INTRODUCTION

The broadcast nature of wireless networks makes them particularly vulnerable to radio interference, which prevents the normal communications (Akyildiz IF, 2002; N. Ahmed, 2005). This interference or jamming can destroy wireless transmission and may occur either by means of unintentional interference or collision at the receiver side or intentional attacks. The jamming attack can be easily launched since it can be implemented by simply listening to the open medium and broadcasting in the same frequency band as the sensor networks (Y.W. Law, 2005, Feb).

In order to cope with this kind of Denial-Of-Service style attack, many strategies and techniques have been developed. The traditional method is to use the sophisticated physical layer technologies such as DSSS (Direct Sequence Spread Spectrum) and FHSS (Frequency Hopping Spread Spectrum),

ABSTRACT

Guaranteeing security of the sensor network is a challenging job due to the open wireless medium and energy constrained hardware. Jamming style Denial-of-Service attacks is the transmission of radio signals that disrupt communications by decreasing the signal to noise ratio. These attacks can easily be launched by jammer through, either bypassing MAC-layer protocols or emitting a radio signal targeted at blocking a particular channel. In this chapter, we survey different jamming attack models and metrics, and figure out the difficulty of detecting and defending such attacks. We also illustrate the existed detecting strategies involving signal strength and packet delivery ratio and defending mechanisms such as channel surfing, mapping jammed region, and timing channel. After that, we explore methods to localize a jammer, and propose an algorithm Geometric-Covering based Localization. Later, we discuss the future research issues in jamming sensor networks and corresponding countermeasures.
which have been widely used in military communication (Y.W. Law, 2005, November). However, it can be too costly for the energy and frequency constrained sensor networks. So many kinds of evasion strategies have been researched, such as wormhole-based anti-jamming techniques (M. Cagalj, 2007), channel surfing (W. Xu, 2007) and timing channel (W. Xu, 2008).

In this chapter, we survey issues related to jamming sensor networks by examining both the attack and defend sides of the problem. We first give two kinds of jamming attack models and two widely used metrics. Then, we would like to introduce approaches to detecting jamming attack and defending mechanisms. After that, we explore methods to localize a jammer, and propose an algorithm Geometric-Covering based Localization. At last, we analyze the future trends of jamming attacks and corresponding countermeasures in wireless sensor networks.

JAMMING ATTACK MODELS AND METRICS

Jamming attack is a kind of Denial of Service attack, which prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on (W. Xu, 2005). We define the jammer in wireless sensor network as an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications. A typical scenario of jamming attack is shown in figure 1. The normal nodes C and D have been jammed by the malicious node X, so the communications between the jammed nodes (C, D) and the normal nodes (A, B, E, H, I) are disrupted.

**Jamming Attack Models**

There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications. It is hard and impractical to cover all the possible attack models that might exit (A. D. Wood, 2007), so we list two kinds of jamming attacks that have been widely researched and proven to be effective in disrupting wireless communication in wireless sensor networks.

1. **Active jammer**
   - The active jammer tries to block the channel irrespective of the traffic pattern on the channel.
     - **Constant jammer**
       - The constant jammer continually emits radio signals and can be implemented using either a waveform generator that continuously sends radio signals\(^{(11)}\) or a normal wireless device that continually sends out random bits to the channel without following any MAC-layer etiquette (W. Xu, 2005).
     - **Deceptive jammer**
       - The deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions, instead of sending out random bits (W. Xu, 2005). As a result, a normal communicator will be deceived into believing there is a legitimate packet and be duped to remain in the receive state (W. Xu, 2005).
   - **Random jammer**
     - Instead of continuously sending out a radio signal, random jammer alternates between sleeping and jamming. Specifically, after jamming for

![Figure 1. An example of Jamming attack in WSN](image-url)