International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue V, May- 2016

TIME-DELAYED BROADCASTING FOR DEFEATING INSIDE JAMMERS

Sooraj K Mohan
ME (CSE)
Jay Shriram Group of Institutions Tirupur
Sooraj.kmohan@yahoo.com

Ms P Mallika ME
Assistant Professor / CSE
Jay Shriram Group of Institutions Tirupur
mallikajaycse@gmail.com

Dr.S.Rajalakshmi
Associate Professor/ CSE
Jay Shriram Group of Institutions Tirupur
mrajislm@gmail.com

ABSTRACT

Jammer in the wireless network jams the user signals adding more interference signals. Due to that user unable to grasp their own signal from the jammed network. The problem is how to recover the jamming signals to receive the emergency broadcasting message. This is called jamming-resistant broadcast communications under an internal threat model. So implement a novel time-delayed broadcast scheme (TDBS), which implements the broadcast operation as a series of unicast transmissions distributed infrequency and time. TDBS does not rely on commonly shared secrets, or the existence of jamming-immune control channels for coordinating broadcasts. Each node follows a unique pseudo-noise (PN) frequency hopping sequence. TDBS differs from classical FHSS designs in two communicating nodes do not follow the same FH sequence, but are assigned unique ones. Unlike the typical broadcast in all receiver tune to the same channel, TDBS propagates broadcast messages as a series of unicast transmissions, spread both in frequency and time. To ensure resilience to inside jammers, the locations of these unicast transmissions, defined by a frequency band/slot pair, are only partially known to any subset of receivers. Assuming that the jammer can only interfere with a limited number of frequency bands, a subset of the unicast transmissions are interference-free, thus the propagating broadcast messages.

Keywords

WSN, Jamming attacks, MAC, and Routing.

1. INTRODUCTION

Jamming-style DoS attacks on physical and data link layer of the wireless sensor networks (WSNs) have recently attracted attention. In particular, Xu et al. propose four generic jammer models, namely the constant jammer, the deceptive jammer, the random jammer and the reactive jammer. A constant jammer emits a constant noise. A deceptive jammer either fabricates or replays are valid signals on the channel incessantly. The random jammer sleeps for a random time and jams for a random time. Lastly, a reactive jammer listens for activity on the channel, and in case of activity, immediately sends out a random signal to collide with existing signal on the channel. According to Xu et al., the constant jammers, deceptive jammers and reactive jammers are effective jammers in they can cause the packet delivery ratio to fall to zero or almost zero, if they are placed within suitable distance from the victims. However these jammers are also *energy-inefficient*, meaning they would exhaust the energy sooner than their victims would when given comparable energy budgets. Although random jammers save energy for sleeping, they are less effective.

Our contribution is to develop jamming attacks that work on encrypted packets, are effective as constant/deceptive/reactive jamming, at the same time more energy-efficient than random jamming or reactive jamming. We implement jamming attacks by exploiting the semantics of the data link layer and show the results quantitatively. The fact of our attacks are applicable to three representative MAC

protocols suggests the same attacks are applicable to wide range of other protocols belonging to same categories as the protocols. Our analysis of the attacks provides new insights into timing considerations of MAC protocols with regards to security, and provides hints on which category of protocols provides the best protection against our attacks so far, the absence of effective countermeasures.

The motivation of this work stems from the concern that if an attacker can program and deploy the general-purpose link-layer jamming network that is able to jam any WSN effectively and energy-efficiently, and if a high entry barrier is not maintained for such a low cost attack, a WSN can never in any practical sense be secure. A counter-argument might be that energy efficiency is no concern to powerful attackers, but even powerful jammers come with a finite energy supply and they would advertise their presence and location if they simply blast away with an exorbitant amount of radio waves this is something a sensible attacker would avoid.

Event masking attacks result in a coverage paradox. Even if an event is sensed by one or more nodes, the network operator cannot be informed on time about the event. We will explain how the solution to this problem is far from trivial. Proactive schemes, in sensors spend their time assessing the state of their communication links, are clearly suboptimal. Equally, jamming detection schemes are generally oversensitive and they generate many false alarms, making the system vulnerable to straightforward Denial of Service (DoS) attacks.

2 RELATED WORKS

In a wireless sensor network, all the mutual communication between sensors and between the network operator and sensors is wireless. This makes it possible for the attacker to jam the communication between sensors and the operator. This figure shows an intruder whose presence is sensed by sensors located within the exposure region. It also shows that all communication from the sensors to the rest of the network is jammed by the adversary, resulting in the presence of the adversary not being report time to the operator. This example shows that an adversary can, by jamming communication between the sensors, effectively delay report about his presence and, in some cases, prevent being detected at all. We speak about the "delay" as the sensor nodes from the exposure region may eventually detect the jamming activity of the adversary. However, this is not easy task considering the limited computational capabilities of sensor nodes. At the time a report arrives at the network operator, it may already be too late to take any meaningful action. Note also that the attacker can use smart jamming strategy to avoid being detected by the nodes that do not sense it. Usually, packets in sensor networks have no protection apart from a simple CRC therefore, only a short jamming pulse is sufficient to destroy a whole packet. Furthermore, even if jamming is detected, the network operator still cannot precisely locate the adversary; only the boundary of the jamming region can be determined.

Therefore, there is a clear need for defense mechanisms that can ensure timely data delivery in spite of jamming attacks. In this work, we assume the existence of an effective attack detection mechanism.

In the case of proactive sensor networks, several simple solutions are possible for ensuring that the operator receives event reports or detects jamming. One solution consists of having sensors periodically report their status to the network operator. If a sensor does not report its status within an expected period, the operator can request a retransmission or conclude that the communication from that sensor is prevented by adversary. If these status reports are sent very frequently, sensor batteries will be exhausted in short time, whereas if they are sent infrequently, the batteries will last longer, but the time elapsed between an events happening its reporting can be long and might render the alarm useless. Another similar

solution is that sensors hold the list of neighbors and periodically poll them to check if the communication links between them are still valid. This solution has similar drawbacks of the first proposal, as it either has high energy cost or opens a time window within event is undetected.

ATTACKS ON ROUTING PROTOCOL

While it is impractical to cover all possible attack models they might exist, in the study, we discuss a wide range of attacks they have proven to effective in disrupting wireless communication. Specifically, we have designed and built the following jammers

Constant jammer: The constant jammer continually emits the radio signal. We have implemented a constant jammer using two types of devices. The first type of device we used as a waveform generator which continuously sends the radio signal. The second type of device we used a normal wireless device. In the paper, we will focus on second type, which we built on the MICA2 Mote platform. Our constant jammer continuously sends out random bits to the channel without following any MAC-layer etiquette. Specifically, the constant jammer does not wait for channel to become idle before transmitting. If the underlying MAC protocol determines whether the channel is idle or not by comparing the signal strength measurement with fixed threshold, which is usually lower than signal strength generated by constant jammer, a constant jammer can effectively prevent legitimate traffic sources getting hold of channel and sending the packets.

Deceptive jammer: Instead of sending out random bits, deceptive jammer constantly injects regular packet the channel without any gap between subsequent packet transmissions. As the result, normal communicator will be deceived into believing there is a legitimate packet and will be duped to remain the receive state. For example, TinyOS, if a preamble is detected, a node remains the receive mode, regardless of whether that node has a packet send or not. Hence, even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected. Further, we also observe that is adequate for the jammer to only send a continuous stream of preamble bits rather than entire packets.

Random jammer: Instead of continuously sending out the radio signal, a random jammer alternates between sleeping and jamming. Specifically, after jamming for tj units of time, it turns of the radio, and enters a sleeping mode. It will resume jamming after sleeping for ts time. tj and ts can be either random or fixed values. During its jamming phase, it can either behave like a constant jammer or deceptive jammer. Throughout this paper, our random jammer will operate as a constant jammer during jamming. The distinction between this model and the previous two models lies in the fact that model tries to take energy conservation into consideration, which has especially important for those jammers do not have unlimited power supply. By adjusting a distribution governing the values of tj and ts, we can achieve various levels of tradeoff between energy efficiency and jamming effectiveness.

Reactive jammer: The three models discussed above active jammers in the sense they try to block the channel irrespective of the traffic pattern on channel. Active jammers are usually effective because they keep the channel busy all the time. As we shall see in the following section, the methods are relatively easy to detect. An alternative approach to jamming wireless communication is to employ a reactive strategy. For the reactive jammer, we take the view point is not necessary to jam the channel when nobody is communicating. Instead, the jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets the reception of the message. We would like to point out that reactive

jammer does not necessarily conserve energy because the jammer's radio must continuously order to sense the channel. The primary advantage for a reactive jammer, however, it may be harder to detect.

3 OUR WORK

In the previous section we saw no single measurement is capable of detecting all kind of jamming attacks. The purpose of jammer is to influence the channel quality between a node and its neighbors. it is not reasonable or needed, try to detect a jammer if the jammer does not effectively interfere with receipt and send of packets at a node. While a node losing its sending ability is a clear sign that it is being jammed, a weak reception capability can be caused by several factors besides jamming, such as a low link quality due to the relatively large distance between the sender and receiver.

We observed in the previous section that PDR (**P**acket **D**elivery **R**atio) is a powerful measurement that is capable of discriminating between jammed and congested scenarios, yet unable to identify whether an observed low PDR is due to natural causes of poor link quality. In order to compensate this drawback, and enhance the likelihood of detection, we will examine two strategies that build PDR to achieve enhanced jammer detection. We augment to use of PDR by applying signal strength measurements are conduct consistency checking to determine whether low PDRs are due to natural causes or due to radio interference. Throughout this section, we assume that a node is only responsible for detecting whether it is jammed, and is not responsible for detecting the jammed condition of neighbors. It follows from the fact that a wireless node is the best source of information regarding its local radio environment and is a less reliable predictor of the radio condition at distant locations. We assume that each node maintains the neighbor list, obtained from the routing layer, which will assist in making more reliable detection decisions. Additionally, we assume that deployment of the network is sufficiently dense to guarantee that each node has several neighbors. All legitimate nodes in the network will participate in the detection protocol transmitting a baseline amount of traffic, by sending heartbeat beacons. This allows each node to reliably estimate PDR over a window of the time, and conclude that the PDR is 0 if no packets are observed during that time period.

Based on the observations we propose a detection protocol shown in Algorithm 1. In the PDRSS algorithm, a wireless node will declare that is not jammed if at least one of its neighbors has a high PDR value. However, if the PDRs are all the neighbors is low, then node may or may not be jammed and we need to further differentiate the possibilities by measure the ambient signal strength. Rather than continually sample the ambient signal levels, which may use precious energy and processor cycles, the function Sample Signal Strength instead reactively measures the signal strength values for a window of time after the PDR values fall below a threshold, and returns the maximum value of the signal strength during the sampling window 2, which is denoted as SS. We note that the duration of the sampling window should be carefully tuned based upon the traffic rate, the jamming model, the measuring accuracy, and the desired detection confidence level.

Algorithm: PDRSS_Detect_Jam
$\{PDR(N) : N \in Neighbors\}$ = Measure_PDR()
$MaxPDR = \max\{PDR(N) : N \in Neighbors\}$
if $MaxPDR < PDRThresh$ then
  SS = Sample_Signal_Strength()
  $CCheck$ = SS_ConsistencyCheck($MaxPDR$, SS)
  if $CCheck == False$ then
    post NodeIsJammed()
  end
end

Algorithm 1: Jamming detection algorithm that checks the consistency of PDR measurements with observed signal strength readings.

The function SS Consistency Check to take as input the maximum PDR value of all neighbors, denoted as Max PDR, and the signal strength reading SS. A consistency check is performed to see whether the low

PDR values are consistent with the signal strength measurements. If the signal strength SS is too large it have produce observed Max PDR value, then SS Consistency Check the returns False, else it returns True. The consistency check may be conducted empirically follows. During deployment, or during a guaranteed time of non-interfered network operation, the table of packet delivery ratios and signal strength values are measured. We may divide the data into PDR bins and calculate the mean and variance of the data within each bin. We may conduct a simple regression to build a relationship between PDR and SS. The output of the binning and the regression is a relationship from which may calculate an upper bound of the maximum SS they would have produced a particular PDR value in a non-jammed scenario. Using this bound, we are partition the (PDR; SS) plane into a benign-region and a jammed-region.

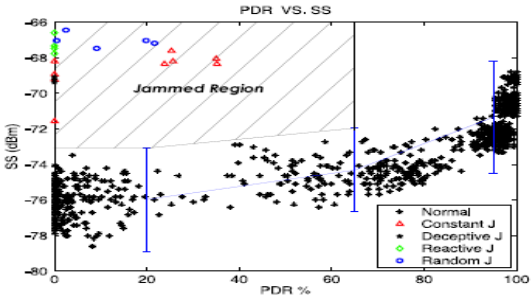

Figure 1: The (PDR; SS) measurements, indicating the relationship between PDR and signal strength. Also presented are the (PDR; SS) values measured for different jammers. The data was binned into three PDR regions, (0; 40), (40; 90) and (90; 100), and the corresponding 99% confidence intervals are presented. The shaded region is the jammed-region, and corresponds to (PDR; SS) values that are above the 99% signal strength confidence intervals and whose PDR values are less than 65%.

We conducted an experiment using MICA2 Motes validate Algorithm 1. We gathered (PDR; SS) values for a source transmitting to a receiver node at the power level of roughly ¡5dBm. The PDR values were calculated using a window of 200 packets, while the SS values were sampled every 1msec to 200msecs in order to provide sufficient resolution to capture the jammer behavior during the reactive jammer attack. The packets were 33 byte long and transmitted at a rate of 20 packets per second. The source receiver separation has varied in order to produce a full spectrum of normal (PDR; SS) values, as depicted in Fig. 1. Using these values, we found the 99% SS confidence bars values for (0; 40) (40; 90) and (90; 100) PDR regions. We depict these confidence bars, and define the corresponding jammed-region to be the region of (PDR; SS) that is above the 99% signal strength confidence intervals and whose PDR values are less than 65%. The jammed-region is shaded and appears in the upper-left corner of Fig. 1. We then performed experiments where we introduced the different jammers. The reactive jammer that we used sent out a 20-byte long interference packet as soon as it detects activities on the channel, while the random jammer had tj = U[0,31] and ts = U[0,31]. We varied the source-receiver configurations as well as the location of the jammer, and measured the resulting PDR and SS values. As can be seen in Fig. 6, the (PDR; SS) values for all jammers distinctively fall within the jammed-region.

CONCLUSIONS

We proposed TDBS, a scheme for jamming-resistant broadcast communications in the presence of inside jammers. In TDBS, broadcast is realized as a series of unicast transmissions distributed in frequency and time. Because the adversary is limited in the number of channels he can jam, several unicast transmissions remain interference-free. We mapped the problem of constructing FH sequences for the TDBS to the problem of 1-factorization of complete graphs. We further developed mechanisms for updating the FH sequences assigned to nodes, when the broadcast group is dynamic. We mapped the problem of minimizing the number of FH sequence changes required for node addition, to the problem of finding rainbow paths in proper edge-colored complete graphs. We

analytically evaluated the security properties of TDBS under both an external and an internal threat model and showed that TDBS maintains broadcast communications even when multiple nodes are compromised.

REFERENCES

[1] M. Abdel Rahman, H. Rahbari, and M. Krunz, "Adaptive frequency hopping algorithms for multicast rendezvous in DSA networks," in Proc. IEEE DYSPAN Symp., 2012, pp. 517–528.

[2] D. Adamy, EW 101: A First Course in Electronic Warfare. Norwood, MA, USA: Artech House, 2001.

[3] L. D. Andersen, "Hamilton circuits with many colours in properly edge-coloured complete graphs," Math. Scandinavica, vol. 64, pp. 5–14, 1989.

[4] K. Appel and W. Haken, "Every planar map is four colorable: Part I," Illinois J. Math., vol. 21, no. 3, pp. 491–567, 1977.

[5] P. Bahl, R. Chandra, and J. Dunagan, "SSCH: slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks," in Proc. MOBICOM Conf., 2004, pp. 216–230.

[6] L. C. Baird, W. L. Bahn, M. D. Collins, M. C. Carlisle, and S. C. Butler, "Keyless jam resistance," in Proc. IEEE Workshop Inf. Assurance United States Military Acad., 2007.

[7] K. Bian, J. Park, and R. Chen, "A quorum-based framework for establishing control channels in dynamic spectrum access networks," in Proc. MOBICOM Conf., 2009, pp. 25–36.

[8] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Broadcast control channel jamming: Resilience and identification of traitors," in Proc. ISIT Conf., 2007, pp. 2496–2500.

[9] P. Chaporkar, K. Kar, X. Luo, and S. Sarkar, "Throughput and fairness guarantees through maximal scheduling in wireless networks," IEEE Trans. Inf. Theory, vol. 54, no. 2, pp. 572–594, Feb.2008.

[10] J. T. Chiang and Y.-C. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in Proc. INFOCOM Conf., 2008, pp. 1211–1219.