jammers such as: channel hoping, spatial retreat, retreat restoration, hybrid attacks, and many cognitive radio approaches[2]. Many of these technics utilize the network itself to adapt to the jammer, which is an appropriate assumpt because without a network communications are irrelivant. Channel hopping is quite simple and can be considered easiet to implement. If a channel is begining jammed simply ẗhoptẗo another channel. This is easily defeated in two cases, the first the jammer follows you or the jammer is simply wideband capable. The second, spatial retreat, is a mechanism to physically evade the areas being jammed. Based on the detection algorithm all nodes in a network try to estimate the jammed region and flee physically in the direction of safer place. Based on their estimation about the jammed region, nodes will utilize shortest path algorithms to determine location of retreat[1]. Retreat restoration is focused around

how to rebuild a network once the jammer has left. Retreat restoration can be done by coordinated or uncoordinated communication, and the transmissions are based on a pre planned hop patterns among nodes[6].

These techniques primarily exploit the dimensionality of their envirmonent by simply avoiding the jammer, and all techniques require intelligent flexible hardware solutions. Solutions that push more of the radio operations from their original implementations into the more flexible software domain. The software focused radios, also know as Software defined radio, have provided a solid platform for very adaptive anti-jamming technologies under the name cogntive radios. These radios have the ability to easily learn and adapt to their envirorment, which is the primary requirement of anti-jamming devices.

Software defined radios, defined as the intersection between hardware radios and computer software[4], provide a platform flexible enough to support highly intelligence operations such that anti-jamming requires.

Types of anti-jamming attacks

Narrow focus of problem to single narrow band jammer, with no mobility.

1.3 Thesis Contributions

1.4 Thesis Organization

Chapter 2

Background

Here is some background you'll need to know about my research.

2.1 Background subsection

Bibliography

[1] Mithun Acharya and David Thuente, *Intelligent jamming attacks, counterattacks and (counter)2 attacks in 802.11b wireless networks*, Proceedings of the OPNETWORK Conference, 2005.

[2] Faraz Ahsan, Ali Zahir, Sajjad Mohsin, and Khalid Hussain, *Survey on survival approaches in wireless network against jamming attack*, Journal of Theoretical and Applied Information Technology **30** (2011), no. 1, 55–67.

[3] Kwang-Cheng Chen and Ramjee Prasad, *Cognitive radio networks*, John Wiley and Sons, 2009.

[4] J. Mitola, *The software radio architecture*, IEEE Communications Magazine (1995).

[5] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou, *A survey on jamming attacks and countermeasures in wsns*, IEEE Communications Surveys and Tutorials **11** (2009), no. 4, 42–56.

[6] Jingpu Shi, Theodoros Salonidis, and Edward W. Knightly, *Starvation mitigation through multi-channel coordination in csma multi-hop wireless networks*, in CSMA Multi-hop Wireless Networks, in Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2006, pp. 214–225.