Using Standard Deviation in Signal Strength Detection to Determine Jamming in Wireless Networks

Kristopher W. Reese
Dept. of Computer Science
Hood College
Frederick, MD 21701
kwr2@hood.edu

Ahmed Salem
Dept. of Computer Science
Hood College
Frederick, MD 21701
salem@hood.edu

George Dimitoglou
Dept. of Computer Science
Hood College
Frederick, MD 21071
dimitoglou@hood.edu

ABSTRACT

As wireless networks become more common in both government and industry settings, jamming becomes a major issue. This paper provides a mathematical approach and equations for analysis of signal strength jamming detection, over the more commonly used packet-loss jamming detection. The approach offered alleviates issues with battery life by cutting the overhead cost of sending and receiving multiple packets before the network can determine that it is being jammed.

Keywords: Wireless Transmission, Ad-Hoc Networks, Sensory Network, Jamming, Jamming Detection, Jamming Avoidance

I. Introduction

A wireless sensor network is a collection of tiny and low power devices that are becoming more common forms of networks over time. These sensor nodes are devices that sense changes in attributes within the scope of the network. Each node consists of a sensing module, a communications module, memory, and a small battery. This information is then sent through wireless transmissions to surrounding nodes to a root node. The root node will convert the information received into human readable information. They hold applications in fields relating to and within computer science.

Jamming avoidance is a well-studied topic in the research community. Jamming avoidance is often solved using channel surfing techniques, described in [1-6]. These papers describe three variations of channel surfing, Coordinated Channel Surfing, Synchronous Spectral Multiplexing, and Asynchronous Spectral Multiplexing. Each method of channel surfing builds on the other models and attempts to resolve the power disadvantages of the other models.

Ahmed et al [1], Wood et al [4], Xu et al [5], and Reese et al [6] define coordinated channel surfing to be the least complex of the variations. In Coordinated Channel Surfing, the jammed node will detect the area jamming and change to a clean channel. With time, surrounding nodes will determine that the node is no longer operating in the original network channel and will begin to switch channels until the jammed node is found. The surrounding nodes will the move back to the original channel, transmitting a signal to all nodes that force the entire network to move to the new channel.

Ahmed et al [1] and Reese et al [6] discuss two forms of spectral multiplex channel surfing techniques. In both cases, the network acts in similar ways. A node will detect area jamming and begin to operate in a new, clean channel. When its surrounding nodes determine that the node is now operating in a new channel, they begin to surf the channels until the node is found. However, rather than sending a signal forcing the entire network to change channels, the surrounding nodes begin to operate in both channels. After determining the operation of the network in multiple channels, surrounding nodes will transmit the channel frequency to the root node of the network where a global clock will be set. This global clock then governs the entire network.

Ahmed et al [1] and Reese et al [6] break the spectral multiplexing class into two forms, synchronous and asynchronous. In a Synchronous Spectral Multiplex network, the global clock will set an allotted amount of time for the network to be running in either the original channel or the new channel. While the network is running on one of the channels all processes on the other channel are halted.

In an Asynchronous Spectral Multiplex network, the global clock governs the surrounding nodes. Unlike in Synchronous Spectral Multiplexing, Asynchronous Spectral Multiplexing allows all nodes to continue transmissions. While the surrounding nodes are working in the new channel, all of the other nodes will continue to transmit on the original channel. The surrounding nodes will become a transitionary node between both channels.

Unfortunately, [1, 4-6] do not recommend any method of jamming detection to determine whether a node is jammed. Wood et al [2] and Karlof et al [3] offer algorithms for mapping jammed networks using a simple statistical model based on packet-loss detection, but do not offer a technique for jamming detection. Their proposed models allow the nodes to probabilistically determine whether the network is being jammed. This method has a lot of overhead involved in determining

network jamming and does not offer the most beneficial method for jamming detection.

This paper will discuss possibilities for jamming detection in wireless ad-hoc sensor networks, as well as a possible extension to Signal Strength detection. Section 2 will summarize and briefly survey three methods of jamming detection for wireless networks. Section 3 offers typical mathematical formulae that could serve in a signal strength algorithm to determine jamming. Section 4 will extend the signal strength mathematics to determine a more probabilistic model for detecting jammed networks. Section 5 summarizes the paper and offers potential future work in wireless ad-hoc sensory networks.

II. Jamming Detection Models

"The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks" [7] discusses three models for detection of jamming in a wireless network. Each of the models builds a basis for the network to determine certain, normal characteristics. This information is then used to compare incoming traffic to the conditions to determine jamming. The proposed models discussed in [7] include Carrier Sensing Time, Packet Delivery Ratio, and Signal Strength Detection.

Carrier Sensing Time detection is based in instances in jamming in which jamming prevents legitimate packets from being transmitted over the network by forcing the network to appear constantly busy to the source. This method seems only natural to track the amount of time that a node waits for the channel to become idle. We then compare the information gathered to the sensing time of a normal clean signal to determine whether the node is being jammed.

Xu et al. [7] emphasizes that this is only true in cases that the legitimate wireless node's MAC protocol employs a fixed signal strength threshold to determine idle states. When a protocol employs an adaptive threshold, the sensing time becomes very small, even during continuous jamming on the network. In this model, the determinacy of jamming relies heavily on applying a protocol that does not employ an adaptive threshold. We could not rely on this model in other any other conditions, making this a less than ideal model for detection of jamming in most networks.

The second model to discuss is the Packet Delivery Ratio (PDR) model. Detection of jamming in this model can be measured in either the sending or receiving node. When measured through the sending node, the sending node can be calculated by tracking the number of acknowledgment packets received in response to another packet being properly received. On the receiving side, the receiving node can determine possible jamming by using a comparison of the ratio of packets that pass the cyclic redundancy check to the number of packets received.

The PDR model is very accurate in determining possible jamming from congestion, but lacks the ability to distinguish jamming from other possible network issues, such as sender battery failure or the sending node moving out of range of the receiving node. The PDR model also has no way of distinguishing other possible Denial of Service attacks on the network from jamming. Though the PDR model proves to be a very important statistic, due to its lack to distinguish network problems from possible jamming does not make it a reliable model for jamming detection.

The third model to discuss is Signal Strength Detection (SSD) model. This model determines jamming by using the measurement of the signal's energy level after being received. The initial energy level could be determined at the initial startup of the network. During the lifetime of the network, each node would listen to the signal's strength, determining an average strength and would compare this to the normal signal's average strength.

SSD has potential to be one of the most effective techniques for jamming detection on a wireless network. Few papers discuss the use of the SSD model, and those that do discuss it, offer theoretical approaches rather than practical approaches for implementation into a network. Subsequent sections in this paper offer the mathematical formulae and a practical approach to the Signal Strength Detection model for determining jamming.

III. Detection formulae

Wireless networks are based on the transmission of radio signals. Physics of these radio waves can give us an accurate representation of the radio waves, including the propagation in many instances, over time. Gathering the signal's radio waves over time involves a lot of overhead that would make the SSD model less attractive than other models. However, when listening to the reception of the signal from the receiving end, one can use this model efficiently.

To determine the average signal strength we turn to mathematics to offer us a viable solution to the comparison of signal strengths. In this model we have two signals, a clean signal which is defined as: $(c(x))$ and a jammed signal which is defined as: $(j(x))$. We determine these over an interval of time $(b-a)$ between the ending of the transmission (b) and the beginning of the transmission (a). Table 1 summarizes all of the symbols used throughout the development of the mathematical model.

Symbol	Description
$\bar{x}$	The average signal strength of a clean signal
$\bar{d}$	The average interval between the clean signal and the jammed signal
σ	Standard Deviation of the clean signal
x	An interval of time over the signal's transmission
$c(x)$	Function representation of the clean signal
$j(x)$	Function representation of the jammed signal
b	Time interval at the end of the transmission
a	Time interval at the start of the transmission

Table 1: Summary of the symbols used throughout this paper

Since basic statistics gives us the equation for finding the mean of points on a line, we can use the equation:

$$(1) \qquad \bar{x} = \frac{1}{n}\sum_{i=0}^{n} c(x_i)$$

To find the average signal strength at specified intervals of time. Since we would want to average the signal strength for all points between $a \to b$, we want the summation of all possible points between the start and end of the transmission.

$$(2) \quad \bar{x} = \frac{1}{b-a}\int_a^b c(x)\,dx$$

This will then give us the average signal strength of either the clean or the jammed signal.

Since our comparison of the signal strengths consists of determining the difference of the average signal strengths, we can further extend the above equation to give us the difference:

$$(3) \qquad \bar{d} = \left[\frac{1}{b-a}\int_a^b j(x)dx\right] - \left[\frac{1}{b-a}\int_a^b c(x)dx\right]$$

We can then further simplify the above formula into a single integration as:

$$(4) \qquad \bar{d} = \frac{1}{b-a}\int_a^b [j(x) - c(x)]dx$$

This formula allows us to find the difference of the average signal strengths between nodes. If the information gained from this integration proves to be an excessively high number, a node could then determine that it is being jammed. Unfortunately, none of the reviewed papers offered a method for determining a limit for jamming in a network.

IV. Extending the SSD model

The main focus of a SSD model is the comparison of the average signal strength to that received from a potentially jammed signal. Jamming typically sends a signal that has a much higher strength than a clean signal would have. The problem that lies in practical application is determining the level at which a node would become jammed. This section proposes one way to approximate the strength at which a node becomes jammed.

Since we know that the signal strength will unlikely be consistent throughout the life of the network, we can use these deviations from the average to find a standard deviation for the node. We can do this by using the Root-Mean-Square (RMS) formula from statistics:

$$(5) \qquad x_{rms} = \sqrt{\frac{1}{n}\sum_{i=0}^{n} c(x_i)^2}$$

Since we want the RMS over the continuous function $c(x)$, we want to use the form:

$$(6) \qquad x_{rms} = \sqrt{\frac{1}{b-a}\int_a^b c(x)^2\,dx}$$

Since we are attempting to find a standard deviation, we must calculate the difference of $c(x) - \bar{x}$ between each x in the clean signal and the average signal strength of the clean signal, defined as $\bar{x}$, our RMS becomes:

$$(7) \qquad \sigma = \sqrt{\frac{1}{b-a}\int_a^b [c(x) - \bar{x}]^2}$$

With knowledge of the standard deviation, we can use this to distinguish whether a signal can be considered jammed. By comparing the difference that was gotten from the formula for $\bar{d}$ to the standard deviation, we can assume that anything above the standard deviation is jammed.

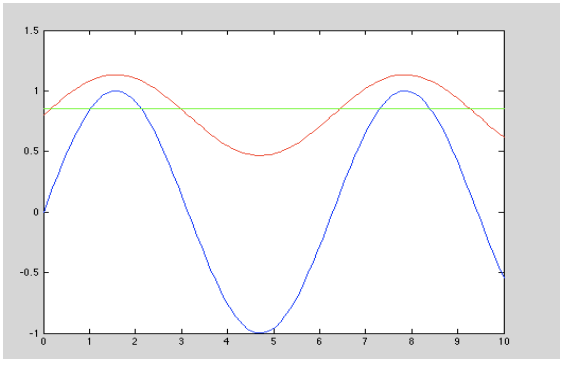

Figure 1: Shows the clean signal (blue line) and compares it to the jammed Signal (red line). The Green Line represents where the standard deviation would lie in comparison to the clean and jammed signals

If, for example, we suppose that a clean signal sends a transmission that is equivalent to all values within $\sin(x)$ while a jammed signal transmits signal strength approximately equal to all values within $\frac{1}{3}\sin(x)+\frac{4}{5}$, as displayed in figure 1, we can us the functions above to determine if the signal is jammed. Upon the first reception of a transmission, at the beginning of the networks life, the node can follow the calculations using the formulae given in the previous section. This will give the node a standard deviation and average value of the clean signal.

By using the Average distance formula, the node will determine that the average distance on an interval of 10 units for $\sin(x)$ is 0.1839. This information is then used to derive the standard deviation of the equation [in this example a result of 0.6659 is given]. With this information, the node will listen for any signal that seems abnormal and conduct a test on the signal's strength.

Suppose that while the node was listening to the signal strengths, the jammed signal is received. After receiving the suspected signal, the node will calculate the $\overline{d}$ value of the signal. Figure 1 shows both the clean signal and the suspected signal. As can be seen in figure 1, the jammed signal lies only slightly higher than the apex of the clean signal. This can be deceptive but by following the $\overline{d}$ formula, the node will determine that the average value of the suspected signal lies outside of the standard deviation [at 0.6774].

Since the $\overline{d}$ value of the suspected signal is greater than the standard deviation of the clean signal, even though it is only by a small amount, the node will determine that it is being jammed. This will force the node to send the surrounding nodes a message, forcing each of the nodes to recognize the jamming and therefore coordinate a form of channel surfing accordingly.

We can compare our model to the solution that is proposed in [7]. Xu et al [7] mentions the use of High-Order Crossings (HOC) to determine jamming using Signal Strength Detection. The HOC technique offers a very theoretical approach to Signal Strength Detection. HOC takes the signal and determines a polynomial equation that closely resembles the model of the signal. The polynomial is overlaid on top of the model of the signal and the number of times the signal crosses the polynomial is counted. If, during the comparison of signal crossings, the HOC count is much lower, jamming can be assumed.

HOCs use complex mathematics to determine the polynomials that will require more computing power, causing the battery life to diminish more quickly. There is also a possibility that this model fails to determine jamming. If the polynomial found lies high on the model of the signal, jamming may cross the polynomial in about the same number of crossings, forcing the network to believe that it is not being jammed.

The model that this paper proposes attempts to alleviate the issues that HOCs give us. The mathematics used in the model proposed involves much less complex mathematics than in HOC. This cuts the cost of computing power, saving the battery power of individual nodes. Using the standard deviation also eliminates the possibility of having a crossing count that might be fairly close. Since the standard deviation will never be excessively high, the possibility of failures of detection will be much less likely than with HOCs.

V. Conclusion & Future Work

In this paper we have presented a basic theoretical proof of concept for detection of jamming across a wireless ad hoc network. This model attempts to resolve the need for multiple packets to be sent to the nodes. This necessity requires power overhead that will cause the lifetime of the battery to be shorter. In our proposed model, we attempt to alleviate this need by using signal strength detection to probabilistically determine jamming. In the future we intend to experiment possibilities to enhance the model. There is potential for false detection of jamming, especially during the beginning of the networks life. The network may also be caught believing that the jamming signal may be the Standard Deviation if Jamming is implemented soon enough in the network. By Simulating and testing real life applications of this model, we hope to determine ways to avoid potential failures. In conclusion the proposed extension to the Signal Strength Detection model is applicable to, and can be implemented with relative ease, in actual wireless networks.

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

[6] Reese, Kristopher; Salem, Ahmed. "A Survey on Jamming Avoidance in Ad-Hoc Sensory Networks." *Proceedings of the Consortium of Computer Science in Colleges Eastern Conference (CCSCE '08).* 2008

[7] Xu, Wenyuan; Trappe, Wade; Zhang, Yanyong; Wood, Timothy. "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks." *Proceedings of the 6th international symposium on Mobile ad hoc networking and computing (MOBIHOC '05)* 2005:46-57