A SURVEY ON JAMMING AVOIDANCE IN AD-HOC SENSORY NETWORKS*

Kristopher W. Reese
Department of Computer Science
Hood College
Frederick, MD 21722
kwr2@hood.edu

Ahmed Salem
Department of Computer Science
Hood College
Frederick, MD 21722
salem@hood.edu

ABSTRACT

Ad-Hoc Sensory Networks present a cheap and efficient way to collect data through wireless transmissions between sensors. These transmissions create new problems that need to be overcome in order to insure that the data being collected is reliable. This paper surveys the latest research in Jamming Avoidance in Ad-Hoc Sensory Networks.

I. INTRODUCTION

Ad-Hoc networks are the most common form of network being deployed in situations that require a form of networking that can be deployed as fast as possible. They have both military and commercial applications, as well as applications in fields, such as robotics. Because of their widespread usage in many fields, the topics listed below may be important to any student taking a Networking/Data Communications class in college. Students taking this course may run into these forms of networks in the future and should know how to avoid jamming in the cases that jamming is possible.

A wireless sensor network is a collection of tiny disposable and low power devices, called sensor nodes. These sensor nodes are the devices in which sensed attributes are converted into a form that a user can understand. Each node is comprised of a sensing module, a communication module, memory, and a small battery.

During the deployment and over the span of the nodes lifetime, several problems can arise. Some problems that a network can be exposed to include: coverage holes, routing

holes, sinkholes & wormholes, as well as jamming holes. However, we will only discuss Jamming Holes and the current research in Jamming Avoidance.

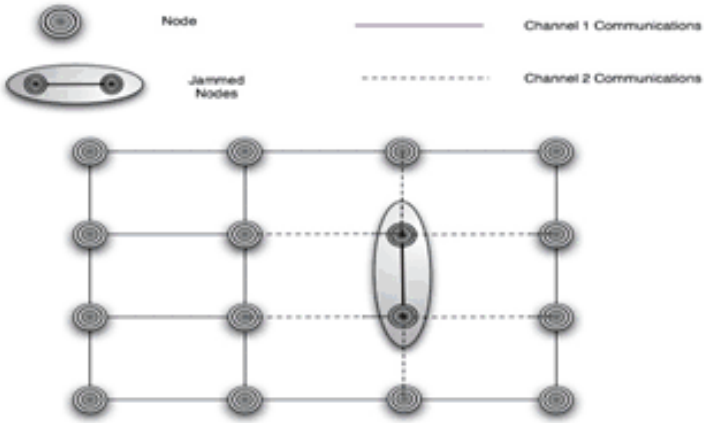

Figure 1: The basic layout of a network with a Jamming Area. This also shows which nodes could potentially work on channel 2 communications with the jammed nodes.

A jamming hole occurs when the radio frequency that is used for communication is blocked intentionally or unintentionally. Unintentional jamming occurs when a node malfunctions and begins continuously transmitting on the networks frequency, which prevents neighboring nodes from communicating with the malfunctioned node. Intentional Jamming occur when an attacking node begins transmitting on the same communications frequency as the network. Though jamming of the network's communications is the most common form of jamming, jamming of a node's sensing capabilities is also possible with a few forms of sensors.

For coverage of jamming holes, Ahmed et al. [1] surveys the protocol JAM. Wood et al. [2] propose this protocol to detect and map jammed regions of the sensor network using heuristics based on available data. However, the JAM protocol assumes that each node has a unique ID that is known to every node in the network. This protocol also relies on the attacked node to broadcast a jamming notification to all un-jammed neighbor nodes. This works if the jamming is intermittent, however for continuous jamming, it is hard to guarantee that the message will be received.

II. CHANNEL SURFING FOR JAMMING

Channel Surfing is a technique that, when used correctly, can present a viable option to resist jamming. In Channel Surfing, a victim node detects that it is being jammed and switches to a new communications frequency. Neighboring nodes then realize the node has disappeared from the network and moves to the next frequency to find the missing node.

Although Channel Surfing is a viable option to resist jamming, it also raises several new challenges. For example, if a node moves to a new frequency due to a poor

connection, the network can enter an unstable state that can cause poor connections across the entire network or potentially bring down areas of the network.

There are several algorithms that are mentioned by Xu et al. [5] that attempt to maximize the efficiency of Channel Surfing techniques. [5] breaks down these algorithms into two groups; Coordinated Channel Switching and Spectral Multiplexing, the latter being further broken down into synchronous spectral multiplexing and asynchronous spectral multiplexing.

Coordinated Channel Switching

In Coordinated Channel Switching, the entire network moves to the channel that a node has moved to due to jamming. The network then resumes normal network operations on this new channel. This form of channel switching requires time for the transition of all network nodes to the new channel. Figure 1 gives an example of this form of channel switching and is explained below.

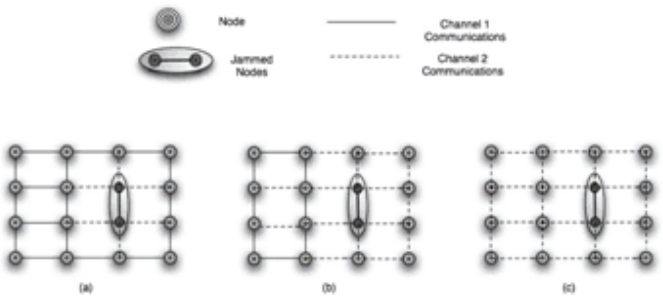

Figure 2: The order in which nodes in a coordinated channel algorithm change.

The Algorithm begins with either a single or multiple nodes being jammed in the network. This is displayed in figure 1 as the nodes in the dark region. In this example, as well as subsequent examples, we assume that a signal is jammed on a single channel with constant noise. However, these algorithms should work for any form of jamming that can be detected by the nodes. After a node realizes that it is jammed, it will switch to a new channel, with a frequency outside of the attacker's frequency, and stand by for contact with a neighboring node. Not only does this allow the node to resist jamming, but also allows the node to resist the jamming that is taking place and allow for continued interoperability in the network.

The neighboring nodes, represented by the nodes connected with dotted lines, will eventually discover that a node, or nodes, has gone missing. The neighboring node then switches to the new channel, sends out a message, and waits for a response from the victim node(s). If the node is found on the new channel, the neighboring node returns to the original channel and broadcasts a signal to the rest of the network that it will continue operations on the new channel. Nodes switch in the order that is indicated by the dotted

lines in Figure 2. The neighbor nodes communicate with the nodes surrounding it, which will send the message to the following nodes.

This form of channel switching does posses its share of challenges. An unreliable link can cause some nodes to miss the channel switch notification. The algorithm takes care of this because a missed node would treat its surrounding nodes the same way and flip to the next channel when it detects that its neighbors are missing. This form of channel switching also relies heavily on the resources of the network. In addition, this form of channel switching forces all of the nodes to waste resources in switching to the next channel.

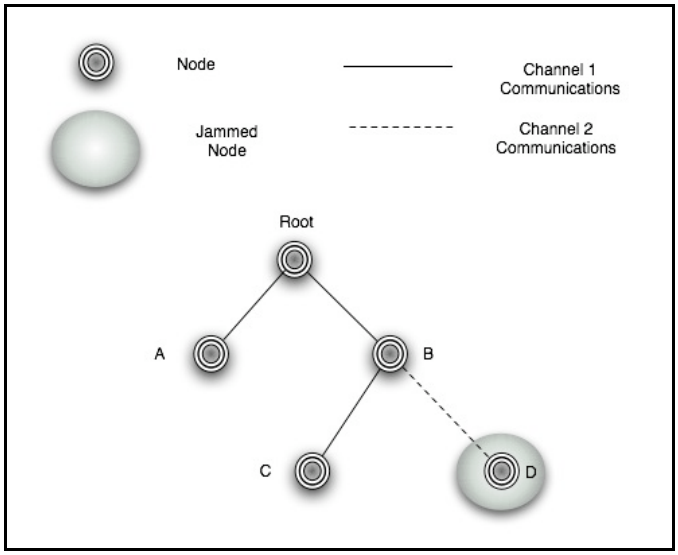

Figure 3: Represents how nodes act in Spectral Multiplexing algorithms (both Synchronous and Asynchronous).

Synchronous Spectral Multiplexing

Spectral multiplexing is very different from Coordinated Channel Switching. Spectral Multiplexing is much lighter on the resources of the network. Only one of the nodes uses its resources in the switching of channels. Responses to jammed nodes are also handled locally rather than by the entire network.

In Synchronous Spectral Multiplexing, the network is governed by a global clock. Each channel of the network operates in an allotted duration of time. During this time, no other channel is used for transmitting packets. Figure 3 represents a layout of nodes in which a Synchronous Spectral Multiplexing may exist. We can see that node D is jammed, as illustrated by the dark region surrounding the nodes. This node is linked to node B, meaning node B serves as the intermediary node. When node B realizes that node D is no longer on channel 1, it switches channels in an attempt to find the victim node. After finding the node on a new channel, the intermediary node switches back to channel 1 to send a message to the root to tell the root that the network will be working in channel 1 as well as the new channel, channel 2.

The intermediary node continues to switch between channels 1 and 2. During the time that the intermediary node is working on the channel 2, all packets being sent on channel 1 halt until the intermediary node switches back to channel 1. This continues until the interference subsides or through the lifetime of the network.

This form of channel switching is much more complex and has more challenges to overcome. In Synchronous Spectral Multiplexing, one of the issues involved is the synchronization process. The challenge of this lies in synchronizing the node schedules rather than the physical clock of each network node. Determining the duration also poses a problem in Spectral Multiplexing. The issue of determining the duration is due in part by the overhead associated with the switching of channels and preventing disconnections between the receiving of packets from another node.

Asynchronous Spectral Multiplexing

Asynchronous Spectral Multiplexing is similar to Synchronous Multiplexing but rather than halting the entire network, nodes are only aware of it's neighbor's channel information rather than of a remote node. This allows a network to continue working in channel 1 while an intermediary node gathers information from the node on channel 2.

Figure 3 is also representative of how an Asynchronous Spectral Multiplexing network may be structured. In this example, we see that node D is being jammed; therefore node B acts as the intermediary node. Node B switches between channels 1 and 2 to receive and send packets between node D, node C, and the root node. While node B works in channel 2, node A and the root node will continue sending and receiving packets between each other.

However, if a node sends a packet to the jammed node, the packet would pause at the root node while node B is working in channel 2. As soon as node B switches back to channel 1, it sends a message to neighboring nodes telling them that it is in the channel. The root node would then send the packet to node B. This algorithm continues until the jamming has subsided or for the entire lifetime of the network.

Asynchronous Spectral Multiplexing also poses similar problems as Synchronous Spectral Multiplexing. Synchronizing the boundary nodes and its children nodes pose a challenge, and though duration between switches is much more flexible, choosing an appropriate time duration is still a challenge.

III. CONCLUSION & FUTURE WORK

These topics leave a lot of research opportunities in the field of Ad-Hoc Networking. Though different methods of channel surfing are discussed, determining that a node is jammed, and deciding when to switch channels is not discussed in these methods. Some future research topics, which may work as good senior projects for students as well, may include; Optimizing algorithms to determine that a node is jammed; Determining the best algorithm to use in certain situations, then finding a way to combine the algorithms to optimize power and lifetime of nodes; as well as many other topics.

REFERENCES

[1] Ahmed, Nadeem, Salil S. Kanhere, and Sanjay Jha. "The Holes Problem in Wireless Sensor Networks: A Survey." *ACM SIGMOBILE Mobile Computing and Communications Review, vol. 9,* 2005: 4 - 18.

[2] Wood, Anthony D.; Stankovic, John A.; and Son, Sang H. "JAM: A jammed-area mapping service for sensor networks." *24th IEEE Real Time System Symposium,* Dec. 2003: 286 - 298.

[3] Karlof, Chris and Wagner, David. "Secure Routing in wireless sensor networks: Attacks and Counter Measures." *1st IEEE International Workshop (SNPA '03).* May 2003

[4] Wood, Anthony D. and Stankovic, John A. "Denial of Service in sensor networks." *IEEE Computer, 35(issue 10).* Oct. 2002: 28-39.

[5] Xu, Wenyuan; Trappe, Wade; and Zhang, Yanyong. "Channel Surfing: Defending Wireless Sensor Networks from Interference." *Proceedings of the 6th international conference (IPSN '07).* 2007: 499 – 508.