Chapter 3

Metrics for Detection of DDoS Attacks

The DDoS attacks are trying to interfere with the physical transmission and reception of wireless communications. Attacks are caused by jamming, exhaustion, collision at MAC layer. At the data link layer, the jammer can only jam the receiver by transmitting high power at the network frequency and lowering the signal-to-noise ratio below the receiver’s threshold. However, it cannot prevent the transmitter from transmitting, and hence it cannot jam the transmitter. At the MAC layer, it can jam the receiver by corrupting legitimate packets through protocol violations, also jam the transmitter by preventing it to transmit by capturing the carrier through continuous transmission and the resources that are targeted are battery power, bandwidth, and computational power [16],[17]. With this modus operandi of the DDoS attacks at the background, we examine the suitability of various metrics for detecting the DDoS attacks in the wireless networks as suggested by different scholars in the next sub sections.

3.1 Carrier Sensing Time (CST)

In Media Access Control (MAC) protocols, such as Carrier Sense Multiple Access (CSMA), each node keeps sensing the time for the carrier to be free so
that it can then send its own packets. The average, time period for which the node has to wait for the carrier (channel) to become free and available to it is called the Carrier Sensing Time (CST). It is calculated as the mean of the time duration elapsed between the instant a node is ready to send its packet and the instant at which the carrier is found free by it for sending its packet. The nodes fix a threshold value of the CST, which if exceeded, allows it to infer that there is a jamming attack aimed at capturing the carrier. The threshold can either be fixed, as in case of 1.1 MAC, or taken as the minimum value over a given time period, as done in case of BMAC. This metric can be applied to only those networks using a MAC protocol based on carrier sensing. Also, this metric is incapable of indicating a physical layer power attack. It also suffers from the problem of fixing thresholds, which is an imprecise process and is computationally taxing on the scarce resources of the WSN node. We therefore, do not find it suitable for our system.

3.2 Packet Send Ratio (PSR)

PSR[5] of a node as the ratio of the number of packets actually sent by the node during a given time period to the number of packets intended to be sent by the node during that given period. ‘The number of packets intended to be sent during a given time period’ is found by calculating the time of the channel’s availability to the node during the given period, much in the same way as in the case of CST, and then by multiplying this available time with the packet
transmission rate. Finally, the PSR is calculated as defined above. The PSR-
calculation is cumbersome and accordingly, we do not find it suitable for our
system either.

3.3 Packet Delivery Ratio (PDR)

Both authors, Xu et al. [5] and Cakiroglu et al. [17] define PDR as the
ratio of the number of packets successfully sent out by the node (i.e., the number
of packets for which the node has got the acknowledgement from the destination)
to the total number of packets sent out by the node, however Xu et al [5] define
two types of PDR: first, one to be measured by the transmitter (source), and
second, one to be measured at the receiver (sink). We, while talking of the PDR,
mean only the first one, i.e., the one measured at the transmitter-end, and shall
discuss the second type, i.e., the one to be measured at the receiver-end,
separately. The PDR is calculated by keeping counts of the acknowledgements of
the successfully delivered packets and the total number of packets sent by the
node and then by finding their ratio as a percentage. PDR is a very good metric
which is capable of being measured accurately by the node without much of
computational overhead, and can indicate the presence of all types of jamming
attacks at the physical or data-link/MAC layer. However, the necessary condition
is that the network must follow a protocol, like TCP, where the system of
acknowledgement of packets exists. We feel that a resource- starved network, like
the WSN, cannot afford the luxury of acknowledgements, and hence reject it from our choice.

### 3.4 Bad Packet Ratio (BPR)

BPR is same as that PDR which is to be measured at the receiver-end, as suggested by Xu et al [5]. However, Cakiroglu et al [17] call it BPR and define BPR as the ratio of the number of bad packets received by a node (i.e., the number of received packets which have not passed the Cyclic Redundancy Check (CRC) carried out by the node) to the total number of packets received by the node over a given period of time. We find BPR to be a very effective metric which can indicate all types of jamming, is easily calculable, and is fit for WSN where the system of acknowledgements is not required. The CRC is a normal procedure which nodes have to do under most of the existing protocols to check whether a received packet is correct or erroneous. If the packet is correct (good packet), it is received or queued for further transmission, and if the packet is erroneous (bad packet), it is dropped and their count is maintained. Therefore, both values, the number of bad packets and the number of total received packets, are readily available for computing the BPR without imposing any significant burden on the system. Also, there is no sampling or fixing of thresholds involved here. We find this metric suitable for our system.
3.5 Standard Deviation in Received Signal Strength (SDRSS)

A system where the node samples its received legitimate signal called the clean signal, over a period of time and finds its standard deviation ($\sigma$) during the period [21]. It then samples the abnormal signal, called the jammed signal, and finds its mean deviation ($d$) from the clean signal over the same period of time. The calculation of $\sigma$ and $d$ are done as per formulae. If $d \leq \sigma$, then there is no jamming; else, there is jamming. Although we will discuss SDRSS subsequently under the method, we do not find it suitable for the WSN due to:

1. It cannot work if the jammer is transmitting at a power level equal to the normal transmitted power level of the nodes, as it would do during many types of jamming attacks.

2. It involves sampling at the node level, and

3. It is computationally communication for a WSN node.

3.6 Bit Error Rate (BER)

The use of BER [21] in combination with the received signal strength (RSS), as it is not only a very effective metric for detecting jamming attack, but is also capable of identifying the reactive jamming attack, which otherwise is very difficult to identify. The BER is calculated as the ratio of the number of corrupted bits to the number of total bits received by a node during a transmission session.
We concur with the authors as far as the effectiveness of this metric is concerned, but find the calculation of the BER heavily taxing for a WSN node, especially in a networking environment where the node will have to keep track of the BER of all radio links with its one-hop neighbors. Calculation and updating of BER, even at the base station level, is not feasible because it involves collection of voluminous data regarding every bit of a valid and invalid packet from the nodes leading to over-taxing of the WSN.

3.7 Received Signal Strength (RSS)

The received signal strength is defined as the power content of the radio signal received at the receiver. It is a measurable quantity and can either be measured by the RF power meter of the node or can be calculated using formulae as per the selected propagation model. The RSS by itself is not a logical metric to indicate jamming. However, when used in combination with metrics like the received jammer power (or noise power) or BER, it forms an effective combination to detect jamming.

3.8 Signals-to-Noise Ratio (SNR) or Signal-to Jammer Power Ratio (SJR)

Although there is a subtle difference between SNR and SJR, we have considered these to be the same because, in our model jammer is the predominant noise source, and have used these terms interchangeably. SNR is calculated as the ratio
of the received signal power at a node to the received noise power (or jammer power) at the node. It is almost an effective metric to identify a jamming attack at the physical layer as there can be no jamming at the physical layer without the SNR dropping low. However, some other metrics like PDR, BPR, or BER which can identify a data-link/MAC layer attack should be used with SNR for making it almost full-proof to detect jamming.

3.9 Energy Consumption Amount (ECA)

ECA [17] defined as the approximated energy amount consumed in a specified time for a sensor network. It can be calculated by measuring the drop in the battery (power-supply) voltage ($v$) of the node and multiplying its squared value with the time duration and then by dividing the result with the average electrical load (resistance) of the node. The authors argue that certain jammers force sensor nodes to remain in BACKOFF period even if they should have switched to IDLE mode, causing them to consume more energy than the normal. They suggest that this consequence can be used to distinguish the normal and jamming scenarios from each other. This metric has two pit falls: firstly, the sampling of the threshold energy consumptions of the node by itself under different traffic-load conditions is a tall order, and secondly, there may not be any perceptible energy consumption differential when the jammer is attacking in a way which does not involve the carrier capture, or when the jammer is resorting to simple power attack.
3.10 Selected Metrics for the Proposed System - SNR and BPR

We select SNR and BPR as the detection attack metrics for our system. However, we prefer to call the BPR as Packets Dropped per Terminal (PDPT) because our PDPT is the average BPR of a node during a simulation cycle. The reasons for this choice have been discussed above, and the same are summarized as follows:

- The received radio power at a node is easily measurable as nodes are/can be provided with RF power meter.
- In our system, the node simply keeps the base station informed about the received radio power, at a time interval as decided by the base station. The base station calculates the jammer (noise) power consumption by subtracting the average legitimate signal power of the node from the current power. The ratio of the two powers is then calculated by the base to get the SNR. Thus there are no overheads involved at the node level.
- The node keeps the base station informed about the number of good packets and total packets received by it during a time interval, as decided by the base station, in a normal routine way. The base station calculates the BPR (or, PDPT) for each node. Thus, the nodes are not burdened additionally.
- The combination of SNR and BPR (PDPT) is capable of detecting any form of DDoS attacks.