FAST JAMMING DETECTION IN WIRELESS SENSOR NETWORKS

by

KARTIK SIDDHABATHULA

Presented to the Faculty of the Graduate School of
The University of Texas at Arlington in Partial Fulfillment
of the Requirements
for the Degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

THE UNIVERSITY OF TEXAS AT ARLINGTON

December 2010

To my family, faculty and friends.

ACKNOWLEDGEMENTS

I would like to thank my supervising professor Dr. Donggang Liu for constantly motivating and encouraging me and also for his invaluable advice during the course of my research. I wish to thank my thesis committee members Dr. Mathew Wright and Dr. Hao Che for their interest in my research and for taking time to serve in my defense committee.

I am grateful to all the teachers who taught me during the years I spent in school, first in India and then in the Unites States. I would like to thank Dr. B. Banerjee for encouraging and inspiring me to pursue graduate studies.

Finally, I would like to express my deep gratitude to my parents for their sacrifice, encouragement, patience and also for sponsoring my undergraduate and graduate studies. I am extremely fortunate to be so blessed. I also thank several of my friends who have helped me throughout my career.

November 24, 2010

ABSTRACT

FAST JAMMING DETECTION IN WIRELESS SENSOR NETWORKS

KARTIK SIDDHABATHULA, M.S.

The University of Texas at Arlington, 2010

Supervising Professor: Donggang Liu

Non-dedicated medium of communication for Wireless Sensor Networks (WSN) makes them vulnerable to jamming attacks where an adversary injects strong signal or noises to interfere with the transmission and thus block the wireless channel. In applications such as border security, people are particularly interested in the areas where the channel is currently jammed. It is therefore crucial to be able to detect the jamming attacks as fast as possible. Existing studies have shown that the most effective indicator of jamming attacks is the packet delivery ratio (PDR). However, current PDR-based schemes use end-to-end packet delivery ratio, which requires one to observe the communication for a long period of time before any good decision can be made. In this paper, a *collaborative detection scheme* is introduced. The main idea is to collectively evaluate the packet delivery ratio in a given area instead of a pair of nodes since the attacker often jams an area of their interest (not just two specific nodes). In other words, we use observations from other nodes, which allows us to detect jamming attacks in a much faster way. We have evaluated the feasibility and performance of our protocol on Telosb motes. The results show that we can effectively detect jamming attacks within one round of communication.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Wireless Sensor Network (WSN) consists of autonomous sensors which are separated in space without any physical contact from one another and used to monitor different physical and environmental conditions. They are used to monitor a physical parameter and report the data to a base station. Their ability to monitor various physical conditions like temperature, sound, pressure, etc. have made them a useful tool in civilian, industrial and scientific applications. Some of the areas where they are playing an important role are border security, land slide detection, green house monitoring, etc. The basic security requirements of confidentiality, integrity and availability are also required by WSN.

Due to their shared medium of communication, WSN are vulnerable to monitoring and eavesdrop on them. One of the biggest security threats to WSN is the Denial of Service (DoS) [1] attacks launched on it using a device known as jammer. A jammer is a device that hampers communication between benign nodes. Jammers can affect the communication by attacking the network layer or the physical layer or the Medium Access Control (MAC) layer. In this thesis we focus on the MAC layer jammers for wireless communication medium. MAC layer jammer is a device which does not adhere to the MAC protocol and emits a radio signal which interferes with the normal working of the WSN and results in a DoS. Depending on the power of jammer and network size, it can either cause a part of the network to fail or it can even bring down the whole network. One of the challenges to the research world is to come up with mechanisms which can help us either prevent/evade [2, 3, 4, 5] or detect [4, 6] these attacks.

Communication is complete when a message sent out by a sender is successfully received by the recipient. Jammer hampers the reception of the packets by the nodes, within its range. By ensuring that the receiver does not receive the message, jammer hampers the communication process. The way jammer works is analogous to a person listening to some music with headphones on. When the person puts on the headphones and listen to music, he/she is unable to hear what others are saying, but are able to speak which others can listen. In this analogy, the node is the person and the headphones is the jammer. All the nodes within the jammer's range find that they are losing messages from other nodes. Because of this influence jammer has on the reception of the nodes, they are being misused in some areas. WSN are being deployed for area monitoring. Border security management is the application of area monitoring feature of WSN. Sensors are used to sense any movement in the area and report any activity to the base station. An adversary can use jammers to disrupt the communication process in the network and use it to his/her advantage to avoid detection and cross the border.

Nodes which lie within a jammer's range see a drop in the number of messages they receive when under attack. Whenever we find that a node lost some messages over a time period, an alert is raised. Our contribution through this thesis is that we come up with a working model of a protocol which can achieve accurate and faster detection by having a shorter time interval. The only disadvantage of having a shorter time interval is more energy consumption by the nodes. The protocol also has a high detection rate and a very low false alarm rate. Previously, the most effective way of detecting jamming was the combination of RSSI and PDR and it also took a lot of communication to make a decision. In the proposed protocol, less communication is required to make a decision also the decision is based only on the number of lost packets at a node.

CHAPTER 2

RELATED WORK

Jamming has attracted researchers for a long time and much work has been carried out in this area. The work carried out in the jamming area has focused on optimizing the jammers as well as jamming detection and methods to prevent/evade jamming. So far there has been two papers which focused on jamming detection [4] and [6]. In [4] authors proposed a system in which the nodes undergo training to know the collision rate in the network. After the training is done the nodes are deployed in the network. If they find that the collision rate has increased i.e. the nodes are loosing more number of packets compared to training period, they declare jamming. The protocol can have a faster detection but faster detection results in lower detection rate and higher false alarm rate. In [6] authors have studied the various jamming attacks on the WSN and also have proposed a detection method based on Received Signal Strength Indicator (RSSI) and Packet Delivery Ratio (PDR). Their detection was based on reading the RSSI value of the network and PDR at a node. Whenever they found RSSI value to be high and PDR to be low they used to declare jamming. In their publication, they also proposed four kinds of jammers. The 4 types of jammers are Constant jammer, which continuously jams the network; Random jammer which shuttles between attack and sleep modes; Reactive jammer which jams the network only when it senses activity on the channel and Deceptive jammer which broadcasts only the preamble upon reception of which all nodes stay in the receiving mode only. They analyzed the effectiveness of the four jammers by implementing their prototypes in MICA2 mote platform. They also evaluated the impact of each jammer on packet send ratio and packet delivery rate on the network.

The other works have focused on the analysis of attack methodology and techniques to evade as well as prevent the jamming attacks. AUSCERT [1] (Australian Computer Emergency Response Team) gave a report on the vulnerability of wireless sensor networks to DoS attacks. They published a report in May 2004 which reported on the vulnerability of IEEE 802.11 which can result in a DoS attack. They studied the attack which targeted the Medium Access Control (MAC) layer of wireless devices. In their report they mentioned that a device which transmits by disabling the Clear Channel Assessment (CCA) for MAC can cause a DoS in the network. In [7] authors studied the effect of jamming on the channel. In their paper they did a theoretical analysis of the saturation output of the IEEE 802.11 MAC when under jamming attack. Authors analyzed the saturation throughput performance of IEEE 802.11 MAC against various types of jammers. They analyzed the impact of jamming rate, packet size and network size on IEEE 802.11 MAC's performance. They did analysis through mathematical analysis, simulations and by implementing a prototype of their model.

Y. W. Law et al. [8] and M. Li et al. [4] studied the various methods of launching DoS attack on WSN. In [8] authors have proposed an efficient jamming attacker model for situations when the attacker has no knowledge about the target protocol. Their attacker model is applicable in cases where packets are encrypted. The proposed jammer works by observing the packets inter arrival time. In [4] authors came up with jamming attack strategies which are easy to launch and which are difficult to detect. M. Li et al [4], M. Strasser et al. [9], Y. W. Xu et al. [2], G. Alfine et al. [5], M. Cagalj et al. [3] have studied on the defense and evasion strategies in case of a jamming attack. In [9] authors proposed a spread spectrum system that enables anti jamming communication. This system is applicable for networks where nodes do not share secret keys. In [5] authors have presented a system called MULEPRO (MULti channel Exfiltration PROtocol) which automatically assigns jammed nodes to different channels. The system works for a multi channel attacker as well. In [5] authors proposed a system for the restoration of communication links when network is under attack. They achieve this through the use of creation of a jamming resistant timing channels. In [3] authors proposed a hybrid network to send out message in case of jamming. They proposed three solutions. In the first one they proposed that some of the nodes in the network to maintain a wired connection which will send out a message out of the jammed area in case of jamming. The other solutions they proposed are frequency hopping to send out the alert message and uncoordinated channel hopping to send the alert. Y. W. Law et al. [8], M. Li et al. [4], W. Xu et al. [2], M. Cagalj et al. [3], W. Xu et al. [6] have focused their work on single channel network whereas M.Strasser et al. [9] and G. Alfine et al. [5] have based their work on multi channel network.

CHAPTER 3

NETWORK AND ATTACK MODEL

We consider the network to be a static network. All the nodes and the jammer in the network are static. All the nodes have limited supply of energy. Nodes use only a single channel for communication. They are not time synchronized. Each node joins the network and runs on its own time interval. They are not aware about their physical location or the location of other nodes in the network. We assume that the communication in the network is encrypted and the nodes share a secret key among themselves to authorize themselves to other nodes. There does not exist any compromised node in the network. For the attacker we assume that the attacker is a constant jammer. It does not have any knowledge of the state of the network regarding the sensor nodes being idle or communicating with each other. It constantly sends random packets to disrupt the communication between the nodes irrespective of channel activity.

An experiment was carried out to see the influence of jammer on the reception of messages by a node using Telsob motes running at power level 1. At that power level motes had an effective range of 15-25 inches. In the experiment 3 nodes were placed in a straight line with a distance of 10 inches from each other. Figure 3.1 shows the experimental setup to test the affect of jammer. In the figure, mote next to the letter J is the jammer, mote next to the letter R is the receiver mote and the mote next to the letter S is the sender mote. Sender node sent 100 packets while the receiver node kept track of the number of packets it received. Hundred trials were carried out in the experiment, with the receiver node being under attack and another

100 trials when not the jammer node sent messages continuously, but with it's MAC being enabled. The enabling of the MAC disabled the jammer feature, though it sent messages at the same rate as before. Figure 3.2 shows the influence of a jammer on the communication between nodes in wireless sensor networks. From the figure we can see there exists a clear distinction in the number of packets a node receives when under jamming attack and when not under attack. In the figure x-axis represents the PDR and the y-axis represents the number of times the PDR was found to have that value.

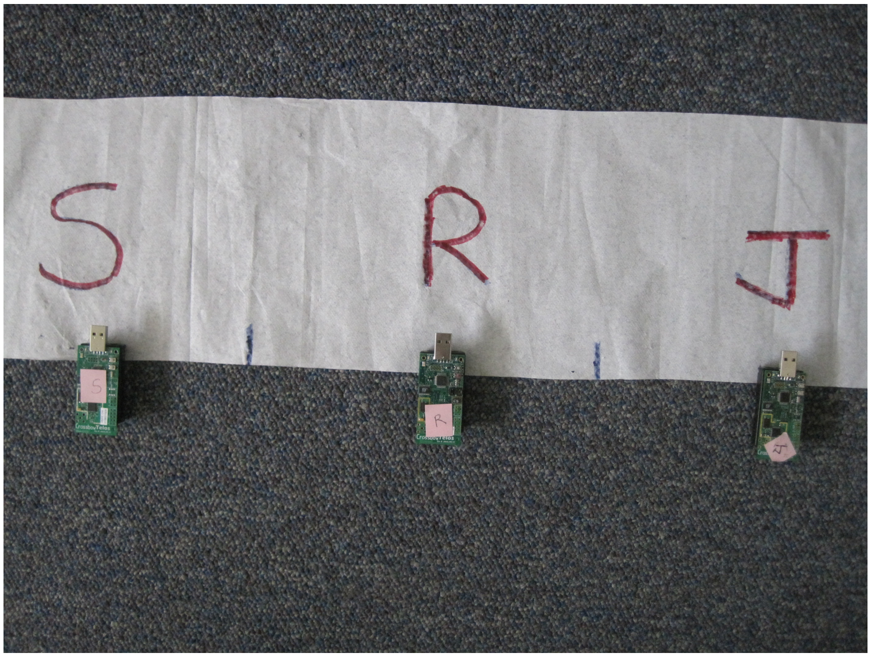

Figure 3.1. Experiment for affect of jammer.

There exists various types of attacker models but our focus in this thesis will be on constant jammer [6].

- **Constant Jammer**: This type of jammers continuously emits a radio signal to cause jamming. The continuous transmission may result in a low life time

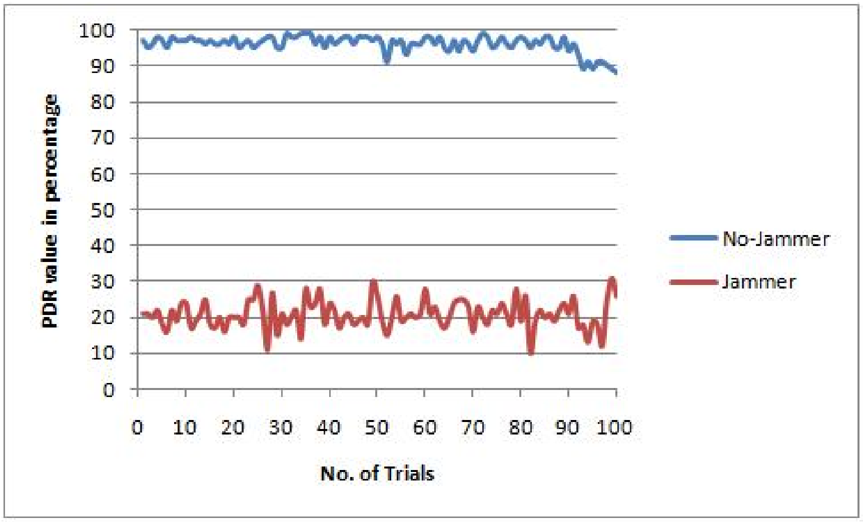

Figure 3.2. Influence of jammer on Packet Delivery Rate.

for the jammer i.e. the attack period may not be very long until unless the jammer has a continuous supply of energy. We have implemented a constant jammer using a telosb mote that uses a CC2420 radio chip. We implemented it by disabling the Clear Channel Assessment (CCA) bit which is used to sense the channel in tinyos. Our jammer continuously sends out a packet irrespective of the activity on the channel.

CHAPTER 4

PROTOCOL

4.1 Protocol

The intuition behind the protocol are that packet loss is the best way to decide jamming. The second intuition is that an observation of packet loss over an area leads to decide regarding the existence of jammer faster, compared to observing the packet loss between a pair of nodes. Generally, we might be forced to wait for a long period to carry out the observation of packet loss, to overcome this we make the motes transmit some packet periodically which will help us to make an observation of packet loss in an area without delay. We divided the time line into multiple time intervals and a loss of messages within a time interval compared to its previous time interval helped us make a decision. From Figure 3.1 we can observe that there exists a huge difference in the PDR's for a node receiving messages in case when it is under attack by a jammer and in a case when it is not under attack from a jammer. Figure 3.1 showed, the influence a jammer has on the reception of packets by the nodes within its range. We used this information to design our protocol to achieve jamming detection. Though our primary goal is to detect jamming accurately in the network, we would like to detect it in the least possible time. By least possible time we mean the time from which a jammer starts jamming or a jammer launches an attack on the network. One possible way to detect jamming at the earliest is to make nodes transmit messages in a much shorter time interval. Regularly broadcasting a message consumes more energy and drains out the batteries of the nodes faster but it is the trade off we need to make in order to detect jamming at the earliest. The message that is broadcasted regularly by the nodes in this protocol is their respective node ID.

4.1.1 Decision Process

To decide regarding the existence of jamming attack in the network, all the nodes running the protocol will have to carry out certain operations repeatedly at a regular time interval. Time interval can be adjusted to make a trade off between detection time and the energy consumption of the nodes. All the operations help the node to decide the existence of jamming in the network. Each node maintains two arrays which (for our ease of understanding) we will call as *Current* and *History*. Array *Current* contains the list of the nodes whose ID was received by the node in the current time interval and the array *History* contains the list of the nodes whose ID was received by the node in the previous time interval. The array has two values 0 and 1. The value 0 for a bit in the array means that the ID of the node corresponding to that bit has not been received. The value 1 for a bit in the array means that the ID of the node corresponding to that bit has been received. Both the arrays are initialized to 0. Marking the nodes whose ID was received helps a node to keep track of the number of messages it received in each time interval. By keeping track of the number of messages the node received in each time interval, node can make a comparison of the number of messages received in current time interval with the one it received in previous time interval. By making a comparison, the node can decide regarding the existence of jammer in its vicinity. If the number of messages received in the current time interval is less than the number of messages received in the previous time interval by a certain threshold then an alert is raised. The operations carried out by each node are as follows:

1. Broadcast ID: Each node in the cluster broadcasts its ID repeatedly at a fixed time interval. This helps the nodes which receive this message to keep track on the number of messages they are able to receive within a time interval. Each node broadcasts it's ID only once during a time interval.
2. Mark ID: Mark the corresponding bit of the ID received in the array *Current* as 1.
3. Decision Making: Carry out the check to determine if there is jamming in the network. All the nodes periodically carry out a check to determine if there is jamming in the network. Based on the result, nodes either raise an alert or they do nothing. The decision regarding the existence of jammer is made according to the following:
   - Let's say the number of nodes whose ID was received in previous time interval t_{n-1} is $X_{t_{n-1}}$ and in current time interval t_n is X_{t_n}. The threshold is say τ. An alert is raised if

     $$X_{t_n} < \tau \times X_{t_{n-1}} \tag{4.1}$$

     Let's define δ as, the number of alert messages sent by a node when an alert is detected . δ can have any value ≥ 1. If the number of alert messages is more than one, then to avoid transmitting alert messages consecutively, each alert message will be separated by a random time period.
4. After the expiry of the time interval, the contents of array *Current* is saved into the array *History* and the array *Current* is reinitialized to 0.

4.1.2 Threshold selection

As mentioned in the protocol, the decision regarding the existence of jammer is solely based on the comparison between the number of messages received by a node in consecutive time intervals. A fixed threshold is used to make the comparison between the consecutive time intervals list of received messages. The decision can be affected by the value of the threshold with which we do the comparison hence the performance of the protocol completely depends on the threshold value. Selection of a good value for the threshold is very important. A good threshold value will help the protocol accurately decide the existence of a jammer. The value for the threshold τ was calculated empirically. The results of the experiment that was carried out to see how jammer works was used to calculate the value of the threshold τ. τ was assigned the value of the average of the minimum PDR in case of jamming and max PDR without jammer.

Figure 4.1 shows the values of PDR's for a receiver node, for cases with and without jammer. The values show the number of messages the receiver node received out of 100. As mentioned in section 3, 100 trials were carried out of each setting of the receiver node under attack and not under attack. τ was assigned a value which lied between the two distributions. We assigned the value of τ to 55 which was between the two distributions.

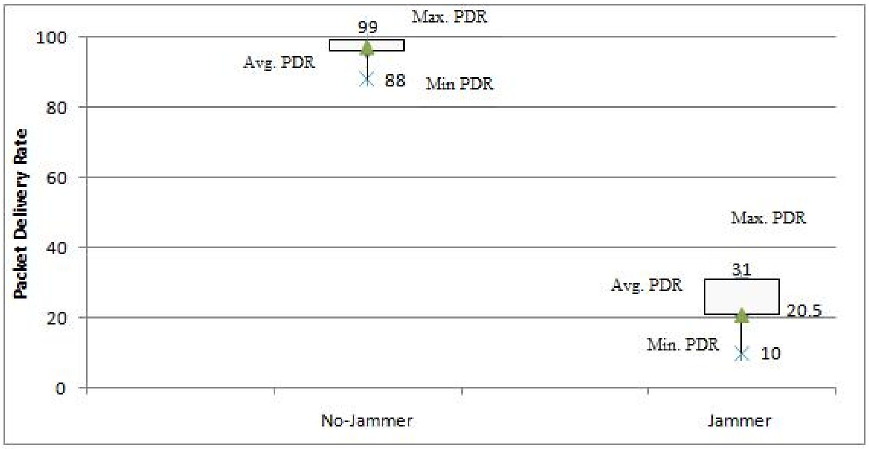

Figure 4.1. PDR comparison: Without jammer and with jammer.

4.2 Theoretical Analysis

In this section we will give the mathematical model for the detection rate and the false alarm rate for the protocol. To do so we introduce some parameters:

1. N: Total number of nodes in the cluster/network.
2. M: Number of jammed nodes in the cluster/network.
3. p: Probability that a message is lost.
4. δ: Number of alert messages sent by a jammed node.

The detection of jamming will be done whenever a jammed node is able to send an alert message out of the jammed area and that message is successfully received by at least one non jammed node. There will be no detection if all the alert messages are lost. Given, that the probability that a message is lost is p and the number of alert messages sent by a node in case of detection is δ, probability that all the alert messages are lost is p^{δ}. The detection will be done when atleast one alert message is out of the jammed area or in other words, when atleast one non jammed node receives at least one alert message, therefore the detection rate R_D can be given as

$$R_D = 1 - p^{M \times \delta} \tag{4.2}$$

Figure 4.2 shows how the detection rate improves with the use of more number of alert messages. Having a high value of δ increases the energy consumption of the node as it will have to send the alert message that many times. The value of δ should be good enough to give us a good trade off between energy and detection. We drew a graph for three values of δ which are 1, 5 and 10 respectively. From the graph we can see that theoretically out of the three values, if jammed nodes send out 10 alert messages, there is a higher chance that atleast one alert message will not be lost and it will be received by atleast one non-jammed node. If more is the chance for an alert message to be not lost then we have a greater probability of detection. From the graph it is clear that if we want to have a higher detection rate then the jammed nodes should send more number of alert messages. The time interval of the node has no influence on the detection rate.

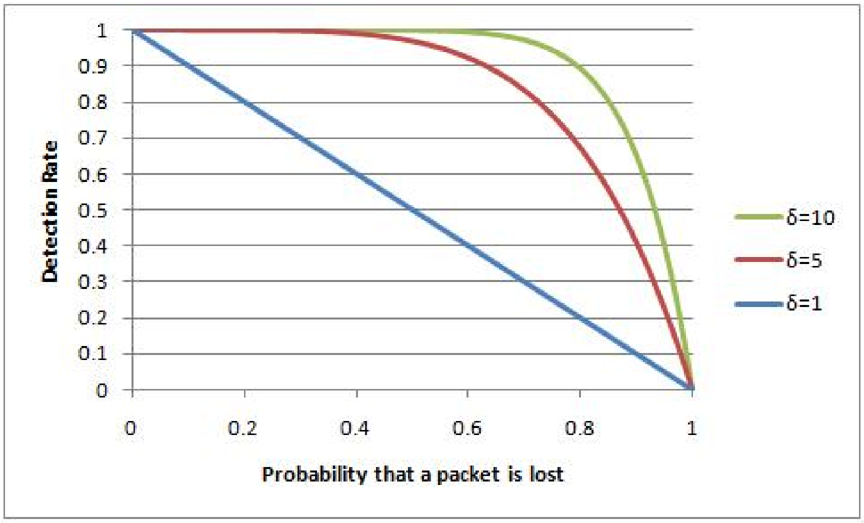

Figure 4.2. Effect of number of alert message on detection rate.

A false alarm is an alert raised by a node in the network without the presence of a jammer. For an alert to be raised, a node should loose $1 - \tau$ times the messages it received in the previous time interval. If a node looses $1 - \tau$ times the messages it received in the previous time interval without being under attack from a jammer, it will raise an alert resulting in a false alarm. Let's say that the number of nodes in a cluster is N and the channel loss rate is p. In that case, we can estimate the average number of messages received by a node in a time interval is $(N - 1)(1 - p)$. It will raise an alarm without the jammer, if it losses $(1 - \tau)$ times its previous time intervals messages. In other words we can also say that $(1 - \tau)(N - 1)(1 - p)$ nodes have failed in the current time interval. The nodes have failed without jammer that means they have lost packets due to packet collision or channel noise. We can estimate the probability of that failure by using binomial distribution. Therefore, the equation for false alarm will be

$$FA = \sum_{i=((X_{t_{n-1}})(1-\tau)+1)}^{N-1} \binom{(N-1)}{i} \times p^i \times (1-p)^{(N-1)-i} \tag{4.3}$$

Equation 4.4 gives the probability of a false alarm being generated in the cluster by any node. According to the protocol, alarm will be raised if more than $(1-\tau)$ times the number of messages received in previous time interval are lost. The summation over i captures all the possibilities of more than $1-\tau$ times the number of nodes active in previous time interval failing in the current time interval and hence resulting in an alarm being generated. Figure 4.3 shows a graph plotted for two different values of N which are 11 and 21. The graph shows that rise in the channel loss rate results in higher false alarm in the network. The false alarm rate is almost similar for both the cases of number of nodes in the cluster/network.

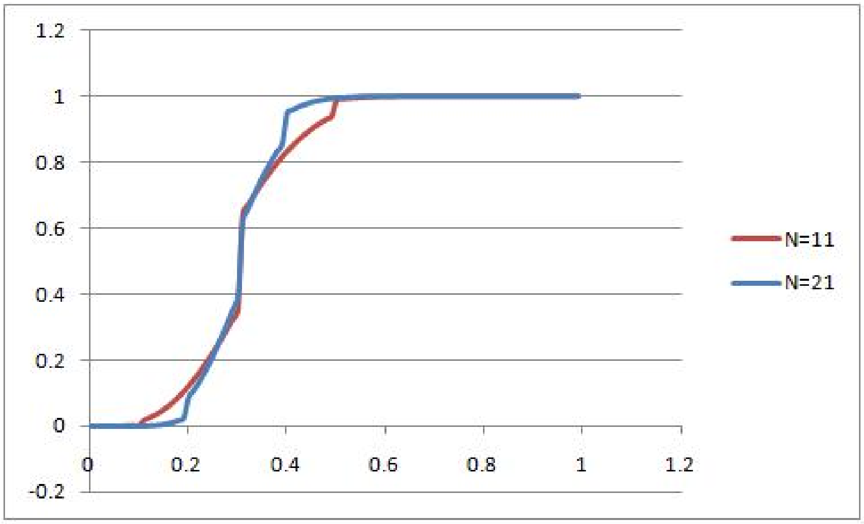

Figure 4.3. False alarm theory.

Detection time is the time difference between the time when the attack was launched and an alert message was successfully received by a non-jammed node. In the protocol, the time at which a node receives a message is completely random as well as the time at which jammer launches attack. A node may receive all the messages at the start of its time interval or may be at the end of its time interval. For the analysis, assuming that there are no packet losses without the presence of the jammer. If suppose the length of the time interval is t time units, dividing it into two sub intervals, one is the first sub interval $\tau \times t$ time units and the other is the second sub interval $(1 - \tau) \times t$ time units. Assuming for the theoretical analysis, that the messages broadcasted by nodes is periodic instead of random. The jammer launches its attack at random time. If the attack is launched during the first sub interval then the attack will be detected at the end of the current time interval and if the attack is launched during the second sub-interval then it will be detected at the end of the next time interval. The average detection time for detection at the end of current time interval will be $t-(t \times \tau)/2$ and the average detection time for detection completed at the end of next time interval will be $2t-(t \times (1-\tau))/2$. Assuming that the probability of receiving a message in first sub-interval is τ and the probability of receiving it in second sub-interval is $1 - \tau$,the overall average detection time for the protocol will then be

$$(\tau \times (t - \frac{(t \times \tau)}{2}) + ((1 - \tau) \times (2t - (t \times \frac{(1 - \tau)}{2})) \tag{4.4}$$

The equation can be further reduced to

$$((\tau \times t) - \frac{(t \times \tau^2)}{2}) + ((1 - \tau) \times (2t - \frac{(t - t \times \tau)}{2})) \tag{4.5}$$

Which can be further reduced to

$$((\tau \times t) - \frac{(t \times \tau^2)}{2}) + (2t - \frac{(t - t \times \tau)}{2}) - 2t\tau + \tau((1 - \tau) \times \frac{(t - t \times \tau)}{2}) \tag{4.6}$$

On further simplification we get,

$$((\tau \times t) - \frac{(t \times \tau^2}{2}) + 2t - \frac{t}{2} + \frac{(t\tau)}{2} - 2t\tau + \frac{(t\tau)}{2} - \frac{(t\tau^2}{2} \tag{4.7}$$

Which can be further reduced to

$$(t\tau) + \frac{(t\tau)}{2} - 2t\tau + \frac{(t\tau)}{2} - \frac{t\tau^2}{2} - \frac{t\tau^2}{2} + 2t - \frac{t}{2} \tag{4.8}$$

Arranging the like terms after adding some like terms

$$2t\tau - 2t\tau + 2t - \frac{t}{2} - \frac{t\tau^2}{2} - \frac{t\tau^2}{2} \tag{4.9}$$

Finally, the equation gets reduced to

$$\frac{3t}{2} - t\tau^2 \tag{4.10}$$

$$d_t = \frac{(3 \times t)}{2} - (t \times \tau^2) \tag{4.11}$$

4.2.1 Variable Definitions

PDR : PDR of a node defines its reception rate. PDR of 97 for a node means if a sender node had sent 100 packets, that node had received 97 packets and lost 3 packets.

p : p represents the channel loss rate. It gives the probability of the messages lost in the network due to either noise in the channel or packet collision.

τ : It gives us the threshold of packet loss in case of jammer being present in the vicinity of a node.

CHAPTER 5

TESTING AND RESULTS

Protocol's performance was tested on telsob motes [10]. Telosb motes use Tinyos [11] platform. The protocol and the jammer have been implemented in Tinyos-2.x [12]. Tinyos is a free and open source component based operating system and platform targeting WSN. Tinyos applications are written in NesC, a dialect of the C programming language which has been optimized for the memory limitations of wireless sensor networks. Telosb motes use a CC2420 chicpcon radio [13]. For our testing, the jammer and the benign motes transmit at the same power level. We also assigned the value of δ to be 10 i.e. each mote sent the alert message 10 times whenever it detected jamming in the network. Each alert message was sent with a random time interval between 0 to 100 milli seconds.

The experiment was carried out inside the lab in an area of 900 sq. inches. The protocol was tested against one constant jammer which was placed at various positions and at different orientation to jam different number of motes for each position and orientation of the jammer. The jammer was placed outside the perimeter of the network. The range of the telosb motes is reduced in an indoor environment. We also further reduced their range by making them transmit at the lowest power level which is 1. The effective range of the motes transmitting at power level 1 was ranging between 15-25 inches. 40 motes which were running the protocol were arranged in a grid topology as it made for an easier deployment. Each mote was placed at a separation of 5 inches. All the motes and the jammer were running at power level 1. The jammer was also programmed to transmit at the same power level as the motes which is power level 1. Figure 5.1 shows the network topology and the jammer's various position for testing the protocol. Depending on the position of a mote in the network, the number of neighbors for a mote varied from 6 to 14 motes. Though the motes were not time synchronized, they were all running at the same interval of time interval. Motes which lied on the edge of the network were having less number of neighbors and motes which lied inside the network were having more number of neighbors. Tests were carried out to record the detection time, detection rate and the false alarm rate of the protocol.

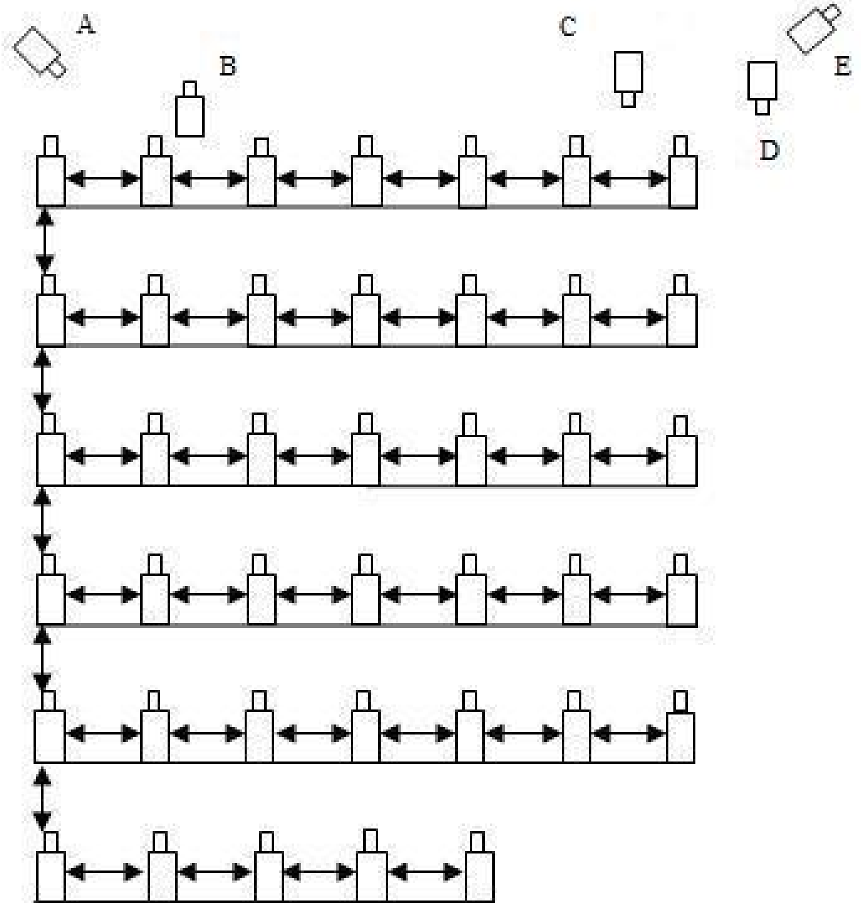

Figure 5.1. Network Layout.

In Figure 5.1, the motes next to the numbers are jammers and each number signifies their position. When the jammer was placed at different position with different orientation, different number of motes were jammed. When the jammer was placed at position A, 16 motes were jammed. When placed at position B, 12 motes were jammed. For position C, 20 motes were jammed. When placed at position D, 8 motes were jammed and at position E, 6 motes were jammed. Figure 5.2 shows the detection rate of the protocol for each case. For the detection rate, 100 attacks were carried out for each position of jammer. For each attack, the protocol's decision was observed on the existence of the jammer. Protocol achieved 100% detection rate when jammer was placed at position E and B. The lowest detection rate was 97% in case of jammer being placed at position D. In the other two cases, when jammer was placed at position A and C, protocol achieved a performance of 98% detection rate.

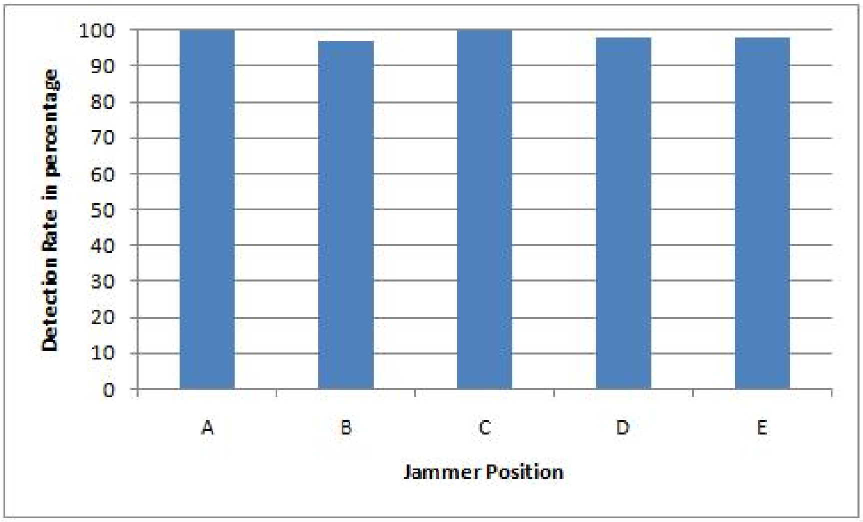

Figure 5.2. Detection Rate.

To calculate the detection time, one of the non-jammed mote was connected to the computer. Whenever that mote received an alert message it would print the reception time on the system. This gave us the time at which detection was complete. To get the time when the attack was launched, another mote was also connected to the computer which sent a message to the jammer on reception of which the jammer starts the attack on the network. That mote will print the time when the jammer is launching the attack on the system screen. By taking the difference between the two times we get the detection time. For the detection time, five time intervals of the protocol were used. At the end of the time interval motes send out a message and also carry out the detection. Figure 5.3 shows the box plot for detection time for five different time intervals which are 5 secs, 10 secs, 20 secs, 30 secs and 60 secs and a curve for the theoretical analysis. The curve represents the theoretical detection time average for each of the time intervals. From the graph it is clear that there exists a huge variation in terms of detection time when recorded empirically and the theoretical analysis. From the graph it is clear that, as the time interval increases the average detection time increases. There are cases where some times detection time is very low and sometimes more than the time interval. The reason for such values is the non-synchronization of motes. Due to unsynchronization, when jammer launches an attack, the motes might have just started their current time interval and might have already received all the messages from the other motes. After the end of that time interval the detection might fail, but it will be successful in the next time interval, that's why the detection time is more than the time interval. The difference between the detection times for theoretical analysis and the real experiments can be attributed to the random reception of messages by a mote.

For the false alarm part, the motes were programmed to transmit a packet, other than their ID every 993 millisecond with a certain probability. Transmitting a packet other than the ID of the mote creates a situation where motes will be running multiple protocols. We wanted to see the affect other protocols might have on our

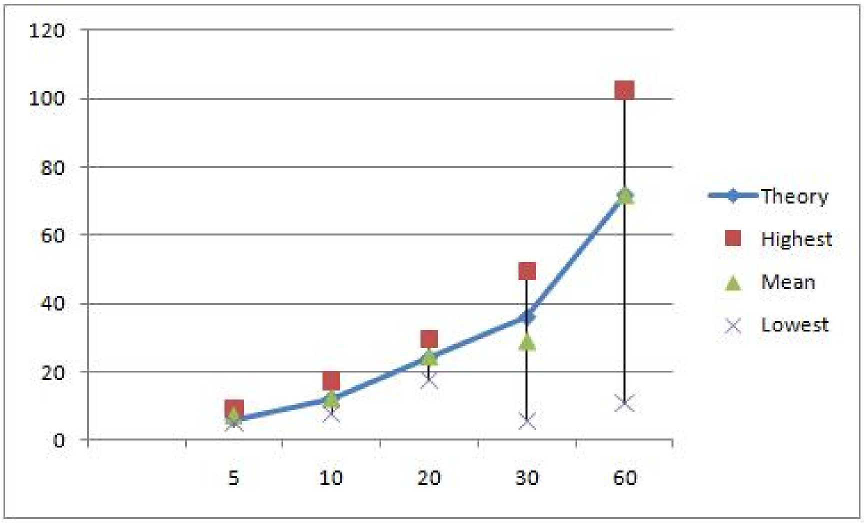

Figure 5.3. Detection Time.

protocol. Additional packets by the motes increases the traffic of the network. With increased traffic the chances of collision increases which results in loss of packets. The experimental setup creates a scenario of the protocol working in parallel to other protocols and increased network traffic. The reason to have the motes send out an extra packet every 993 ms instead of 1 sec is to avoid a deadlock situation. If the motes will send out an extra packet every 1 sec then there will be a deadlock every 10 secs for the system resources. The jammer was removed and only the 40 motes operated for 3 hours with a time interval of 10 secs i.e a total of 1080 intervals. Interestingly in all the cases with different probabilities for the additional packet being transmitted, only once was an alert raised in the network. Therefore the false alarm rate of the protocol is

$$\frac{1}{1080} \times 100 \approx 0.09\%. \tag{5.1}$$

CHAPTER 6

CONCLUSION AND FUTURE WORK

Wireless Sensor Networks are being widely used in various fields for different types of data collection and monitoring. They are a useful commodity in various civilian, industrial and scientific applications. Jamming attacks are one of the most popular attacks on WSN to cause a DoS. There is a need for early detection of these attacks accurately. Our contribution through this paper is that we have successfully proved through experiments that an observation of packet loss over an area gives us a faster detection compared to an observation between a pair of nodes. The protocol is topology independent. The protocol makes the detection rate independent of the time interval as the detection is purely dependent on the threshold. Time and location information of a node is irrelevant for the decision process. The protocol also gives the administrator control over detection time by controlling how frequently the administrator would like to broadcast the ID and carry out detection. The administrator can decide on what time interval to have which, gives him/her a good trade off between detection time and energy consumption without compromising on the detection rate. From the experiment we also found that the protocol has a very low false alarm rate. In our future work we would like to test our protocol against different attacker models. We would like to study the performance of our protocol when the network is under attack by Random jammer, Reactive jammer and Deceptive jammer.

REFERENCES

[1] AUSCERT, “Denial of Service Vulnerability in IEEE 802.11 Wireless Devices.” http://www.auscert.org.au/render.html?it=4091.

[2] W.Xu, W.Trappe, and Y.Zhang, “Anti-jamming Timing Channels for Wireless Networks,” in *Conference On Wireless Network Security*, 2003, pp. 203–213.

[3] S. M.Cagalj and J.P.Hubaux, “Wormhole-Based Antijamming Techniques in Sensor Networks,” in *IEEE Transactions on Mobile Computing*, 2007, pp. 100–114.

[4] M.Li, I.Koutsopoulos, and R.Poovendran, “Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks,” in *Proceedings of INFOCOM*, 2007, pp. 203–213.

[5] G.Alnie and R.Simon, “A Multi-channel Defense Against Jamming Attacks in Wireless Sensor Networks,” in *International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2007, pp. 95–104.

[6] Y. W.Xu, W.Trappe and T.Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, Mobihoc 05, pp. 46 – 57.

[7] C. K. E. Bayraktaroglu, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, “On the Performance of IEEE 802.11 under Jamming,” in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 1265 – 1273.

[8] Y.W.Law, L.V.Hoesel, J.Doumen, P.HartelL, and P.Havinga, “Energy Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols,” in *Workshop on Security of ad hoc and Sensor Networks*, 2005, pp. 76 – 88.

[9] C. M.Strasser and S.Capkun, “Efficient Uncoordinated FHSS Anti-Jamming Communication,” in *International Symposium on Mobile Ad Hoc Networking and Computing*, 2009, pp. 207–218.

[10] Telosb, *http* : *//www.willow.co.uk/html/telosb_mote_platform.html*.

[11] Tinyos, http://www.tinyos.net/.

[12] Tinyos-2.x, http://www.tinyos.net/tinyos-2.x/doc/.

[13] CC2420, http://docs.tinyos.net/index.php/CC2420.

BIOGRAPHICAL STATEMENT

Kartik Siddhabathula was born in Visakhapatnam, India, in 1984. He received his B.Tech. degree from Biju Patnaik University of Technology, India, in 2008 in Computer Science. From August 2008, he is doing his Masters in the department of Computer Science at University of Texas at Arlington. His current research interest is in the area of Security for Wireless Sensor Networks.