Fuzzy Based Detection and Prediction of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network

C Balarengadurai[1] and Dr. S Saraswathi[2]

[1] Research Scholar,
Department of Computer Science and Engineering,
Manonmaniam Sundarnar University, Tirunelveli, India

[2] Professor,
Department of Information Technology,
Pondicherry Engineering College, Puducherry, India

Abstract

Detection and Prediction mechanism against distributed denial of service (DDoS) attacks is a critical component of any security system in which, these attacks can affect the availability of a node or an entire network. In this work, we focus the detection and prediction mechanism against DDoS attacks in IEEE 802.15.4 using Fuzzy logic system. The main contribution of Fuzzy based detection and prediction system (FBDPS) is to detect the DDoS attackers by comparing the energy consumption of sensor nodes. The nodes with abnormal energy consumptions are identified as malicious attacker. Furthermore, FBDPS is designed to distinguish the types of DDoS attack according to the energy consumption rate of the malicious nodes. By stimulation results, we finalized potential areas in DDoS attacks and provide evidence of effectiveness for detection and prediction of DDoS attacks with improved detection rate.

Keywords: DDoS; Detection; FBDPS; IEEE 802.15.4; MAC Layer; Prediction; Security.

1.Introduction

IEEE 802.15.4 Low rate wireless personal area networks (LR-WPAN) offer device level wireless connectivity. They bring to light a host of new applications as well as enhance existing applications. One of the most serious issue of security exists in wireless networks especially some attacks are medium dependent and do not exist in the earlier counterpart [1].DDoS is that lots of clients simultaneously send service requests to certain server on the internet thro wireless network such that this server is too busy to provide normal services for others. Attackers using legitimate packets and often changing package information, so that traditional detection methods based on feature descriptions are difficult to detect it, in figure 1. Traditionally distributed denial of service (DDoS) attacks in IEEE 802.15.4 MAC layer is jamming, exhaustion, and collision. *Jamming* is a typical attack in wireless networks, which can disrupt wireless communication by emitting interference signals. It aims to weaken or zero out the availability of the system services. [2], [3], [16] proposed DEEJAM protocol is an amalgamation of frame masking, channel hopping, packet fragmentation and redundant encoding in order to detect the four defensive mechanisms for hiding communication from jammer, evading its search and reducing its impact. Various jamming attacks and defending strategies [4],[5],[6],[7] are proposed in which attackers launch jamming attacks at the MAC layer by either corrupting control packets or occupying the channel for the maximum allowable time, so that the network throughput can be decreased and unable to detect the attack at the high detection rate. An *exhaustion* attacker tries to consume or waste away resources of other nodes present in the network. The resources that are targeted are battery power, bandwidth, and computational power, which are only limitedly available in wireless networks. [12], [13] proposed a method for auditing the security policy on a fuzzy logic based intrusion detection system, to check the network for possible penetration attempts. [14] Proposed an interleaved hop-by-hop authentication mechanism using SVM, to defend against false report injection attacks. A *collision attack* against the link layer, like jamming, which occurs when an attacker sends a signal at the same time and frequency as a legitimate in a transmission to corrupt the entire packet [3],[10],[11]. The related work against jamming attacks can be applied to collision attacks. Another solution is to use Error correcting codes [15],[19],[20],[25],[26] which are efficient in situation where errors occur on a limited number of bytes but this solution presents also an expensive communication overheard. This makes it difficult for a node under attack to distinguish collision attacks from normal collisions. The above stated techniques for DDoS attacks are more complex involving attack detection and Prediction rate is very minimal, complicated calculation and results are more overhead for IEEE 802.15.4.The rest of the paper is organized as follows; Section 2 describes the proposed method for our system which deals with the attacks detection and attacks prediction methods using fuzzy systems. Next, section 3 deals with the performance analysis and evaluation parameter and finally, we conclude in section 4.

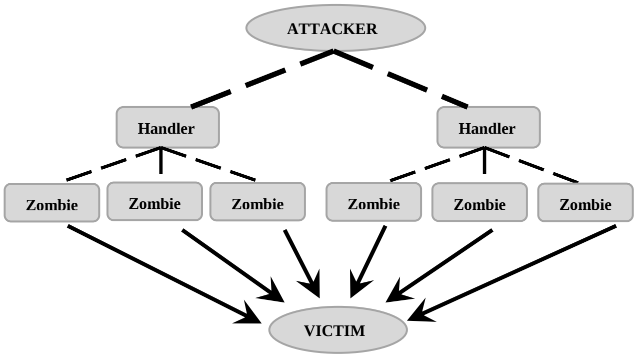


Figure 1 DDoS Attack

2.1 Description

In this paper, we adopt FBDPS in a cluster-based wireless network. Nodes can be 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 which only detect malicious attacks based on behavior or interactions between nodes within a period of time. We believe our energy consumption rate approach in this paper is novel and has many advantages. A prediction method is introduced to predict all the nodes' energy consumption rate in base station and detect some energy sensitive attacks which require abnormal energy. 2. Furthermore, FBDPS distinguishes various malicious attacks 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 FBPDS a new, lightweight and efficient solution that can detect various attacks applied in any cluster-based WSNs. The rest of section 2 deals with the detection and prediction attacks using fuzzy systems.

2.2 Detection of DDoS Attacks

The DDoS attacks to be an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications. This can be achieved by the jamming, exhaustion, collision are by attacking at MAC layer. At the MAC layer, the jammer can only jam the receiver by transmitting at 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 and 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. With this modus operandi of the DDoS attacks at the background, we examine the suitability of various metrics, as suggested by different scholars, for detecting jamming attack on a wireless networks[8],[9],[23],[24].We select SNR and BPR as the DDoS 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 [26]**.** The purpose of DDoS attack detection is met in its entirety if the detection rate is close to 100%. It is achieved through fuzzy logic system. The fuzzy logic engine uses two types of traffic parameters to generate a Level of Attack (LOA) are Bad Packet Ratio and Signal-to-Noise Ratio. The fuzzy logic engine considers both SNR and PDPT parameters as input to make the decision for the attack detection. Based on the outcome of the fuzzy rules, the LOA can be categorized into Low, Medium and High. It helps to reduce the overall energy computation rates incurred by the DDoS attacks detection scheme. The FLS mainly consists of four blocks namely fuzzifier, fuzzy rule, fuzzy inference and defuzzifier. The FLS figure was shown in [20], [21].

2.2.1 Fuzzy Sets and Membership functions

If *X* is a collection of objects, called the universe of discourse denoted generically by *q*, then a fuzzy set *A* in *X* is defined as a set of ordered pairs:

$$A = \{(q, \mu_A(q)) : q \in Q\} \qquad (1)$$

Where, $\mu_A(q)$ is called the membership function (MF) for the fuzzy set A. The MF maps each element of *Q* to a membership grade (or membership value) between 0 and 1.We defines three fuzzy sets each over the two universes of discourse for input namely, SNR and PDPT; the values are LOW, MEDIUM, and HIGH. For output, three four fuzzy sets are defined over the universe of discourse, LOA: the values are LOW, MEDIUM, and HIGH where SNR and PDPT are the crisp inputs to the system and LOA is the crisp output obtained from the system after defuzzification using the centroid method.

2.2.2 Fuzzification

Fuzzification is the process of mapping the real valued point to a fuzzy set. It converts obtained inputs into fuzzy linguistic variable inputs. The two parameters are taken into account for determining the level of attack. Fuzzification of the two crisp inputs SNR and PDPT are determining the degree to which these inputs belong to each of the appropriate fuzzy sets, which are mapped into fuzzy membership functions. To define the fuzzy membership function, trapezoid shape has been chosen in this detection method. We define the membership function below:

$$\mu_A(q) = \begin{cases} \frac{q-a}{b-a}, a \le q \le b \\ 1, b \le q \le c \\ \frac{d-q}{d-c}, c \le q \le d \\ 0, otherwise \end{cases} \quad (2)$$

Where the different values of the variables are as given in [22] which have been fixed through two phases: firstly, as per the mean of the values obtained from the proficient, and secondly, by the correction of these values through a feed-back factor generated by comparing the actual result and the expected result.

2.2.3 Fuzzy Inference

When an input is applied to a FLS, the inference engine computes the output set corresponding to each rule. The behavior of the control surface which relates the inputs (SNR, PDPT) and output (LOA) variables of the system is governed by a set of rules. A typical rule would be if x is A then y is B, when a set of input variables are read each of the rule that has any degree of truth in its premise is fired and contributes to the forming of the control surface by approximately modifying it. When all the rules are fired, the resulting control surface is expressed as a fuzzy set to represent the constraints output. Based on the lingusitic variables, nine rules are framed that represent the membership functions .The fuzzy rule base is given in table 1.

Table 1 Fuzzy Rule Base

Sl.No	SNR	PDPT	LOA
1	Low	Low	Low
2	Low	Medium	Low
3	Low	High	Medium
4	Medium	Low	Low
5	Medium	Medium	Medium
6	Medium	High	High
7	High	Low	Medium
8	High	Medium	High
9	High	High	Medium

2.2.4 Defuzzification

Defuzzification is the process of conversion of fuzzy quantity into crisp quantity. The defuzzifier computes a crisp output from these rule output sets. It can be performed in different methods. We have chosen the centroid of region gravity (COG). In this method, the centroid of each membership function for each rule is first evaluated. The final output LOA, which is equal to COG, is then calculated as the average of the individual centroid weighted by their membership values as follows:

$$LOA = COG = \frac{(\sum_{q=a}^{b} \mu_A(q) * q)}{\sum_{q=a}^{b} \mu_A(q)} \quad (3)$$

Where LOA/COG is the output of the defuzzification, $\mu_A(q)$ and q are the input variables of the membership function A. The complete process of calculating the crisp values of the LOA from the input values SNR and PDPT for every node is done through NS-2 stimulation in the next section. This approach reduces the processing load in the nodes, transferring most of the necessary calculations to the coordinators. This model is able to detect unfair nodes in the MAC layer, so that it can be used to hinder attacks.

2.3 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 paper, 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.

2.3.1 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 *Es*.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 [17] with the last four states.

2.3.2 Operation State Transition Model

As shown in Fig.2, 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 α shifts to state β with a probability of $p_{\alpha\beta}$, for α, β= 1,2,3,4.

In a series of n time-steps, the operation states of a sensor nodes can be denoted as $X=\{X_0, X_1,..., X_n\}$. $P_{\alpha\beta}^{(n)}$ represents the probability of transition from state α to state β in n time-steps.Therfore, the n-stage transition probabilities can be defined as

$$P_{\alpha\beta}^{(n)} = P\{X_n = \beta \mid X_1 = \alpha\} \tag{4}$$

$P_{\alpha\beta}^{(n)}$ can be calculated by the chapman-kolmogorov equations[17]:

$$P_{\alpha\beta}^{(n)} = \sum_{k=0}^{n} p_{\alpha k}{}^{(r)} p_{k\beta}{}^{(n-r)} \quad 0 < r < n \tag{5}$$

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 α , the cluster head counts the number of time-steps the node will stay in state β . This is given by

$$\sum_{t=1}^{T} P_{\alpha\beta}{}^{(t)} \tag{6}$$

Second, the cluster head calculates the amount of energy dissipation in the next T time-steps, E^T . This is given by

$$E^T = \sum_{\beta=1}^{4} (\sum_{t=1}^{T} P_{\alpha\beta}{}^{(t)}) * E_\beta \tag{7}$$

Let E_β be the amount of energy dissipated in state β 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.

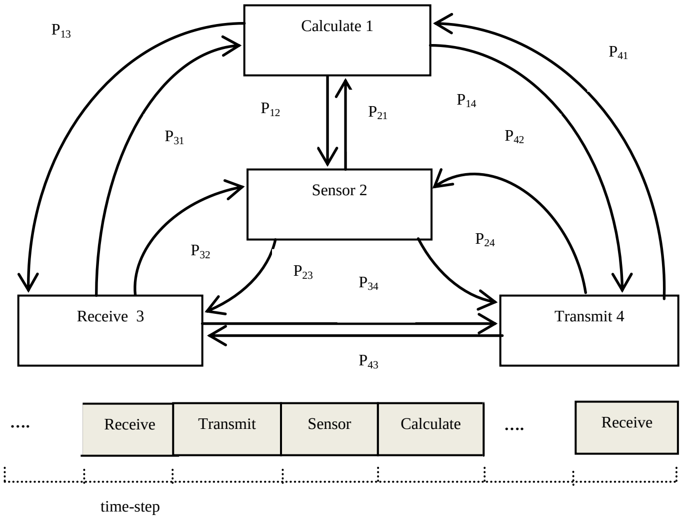


Figure 3 Transition Model

2.3.3 Prediction Algorithm

Let *PC* be the PAN coordinator

Let N_i be the nodes in the network
Let α_{+ve} and β_{-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 [18] .The trust value T_i of the node N_i relating to *PC* is given using the beta probability distribution is given by

$$T_i = \beta(\alpha_{+ve} + \alpha_0, \beta_{-ve} + \beta_0) \tag{8}$$

Where α_0, β_0 is the initial trustworthiness of the nodes.

In the above equation(8), 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

$$P(T_i) = P(\beta(\alpha_{+ve} + \alpha_0, \beta_{-ve} + \beta_0)) = \frac{\alpha_{+ve} + \alpha_0}{\alpha_{+ve} + \beta_{-ve} + \alpha_0 + \beta_0} \tag{9}$$

By equation (9), if any new node N_j joins, then the PC sets

$$\alpha j_{+ve} = \beta j_{-ve} = 0 \tag{10}$$

The above equation (10) reveals the probability of the new node N_j being either honest or malicious.

2.3.3.1 Trusted communication among the PC and the Node

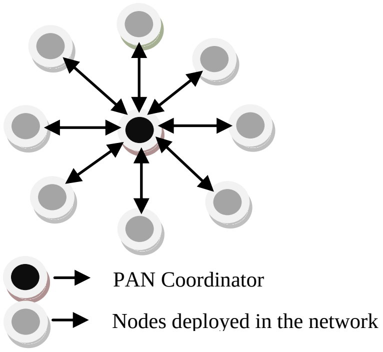


Figure 4. Architecture

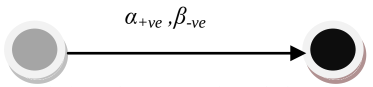
Each node that is keen in performing the channel access initially waits for a pre-defined time period TP (Estimated using equation (9)) and then executes the clear channel evaluation process (E_{CC}) is defined by

$$TP = ramdom(2^{\phi} - 1) * k \qquad (11)$$

Where ϕ the minimum value of the backoff time and k is is the unit of ϕ .If the channel access is busy, then increment ϕ 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 the 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 α_{+ve}^{new} and negative interaction β_{-ve}^{new} of node N_i 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 α_{+ve}^{new} and β_{-ve}^{new} using the following cases.

```
Case 1
    If success_rate > $Th_{+ve}$
    then
    $\beta_{-ve}^{new} = \beta_{-ve} * AF + 1$
    $\alpha_{+ve}^{new} = \alpha_{+ve} * AF$
    end if
Case 2
    If failure_rate> $Th_{\_ve}$
    then
    $\alpha_{+ve}^{new} = \alpha_{+ve} * AF + 1$
    $\beta_{-ve}^{new} = \beta_{-ve} * AF$
    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 success rate is more than the threshold value (Th_{+ve}), negative interaction is incremented representing that the node are malicious. Conversely if the node failure rate is more than threshold value (Th_{-ve}), positive interaction is incremented representing that the node are normal.

2.3.3.2 Attacker classification Algorithm

After prediction, the network identifies the type of DDoS attacks launched by these malicious nodes.

Let k is the size of the data packets.
Let E_c be the energy comparison results .

$$E_c = E_p - E_c \qquad (12)$$

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 Jamming, exhaustion and collision are the set of attacks that energy consumptions are 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 $E_{c.}$ $Ec \in D$ is regarded as the node that launched with the DDoS attack A_i , $i \in \{1,2,3\}$.

Case 1:

$E_c \geq M(E_{Tx} * k + \varepsilon_{amp} * k * d_{\max}{}^2)$, then sensor node N_i is regarded as malicious one launching the jamming attack.

Case 2:

$E_c \leq M(E_{Tx} * k + \varepsilon_{amp} * k * d_0{}^2)$, then sensor node N_i is regarded as malicious one launching the exhaustion attack.

Case 3:

$2(E_{Tx} * k + \varepsilon_{amp} * k * d_0{}^2) \leq Ec \leq (M-1)(E_{Tx} * k + \varepsilon_{amp} * k * d_0{}^2)$, then sensor node N_i is regarded as malicious one launching the collision attack.

The complete process of energy consumption results is done through NS-2 stimulation in the next section.

3. Performance and Evaluation of IEEE 802.15.4

In this section, the DDoS attacks are addressed in the prevision section using NS2 to improve the excellence on the performance of IEEE 802.15.4 LRWPAN.

3.1 Simulation setup

The performance of the proposed fuzzy based detection technique (FBDT) is evaluated using NS2 simulation. A network which is shown is figure 5 is deployed in an area of 50 X 50 m is considered. The IEEE 802.15.4 MAC layer is used for a reliable and single hop communication among the devices, providing access to the physical channel for all types of transmissions and appropriate security mechanisms. The IEEE 802.15.4 specification supports two PHY options based on direct sequence spread spectrum (DSSS), which allows the use of low-cost digital IC realizations. The PHY adopts the same basic frame structure for low-duty-cycle low-power operation, except that the two PHYs adopt different frequency bands: low-band (868/915 MHz) and high band (2.4 GHz). The PHY layer uses a common frame structure, containing a 32-bit preamble, a frame length. The simulated traffic is exponential with UDP source and sink. Table 2 summarizes the simulation parameters used.

Table 2 Simulation Parameters

No. of Nodes (N)	100
Area Size	50 X 50 meter
MAC	IEEE 802.15.4
Simulation Time	25 sec
Transmission Range(r)	100m
Routing Protocol	FBPDS
Traffic Source	Exponential
Packet Size	250 bytes
Transmission Rate	50, 75,100,125 and 150 kb.
Node ratio	50%, 100%
Channel bandwidth	1Mb/s

3.2 Performance Metrics of Detection of DDoS attacks

The performance analysis of our proposed model has been implemented in network stimulation environment by using two criteria. They are true detection rate (TDR) and false positive rate (FPR). TDR indicate the proportion of how often the system successfully detects the attacks from the starting to the ending and the ratio of the number of nodes are correctly identified by the system to be falling under a jamming class (low, medium, high) to the number of nodes as identified, taken out of one hundred. The FPR indicates the proportion of events in which an attack is detected when no real attack exists and the ratio of the number of nodes are incorrectly identified by the system to be falling under detection attack class (low, medium, or high) to the number of nodes as identified, taken out of one hundred. The TDR and FPR can be calculated by using attack detection ratio (ADR).ADR is mathematically defined as: *ADR= (S/C)*100*, where 'S' is the number of nodes successfully jammed by the jammer and the lower cut-off value of the LOA as decided by the base station, where 'C' is the number of nodes covered by the jammer within the communication range. The ADR is defined as the percentage of detected jammed nodes to total nodes in the network. The ADR parameter can be configured as 50% and 100%, and to maintain these ratios, varied numbers of node were located in the network. The stimulation has been repeated with varied topologies and the average values are obtained from the results were recorded.

3.3 Performance Metrics of Energy consumption

Our scheme predicate DDoS attacks by comparing the energy consumptions and the prediction results of s nodes present in the network. The average energy consumption of sensor nodes along the time line is shown in Fig.4, where x-axis presents time and y-axis represents the average energy consumptions of sensor nodes.

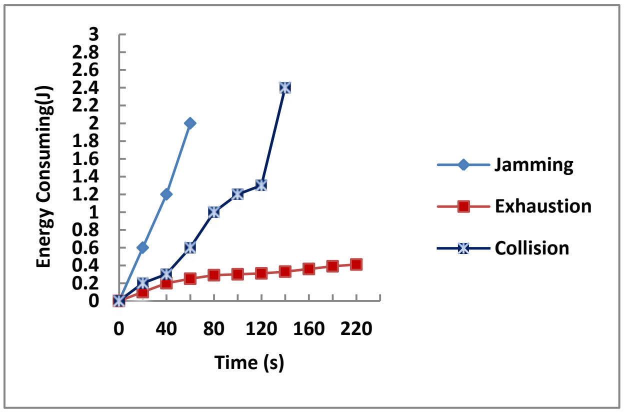


Figure 4: Graphical representation for energy consumption of DDoS attacks

The square dotted line represents the average energy consumed by the nodes launching with *jamming* attacks.

The malicious node maximizes its broadcast range as well as the signal strength. In that case, the energy consumption would be significantly large. As can be seen in Fig.5, the nodes launching *jamming* can only operate 60s.

The square cross represents the average energy consumed by the nodes launching *exhaustion attack*. The packet drop rate is set to 50%. The difference between the prediction results and the average energy consumption of *exhaustion attacks* rises after 60s of the simulation, and FBDPS can detect this attack.

The square-cross line represents the average energy consumed by the nodes launching *collision attack*. The malicious node would create *M* identities with one real identity and *M-1* fake nodes. These entire *M-1* fake nodes are deployed in other clusters and would be actually controlled by the malicious node that launches the *collision attack*. Therefore, the malicious node would spend *M-1* times energy than the predict result.

3.4 Experimental results

3.4.1 DDoS attack detection rate

The value of TDR and FPR for 100 nodes configuration for different types of DDoS attacks and we compare our results TDR and FPR with existing model (em) [16] indices are given in table 3 and table 4. In the table 3 and table 4 shows that our performance parameters indicates good attack detection results and are either better or matching with the existing method of DDoS attack detection. Figure 5a and Figure 5b shows the graphical representation of TDR for 100 nodes configuration for different types of DDoS attacks indices of 50% and 100% and our results TDR % compared with existing model.

Table 3. TDR for 100 nodes configuration for LOA (ADR=50%, ADR=100%) and Comparison of our results TDR % with existing model [EM]

DDoS Attacks	TDR % for 100 nodes configuration			
	ADR 50% (LOA≤50)	ADR 50% (LOA≤100)	EM	FBDT
Jamming	99.55	99.80	94.5	99.8
Exhaustion	99.40	99.60	93.5	99.6
Collision	99.15	99.55	93.2	98.55

Table 4. FPR for 100 nodes configuration for LOA (ADR=50%, ADR=100%) and Comparison of our results FDR % with existing model [EM]

DDoS Attacks	FDR % for 100 nodes configuration			
	ADR 100% (LOA≤100)	ADR 50% (LOA≤50)	EM	FBDT
Jamming	0.02	0.01	0	0
Exhaustion	0.01	0	0.01	0
Collision	0.01	0	0.01	0

3.4.2 Packet delivery Ratio

In our stimulation results after detection of attacks, the packet delivery ratio of PAN coordinator with GTS in collision, exhaustion and jamming are 99.9%, 99.9% and 94% respectively in the figures 6, 7 and 8. With the help of our proposed technique in IEEE 802.15.4 the packet delivery is close to 100%.

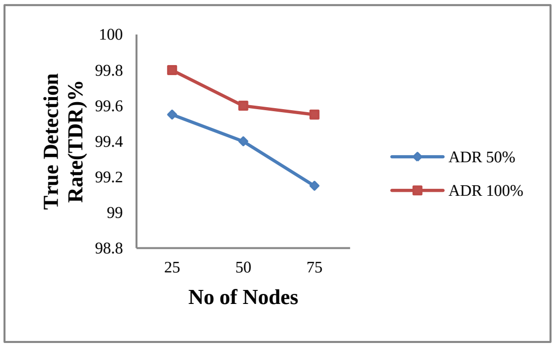


Figure 5a. Graphical representation of TDR % for 100 nodes configuration of ADR=50% and ADR=100%.

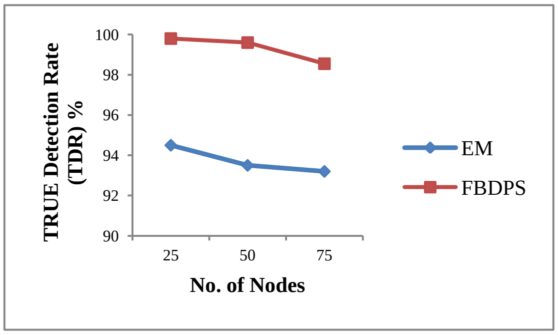


Figure 5b. Graphical representation of TDR % for 100 nodes and compared with existing system

4. Conclusions

We Presented the DDoS attacks in IEEE 802.15.4 MAC layers, the determinant metrics of attack detection, attack prediction and the existing methods of DDoS attacks.. For detection of attacks we select the PDPT and SNR as inputs to our fuzzy interference system which gave the level of attack (LOA) as output. The output has been evaluated based on the neighbor nodes and energy consumption. By stimulation, we then evaluated the attacks detection rate (ADR) performance having average of 99.75% of TDR with 0.01% of FPR, packet delivery ratio also having closely 100% compared with existing system [16] and found that our performance is better in most of the cases in the existing models. For prediction, our proposed scheme adopts the prediction method to predict the malicious nodes based on energy consumption. Finally, the effectiveness of our scheme through stimulation and demonstrated that it can be used to detect and predict the DDoS attacks with enhanced reliability and accuracy.

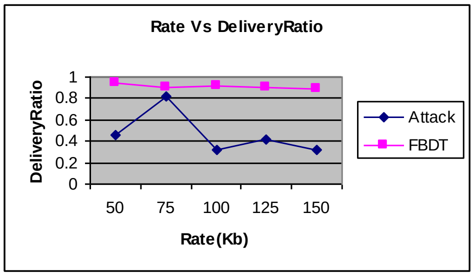


Figure 6. Collision –Packet delivery ratio

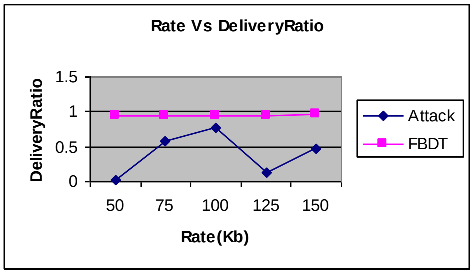


Figure 7. Exhaustion-Packet delivery ratio

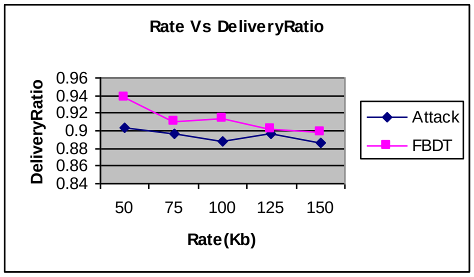


Figure 8 Jamming –Packet delivery ratio

References

[1] Faraz Ahasan, Alizahir(2010) ‘Survey of Survival Approach in Wireless network against jamming attacks’ *Journal of Theoretical and Applied Information Technology*, Vol 30, No.1,pp.55-64, 2010.

[2] Anthony D. Wood, John A. Stankovic, and Gang Zhou ‘DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks’, *IEEE conference on SECON*, Vol.18, No 21, pp. 60-69,USA,2007.

[3] Jianliang Zheng, , Myung J. Lee, , Michael Anshel ‘Towards Secure Low Rate Wireless Personal Area Networks’, *IEEE Transactions on Mobile Computing*, Vol. 20, No. 20,2010.

[4] R. Negi and A. Perrig ‘Jamming analysis of MAC protocols’, *Carnegie Mellon Technical Memo*, Vol23, No 4, pp. 77-83,2003.

[5] Y. Law, L. Hoesel, J. Doumen, P. Hartel, and P. Havinga ‘Energy efficient link-layer jamming attacks against wireless sensor network MAC protocols’, *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, pp. 76–88, Nov 2005

[6] B. Yu and B. Xiao ‘Detecting selective forwarding attacks in wireless sensor networks’, *In Proceedings of 20th International Parallel and Distributed Processing Symposium IPDPS* ,pp: 1–8,2006.

[7] B. Xiao, B. Yu, and C. Gao, ‘Chemas: Identify suspect nodes in selective forwarding attacks’, *Journal of Parallel and Distributed Computing (JPDC - Elsevier)*, pp. 1218–1230, 2007.

[8] Faraz Ahasan, Alizahir ‘Survey of Survival Approach in Wireless network against jamming attacks’ *Journal of Theoretical and Applied Information Technology*, Vol 30, No.1,pp.55-64, 2010

[9] B. Xiao, B. Yu, and C. Gao ‘Chemas: Identify suspect nodes in selective forwarding attacks’, *Journal of Parallel and Distributed Computing (JPDC - Elsevier)*, pp. 1218–1230, 2009.

[10] A. El-Semary, J. Edmonds, J. Gonzalez-Pino, M. Papa ‘Applying Data Mining of Fuzzy Association Rules to Network Intrusion Detection’, *In Proc. of IEEE Information Assurance Workshop*, pp.100-107, 2006.

[11] N. Liao, S. Tiana, T. Wanga ‘Network forensics based on fuzzy logic and expert system’, *Journal of Computer Communications*, Vol. 32, No. 17, pp. 1881-1892, 2009

[12] M. Mohajerani, A. Moeini ‘An Approach to a New Network Security architecture for Academic Environments’, *Springer-Lecture Notes in Computer Science*, Vol.2434, pp.252-260, 2002

[13] A. Sodiya, S. Onashoga, B. Oladunjoye ‘Threat Modeling Using Fuzzy Logic Paradigm’, *Issues in Informing Science and Information Technology* Vol 4, pp. 53-61., 2007.

[14] J. H. Kim, T. H. Cho ‘Interleaved Hop-by-Hop Authentication using fuzzy logic to defend against of False Report Injection by Replaying an attack’, *International Journal of Computer Science and Network Security*, Vol. 9, No.7, pp. 91-96.2009

[15] Hang Liu, Hairuo Ma, Magda El Zarki, and Sanjay Gupta , ‘Error control schemes for networks: An overview’, *International* Journal *of Mobile Networks and Applications*, Vol.2, No.2, pp.167-182 .2007

[16] Cakiroglu M, Ozcerit A.T ‘Jamming detection mechanisms for wireless sensor networks’. *in Proceedings of the 3rd International Conference on Scalable Information Systems*, pp:04-06 ,Italy,2008.

[17] Vullers, R. J. M., Schaijk, R.V., Visser, H. J., and Penders, J. H. Energy Harvesting for Autonomous Wireless Sensor Networks. IEEE Solid-State Circuits Magazine. 2, 2, 29- 38, 2010.

[18] Ries, Sebastian(2009), ‘Extending Bayesian trust models regarding context-dependence and user friendly representation’, *in Proceedings of the 2009 ACM symposium on Applied Computing*, pages 1294-1301, NewYork, NY, USA,

[19] C.Balarengadurai, S Saraswathi, “A Fuzzy based Detection Technique for Jamming Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network” *in proceedings of Advances in Intelligent Systems and Computing-Springer Verlag-LNEE*, pp: 422-433,2012.

[20] C.Balarengadurai, S Saraswathi, "Detection of Exhaustion attacks over IEEE 802.15.4 MAC Layer using Fuzzy systems*" IEEE Conference on ISDA,* pp: 527-532,2012.

[21] C.Balarengadurai, S Saraswathi, "Fuzzy logic-based detection of DDoS attacks in IEEE 802.15.4 low rate wireless personal area network*" Int. J. Trust Management in Computing and Communications, Vol. 1, Nos. 3/4, pp:* 243-260,*2013.*

[22]Jang, J.S.R.; Sun, C.T.; Mizutani, E(2007). 'Neuro-Fuzzy and Soft Computing: A Computational Approach to Learning and Machine Intelligence', *Dorling Kindersley (India) Pvt. Ltd.: pp: 99-115, 2011.*

[23]V. Rodoplu, and T. Meng, "Minimum energy mobile wireless networks," *IEEE J. S elected Areas in Communications, vol. 17,no. 8, pp. 1333-1344, Aug 2008*.

[24] Salman A. Khan, Zubair A. Baig, "On the Use of Unified And-Or Fuzzy Operator for Distributed Node Exhaustion Attack Decision-making in Wireless Sensor Networks" *IEEE Transaction on Fuzzy systems, PP: 978-987,2010.*

[25] Sheng Jie Tang Liangrui "A Triangle module operator and Fuzzy Logic Based Handoff Algorithm for Heterogeneous Wireless Network"*12thIEEE International Conference on Communication Technology*, *ISBN:978-1-4244-6868-3, pp: 448-451, 2011.*

[26] Sudip Misra , Ranjit Singh ,S. V. Rohith Mohan "Information Warfare Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System" *Sensors open access Vol:10, PP:3444-3479; doi:10.3390/s100403444, 2010*.

Biographical notes

Mr. C. Balarengadurai received his B.Tech in Information Technology from Anna University Chennai, M.Tech in Information Technology from Sathyabama University Chennai and pursing his Ph.D in Manonmaniam Sundarnar University Tirunelveli, Tamilnadu. He is working as Associate professor in Computer Science & Engineering at Aurora's Engineering College, Bhongir. His area of interest includes Computer Networks, Compiler Design, and Artificial Intelligence and Wireless Networks. He is a life member of ISTE, IE, and member of IEEE and CSI.

Dr. S Saraswathi received her B.Tech in Computer Science and Engineering from Pondicherry Engineering College, Puducherry, M.Tech in Computer Science and Engineering from Pondicherry University, Puducherry and Ph.D in Speech Processing form Anna University Chennai., She is working as professor in Information Technology Pondicherry Engineering College, Puducherry. Her research area includes Speech Processing, Natural Language Processing, and Artificial Intelligence and Wireless Networks. She published 36 papers in national and International Conference, 30 papers in various Journals like IEEE, Springer, ACM, Elsevier and etc. She is a member of IEEE, CSI, ISTE and IE.