International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011

Improving Reliability of Jamming Attack Detection in Ad hoc Networks

Geethapriya Thamilarasu[1], Sumita Mishra[2] and Ramalingam Sridhar[3]

[1] State University of New York, Institute of Technology, Utica, NY, USA
[2] Rochester Institute of Technology, Rochester, NY, USA
[3] University at Buffalo, Buffalo, NY, USA

***Abstract*—**Defense against denial of service (DoS) attacks is a critical component of any security system as these attacks can affect the availability of a node or an entire network. In this work, we focus on jamming type DoS attacks at the physical and MAC layers in 802.11 based ad hoc networks. Collisions in wireless networks occur due to varying factors such as jamming attacks, hidden terminal interferences and network congestion. We present a probabilistic analysis to show that collision occurrence alone cannot be used to conclusively determine jamming attacks in wireless channel. To increase the reliability of attack detection, it is necessary to provide enhanced detection mechanisms that can determine the actual cause of channel collisions. To address this, we first investigate the problem of diagnosing the presence of jamming in ad hoc networks. We then evaluate the detection mechanism using cross-layer information obtained from physical and link layers to differentiate between jamming and congested network scenarios. By correlating the cross-layer data with collision detection metrics, we can distinguish attack scenarios from the impact of traffic load on network behavior. Through simulation results we demonstrate the effectiveness of our scheme in detecting jamming with improved precision.

***Keywords*:** Jamming, Cross-layer, Security, Ad hoc Networks

1. Introduction

In recent years we have witnessed a surge in numerous security vulnerabilities and attacks targeting wireless networks. The broadcast nature of the wireless medium in particular renders these networks susceptible to a range of attacks. Denial of Service (DoS) is one such security threat that prevents authorized users from gaining access to the wireless channel by disrupting network operations, impacting network connectivity and availability.

One of the simplest DoS attacks is jamming the wireless communication medium. In conventional jamming attacks, an adversary interferes with the radio frequency communication by transmitting continuous jamming signals or several short pulses. Traditionally jamming has been addressed as a physical layer attack. However, literature research in recent years shows that different protocol layers are vulnerable to jamming security attacks [1], [2]. For instance, IEEE 802.11 protocols designed for wireless networks assume that all nodes strictly adhere to the protocol rules for transmission. However, a malicious jammer node can cause network disruption in these networks by not conforming to the 802.11 MAC layer protocol rules. Research shows that different jamming attacks and countermeasures have been explored in detail. For instance, Wu *et al.* studied four different types of jammers namely constant, reactive, deceptive and random at the lower layers of the sensor network [3]. Noubir and Lin demonstrated that jamming can be used to attack higher layer network functionalities [2]. Thuente and Acharya showed that an intelligent adversary can launch jamming attacks at MAC layer by corrupting control packets, or falsely reserving the channel for maximum number of slots and deny availability [4].

Conventional defense techniques against physical jamming use spread spectrum techniques, which are not always feasible in resource constrained ad hoc networks. Several approaches have been investigated in literature for defeating jamming attacks [5]. Liu *et al.* proposed an architecture called SPREAD to mitigate the impact of smart jammers that target multiple layers [6]. Cagalj *et al.* proposed wormhole-based anti-jamming techniques for sensor networks where sensors within a jammed region establish communications outside the jammed area to notify the network operator of the presence of a jammer [7]. Navda *et al.* proposed a mechanism to protect 802.11 networks from jamming attacks by having the legitimate transmission hop among channels to hide the transmission from the jammer [8]. Chiang *et al.* proposed a spreading code at the physical layer to circumvent the jammers [20]. Li *et al.* treated jamming in sensor networks as an optimization problem to derive the optimal attack and detection strategies. In this work, jamming detection is based mainly on the measurable percentage of incurred collisions [9]. Hamieh *et al.* proposed a mechanism to detect jamming attacks by measuring the correlation between error and correct reception times [21].

Access points are commonly used to monitor the channel for jamming attacks in wireless LANs. Raya *et al.*, proposed a DOMINO system that conducts tests on the access point to detect MAC layer misbehaviors such as backoff manipulation [10]. Such infrastructure based monitoring schemes are however difficult to implement in ad hoc networks with no fixed infrastructure. This presents the need for a decentralized monitoring mechanism to detect jamming attacks in ad hoc networks. Rachedi *et al.* proposed a cross-layer monitoring mechanism to evaluate node cooperation and lower false positives rate using information from physical, MAC and routing layers [11].

Even with a monitor deployed in the network, jamming attacks are difficult to detect as they are often indistinguishable from other network abnormalities. For instance, collisions in wireless channel can occur as a result of jamming attack or due to interference from hidden terminal transmissions. Wu *et al.* showed that empirical

measurements based on signal strength and packet delivery ratio are combined to diagnose the presence of a jammer [3]. The authors here made an important observation that no single measurement is sufficient to reliably classify jamming attack. We build our work on the basis of this observation and develop a detection mechanism that removes the ambiguity in detecting jamming from congested scenarios. In this work, we focus on detecting jamming attacks that occur at both physical and MAC layers of an 802.11 ad hoc network. We present a distributed monitoring mechanism to choose monitor nodes responsible for identifying channel collisions. Using cross-layer measurements from physical and link layers, we derive the channel utilization metric used to estimate congestion in wireless networks. We develop a two phase detection mechanism, where Phase I detection consists of tests executed at the monitor by observing the physical and MAC layer behavior of the nodes. Phase II detection mechanism correlates the information obtained from Phase I with congestion measurement to differentiate between jammed and congested network conditions.

2. Problem Description

Jamming is defined as a DoS attack that interferes with the communication between nodes. The objective of the adversary causing a jamming attack is to prevent a legitimate sender or receiver from transmitting or receiving packets. Adversaries can launch jamming attacks at multiple layers of the protocol suite. In this work, we focus on attacks at the physical and MAC layer that result in collisions in the wireless network. Physical jamming is launched by continuous transmissions and/or by causing packet collisions at the receiver. Virtual jamming occurs at the MAC layer by attacks on control frames or data frames in IEEE 802.11 protocol [12]. We elaborate the attack models in the following sections.

2.1 Physical Jamming (Physical Layer)

Physical or Radio jamming in a wireless medium is a simple but disruptive form of DoS attack. These attacks are launched by either continuous emission of radio signals or by sending random bits onto the channel [3]. The jammers causing these attacks can deny complete access to the channel by monopolizing the wireless medium. The nodes trying to communicate have an unusually large carrier sensing time waiting for the channel to become idle. This has an adverse propagating effect as the nodes enter into large exponential back-off periods.

2.2 Virtual Jamming (MAC Layer)

In IEEE 802.11 based MAC protocols, virtual carrier sensing is used at the MAC layer to determine the availability of the wireless medium. Jamming can be launched at the MAC layer through attacks on the RTS/CTS frames or DATA frames [4, 12]. A significant advantage of MAC layer jamming is that the adversary node consumes less power in targeting these attacks as compared to the physical radio jamming. Here, we focus on DoS attacks at the MAC layer resulting in collision of RTS/CTS control frames or the DATA frames.

2.2.1 RTS/CTS Collision Attack (MAC Layer)*:* In this attack model, the main objective of the adversary is to randomly disrupt network transmissions by colliding with RTS/CTS control frames. Continuous collision of RTS frames denies channel availability to genuine network nodes. However, since it is difficult to predict the RTS transmission period, the adversary needs to transmit continuously similar to physical jamming to maximize the network disruption.

2.2.2 DATA Collision Attack (MAC Layer): In IEEE 802.11 MAC protocol, whenever a node transmits an RTS or CTS, all nodes in its transmission range defers their transmissions. However, when a node A tries to communicate with another node B, a malicious node X in the receiver's range can jam the channel by interrupting the radio transmission. The adversary can thus launch a DATA collision attack by not adhering to IEEE 802.11 MAC protocol rules and transmitting a packet during an on-going transmission.

2.3 Challenges in Detecting Collisions in Wireless Networks

Unlike wired Ethernet, collision detection is difficult to realize in wireless networks. Since collision occurs at the receiver and not at the transmitter, it is not possible for the sender to detect collisions. Receivers often utilize error detecting codes to detect packets corrupted due to collision. However in unreliable wireless networks, we cannot always rely on the receiver feedback. IEEE 802.11 wireless networks implements CSMA/CA, carrier sensing with collision avoidance to prevent collisions in the channel. The protocol uses an ACK packet to confirm successful transmission of a packet; hence failure to receive an ACK is often used as a collision indicator.

Apart from an adversarial DoS attack, collisions often occur due to varying factors in wireless networks. We consider various causes of collisions here:

2.3.1 Direct Collisions

In 802.11, distributed coordination function enables the nodes to access the channel randomly. This increases the possibility that two nodes may begin transmission at the same time. Since the packet transmissions start simultaneously, packets overlap and cause collisions at the receiver.

2.3.2 Hidden Terminal Collisions*:* Carrier sensing multiple access with collision avoidance (CSMA/CA) is commonly used in wireless networks to sense the wireless channel first before transmission in order to avoid collisions with other transmitting nodes. Collision may however occur due to hidden terminal problems, where a sender's transmission lies outside the geographical transmission range of another node transmitting in the receiver's range. Several MAC protocols such as MACA and 802.11 use RTS/CTS handshaking mechanism to resolve the collisions due to these hidden terminal nodes [13]. However, research shows that even with RTS/CTS handshake, 802.11 based MAC protocols do not completely solve the hidden terminal problems due to large

interference range [14]. Moreover, due to their significant overhead in mobile ad hoc networks, RTS/CTS handshake is often disengaged from the MAC protocol operation resulting in higher collisions.

2.3.3 Network Congestion*:* Congestion in 802.11 networks is due to high utilization of the shared wireless medium by the nodes. The congestion state is often caused due to heavy traffic load from few nodes in the channel or high density of nodes competing for channel access to transmit data. When there are a large number of users in the network, collisions are more frequent. Such collisions due to traffic load and channel contention can degrade the network performance to a large extent.

We observe from the above mentioned factors that, in 802.11 based wireless ad hoc network, packet collisions may occur either due to intentional jamming attacks or as a consequence of inadvertent hidden terminal problems and network congestion. Hence, it is of utmost importance that proper consideration of various collision factors needs to be taken into account towards detecting the presence of jamming attacks in the wireless channel.

3. Collision Probability Analysis

In this section, we present a simple probabilistic analysis of collision in wireless networks, under attack and hidden terminal conditions. According to Bianchi model [15], for a fixed number of contending stations n, let τ be the transmission probability that a station transmits randomly. The receiver in a wireless channel experiences collision if there is more than one node simultaneously transmitting in either the receiver's transmission range D or in its interference range I.

Probability of collision at a node δ is given by

$$\begin{aligned}\delta &= Pr(\text{atleast one transmission in range D}) \\ &\quad -Pr(\text{exactly one transmission in range I}) \\ &= 1-(1-\tau)^n - n\tau(1-\tau)^{m+n-1}\end{aligned} \quad (1)$$

where m is the number of nodes in the interference range

Let p be the probability of an adversary launching a collision attack in the channel and q be the probability of a hidden node in the interference range transmitting a packet. When there is an adversary transmitting, the probability of collision at node i is

$$\begin{aligned}\delta_1 &= p.Pr(\text{atleast one transmission}) + (1-p)\delta \\ &= \delta + pn_i\tau(1-\tau)^{m+n-1}\end{aligned} \quad (2)$$

Similarly probability of collision at node i due to the transmission of a hidden node in interference range is given by

$$\delta_1 = \delta + qn_i\tau(1-\tau)^{m+n-1} \quad (3)$$

It is obvious from equations 2 and 3 that the collision probability is dependent on the equally likely events of adversary or hidden terminal transmission in the channel. If $p \approx q$, then the probability of collision is same regardless of the cause. Even without the presence of adversary, wireless channel is subject to collision with probability δ due to channel contention and network load. This implies that collision monitoring mechanism in the wireless medium needs to account for the different causes of collision for reliably detecting potential malicious activity.

4. Collision Monitoring Process

Traditional detection mechanisms in wired networks comprised of monitoring the network layer to analyze packet level transmissions. In wireless networks, such schemes cannot be used to detect DoS attacks such as jamming that occur at lower layers. In such cases it is necessary to monitor the wireless channel transmissions. Due to the broadcast nature of wireless channel, communication between nodes can be overheard by all nodes in their transmission range. We utilize this feature to our advantage and employ channel monitoring mechanism to detect collisions in wireless networks.

We assume monitor nodes are randomly distributed within a topology according to Poisson point process with density λ. We assume all nodes have same transmission range and carrier sensing range. A collision attack occurs in the region of interest x when the malicious node lies in the transmission or interference range of B and disrupts any transmission in region x. A hidden terminal collision occurs during A's transmission when at least one node in Interference range and out of A's sensing range transmits simultaneously.

The monitor can successfully identify the collisions (attack or otherwise) only if the event occurs within the interference range of the monitor (R_i). Following an Elfes sensing model [16], the probability that a monitor detects collision event at a distance x is given as

$$\begin{aligned}P(x) &= 1, x < R_i \\ &= e^{-\lambda(x-Rs)}, R_s < x < R_i \\ &= 0, x > R_i\end{aligned} \quad (4)$$

For monitor nodes randomly deployed over area A, the probability that there exists a monitor node at a location with distance x to the event is $2\pi x dx/A$. Probability that the collision is sensed by the monitor is

$$P_{det} = \frac{1}{A}\int p(x)2\pi x dx \quad (5)$$

Depending on the variations in the network, number of nodes in the network that act as monitors can be determined proactively or reactively. In case of proactive monitor selection, at the time of network deployment, subset of network nodes are randomly chosen as monitors. The role of monitors is periodically reassigned to different nodes to ensure that the monitoring process does not drain the energy resources of fixed nodes. In reactive monitor selection, nodes are assigned as monitors when the network suffers from frequent collisions and retransmissions. Higher numbers of monitors are chosen in regions where collisions are more frequently observed.

Although monitors can successfully detect collisions in the wireless channel, it cannot positively assert the presence of a jamming attack. Due to the possibility of hidden terminal and traffic load collisions in ad hoc networks, the monitors perform another level of detection to remove ambiguity in its decision.

5. Congestion Estimation using Channel Utilization

In this section, we present the cross-layer measurement of channel utilization to determine collisions due to network congestion. As discussed in [17], probability of packet loss due to hidden terminal collisions is a function of traffic load at the hidden terminal node. Heavy traffic load in the node's transmission or interference range can result in a congested network leading to packet collisions. To effectively identify collision attack, it is essential to classify the congestion level in the network. In this work, we perform congestion estimation to detect network collisions.

Congestion estimation has been extensively studied in literature. Several metrics such as queue length, packet delivery ratio and throughput have been used to measure network congestion. Since throughput degradation can also occur due to hidden terminal interferences, lossy channels or packet collisions, it cannot clearly indicate congestion. In addition, throughput is directly influenced by data transmission rate in wireless links. Hence, for wireless networks, congestion can be better characterized based on the amount of time the channel is utilized or reserved by nodes for transmission. Recently several studies have proposed the use of channel (medium) utilization as a solid measurement metric to evaluate congestion in the network [18], [19].

In this paper, we use a measurement driven approach to characterize congestion through channel utilization. We follow the methodology proposed by Jardhosh *et al.*. where channel busy time (CBT) is used as a direct measure of channel utilization to classify network as highly congested, moderately congested or uncongested [19].

5.1 Channel Busy Time

Channel Busy Time is defined as the fraction of time interval during which the wireless channel is busy or occupied. Channel busy time measurement as outlined by Jardosh *et al.*. includes the time spent in packet transmission, reception and inter frame spacing delays preceding the transmission of control and data frames in 802.11 wireless network [19]. However, it fails to include channel noise, errors and hidden terminal transmissions due to which the channel may be busy. IEEE 802.11 standard defines both physical and virtual carrier sensing to avoid interference in wireless networks. In this work, we utilize the physical carrier sensing capability of 802.11 networks to more accurately determine the channel busy time. The wireless channel state is reported as busy, if its 802.11 clear channel assessment (CCA) mechanism senses the energy above the threshold that is determined by antenna sensitivity.

Carrier sensing time (TCS) is the duration of the time for which the channel is sensed busy. With physical layer carrier sensing, any transmission outside a node's transmission range but within its sensing range can be identified as a busy channel. This provides an improved estimation of congestion at hidden terminal transmissions.

Our channel busy time is thus measured using carrier sensing time at the physical layer as well as control/data frames transmission duration at the MAC and network layers.

Channel occupancy is dependent on the traffic pattern at the MAC as well as the network layers. Our measurement of $T(Ch_{busy})$ includes carrier sensing time at the physical layer (T_{CS}), transmission duration of control frames(T_{CTL}) and data frames ($T_{DATA)}$ at MAC and network layers, back off periods(T_{BO}) and the delay components introduced by the inter-frame spacing(T_{SIFS} and T_{DIFS}) in 802.11 based MAC protocol. The control frames include the transmission of route request, route response packets at the network layer as well as the RTS/CTS/ACK packets at the MAC layer.

We calculate Channel busy time ($T(Ch_{busy})$)as

$$T(Ch_{busy}) = \sum_{\forall i=1}^{t} (T_{CTL} + T_{DATA} + T_{BO} + T_{DIFS} + T_{SIFS} + T_{CS}) \qquad (6)$$

where t is the monitoring duration.

5.2 Channel Utilization

Channel utilization in wireless networks is computed by adding the total time spent on transmission of all data and control frames, as governed by the Channel busy time. We define channel utilization (U_{Ch}) as the fraction of time the channel is busy over the total duration. That is,

$$U_{Ch} = \frac{T(Ch_{busy})}{T(Ch_{busy}) + T(Ch_{idle})} \qquad (7)$$

where $T(Ch_{busy})$ and $T(Ch_{idle})$ are the time spent by the channel in the busy and idle modes respectively.

We conducted simulations of ad hoc network with 10-100 nodes to evaluate the channel utilization. We plot the channel busy time metric versus channel utilization calculated based on the data collected by the chosen monitor nodes.

Figure 1 shows a strong linear correlation between the channel busy time measure from different layers and channel utilization calculated for the monitoring duration. The high degree of correlation indicates that channel busy time can be used to measure channel utilization with high precision. Similar results have been observed for IETF wireless LAN scenarios [18].

Channel utilization can be used to effectively identify the various states of congestion in wireless network. From the experimental results, we can classify the network as *Highly Congested, Moderately Congested and Non Congested*.

Various network factors such as traffic load or node density can result in collisions due to congestion. To study the correlation between these factors and channel utilization we simulated a small scale ad hoc network with varying load and node density.

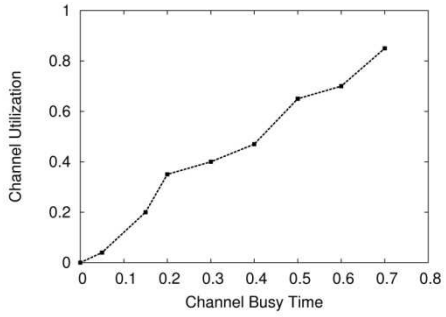


Fig 1: Channel Busy Time vs. Channel Utilization

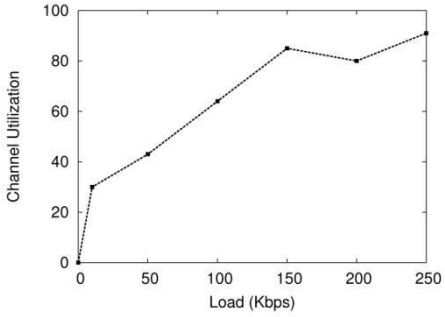


Fig 2: Impact of load on Channel Utilization

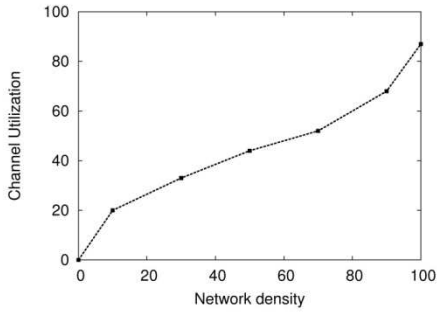


Fig 3: Impact of Node density on Channel Utilization

Figure 2 shows the impact of network load versus channel utilization. From the plot, we observe that as the traffic load increases the channel utilization increases from 35% to 90%. With an increase in network traffic, a large number of data frames and retransmissions occur. Under these conditions, average number of packet collisions also increases. High levels of channel utilization can clearly indicate the presence of collisions under various levels of congestion in the network. Similarly, in Fig. 3, we present the impact of node density on channel utilization. With higher number of nodes contending for the wireless channel, there is an increase in larger number of RTS frame transmissions and retransmissions to access the medium. When the number of nodes increases from 30 to 100, percentage of channel utilization increases from 20% to 85%. This shows that we obtain high levels of medium utilization when the number of packet collisions due to channel contention is high.

Previous solutions using CBT as the measurement metric relied on the sniffers in the wireless network to record all transmitted frames. However, this scheme failed to detect frames dropped due to bit errors, traffic load and frames that could not be recorded due to hidden terminal problem. Hence if there is large number of unrecorded frames, data set cannot be used to draw conclusions on the congestion level in the network. Since channel errors, varying traffic and hidden terminals are frequent problems in ad hoc networks, it is essential for channel busy time to be measured based on all these factors. Also sniffer locations were based on the apriori information about the access point topology in the network. In truly ad hoc networks, we do not have the flexibility and hardware to provide exclusive sniffers to monitor frames. By reactively choosing monitor nodes based on the collision regions, our distributed monitoring mechanism is capable of gathering information from different regions. Apart from recording the control/data frames, our monitors also record scrambled frames (error frames) and relevant information about the channel state from the physical layer. In the next section, we discuss the various metrics used at the monitor for detecting collision attacks.

6. Collision Detection

In this section, we present the two phase detection mechanism employed at the monitor nodes to detect jamming attacks. We describe the detection mechanisms in detail below.

6.1 Phase I Detection -Using passive monitoring

During its first detection phase, the monitor conducts preliminary tests to detect collision occurrences in the wireless channel.

Table I: Metrics affected by jamming attacks

Jamming attack Effect on Network	**Physical Jamming Large carrier sensing time**
Collision Attack CRC Errors	Increased number of retransmissions
NAV Attack Idle channel for long durations	Spurious RTS/CTS frames False channel reservation
Jamming attack Effect on Network	Physical Jamming Large carrier sensing time
Collision Attack CRC Errors	Increased number of retransmissions

Algorithm 1 Phase I Testing
loop for monitoring duration t
for each monitored node i
run Test j

Table I shows the impact of physical and MAC layer jamming on the network measurements. The monitor uses the following metrics obtained from the physical and link layers to identify collisions.

1) *Carrier Sensing Time:* Based on 802.11 standard, every node in the wireless network performs physical carrier sensing to sense the medium before transmission. When a malicious node attempts to continuously jam the wireless channel, the medium is always sensed busy for transmission. As a result, legitimate nodes in the network contending for channel access have a high carrier sensing duration. When the monitored nodes on an average have high carrier sensing time, it is possible that the region is being jammed. Carrier sensing time (Tcs) is thus used as an initial measure to indicate physical jamming conditions.

Test 1: PHY Jamming

$$if\ (T_{cs} > \eta)$$

where η is an empirical threshold value obtained through simulation experiments.

2) Bit Errors: When a node experiences collision due to different signals received at the same time, it drops the frames due to bit errors. Although such error frames are not usually recorded, average number of bit errors can provide meaningful insights into the current state of collision in a wireless channel.

Test 2: PHY/MAC Jamming

$$if\ (E[e_i] > \grave{o})$$

where E represents the acceptable value of bit errors in a wireless channel.

3) Frame retransmissions: Virtual Jamming attacks at the MAC layer causing collisions of RTS/CTS frames or DATA frames results in repeated retransmissions of the control or data frames respectively. Average number of frame retransmissions observed by the monitor node is an useful indicator of such collision attacks. The monitor runs the test to check if the average number of retransmissions of a node i (E[Ri])is greater than sum of the average number of retransmissions of all the other nodes in the network.

Test 3: MAC Jamming

$$if\ (E[R_i] > \sum_{j \neq i}^{n} E[R_j])$$

If any of the above executed tests is true, it indicates the presence of a possible jamming attack in the network. The monitor then calls phase 2 detection in order to confirm the detection.

6.2 Phase II Detection -Using Cross-layer measurements

In Phase II detection, we address the challenge of reliably differentiating the collisions in the network caused either due to jamming attacks or congested conditions. In this work, we propose a cross-layer based measurement driven approach where congestion estimation using physical, MAC and network layer measurements is used to identify collisions. Congestion estimation using channel utilization was presented in section 5. The monitor periodically runs jamming tests as well as evaluates the congestion status of the channel. Correlating results obtained from Phase I detection tests with estimated congestion level in the network facilitates accurate decision on jamming threats.

We outline the Phase II detection algorithm below:

Initially, we assume an optimistic network scenario and assign high confidence level to signify no jamming attacks. When any of the executed Phase I detection test results are true, the monitor node evaluates congestion state to check if the test results can be attributed to congested behavior. If the network is highly congested, monitor determines jamming attack with high probability. Non-congested network scenarios combined with Phase I results indicate the presence of jamming with a high likelihood ratio. If however the network was moderately congested, Phase I results are alone not sufficient to detect jamming. In this case, we lower the confidence level in the network and repeat the detection algorithm after a duration interval D. Since the network confidence level is lowered any suspicious result when the process is repeated is classified as an attack.

If a malicious node launches attack under congested network, it becomes more challenging to discern the cause of the network misbehavior. In such cases, use of any rate adaptation algorithm to lower the bit rate in the network, can alleviate the effects of congestion. Decrease in bit rate lowers the congestion state and its impact on the network conditions. This enables better classification of jamming attacks from congested network behavior.

Algorithm 2: Phase II Detection Algorithm

Initial Conditions: CONFIDENCE = HIGH;

Process:
if (Phase I test conditions TRUE) then
do CheckCongestionState()**;**
end if
CheckCongestionState()
if (Highly congested network) **then**
post no attack;
end if
if (Non congested network) **then**
post Jamming attack ;
end if
if (Moderately congested network) **then**
if (CONFIDENCE == LOW)
then
post Jamming attack ;
else
CONFIDENCE = LOW

repeat process after duration D;
end if

end if

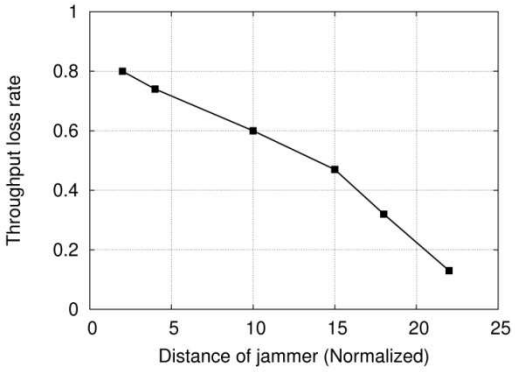
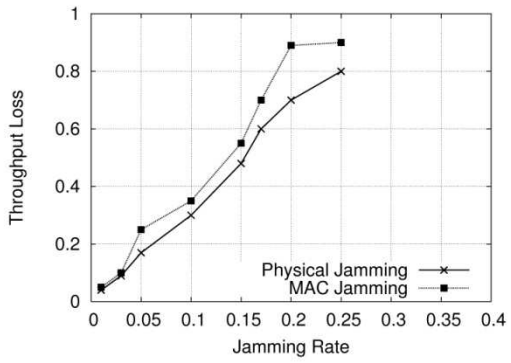
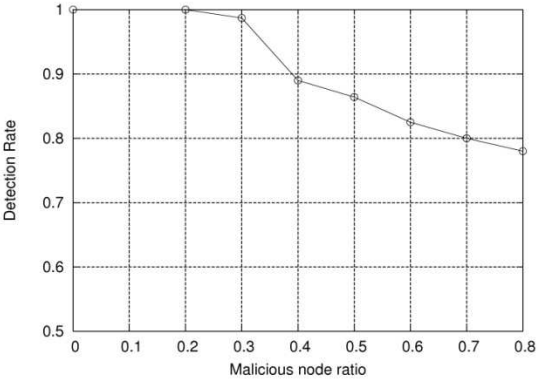


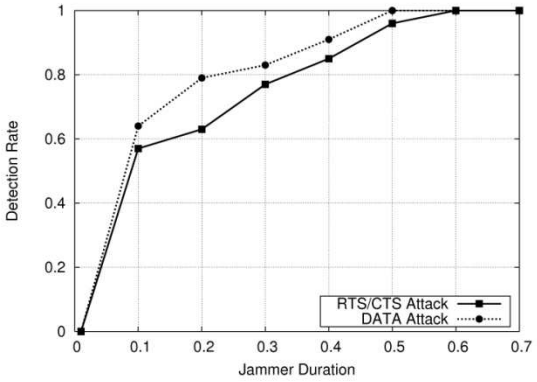
Fig 4 (a) Effect of Jammer Distance on Throughput loss



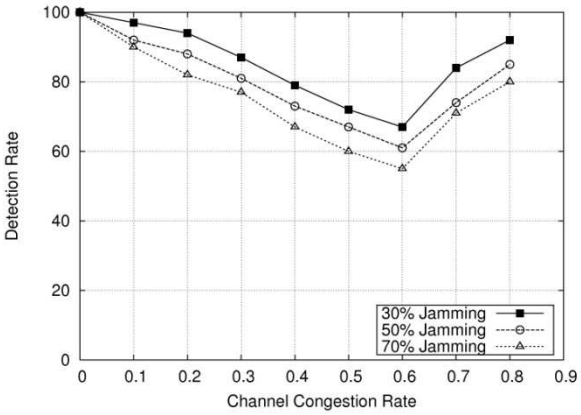
(b) Effect of Jammer Rate on Throughput loss



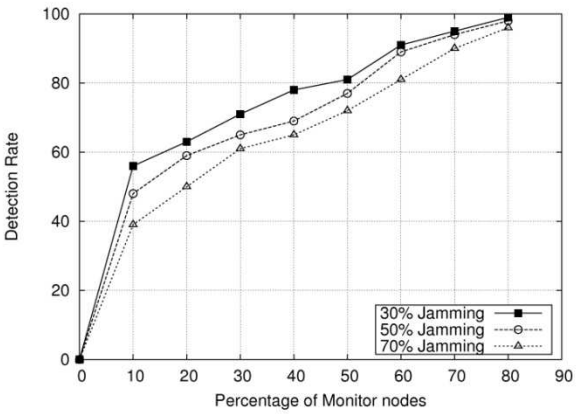
(a)



(b)



(c)



(d)

Fig. 5. Detection Accuracy :(a) Impact of malicious node ratio on detection rate; (b)Impact of jamming duration on detection rate; (c) Impact of channel congestion rate on detection rate; (d) Impact of monitor node ratio on detection rate

7. Simulation Results

We investigate the performance of the proposed detection mechanism by an extensive simulation study. We run our experiments using the GloMoSim network simulator framework [22]. To simulate attacks, the jammer nodes are activated 20 seconds after the ad hoc network starts operating, to allow the nodes to settle down into a steady state before the jamming starts, thereby simulating the attack scenario described in Section 3.

In our simulation setting, we place nodes uniformly on a 1000m by 1000m terrain. We setup a 1 Mbps IEEE 802.11 network with a two-ray ground propagation model at the physical layer. Simulations use CBR (Constant Bit Rate) application generating traffic of data packets of 512 bytes with an inter-arrival packet time of 2 packets per second. Simulation time is 900 seconds and each simulation is repeated 10 times for different seed values to obtain steady state performance metrics.

We model the malicious nodes to perform one or more of the jamming attacks at the physical and MAC layers. Initially, a subset of nodes in the network is randomly pre-deployed as monitor nodes. Once the attack is initiated, the network subsequently follows reactive monitor selection to choose the monitors.

7.1 Experimental Parameters and Evaluation Metrics

The major variables that constitute our experiments are

1) Jammer parameters -Jamming rate and distance of the jammer characterize the jammers behavior. The rate at which the jammer transmits to launch collisions and the distance of jammer to the region directly affects the network degradation.

2) Malicious node ratio -The malicious node ratio represents the number of attackers in the network. Higher number of malicious nodes implies higher possibility of jamming.

3) Channel congestion rate -is defined as the rate of congestion estimated in the current channel. Highly congested channel can lead to greater number of collisions increasing the false alarm rate in the network.

We propose the following metrics to evaluate the performance of our detection scheme:

- Detection rate: Detection rate measures the ratio of number of detected malicious collisions to the total number of collisions including undetected ones.
- False positive rate: False positives rate or the mis-alert rate measures the ratio of the number of detected collisions, due to channel congestion, to the total number of detected collisions.

7.2 Jammer Efficiency

We first verify the impact of jamming at different layers on network performance. Figure 4(a) demonstrates the effect of jammer distance on the network throughput for the case of physical jamming attack. We observe that the distance of the jammer from the jammed node(s) directly affects the reduction in throughput performance. When the jammer is at a closer range to the targeted node, the effect of jamming is more pronounced. However, as the distance of the jammer node increases, power of the jamming signal reaching the target node decreases hence impacting the target node with less severity. The effect of jamming thus diminishes with increasing distance of the jammer node resulting in less throughput loss. For instance, in our simulation scenario, when the jammer's range is below 10, it is more successful in affecting the network.

Figure 4(b) shows the throughput reduction for a packet size of 1500 bytes under PHY and MAC jamming rates. The plot indicates a high reduction in network throughput with the increase in jamming rate. It is also interesting to observe that for large fraction of jamming rates, MAC layer jamming reduces the network throughput 20− 30% more than physical jamming.

7.3 Detection Accuracy

We implement the detection module at the monitor nodes and evaluate the effectiveness of our cross-layer mechanism for jamming detection. Using simulation studies, we evaluate the impact of number of malicious nodes, number of monitor nodes, channel congestion rate and jammer duration on the detection accuracy.

In Fig. 5(a), we plot the detection performance of the monitor, for varying ratio of malicious nodes in the network. For a scenario of 30% of nodes acting as monitors, we observe that the percentage of detection decreases with increasing number of malicious nodes. This is because, with an increase in the malicious jammers, the number of nodes that are monitored by a single node increases, increasing the hidden terminal problems. Although it is difficult for monitor to cover a wide range, we observe that even when 65% of the nodes are compromised, we obtain reasonable detection rate of about 80%. Figure 5(b) presents the performance of the monitor for jamming control and data frames. We observe that with increased jammer duration, the monitor has a high detection rate in detecting both RTS collisions and DATA collisions.

Figure 5(d) illustrates that as we choose more number of monitors, jamming attacks can be detected more accurately. As monitor nodes increase, the duration of channel observation increases. Thus percentage of detecting any abnormal behavior in the channel is high.

We then test the impact of channel congestion levels on false positive rate. As shown in Fig. 6, the channel congestion rate significantly affects the false alarm rate. An increased congestion level causes more collisions making it difficult to distinguish jammed collisions from collisions due to network conditions. By providing reliable channel congestion estimation, we observe that we are able to keep the false positive rate very low around 7-8 % for large fractions of the

congested network state.

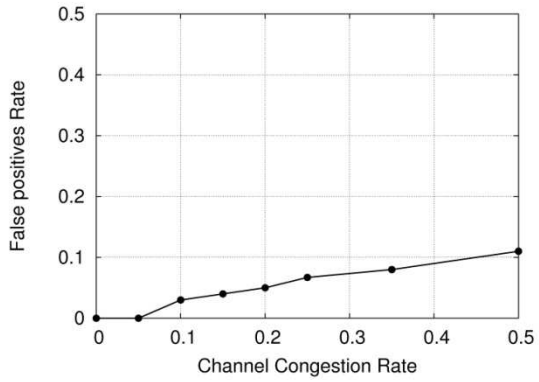


Fig. 6: Channel Congestion Rate vs. False positives

8. Conclusion

In this paper, we studied the effects of jamming at physical and MAC layers in a wireless ad hoc network and presented a detection algorithm to reliably detect jamming attack. Our analysis showed that collisions due to jamming attacks are not different from collisions due to hidden terminal and/or network congestion. To improve the detection accuracy, we utilized the channel utilization metric to evaluate network congestion state and then performed tests to classify whether collision is due to jamming or network traffic conditions. We evaluated the effectiveness of our scheme through simulations and demonstrated that it can be used to detect attacks with enhanced reliability and accuracy.

References

[1] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," *IEEE Computer*, vol. 35, pp. 53–57, 2002.

[2] G. Noubir and G. Lin, "Low-power dos attacks in data wireless LANs and countermeasures," *SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, pp. 29–30, 2003.

[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *MobiHoc '05:Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pp. 46–57, 2005.

[4] D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proceedings of the 25th IEEE Communications Society Military Communications Conference (MILCOM)*, October 2006.

[5] A. Wood, J. Stankovic, and G. Zhou, "Deejam: Defeating energyefficient jamming in IEEE 802.15.4-based wireless networks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. 4th Annual IEEE Communications Society Conference on*, pp. 60–69, June 2007.

[6] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "Spread: Foiling smart jammers using multi-layer agility," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, vol. 6-12, pp. 2536 – 2540, May 2007.

[7] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-based anti jamming techniques in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp. 100–114, 2007.

[8] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pp. 2526–2530, May 2007.

[9] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, pp. 1119–1133, 2010.

[10] M. Raya, J.-P. Hubaux, and I. Aad, "Domino: A system to detect greedy behavior in IEEE 802.11 hotspots," in *In Proceedings of the 2004 International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pp. 84–97, June 2004.

[11] A. Rachedi and A. Benslimane, "Toward a cross-layer monitoring process for mobile ad hoc networks," *Security and Communication Networks*, vol. 2, no. 4, pp. 351–368, 2009.

[12] D. Chen, J. Deng, and P. K. Varshney, "Protecting wireless networks against a denial of service attack based on virtual jamming," in *MOBICOM -Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking*, ACM, 2003.

[13] "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE 802.11," 1999.

[14] K. Xu, M. Gerla, and S. Bae, "How effective is the IEEE 802.11 rts/cts handshake in ad hoc networks," in *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*, vol. 1, pp. 72–76, 17-21 2002.

[15] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 3, pp. 535–547, 2000.

[16] A. Elfes, "Occupancy grids: A stochastic spatial representation for active robot perception," in *Autonomous Mobile Robots: Perception, Mapping, and Navigation*, vol. 1, pp. 60–70, IEEE Computer Society Press, 1991.

[17] H. Khalife and N. Malouch, “Interaction between hidden node collisions and congestions in multihop wireless ad-hoc networks,” in *Communications, 2006. ICC ’06. IEEE International Conference on*, vol. 9, pp. 3947–3952, June 2006

[18] P. Acharya, A. Sharma, E. Belding, K. Almeroth, and K. Papagiannaki, “Congestion-aware rate adaptation in wireless networks: A measurement-driven approach,” in. 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON ’08 pp. 1–9, June 2008.

[19] A. P. Jardosh, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding- Royer, “Understanding congestion in IEEE 802.11b wireless networks,” in Proceedings of the Internet Measurement Conference, pp. 279–292, Oct. 2005.

[20] Chiang, J. T.; Hu, Y.-C., "Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks," IEEE/ACM Transactions on Networking, vol .99, pp.1, 2010

[21]Hamieh, A.; Ben-Othman, J.; "Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution," IEEE International Conference on Communications, ICC '09. vol., no., pp.1-6, June 2009

[22] X. Zeng, R. L. Bagrodia, and M. Gerla, “Glomosim: a library for parallel simulation of large-scale wireless networks,” May 1998