CHAPTER 3

SECURE RPL TRUST MECHANISMS AGAINST DDOS ATTACKS OVER IOT

Chapter 3 deals with the design of two Trust based DDoS detection mechanisms in the RPL network. The TDD mechanism explains the data frequency based detection methodology with a trust calculation for identifying a DOS attack on the RPL network. The SLTD based detection methodology explains about the accurate DDoS attack detection using subjective logic and trust calculation. This chapter also discusses the performance comparison of both the detection mechanisms with their respective existing schemes.

3.1 Effect of DDoS Attack in RPL network

In the era of modern information technology, there is an immense growth of the Internet of Things (IoT) with the diverse applications that are augmented efficiently (Li et al., 2015). However, the IoT devices and applications face many vulnerabilities and are threatened to be attacked by malicious nodes (intruders) (Conti et al., 2018). One of the dangerous attacks is DOS attacks that create a flood in the server by continually sending false requests. When multiple users create this attack for targeting the network from different locations, such an attack is identified as a distributed denial-of-service attack (DDoS) (Peraković et al., 2015). The basic idea of DDoS attack is that the malicious node manipulates the source route header of the received packets, and then generates and sends a large number of invalid packets to the targeted node, which causes the legitimate nodes to accept the received packets leading to significant energy consumption and node failures. As a result of node failures, a significant number of

packets are dropped by legitimate nodes, which exhausts the network performance in terms of communication bandwidth and node energy (Mahjabin et al., 2017).

3.1.1 Role of Trust in Attack Detection

The easily deployed DoS attack has a considerable impact on IoT devices compared to other cyber-attacks. There is a requirement of a reliable and robust security mechanism for detecting these attacks. IoT has enormous benefits in the emerging smart applications, and the security uncertainty is also proliferating due to its open-mindedness. Even though, several security mechanisms such as authentication procedures and access control mechanisms are implemented. These conventional schemes are no longer suitable for addressing the security problems of the distributed system due to its lack of supporting scalability and center-dependence (Zhang & Green, 2015). On the other hand, trust is a conceptual idea that helps to make prominent decisions for different types of IoT devices, whether they belong to homogeneous and heterogeneous networks (Zhang & Vasilakos, 2014). Many researchers consider trust management as one of the possible solutions to a loT security. In IoT, trust management plays a crucial role in ensuring security throughout the network (yan et al., 2017). Therefore, assuring trustability among nodes helps in trustworthy data fusion and mining, qualified services, and improved user's information security and privacy.

3.2 Trust based DDOS Attack Detection (TDD)

The growth in the popularity of IoT devices has to lead to significant threats to security, which opens the door to new security attacks in the network. One of the prominent attacks is DDoS attacks that degrade the network performance by flooding fake data packets from different sources to the gateway node (Kamgueu et al., 2017). In RPL protocol, for constructing a Destination-Oriented Directed Acyclic Graph (DODAG), certain objective functions, metrics, and conditions are applied for computing the best route. As RPL allows data traffic through multiple routes, it enables the network to carry the traffic with a different set of necessities at the same time. The DDoS attacks utilize this opportunity to perform malicious activities in the network (Tomic & McCann, 2017). There are several security mechanisms implemented for

detecting malicious activities of DDoS attacks in the network. Among them, trust-based detection mechanisms help in detecting malicious behavior of nodes with the certainty of separating the legitimate nodes from the malicious ones in the network.

3.2.1 TDD Protocol Overview

The proposed TDD mechanism constructs a trust based detection model for detecting DDoS attacks in the RPL network. Each node monitors the neighbor nodes by counting the number of incoming data packets from the source and thereby checking whether the value crosses the assigned threshold. The neighbor nodes of the source nodes use the overhearing concept to determine the incoming packets, and trust is estimated based on whether the node sends the incoming packets within the assigned threshold. Then the neighboring nodes send the node list which has a low trust value in the form of alarm to the gateway nodes. Then, the gateway nodes estimate the data frequency-based trust determination for detecting the DDoS attack in the network. Then, the gateway nodes send the malicious node list to all the nodes for dropping the malicious data packets sent by the attacker nodes. Therefore, the proposed model accurately detects the DDoS attacker in the network with better energy consumption and network lifetime.

3.2.2 Trust Evaluation and Attack Detection

The proposed methodology evaluates initial trust calculation through neighboring nodes, and the gateway node performs final decision making. Initially, the gateway node assigns the trust value of all the nodes as one. Then, the gateway node estimates the number of incoming packets for a specified interval and determines the assigned threshold. The number of data packets generated for a fixed time interval is termed as data frequency (dF_o). The number of packets received for a fixed period is also calculated. This period is utilized for constructing the DoDAG structure, where it is equal to the three-time of the DIO message broadcasting interval of the DODAG information object (DIO) message. Then the data frequency is estimated using equation 3.1

$$DF_o = t * (\text{Packets generated per second}) \quad \ldots (3.1)$$

For instance, consider a scenario where the nodes generate five packets per second. The overall period is 200 seconds, and the DIO message broadcasting interval is 10 seconds. Let 50 packets be generated by a node in 't' time. However, it is assumed that the attacker nodes perform a spurious transmission and sends the data packets above the estimated packets. These nodes which have crossed the data frequency rate are identified and marked in the gray list by the gateway node.

Final decision making and Attack Detection: The gateway nodes place the nodes that show malicious behavior on the gray list before initiating the next DIO broadcast. The process is continued for three rounds, and the malicious nodes are updated in the gray list. Then for detecting the DDoS attacker, the following equation is applied to each node in the gray list.

$$\text{Attack Possibility}_n = 1 - \left\{\left(DF_o * (|i| + 1) / \sum_{i=1} DF_i\right)\right\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.2)$$

Then, after calculating equation 3.2, the nodes that have attack possibilities greater than zero are placed in the block list with the updated trust value. Then for each node in the block list, the following equation is calculated in determining the current trust value.

$$\text{Current Trust}_n = \text{Previous Trust}_n - \text{Attack Possibility}_n \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.3)$$

From equation (3.3), the nodes that have a trust value less than one are termed as untrusted nodes. These untrusted nodes are attached to the DIO message and broadcasted to all the nodes, which in turn drops the data packets sent by the attacker nodes.

3.3 Performance Evaluation of TDD

The proposed TDD mechanism implements a data frequency-based DDoS attack detection for improving the accuracy and performance of the system. The proposed methodology is compared with the packet frequency-based DDoS attack detection mechanism (Chen et al., 2016). The performance evaluation is carried out in the Contiki 3.0 operating system. The Proposed

technique calculates data frequency for determining the possibility of an attack. Initially, the gray list is maintained by the gateway, and after checking thrice, the block list is created consisting of DDoS attacker nodes. This technique is also capable of detecting attackers with accuracy and discarding their data packet for reducing its impact on the network. All the decision is performed by the gateway node instead of neighboring nodes. The gateway node is assumed to have higher energy compared to other nodes in the network, and hence they have less chance to be affected.

3.3.1 Simulation Setup and Performance Metrics of TDD

The proposed methodology is implemented using the Cooja simulator in the Contiki operating system. The TDD methodology is constructed in a 150 m^2*150m^2 grids with varying nodes in terms of 30, 40, and 50 nodes. The communication range of each node is set to 50m, and the total simulation runs for 5 minutes. Every node transmits the data in an interval of 20s with a size of 127 bytes. The 802.15.4 MAC layer protocol and Two Ray Ground propagation model are used in MAC and Physical layer respectively. The performance of the proposed methodology is evaluated based on the performance metrics such as power consumption, throughput, detection accuracy, and routing overhead. The performance metrics are defined as follows

Detection accuracy: It is defined as the number of attacker nodes detected to the total number of attackers actually present in the network.

Throughput: It is defined as the total number of data packets delivered in simulation time.

Overhead: It is defined as the number of control packets involved in the data transmission process.

Power Consumption: It is the amount of power consumed by nodes to deliver packets from source to destination.

Table 3.1: Simulation Parameters for TDD Mechanism

Simulator	Cooja
Number of Nodes	31,41,51
Area	150m x 150 m

Communication Range	50m
Data Transmission Interval	20 s
Data packet size	127 bytes
Transport Layer Agent	UDP
MAC	802.15.4
Simulation Time	5 minutes

3.3.2 Simulation Results of TDD

The performance analysis between the proposed TDD mechanism and the Packet frequency-based attack detection mechanism is performed. The performance metrics such as detection accuracy, overhead, energy consumption, and throughput are placed in the y-axis while the Number of attackers varied in the form of 1 attacker, 2 attackers, and 3 attackers are placed in the x-axis. The simulation results are obtained by varying the number of nodes in terms of 31 nodes, 41 nodes, and 51 nodes.

Number of Attackers Vs. Detection Accuracy: The simulation results in terms of detection accuracy are shown in Figure 3.1, Figure 3.2, and Figure 3.3 for the proposed scheme and existing PFDD scheme, which is obtained for different node variations of 31 nodes, 41 nodes, and 51 nodes respectively.

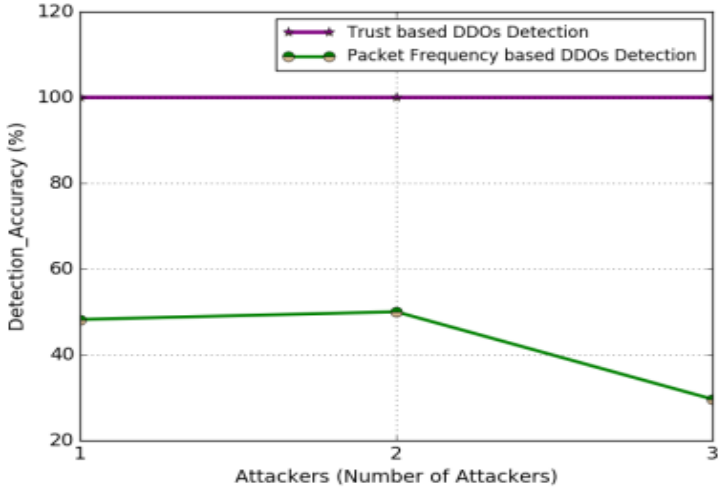

Figure 3.1: Number of Attackers Vs. Detection Accuracy for 31 Nodes

Figure 3.1 presents the performance of the proposed TDD mechanism with the Packet frequency detection mechanism in terms of detection accuracy for 31 nodes. Figure 3.1 show that the proposed TDD scheme maintains 100% detection accuracy even when the number of attackers is increased from 1 attacker to 3 attackers. Whereas, the existing Packet frequency based detection mechanism exhibits a poor detection accuracy and decrease in performance when the attackers are increased. Similarly, Figure 3.2 and Figure 3.3 prove the proposed scheme shows better performance in terms of detection accuracy even when the number of nodes is increased. The proposed mechanism outperforms in terms of detection accuracy as the detection mechanism considers two sets of the list, such as gray list and block list based on the number of incoming packets and data frequency for detecting the attacker nodes, which improves the accuracy. However, the existing scheme does not define a proper threshold for determining the DoS attacker, leading to the misdetection of legitimate nodes as attacker nodes.

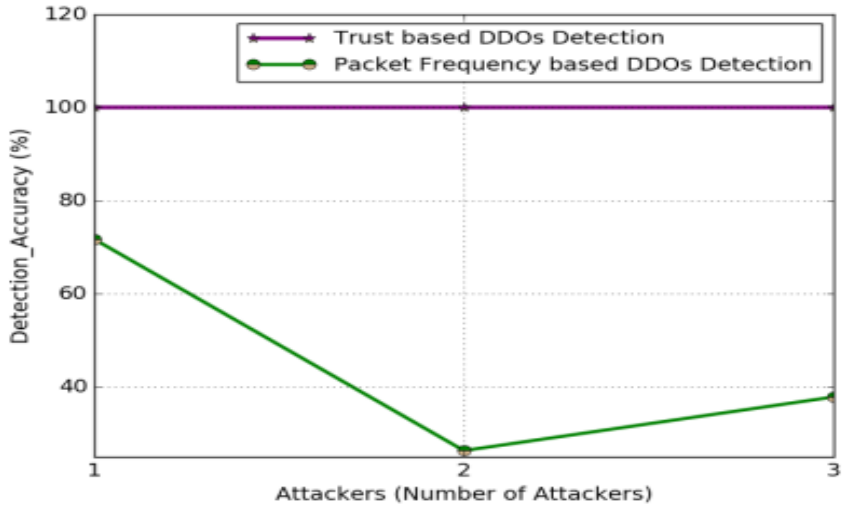

Figure 3.2: Number of Attackers Vs. Detection Accuracy for 41 Nodes

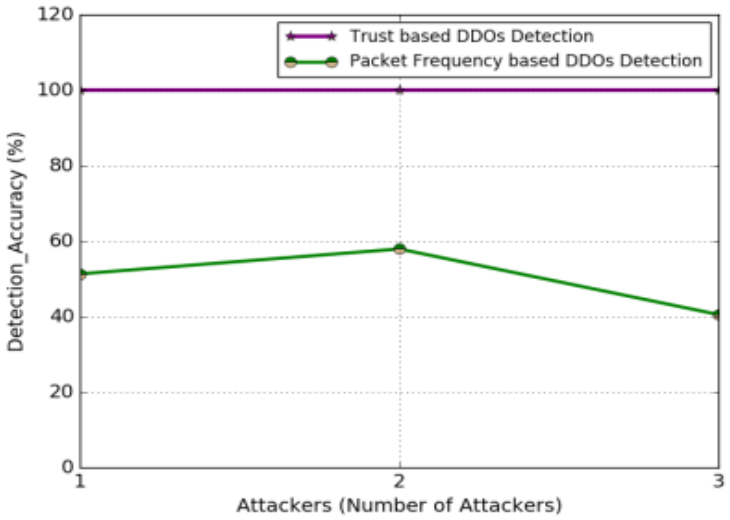

Figure 3.3: Number of Attackers Vs. Detection Accuracy for 51 Nodes

Number of Attackers Vs. Throughput: Figure 3.4, Figure 3.5 and Figure 3.6 present the performance comparison of metrics in terms of throughput between the proposed TDD mechanism and packet frequency-based attack detection mechanism for 31 nodes, 41 nodes, and 51 nodes deployed network environment respectively. Figure 3.4 shows the proposed TDD mechanism exceeds the existing packet frequency-based attack detection by 85 bps approximately in the network scenario of 31 nodes with 3 DDoS attackers.

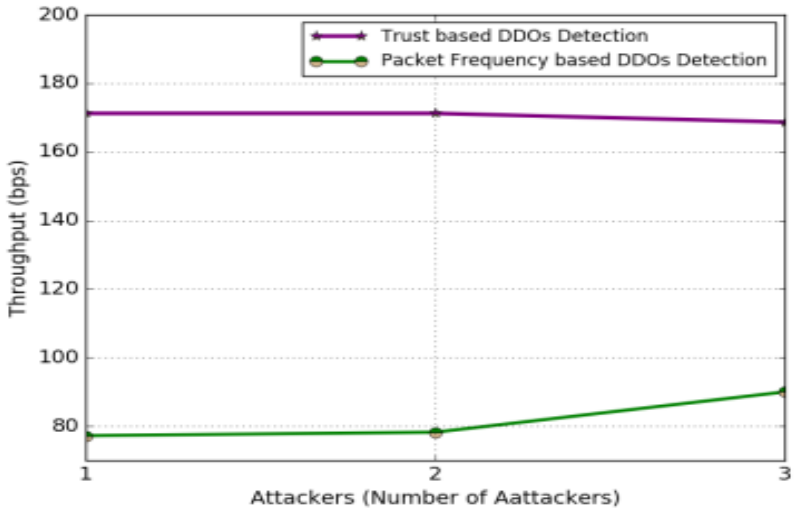

Figure 3.4: Number of Attackers Vs. Throughput for 31 Nodes

In Figure 3.5 and Figure 3.6, the proposed TDD mechanism provides a better throughput for varying attackers compared to the existing methodology. The throughput of the proposed scheme is higher compared to the existing packet frequency based detection methodology as the accurate detection of the DDoS attacker on the network reduces the chances of node failures and frequent data dropping. In contrast to the proposed scheme, the existing Packet frequency based detection scheme fails to provide a better throughput as the neighbor nodes lack in detecting the attacker nodes accurately, and false detection of legitimate nodes as attacker nodes leads to the dropping of normal packets.

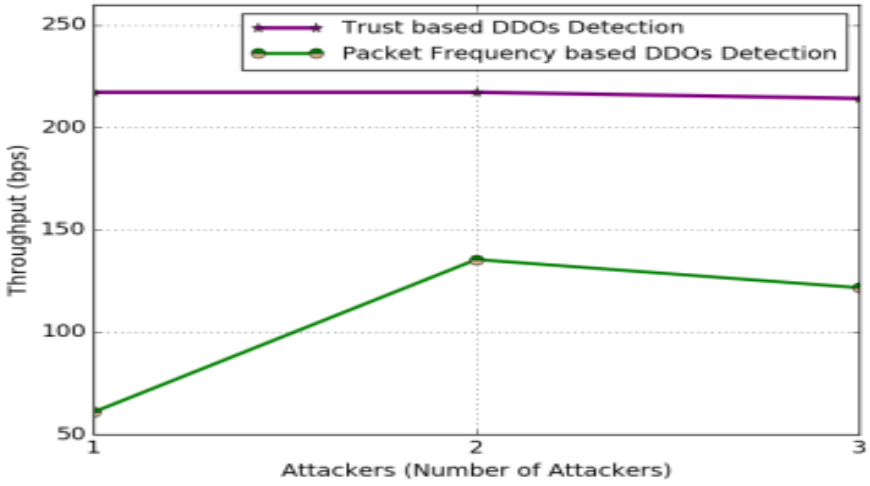

Figure 3.5: Number of Attackers Vs. Throughput for 41 Nodes

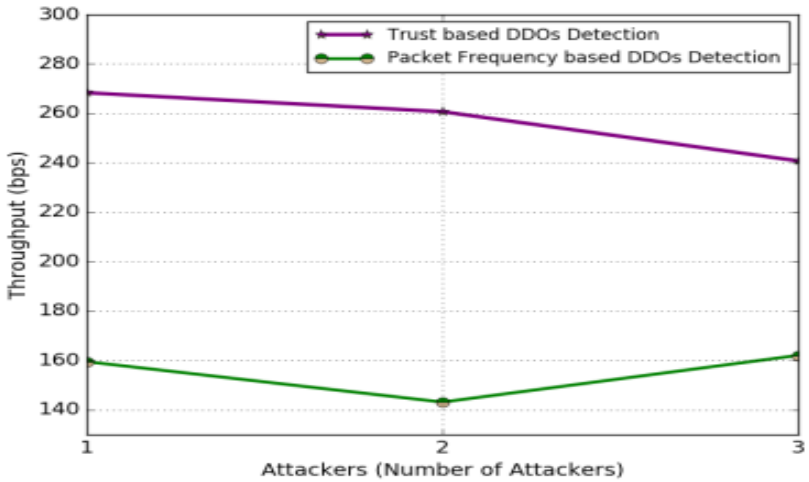

Figure 3.6: Number of Attackers Vs. Throughput for 51 Nodes

Number of Attackers Vs. Overhead: Figure 3.7, Figure 3.8, and Figure 3.9 show the performance analysis of the proposed scheme by comparing it with the existing packet frequency-based attack detection mechanism using overhead metrics. In the 31 nodes based network scenario, as shown in figure 3.7, the proposed mechanism shows a lesser number of control packet exchanges compared to the existing mechanism. As the proposed scheme uses neighbor nodes for initial calculation, and gateway nodes perform final decision making, the number of control packets exchanged is slightly increased with the increasing attacker nodes in the network.

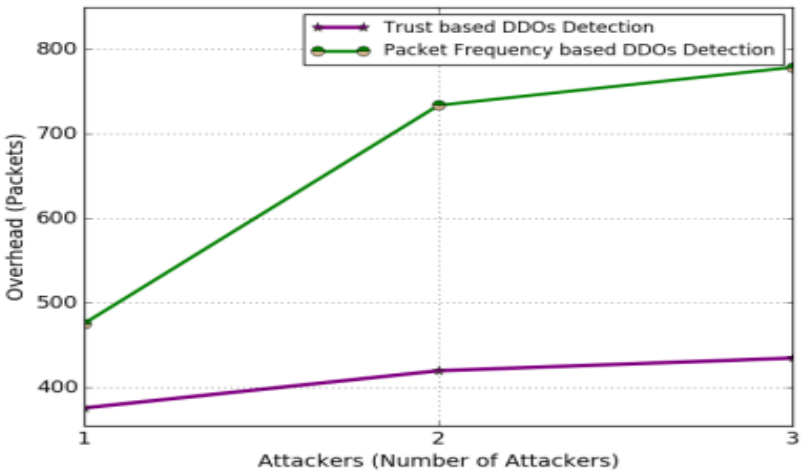

Figure 3.7: Number of Attackers Vs. Overhead for 31 Nodes

Whereas, existing scheme shows poor performance in terms of overhead. The reason is that the neighbor nodes perform packet frequency-based attack detection, and also the inability to accurately detecting the attacker nodes leads to large control packet exchanges.

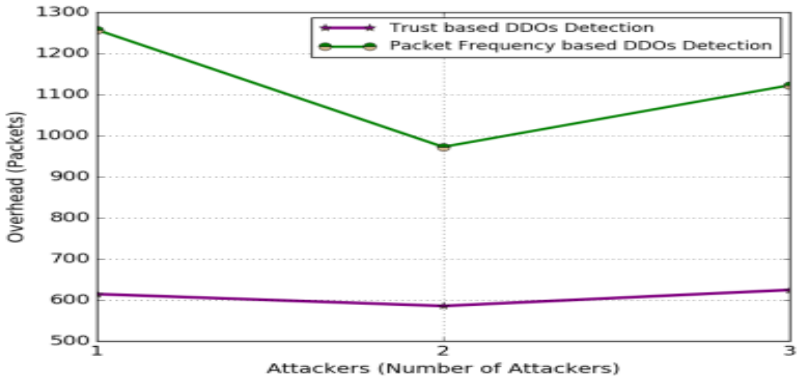

Figure 3.8: Number of Attackers Vs. Overhead for 41 Nodes

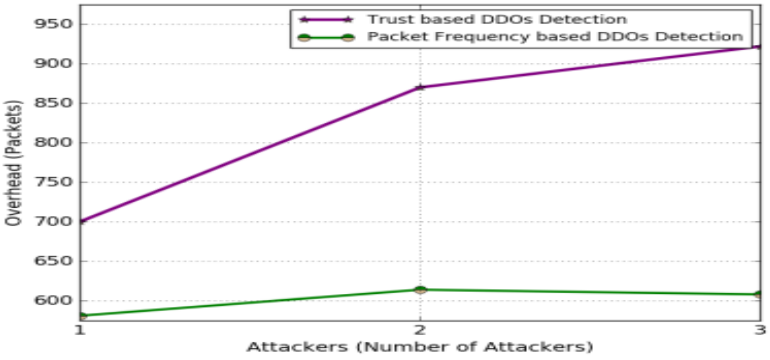

Figure 3.9: Number of Attackers Vs. Overhead for 51 Nodes

Similarly, in Figure 3.8 and Figure 3.9, when the number of nodes is increased, overhead is gradually increased in both proposed and existing DDoS attack detection scheme. Both these attack detection mechanisms require neighbor nodes to monitor parameters for the final decision making procedure, and as more nodes are added to the control packets generated are also increasing.

Number of Attackers Vs. Power Consumption: Figure 3.10, Figure 3.11, and Figure 3.12 shows the performance comparison in terms of power consumption between the proposed TDD mechanism and Packet frequency-based attack detection for different node densities

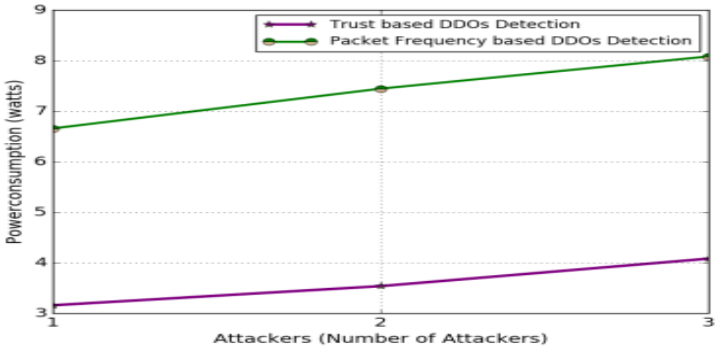

Figure 3.10: Number of Attackers Vs. Power Consumption for 31 Nodes

Figure 3.10 shows that the power consumption of the proposed scheme is better compared to the existing scheme, and both these detections exhibiting a gradual increase in power consumption with increasing attacker nodes. For a growing network environment with 41 nodes and 51 nodes respectively, as shown in Figure 3.11 and Figure 3.12, the power consumption is maintained low by the nodes in the proposed TDD mechanism compared to the existing packet frequency-based attack detection. As in the proposed TDD mechanism, the gateway node performs the final decision making, and hence the neighboring nodes exhibit less power consumption. However, the existing packet frequency based detection is performed mainly by neighboring nodes, and heavy computation, in turn, increases the power consumption.

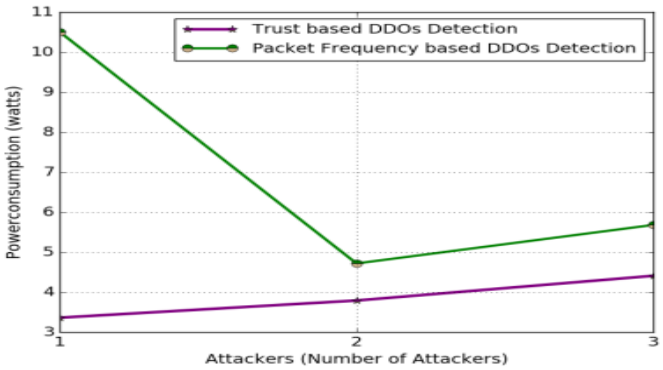

Figure 3.11: Number of Attackers Vs. Power Consumption for 41 Nodes

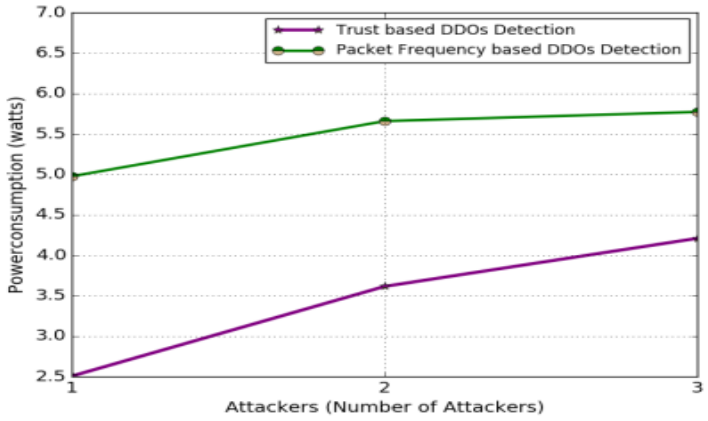

Figure 3.12: Number of Attackers Vs. Power Consumption for 51 Nodes

3.4 Subjective Logic-based Trust Mechanism against DDoS (SLTD)

The subjective logic-based trust mechanism is adopted for detecting DDoS attacks in the network. The subjective logic is suited for detection mechanisms as it designs uncertainty models with possible positive and negative statements. In a subjective logic-based trust model, trust relationships are mainly defined by the reliability and the evaluation composes of three components, mainly belief, disbelief, and uncertainty with respective probability for expressing the trust degree. The advantage of subjective logic is that it models the situations more realistically providing conclusions with accurately reflecting the uncertainty using the evidence that is collected from different observers. The subjective logic uses a dynamic base rate operator for presenting the expectation of an opinion. The base rate is an essential parameter of subjective logic, as distinctly collected evidence helps in providing an expected level of opinion overcoming the uncertainty.

3.4.1 SLTD protocol Overview

The subjective logic-based trust approach against DDOS attacks is proposed for IoT. In the SLTD protocol, direct and indirect trust value calculation is performed by the neighboring nodes, and the gateway node performs final decisions. For calculating direct trust and indirect trust, the number of incoming packets is monitored by the neighboring nodes. The nodes that send the incoming packets exceeding a specific limit are sent in the form of an alarm to the gateway node.

Then, the gateway node performs the final trust calculation based on subjective logic for determining the DDoS attack. The trusted nodes or attacker nodes detected are broadcasted to all the nodes in the network. The proposed scheme adopts the subjective logic for generating and adjusting the trust values for each sensor node, according to node observations. Finally, the attacker node is detected by using threshold value and total trust value.

3.4.2 Subjective Logic-based Trust Evaluation

Trust estimation is performed in the form of two phases, such as the initial trust calculation and subjective logic-based attack detection. In the SLTD protocol, during data transmission, each node counts the number of incoming packets and it measures the trust value of the source based on the number of packets crossing the assigned threshold. As the attacker source generates a number of packets exceeding the limit, the automatically direct trust value estimate of the attacker source by the router node gets decreased.

$$\text{Direct Trust} = 1/\text{Number of packets crossing the limit} \ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.4)$$

The neighbor nodes monitor the routing behavior of the source node by overhearing the data transmission between the source node and the router. Trust is calculated by considering the monitored information, which is the number of data packets crossing the limit. The nodes that have an increasing number of data packets generated above the threshold value have indirect trust that gets reduced simultaneously. The neighbor nodes which perform the indirect trust computation send node list with the reduced trust value to the gateway node. Finally, the gateway calculates the final trust using subjective logic and broadcast the information about the attacker node to all the nodes in the network. The nodes receiving the broadcast maintain the list and drop the data packet that comes from an attacker source without forwarding it. It minimizes unnecessary network traffic and energy consumption.

3.4.3 DDOS Attack Detection

Consider the node a and b be the neighboring nodes of the node. Let 'Ev' denotes the evidence, and it is categorized as belief, disbelief, and uncertainty. Belief represents the genuine of the node's behavior and disbelief represents the malicious behavior of the node. Uncertainty represents the unpredictable behavior of the node s. Both the positive evidence trust (PE_T) and trust based on negative evidence (NE_T) are calculated.

Trust is estimated using positive evidence as follows:

$$PE_T = b_s^a u_s^a + b_s^b u_s^b / k \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots . . (3.5)$$

Trust is estimated using the negative evidence as follows,

$$NE_T = b_s^a u_s^a + b_s^b u_s^b / k \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots . \dots\dots . . (3.6)$$

where, $k = u_s^a + u_s^b - u_s^a u_s^b$

b_s^a -The belief of node a on node s

d_s^a -The disbelief of node a on node s

u_s^a -Uncertainty of node a on node s

If the node exhibits substantial wrong evidence, then the trust is estimated based on equation 3.6, and it represents the attacker nodes. Similarly, if the number of positive evidence is greater, then the trust is estimated based the equation 3.5. Finally, the trust with reduced value is detected as the DDoS attacker and the data packets arriving from those nodes are simply discarded without forwarding.

3.5 Performance Evaluation of SLTD

The proposed methodology designs a subjective logic-based trust calculation for detecting DDoS attackers with high accuracy and improved performance. In SLTD, the initial trust calculation is performed by the neighboring nodes and the subjective logic-based attack detection is performed by the gateway nodes. The proposed model is implemented in the Cooja simulator in the Contiki operating system. In the proposed approach, trust calculation is based on the subjective logic and attackers in both source nodes and neighboring nodes are determined. Hence, data flooding through the attacker neighbor is blocked. However, the drawback of the existing detection approach is that the attackers posing as the neighboring nodes are undetected which in turn

affects performance. The performance of the proposed methodology is compared with the RPL network-based Intrusion detection scheme without the application of subjective logic.

3.5.1 Simulation Setup and Performance Metrics of SLTD

The proposed SLTD methodology is constructed in a random topology environment with 31, 41, and 51 nodes using the Cooja simulator. The nodes are deployed in an area of 500m*500m with a communication range of each node set to 50 m. The performance of the SLTD is compared with the detection mechanism without subjective logic based on performance metrics such as detection accuracy, throughput, routing overhead, and energy consumption.

Table 3.2: Simulation Parameters of SLTD

PARAMETERS	**VALUES**
Number of Nodes	31,41,51
Area	500m x 500m
Communication Range	50m
Routing Protocol	RPL
Transport Agent	UDP
Simulation Time	60seconds

Detection Accuracy: It is defined as the ratio of the number of attacker nodes that are detected by the number of attacker nodes present in the network.

Detection Accuracy = Number of attacker nodes detected/ Total number of attacker nodes

Power Consumption: It is defined as the power consumed by the nodes in the network for transferring data packets to the destination.

Throughput: It is defined as the rate of data delivered successfully at the destination. It is expressed as bits per second.

Routing Overhead: The total number of control packets transmitted during the data transmission. It is represented in terms of packets.

3.5.2 Simulation Results of SLTD

The performance of the proposed subjective logic-based intrusion detection mechanism and intrusion detection mechanism without subjective logic is compared based on performance metrics such as detection accuracy, overhead, throughput and energy consumption by varying the nodes in terms of 31, 41, and 51 nodes over a 500m* 500m environment. The number of attackers is varied in the x-axis, while the performance metrics are varied in the y-axis.

Number of Attackers Vs. Detection Accuracy: Figure 3.13, Figure 3.14, and Figure 3.15 shows the performance in terms of detection accuracy between proposed intrusion detection with subjective logic and intrusion detection mechanism without the application of subjective logic. In Figure 3.13, the proposed subjective logic-based intrusion detection mechanism exhibit a 100% detection accuracy, whereas the existing scheme shows a poor detection accuracy as the number of attacker nodes is increased.

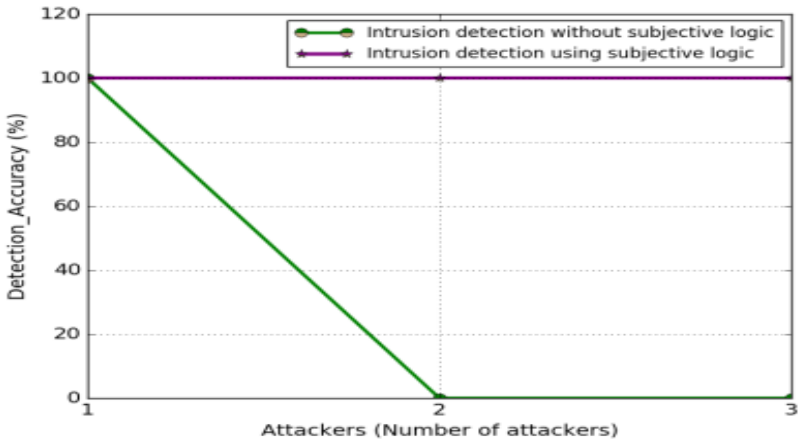

Figure 3.13: Number of Attackers Vs. Detection Accuracy for 31 Nodes

The proposed scheme maintains constant detection accuracy with increasing nodes from 41 to 51 nodes, as shown in Figure 3.14 and Figure 3.15, respectively.

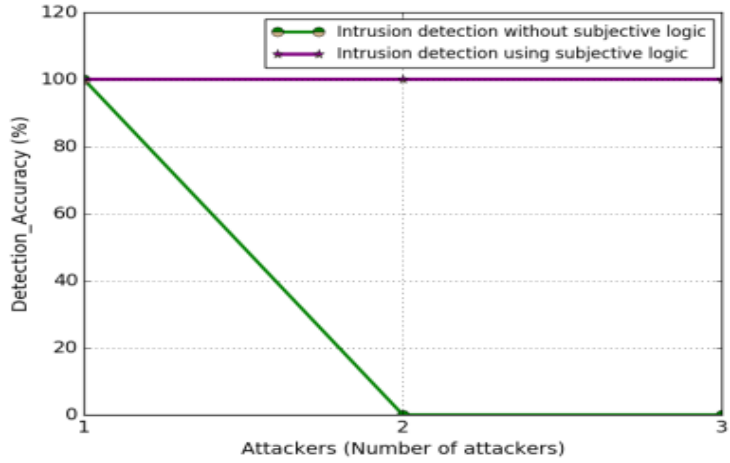

Figure 3.14: Number of Attackers Vs. Detection Accuracy for 41Nodes

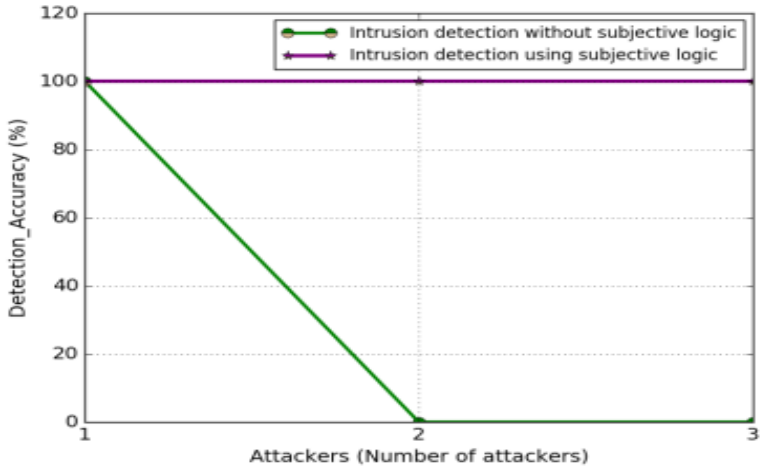

Figure 3.15: Number of Attackers Vs. Detection Accuracy for 51 Nodes

As the proposed scheme adopts the subjective logic for detection techniques, the attacker nodes in the network are accurately detected without any falsely detected normal nodes. However, the intrusion detection based attack detection mechanism detects the attacker nodes based on only the direct and indirect trust values. The direct and indirect trust calculation considers only the incoming data packets for determining the trust value, and hence the false detection of normal nodes as attacker nodes is high in the existing scheme.

Number of Attackers Vs. Throughput: In Figure 3.16, Figure 3.17 and Figure 3.18, the performance results in terms of throughput for the proposed intrusion detection scheme with subjective logic mechanism and intrusion detection mechanism without subjective logic.

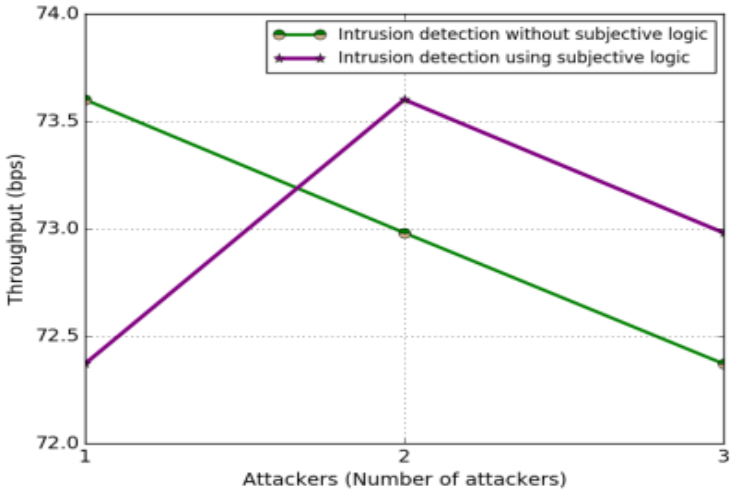

Figure 3.16: Number of Attackers Vs. Throughput for 31 Nodes

The proposed scheme shows a slight decrease in throughput compared to the intrusion detection mechanism without subjective logic in the presence of a single attacker, as shown in Figure 3.16. However, as the number of attackers is increased the proposed scheme shows a better throughput as the accurate detection of attackers helps in smooth transmission in the RPL network. In Figure 3.17, the performance is dynamic variation in throughput in the network scenario with 41 nodes. The proposed mechanism works better in multiple attacks, whereas the intrusion detection mechanism without subjective logic works well with single attacks.

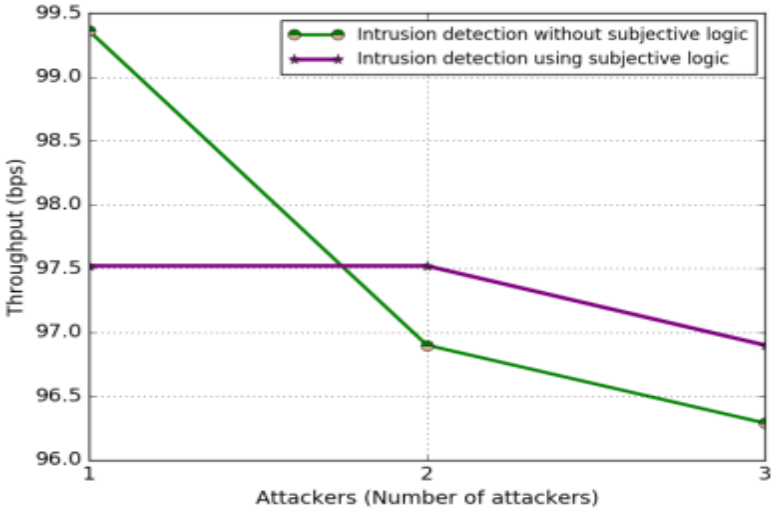

Figure 3.17: Number of Attackers Vs. Throughput for 41 Nodes

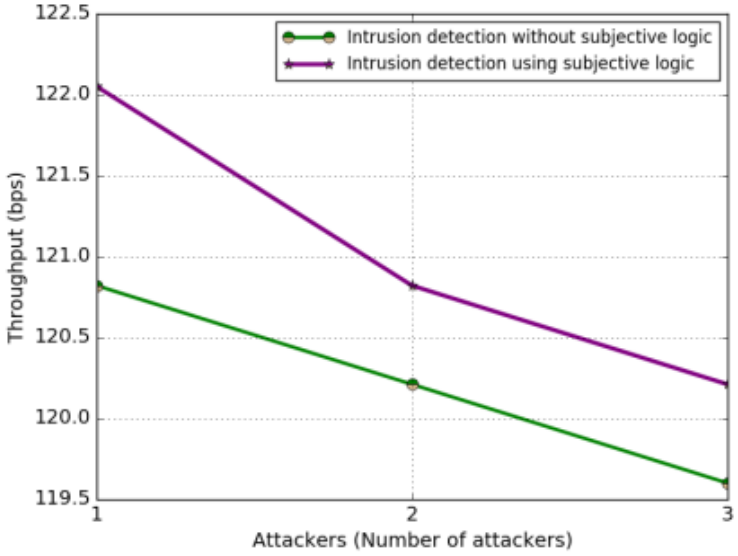

Figure 3.18: Number of Attackers Vs. Throughput for 51 Nodes

As the number of nodes is increased to 51 nodes, as shown in Figure 3.18, the performance in terms of throughput is improved in the proposed intrusion detection mechanism compared to the Intrusion detection without subjective logic.

Number of Attackers Vs. Overhead: Figure 3.19, Figure 3.20, and Figure 3.21 presents the performance results in terms of overhead for the proposed intrusion detection with subjective

logic and intrusion detection without subjective logic. As shown in Figure 3.19, the proposed mechanism outperforms the intrusion detection without logic with a reduced overhead in terms of 5 packets to 6 packets difference for varying attackers from 1 to 3 nodes, respectively.

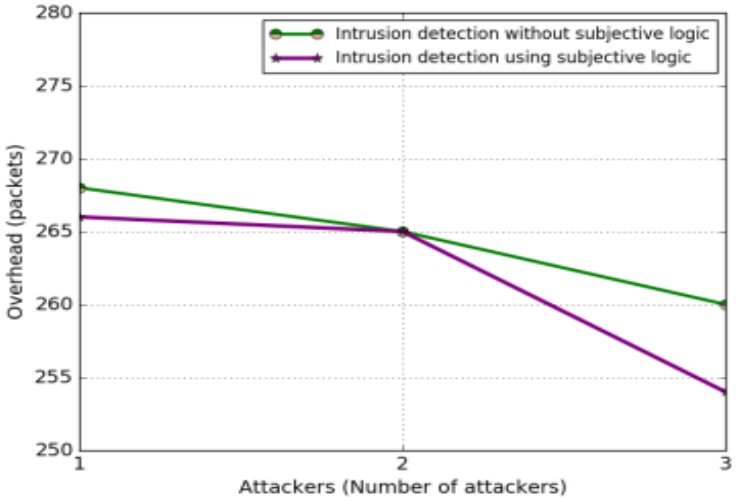

Figure 3.19: Number of Attackers Vs. Overhead for 31 Nodes

For the network scenario with 41 nodes with a single attack, as shown in Figure 3.20, the overhead is slightly higher in the proposed scheme in comparison with intrusion detection without subjective logic. As the attackers are increased, the performance of intrusion detection with subjective logic in terms of overhead is gradually improving with the difference in control packets between the two detection mechanism as 6 packets and 4 packets in two attackers and three attackers' scenarios respectively. The difference in control packets is largely reduced in the proposed scheme as the number of nodes is increased to 51 nodes, as shown in Figure3.21. As the misdetection of normal nodes as attacker nodes increases in the intrusion detection mechanism without subjective logic, the original packets are dropped, and node failures occur frequently resulting in increased overhead whereas the detection of attackers using subjective logic avoids node failures and reduces exchanges of control packets.

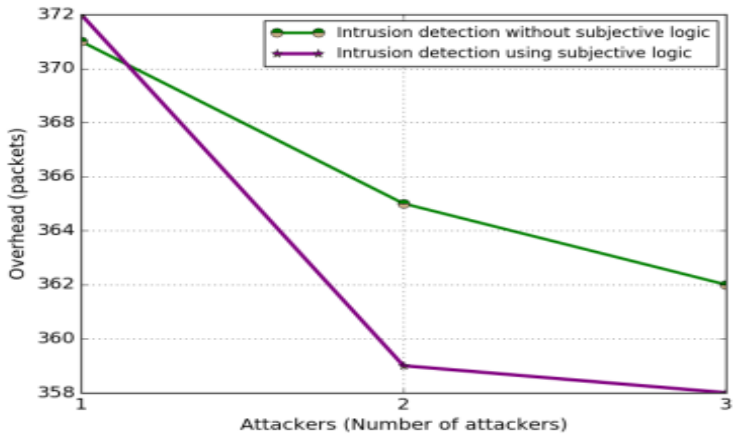

Figure 3.20: Number of Attackers Vs. Overhead for 41 Nodes

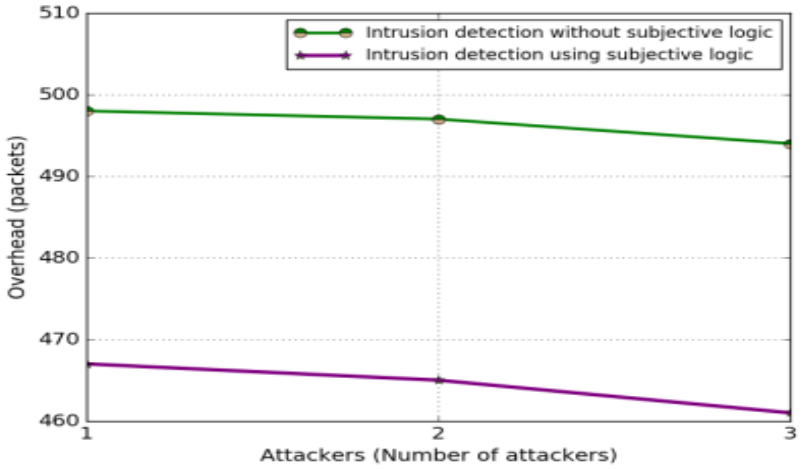

Figure 3.21: Number of Attackers Vs. Overhead for 51 Nodes

Number of Attackers Vs. Power Consumption: Figure 3.22, Figure 3.23, and Figure 2.24 show the performance comparison in terms of power consumption between the intrusion detection mechanism with subjective logic and intrusion detection mechanism without subjective logic in an RPL environment. In Figure 3.22, in the RPL environment with 31 nodes deployed, the performance is analyzed by varying the attacker nodes. The proposed scheme utilizes less power consumption compared to the intrusion detection mechanism based on subjective logic.

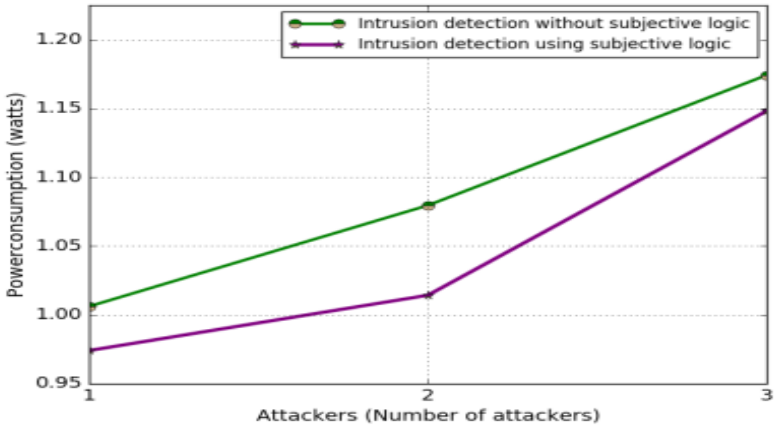

Figure 3.22: Number of Attackers Vs. Power Consumption for 31 Nodes

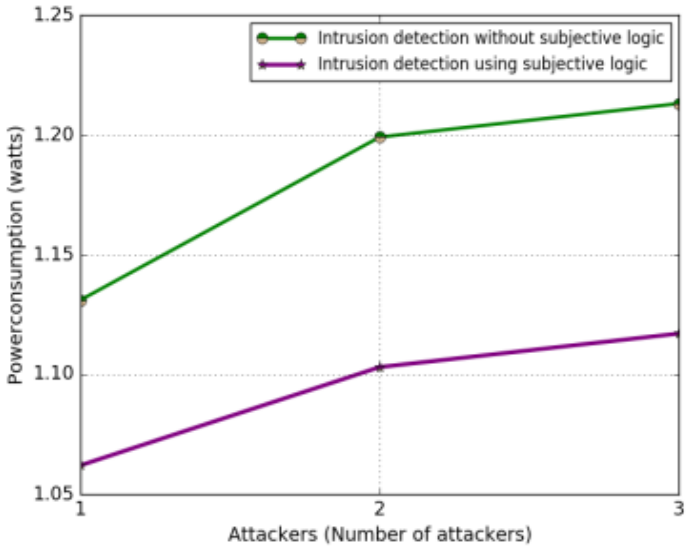

Figure 3.23: Number of Attackers Vs. Power Consumption for 41 Nodes

Even when the network scenario with 41 and 51 nodes, the proposed scheme maintains a low power consumption compared to the existing scheme, as shown in Figure 3.23, and Figure 3.24. The reason is due to the accurate detection of attacker nodes, the power consumption by individual nodes is reduced, whereas in intrusion detection without subjective logic, the attacker nodes posing as a neighbor is not accurately detected, and this leads to data flooding through them resulting in high power consumption.

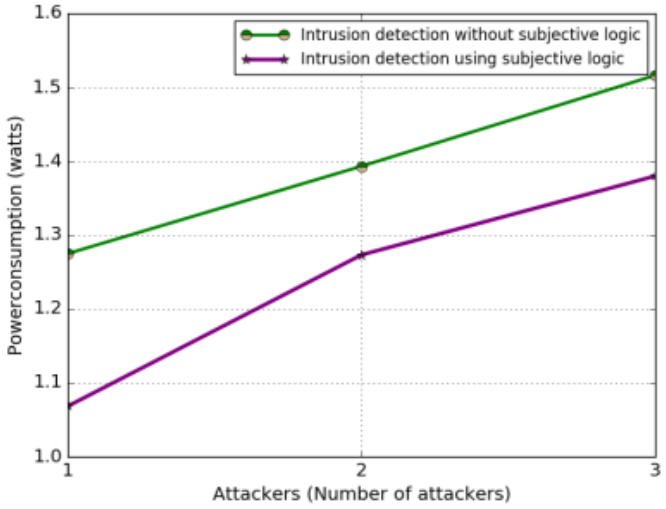

Figure 3.24: Number of Attackers Vs. Power Consumption for 51 Nodes

SUMMARY

Chapter 3 discussed the two proposed trust based detection mechanisms designed against the DDoS attack. In TDD mechanism, the trust evaluation and Data frequency-based attacker detection are explained in detail. Then, the performance comparison between the proposed TDD mechanism and Packet frequency based detection mechanism is performed in terms of performance metrics such as detection accuracy, overhead, power consumption, and throughput. The second mechanism is SLTD that presented with two phases, such as incoming packet based direct and indirect trust calculation. Finally, the performance of the SLTD is carried out.