Chapter 5

Prediction of DDoS Attack Scheme

Distributed denial of service attack can be launched by malicious nodes participating in the attack, exploit the lack of entry point in a wireless network, and generate large volumes of traffic, from multiple-ends of the network, towards a set of victim nodes. Many Wireless networks are organized into clusters to raise their security. However the broadcast nature of wireless communication causes the nodes vulnerable to various malicious attacks. More specifically these networks are vulnerable to DDoS attacks due to the use of the clustering scheme in real-world scenarios. Cluster head nodes are selected to manage local clusters, which are ideal targets for adversaries to compromise. If one single node is captured by adversaries and turned into malicious head, an entire local cluster would be affected by DDoS attacks. A distributed denial of service attack can be launched by one of three adversary types, namely, jamming attack, exhaustion attack and collision attack, as described in chapter 2. There are only a few prediction methods as discussed in chapter 2, which involves fixing threshold of the prediction parameter for each node under different conditions, the behaviors of malicious nodes and consume large quantity of energy in monitoring suspicious nodes.
The disadvantage of the schemes is that the network lifecycle may become shorter as the schemes process large quantity of data and transmit it frequently. Moreover the networks suffer a high false prediction rate as their prediction schemes are deceive by DDoS attacks. Hence, schemes are not suitable for wireless networks, and it is critical to develop an effective security mechanism for IEEE 802.15.4 to predict DDoS attacks.

5.1 Description

Our goal is to design security mechanisms to predict the attacks caused by the malicious node. More specifically, we consider a scenario where a normal node could be compromised and deceived as a malicious inside the jammer present in the network. The attacker could use any cryptographic information known by the normal node to facilitate the DDoS attack. For example, the jammer could always predict the next channel used for communication and launch jamming signals to block the eligible network traffic. The goal of our proposed security mechanism is to construct the fuzzy based prediction system in a cluster-based wireless network, in which the nodes are managed locally by cluster heads. Rotating cluster heads makes it possible to select malicious nodes as cluster heads. Adversaries can compromise any node in the network and launch DDoS attacks in IEEE 802.15.4 MAC layer such as jamming, exhaustion, and collision. As malicious nodes require abnormal energy to launch an attack, we focus on
malicious nodes energy consumption rate in order to discover the compromised nodes. The two notable features of our scheme are listed as follows:

1. In contrary with the traditional detection methods detect malicious attacks based on behavior or interactions between the nodes within a period of time as described in chapter 4. A prediction method is introduced to predict the entire nodes energy consumption rate in base station and predict some energy sensitive attacks which require abnormal energy.

2. Prediction technique distinguishes various malicious attacks like jamming, exhaustion, collision according to the energy consumption rate. Energy thresholds are set to classify the malicious attacks, so that we can be aware of the types of attacks.

To our best knowledge, the concept of energy prediction in detection area has never been discussed in any previous research works. These two specific features mentioned above collectively make fuzzy system to predict a new, lightweight and efficient solution that can predict various attacks applied in any cluster-based wireless networks. Furthermore, our scheme is designed to distinguish the types of distributed denial of service (DDoS) attack according to the energy consumption rate of the malicious nodes. The primary simulation experiments prove that our method can predict and recognize malicious attacks effectively.
5.2 Fuzzy System for Prediction of DDoS Attacks

An energy efficient cluster formation for wireless networks using subtractive and fuzzy c-means approach in which, to increase the growth of wireless application demands for the wireless network to have the capability to trace the locations of node user [58]. L.chou et al [59] proposed the location updating scheme using fuzzy logic controls have been adaptively adjusts size of the location area for each user. Different approaches in improving the reliability and accuracy of measurement information from the sensor networks [60]. It offers a way of integrating sensor measurement results with association information, derived at aggregating nodes by using some optimization algorithm. They have considered both neuro-fuzzy and probabilistic models for sensor results and association information. The models carry out classification of the information sources, available in sensor systems and wireless networks. We have chosen a fuzzy logic in the base station for selecting the cluster-heads (PAN Coordinator) to predict the attacks. Several reasons support our use of fuzzy system in LRWPAN:

1. Representing the problem in mathematical (or probabilistic) model domain involves dealing with several variables and parameters at a time. Moreover these variables are to be defined separately for each scenario, in order to provide a collective output on the basis of the multiple input variables. Problem arises as the number of these variables increases. The mathematical model becomes too complex to handle so many parameters at a time, limited by the effective combination of different parameters together. Fuzzy logic
systems on the other hand have got an inherent ability to integrate numeric (‘fuzzy’) and symbolic (‘logic’) aspects of reasoning. Therefore different parameters like concentration, energy, and centrality can be combined easily to give the desired result by defuzzifier the output fuzzy set.

2. Fuzzy system is capable of making real-time decisions, even with incomplete information. Conventional control systems rely on an accurate representation of the environment, which generally does not exist in reality. Fuzzy logic systems, which can manipulate the linguistic rules in a natural way, are hence suitable in this respect. In addition, it can be used for context by blending different parameters - rules combined together to produce the suitable result.

3. Fuzzy system offers a full range of operators to combine uncertain information in a better way than any other systems. Fuzzy logic control techniques can be used to design individual behavior units. Fuzzy controllers incorporate heuristic control knowledge in the form of if-then rules. They have also demonstrated a good degree of robustness in face of large variability and uncertainty in the parameters. In fact considering only one parameter like energy is not suitable to select the cluster-head properly. This is because other conditions like centrality of the nodes with respect to the entire cluster, too gives a measure of the energy dissipation during transmission for all nodes. The more central the node is to a cluster the more is the energy efficiency for other nodes to transmit through that selected node. The concentration of the nodes in a given region too affects in some
way for the cluster-head selection. It is more feasible to select a cluster-head in a region, where the node concentration is high. In this paper, we design a fuzzy system for PAN Coordinator selection initiation to predict the DDoS attacks.

5.3 Prediction of DDoS attacks

The malicious nodes have to use additional energy to launch DDoS attacks. Therefore, we preliminarily focus on prediction method to predict the malicious nodes. In this prediction technique, Fuzzy Markov chains model is adopted to periodically predict energy consumption of sensor nodes. The difference between the predicted and the real energy consumption of sensor nodes can be used to predict malicious nodes.

5.3.1 Energy Dissipation for Prediction of Attacks

The energy dissipation in sensor nodes depends on the energy consumption in different working states and the time they operate in each state. The sensor nodes have five operation states:

1) **Sleeping** state: A sensor node operates in sleeping state does not interact with other nodes. Therefore, there is no need to evaluate the trust of the sleeping node. The energy dissipation of the sleeping node in the round time is $E_s$.

2) **Sensing** state: In the sensor operation, sensor nodes are responsible to sensing physical parameters, such as temperature, atmospheric pressure etc.
3) **Calculating** state: Sensor nodes process the received data.

4) **Transmitting** state: Sensor nodes transmit data packets between the clusters and the base station.

5) **Receiving** state: Sensor nodes receive data packets.

It is believed that the energy dissipation mainly focuses on the last four states. Therefore, each sensor node can be modeled by a Fuzzy Markov chain [61] with the last four states.

### 5.3.2 Operation State Transition Model

![Transition Model Diagram](image)

**Figure 5.1: Transition Model**

As shown in figure 5.1, the operation states of any sensor node shift when the node sends and receives packets, calculates data and senses information.
Furthermore, the time-step is the minimum time unit of the four operation states. Each state covers several time-steps. In one time-step, state \( \alpha \) shifts to state \( \beta \) with a probability of \( p_{\alpha \beta} \), for \( \alpha, \beta = 1,2,3,4 \).

In a series of \( n \) time-steps, the operation states of a sensor nodes can be denoted as

\[ X = \{X_0, X_1, \ldots, X_n\} \]

\( P_{\alpha \beta}^{(n)} \) represents the probability of transition from state \( \alpha \) to state \( \beta \) in \( n \) time-steps. Therefore, the \( n \)-stage transition probabilities can be defined as

\[
P_{\alpha \beta}^{(n)} = P\{X_n = \beta \mid X_1 = \alpha\} \tag{5.1}
\]

\( P_{\alpha \beta}^{(n)} \) can be calculated by the chapman-kolmogorov equations:

\[
P_{\alpha \beta}^{(n)} = \sum_{k=0}^{n} p_{\alpha k}^{(r)} p_{k\beta}^{(n-r)} \quad 0 < r < n \tag{5.2}
\]

If a cluster head knows \( P_{\alpha \beta}^{(n)} \) for its sensor node as well as the initial states \( X_0 \) of sensor nodes, it is possible to predict the energy consumption information of all sensor nodes in the cluster. The prediction process is shows as follows:

First, when the sensor node is in current state \( \alpha \), the cluster head counts the number of time-steps the node will stay in state \( \beta \). This is given by

\[
\sum_{t=1}^{T} P_{\alpha \beta}^{(t)} \tag{5.3}
\]
Second, the cluster head calculates the amount of energy dissipation in the next $T$ time-steps, $E^T$. This is given by

$$E^T = \sum_{\beta=1}^{4} \left( \sum_{i=1}^{T} P_{\alpha\beta}^{(i)} \right) * E_\beta$$

(5.4)

Let $E_\beta$ be the amount of energy dissipated in state $\beta$ for one time-step. Finally the cluster head node calculates the energy dissipation rate (EDR) of the sensor nodes for the next $T$ time-steps. The cluster head node can maintain estimations for the dissipated energy in each node by decreasing the value EDR periodically for the amount of the remaining energy from each node. Given the energy dissipation prediction, cluster heads send the prediction results to the base station where trust information is stored. According to the prediction method, prediction technique first compares the energy prediction results with the actual energy consumption at the node. Then the scheme searches nodes which spent significantly abnormal energy than other remaining nodes. The nodes with abnormal energy consumption are regarded to be malicious. Finally our scheme categorizes the types of DDoS attacks launched by malicious nodes.

### 5.3.3 Prediction Algorithm

Let $PC$ be the PAN coordinator

Let $N_i$ be the nodes in the network
Let $\alpha_{+ve}$ and $\beta_{-ve}$ represents the number of positive and negative interactions of $N_i$ received from neighboring node in the network as observed by PAN coordinator and $\beta(\alpha, \beta)$ in the beta probability distribution [62]. The trust value $T_i$ of the node $N_i$ relating to $PC$ is given using the beta probability distribution as given by

$$ T_i = \beta(\alpha_{+ve} + \alpha_0, \beta_{-ve} + \beta_0) $$

(5.5)

where $\alpha_0, \beta_0$ is the initial trustworthiness of the nodes.

In the above equation (5.5), the positive interaction represents the MAC protocol functioning is normal and the negative interaction represents the malicious or unfair functioning of the MAC protocol. Thus the probability of well-performing node is computes using the following formula that considers the trust among the $PC$ and $N_i$ is defined as

$$ P(T_i) = P(\beta(\alpha_{+ve} + \alpha_0, \beta_{-ve} + \beta_0)) = \frac{\alpha_{+ve} + \alpha_0}{\alpha_{+ve} + \beta_{-ve} + \alpha_0 + \beta_0} $$

(5.6)

By equation (5.6), if any new node $N_j$ joins, then the PC sets

$$ \alpha j_{+ve} = \beta j_{-ve} = 0 $$

(5.7)

The above equation (5.7) reveals the probability of the new node $N_j$ being either honest (normal) or malicious nodes.
5.3.4 Trusted communication among the PC and the Node

In figure 5.2, each node that is keen in performing the channel access initially waits for a pre-defined time period TP (Estimated using equation (5.6)) and then executes the clear channel evaluation process (E_{CC}) as defined by

\[ TP = random(2^\phi - 1) \times k \]  

(5.8)

\[ \phi \] is the minimum value of the backoff time and k is the unit of \( \phi \). If the channel access is busy, then increment \( \phi \) as \( \phi = \phi + 1 \), then it waits for random duration TP. Finally execute E_{CC} again. When the channel access gets failed, then the channel failure warning message (W_{CF}) is intimated. This is referred to as nodes communication status (CS). The guaranteed time slot (GTS) is allocated by each node to assure their data transmission to the PC. GTS includes seven time slots and the process of its allocation involves sending the request at the time of contention period (T_c) and waiting for the reply from PC. The following steps
illustrate the process by which the nodes communicate with PC and estimate their trust value to detect the attacks. The trust value describes to the nodes behavior.

1) Following each channel access and GTS request, each node reports CS and GTS to PC.

2) The node also maintains two records such as $I_{+ve}$ and $I_{-ve}$ which are reported to PC.

3) PC receiving the operational data’s of MAC sub layer from the nodes executes the trust value estimation as described in the previous section. This is performed by comparing the received information from the nodes with the prior information on the node’s behavior in the network.

4) The trust value update process is initiated by PC after time $t$. It takes the information received during past time slot into consideration and computes the new positive interaction $\alpha_{+ve}^{new}$ and negative interaction $\beta_{-ve}^{new}$ of node $Ni$ that are received from other nodes in the network.

5) PC estimates the positive and negative threshold value ($Th_{+ve}$ and $Th_{-ve}$) using the information gathered at the time $t$ and updates $\alpha_{+ve}^{new}$ and $\beta_{-ve}^{new}$ using the following cases.
Case 1

\[ \text{if } ECR > Th_{+ve} \]
\[ \text{then} \]
\[ \beta_{-ve}^{new} = \beta_{-ve} \times AF + 1 \]
\[ \alpha_{+ve}^{new} = \alpha_{+ve} \times AF \]
\[ \text{end if} \]

Case 2

\[ \text{if } ECR > Th_{-ve} \]
\[ \text{then} \]
\[ \alpha_{+ve}^{new} = \alpha_{+ve} \times AF + 1 \]
\[ \beta_{-ve}^{new} = \beta_{-ve} \times AF \]
\[ \text{end if} \]

where AF is the ageing factor which indicates the amount of past historical values to be used. In the above cases, if the node ECR is more than the threshold value (Th_{+ve}), negative interaction is incremented representing that the node are malicious. In this case our proposed scheme predicts the malicious nodes observed in the network. Conversely if the node ECR is more than threshold value (Th_{-ve}), positive interaction is incremented representing that the node are normal observed in the network. In the next subsection deals the prediction algorithm to classify the type of DDoS attacks.

5.3.5 Prediction of Malicious Nodes Classification Algorithm

After prediction, the network identifies the type of DDoS attacks launched by these malicious nodes.
Let $k$ be the size of the data packets.

Let $E_c$ be the energy comparison results.

$$E_c = E_p - E_c$$  \hspace{1cm} (5.9)

Where $E_p$ and $E_c$ represents the energy prediction result and energy real consumption of the sensor node $N_i$. The possible DDoS attacks such as jamming, exhaustion and collision are the set of attacks that energy consumptions lower than prediction results. To classify these attacks our scheme has set of three domains $d = \{d1, d2, d3\}$ to distinguish them. The energy comparison results not only indicate the malicious node but also lead us to the types of the attacks. Our scheme partitions the energy comparison results into three domains. The malicious nodes with the energy comparison result $E_c$. $E_c \in D$ is regarded as the node that launched with the DDoS attack $A_i$, $i \in \{1,2,3\}$.

Case 1:

$$E_c \geq M(E_{tx} * k + e_{amp} * k * d_{max}^2),$$

then sensor node $N_i$ is regarded as malicious (M) one launching the jamming attack. In this case, the jamming attack consumes more energy transmit power $E_{tx}$ and amplifier power $e_{amp}$ for unwanted data transmission (k Packets) which are disturbing the communication channel, corrupting the data during the transmission and diverting the communication from the neighbors node.
Case 2:

\[ E_c \leq M(E_{\text{tx}} k + \varepsilon_{\text{amp}} k d_0^2) \] , sensor node \( N_i \) is regarded as malicious one launching the exhaustion attack. The exhaustion attack consumes more energy transmit power \( E_{\text{tx}} \) and less amplifier power \( \varepsilon_{\text{amp}} \). Due to less amplifiers power the \( k \) packets are not capable to communicate with the neighboring nodes, an attacker automatically consume or waste away resources of other nodes present in the network and leads to quick battery drain from the node in the communication region.

Case 3:

\[ 2(E_{\text{tx}} k + \varepsilon_{\text{amp}} k d_0^2) \leq E_c \leq (M - 1)(E_{\text{tx}} k + \varepsilon_{\text{amp}} k d_0^2) , \] then sensor node \( N_i \) is regarded as malicious one launching the collision attack. Due to high SNR power, the \( K \) packets are corrupted and diverting the communication from the PC to other node and finally collision will occur due to jamming signals.

### 5.4 Conclusions

The critical nature of applications of IEEE 802.15.4 MAC Layer demand the need for their protection against malicious attacks that may be launched against sensory resources by the adversary-class. Several attacks such as: Jamming attack, exhaustion attack and collision attack have been modeled and analyzed in the literature survey. Some of the techniques predict the attacks by individual nodes
only. There is no communication with their neighboring nodes, due to which there is a possibility for more malicious nodes to be present in the network, hence it was unable to predict the attacks. An improved version of an attack against the availability of sensory resources is the distributed denial of service attack by using fuzzy system to predict the DDoS attacks in the IEEE 802.15.4 MAC layer which is able to communicate with all the neighbors present in the network. Fuzzy Markov chains model is adopted to periodically predict the energy consumption of sensor nodes. The fuzzy based prediction system in a cluster-based wireless network, in which the nodes are managed locally by cluster heads. Rotating cluster heads makes it possible to select malicious nodes as cluster heads. Prediction method is introduced to predict the entire nodes energy consumption rate in base station and predict some energy sensitive attacks which require abnormal energy. Prediction technique distinguishes various malicious attacks like jamming, exhaustion, collision according to the energy consumption rate. Energy thresholds are set to classify the malicious attacks, so that we can be aware of the types of attacks. It helps to reduce the overall energy computation rates incurred by the DDoS attacks. All the detailed experimental results and performance analysis are discussed in the chapter 6.