CHAPTER 6

CONCLUSIONS AND FUTURE WORKS

This chapter deals with the conclusions of the proposed trust-based detection mechanisms designed for detecting DDoS attack, selective forwarding attack, and malicious dropping attacks in the RPL network. This chapter also provides possible future works that contribute to improving the attack detection solutions.

6.1 Conclusions

With the exponential growth in the Internet of Things (IoT), its reach has extended to almost all application sectors such as healthcare, industrial manufacturing, smart homes, transportation, agriculture, and so on. Even though IoT aims to provide ubiquitous connectivity with effective solutions, the open deployment of IoT devices gives rise to security issues. The security threats specifically utilize the resource constraints and physical characteristics of IoT for launching security attacks to degrade network performance and disrupt its services. Therefore, the proposed trust-based detection mechanisms focus on detecting security attacks such as DDoS attacks, selective forwarding attacks, and dropping misbehavior attacks accurately for improving network performance and security. The complete research work is divided into three folds.

The initial contribution focuses on detecting the DDoS attack in the RPL network. It designed solutions to detect DDoS attacks are Trust based DDoS Detection (TDD) and Subjective Logic-based Trust Mechanism against DDoS (SLTD). The performance results between the TDD mechanism and the existing packet frequency-based DDoS Detection are presented in Table 6.1.

Table 6.1: Performance Results of TDD Mechanism and Packet Frequency-based DDoS detection

Performance Metrics	**Number of Attackers**	**Proposed TDD mechanism**	**Existing Packet Frequency-based DDoS Detection**

		31 Nodes	41 Nodes	51 nodes	31 Nodes	41 Nodes	51 Nodes
Detection Accuracy (%)	1	100	100	100	48.2	71.7	51.28
	2	100	100	100	50	26.31	57.89
	3	100	100	100	29.62	37.83	40.5
Throughput (bps)	1	171.22	217.22	268.33	77.17	60.82	159.46
	2	171.22	217.22	260.66	78.2	135.44	143.11
	3	168.66	214.15	240.73	89.95	121.64	162.02
Overhead (packets)	1	376	614	700	476	1257	581
	2	420	585	870	734	972	614
	3	435	624	922	779	1122	608
Power Consumption (watts)	1	3.15	3.35	2.50	6.65	10.50	4.98
	2	3.53	3.78	3.61	7.44	4.71	5.66
	3	4.07	4.40	4.21	8.07	5.67	5.77

Table 6.2 presents the performance results of the SLTD mechanism and intrusion detection without subjective logic. The TDD mechanism considers data frequency for detecting the attackers accurately. The initial trust calculation is performed by the neighbor nodes that update the gray list based on the number of incoming packets, and the block list is created by the gateway node based on the data frequency. The final blacklist is considered for detecting the accurate DDoS attackers in the network. The performance of the TDD mechanism is evaluated with the existing packet frequency based detection mechanism in terms of power consumption, throughput, detection accuracy, and routing overhead by varying the number of nodes as 31 nodes, 41 nodes, and 51 nodes.

Table 6.2: Performance Results of SLTD mechanism and Intrusion detection without Subjective Logic

Performance Metrics	**Number of Attackers**	**SLTD Mechanism**	**Existing Intrusion detection without Subjective Logic**

		31 Nodes	**41 Nodes**	**51 nodes**	**31 Nodes**	**41 Nodes**	**51 Nodes**
Detection Accuracy (%)	1	100	100	100	100	100	100
	2	100	100	100	0	0	0
	3	100	100	100	0	0	0
Throughput (bps)	1	72.37	97.52	122.05	73.6	99.36	120.82
	2	73.6	97.52	120.82	72.98	96.90	120.21
	3	72.98	96.90	120.21	72.37	96.29	119.6
Overhead (packets)	1	266	373	467	268	371	498
	2	265	359	465	265	365	497
	3	254	358	461	260	362	494
Power Consumption (watts)	1	0.97	1.06	1.06	1.00	1.31	1.27
	2	1.01	1.10	1.27	1.08	1.19	1.39
	3	1.15	1.11	1.38	1.17	1.21	1.52

The performance results show that the proposed TDD mechanism maintains better detection accuracy for the varying network environment with varying attacker nodes, whereas the existing packet frequency based detection scheme has minimum detection accuracy even in one attacker scenario. The proposed TDD mechanism exhibits improved throughput of 78bps compared to existing work in 3 attacker scenario with 51 node density as the accurate detection of attackers avoids unnecessary dropping of original packets. In the RPL network with 31 nodes, the proposed scheme exhibits 26% less overhead compared to the existing packet frequency-based DDoS detection mechanism in the presence of one DDoS attacker. Similarly, In the presence of three DDoS attackers, the power consumption of the proposed scheme in the network scenario with 51 nodes is 27% decreased compared to the existing packet frequency-based DDoS attacker.

The SLTD mechanism considers the subjective logic technique for detecting DDoS attacks in the RPL network. Initially, the neighbor nodes perform direct and indirect trust calculations based on

the incoming packet count. Then, the final trust is calculated by the gateway node based on subjective logic that considers belief, disbelief, and uncertainty factors for detecting the DDoS attackers accurately in the network. The performance is carried out between the proposed SLTD mechanism and the intrusion detection mechanism without subjective logic. The performance results show the proposed SLTD mechanisms outperform in terms of detection accuracy, throughput, reduced overhead and decreased power consumption compared to intrusion detection without subjective logic. The proposed SLTD mechanism achieves 100% detection accuracy in a 51 node scenario consisting of three DDoS attackers. The proposed scheme accurately detects the attacker as it adopts the subjective logic-based attack detection. Even in the application of subjective logic technique along with direct and indirect trust calculation in the intrusion detection process, the proposed SLTD mechanism maintains a 0.5% lesser overhead than the overhead of existing intrusion detection without subjective logic technique. Similarly, in terms of power consumption, the proposed scheme consumes 1.38 watts power even in the presence of three DDoS attackers, whereas the existing scheme exhibits 1.52 watts power consumption.

Table 6.3: Performance Results of TSF-RPL and Trust-based RPL network

Performance Metrics	**Number of Attackers**	**TSF-RPL**			**Trust-based RPL**		
		31 Nodes	**41 Nodes**	**51 nodes**	**31 Nodes**	**41 Nodes**	**51 Nodes**
Detection Accuracy (%)	1	100	100	100	82.75	89.74	91.83
	2	100	100	100	64.28	92.1	85.41
	3	100	100	100	62.96	81.0	95.74
Throughput (bps)	1	148.42	195.04	155	63.17	34.34	38.02
	2	122.66	133.09	172	55.22	41.09	41.09
	3	120.21	120.82	156	37.6	36.08	39.25
Overhead (packets)	1	311	434	489	916	1237	1231
	2	359	490	558	821	1245	1265
	3	333	551	595	917	1311	1205
Power	1	4.63	4.00	3.79	7.38	7.81	7.38

Consumption (watts)	2	4.60	4.17	4.01	6.67	7.60	7.60
	3	4.55	4.84	4.16	6.95	7.67	7.37

The design of trust-based selective forward attack detections is the second contribution, and so author proposed Trust-Based Selective Forwarding Attack Detection in RPL (TSF-RPL) and Multi-Level Trust-Based Secure RPL over IoT (MLT-IoT). The performance results of the TSF-RPL and trust-based RPL network are presented in table 6.3, and table 6.4 represents the performance results of MLT-IoT and Neighbor Based Trust Dissemination (NBTD) mechanism. The TSF-RPL mechanism involves two phases, such as trust evaluation and trust-based secure data forwarding. The trust evaluation is performed on all nodes based on routing behavior and updates the packet dropping rate. In the trust-based secure data forwarding phase, the obtained packet dropping rate of each node is compared with the fixed threshold value and sends the node list that fails the condition to the gateway node. The performance of the proposed TSF-RPL is compared with the existing trust-based RPL network in terms of detection accuracy, overhead, throughput, and power consumption. The simulation results show that the proposed TSF-RPL provides better performance with better detection accuracy for all node density scenarios due to effective trust evaluation model that fixes a trust threshold for successful attack detection. The proposed TSF-RPL model shows a 30% increase in throughput compared to the existing trust-based RPL network. In terms of overhead, the total number of control packets is maintained less in TSF-RPL compared to the existing trust-based RPL network, even the numbers of attackers are increased from 1 to 3 in the network. The proposed TSF-RPL improves the power consumption by 52.8% when the number of nodes is 30 and the attackers are 3 in the network.

The MLT-IoT mechanism utilizes the concept of overhearing in a multi-level manner for detecting selective forwarding attackers in the RPL network. In the first level of the MLT-IoT scheme, the nodes alert the gateway in case of suspicious behavior of nodes based on trust calculation determined using node behavior. In order to confirm the attackers, the second level of trust calculation for suspected nodes is performed and updated by the border nodes. The performance comparison is performed between the MLT-IoT mechanism and the existing NBTD mechanism. The proposed MLT-IoT mechanism attains 100% detection accuracy compared to

the existing NBTD mechanism even in the presence of increasing attackers nodes 1 to 3 attackers. The proposed MLT-IoT outperforms the existing work in terms of throughput by 23.8% in the 51 node density RPL network with the presence of 5 DDoS attackers. The overall overhead of the proposed scheme is improved by 8.75% compared to the existing NBTD scheme. The proposed scheme exhibits less energy consumption and power consumption in terms of 36.09% and 18.38%, respectively compared to the existing work as the gateway nodes handle the detection of 5 DDoS attackers in 51 nodes scenario.

Table 6.4: Performance Results of MLT-IoT and Existing NBTD Mechanism

Performance Metrics	**Number of Attackers**	**MLT-IoT Mechanism**			**Existing NBTD Mechanism**		
		31 Nodes	**41 Nodes**	**51 nodes**	**31 Nodes**	**41 Nodes**	**51 Nodes**
Detection Accuracy (%)	1	100	100	100	0	100	0
	2	100	100	100	50	50	50
	3	100	100	100	66.6	33.3	33.3
	4	96	97.2	97.8	25	25	25
	5	96	97.1	95.5	20	20	20
Throughput (bps)	1	235.5	298.08	345.92	228	279.68	339.22
	2	195.65	263.73	279.68	148	256.37	274.16
	3	191.36	210.37	275.05	137	180.93	272.93
	4	103.65	178.48	232.45	80	69.30	188.29
	5	83.41	104.88	175.41	59	57.65	141.68
Overhead (packets)	1	254	387	675	347	609	799
	2	464	534	766	495	658	838
	3	477	692	892	498	746	944
	4	544	738	918	546	750	956
	5	550	1002	929	560	1055	986
Power Consumption	1	3.39	3.91	4.58	4.70	5.53	6.20
	2	3.59	4.58	4.80	5.60	6.35	6.21
	3	3.75	5.01	4.83	5.78	6.73	6.55

(watts)	4	3.84	5.55	4.85	5.83	6.86	6.92
	5	4.09	5.62	5.15	5.98	7.50	7.01
Energy Consumption (mJ)	1	762	938.30	1260.62	769	1171.60	1427.08
	2	794	1219.08	1317.68	1000	1423.35	1487.08
	3	837	1331.76	1335.79	1051	1519.26	1533.19
	4	883	1531.37	1366.07	1077	1573.68	1734.51
	5	959	1563.27	1479.13	1090	1880.65	1751.94

The final contribution is based on the S-MODEST that designs game theory-based detection technique for detecting dropping misbehavior attacks in the RPL network. There are three components included in the S-MODEST model that includes building routing behavior trust on the non-zero sum game model, emphasizing strength and lightweight defense system, and coalition formation using the evolutionary game model. The context-aware route selection and adoption of the non-cooperative game theory model helps in differentiating the malicious attackers from normal nodes. The performance of the S-MODEST model is compared with the SecTrust model. Table 6.5 shows the performance results of the S-MODEST and SecTrust model in terms of the network area. The proposed S-MODEST scheme exhibits reducing detection accuracy from 100% to 57.2% from $100m^2$ to $300m^2$ areas, respectively as the distance between the nodes increases but providing a better performance compared to the Sectrust model

Table 6.5: Performance Results of S-MODEST and SecTrust Model in terms of Network Area

Performance Metrics	**Nodes**	**S-MODEST Model**					**SecTrust Model**				
		Area (m*m)					**Area (m*m)**				
		100	**150**	**200**	**250**	**300**	**100**	**150**	**200**	**250**	**300**
Detection Accuracy (%)	30	96.4	100	60.7	59.6	57.2	33.3	21.2	14.6	11.2	9.2
	60	98.27	100	63.22	62.5	60.2	33.33	21.2	14.6	12.3	11.2
Throughput	30	69.51	65.42	41.91	40.12	39.56	65.42	47.02	20.44	18.6	14.2

(bps)	60	184	140.53	113.4	110.2	108.2	128.8	113.4	82.8	78.2	65.2
Normalized Overhead	30	4.57	4.18	3.26	3.0	2.45	5.17	5.52	4.89	3.23	2.78
	60	7.21	7.02	6.78	6.5	5.89	8.92	7.13	7.03	6.89	6.12
Energy Consumption (J)	30	0.584	0.544	0.469	0.35	0.302	0.784	0.74	0.530	0.47	0.41
	60	0.211	0.201	0.187	0.175	0.168	0.281	0.206	0.204	0.201	0.198

In 30 node topology, the throughput of the proposed SMODEST methodology shows a 6.6% increase compared to the existing work, and the S-MODEST exhibits a 17.8% decrease in energy consumption compared to the SecTrust model in the network area of 300m^2.

Table 6.6: Performance Results of S-MODEST and SecTrust Model in terms of Number of Attackers

Perform-ance Metrics	**Nodes**	**S-MODEST Model**					**SecTrust Model**				
		Number of Attackers					**Number of Attackers**				
		1	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
Detection Accuracy (%)	30	96	96	92	90	87	100	89.6	33	25	18
	60	95.0	94.91	87.93	85.4	80.2	93.3	93.22	29.89	21.5	14.5
Throughput (bps)	30	88.93	78.71	71.55	68.5	65.3	66.62	63.37	60.44	56.4	54.23
	60	331.2	322.0	288.2	265	254	318.9	223.8	226.9	225.56	220.56
Normalized Overhead	30	2.86	3.03	4.22	4.50	4.65	2.38	4.88	5.0	5.12	5.14
	60	2.73	2.75	2.96	3.5	3.8	2.67	3.38	3.51	4.8	5.03
Energy Consumption (J)	30	0.565	0.631	0.672	0.695	0.714	0.390	0.688	0.786	0.784	0.815
	60	0.200	0.200	0.210	0.235	0.265	0.229	0.255	0.266	0.278	0.29

											4

The performance results of the S-MODEST and SecTrust Model in terms of the number of attackers are shown in Table 6.6. The proposed S-MODEST exhibits 87% of detection accuracy in a 30 node network scenario with five malicious nodes, which decreases to 80.2% when the network scenario has 61 numbers of nodes. In 61 node topology, the proposed scheme has 33bps higher throughput compared to the existing SecTrust model. The proposed scheme in the network topology with 31 nodes exhibits a 10.5% decrease in normalized overhead compared to the SecTrust model in the presence of 5 attacker nodes. Similarly, in the 30 node network scenario, the S-MODEST with 0.8 dropping behavior attains 31.4% routing enforcement, whereas in the same scenario with 60 node topology, it reaches 21.45% of route enforcement.

Table 6.7: Performance Results of S-MODEST and SecTrust Model in terms of Data Interval

Performance Metrics	**Nodes**	**S-MODEST Model**					**SecTrust Model**				
		Data Interval (Seconds)					**Data Interval (Seconds)**				
		10	**20**	**30**	**40**	**50**	**10**	**20**	**30**	**40**	**50**
Detection Accuracy (%)	30	93.0	92	92	90	84	22.62	19	17	13	11.1
	60	94.1	93.1	93.1	92.1	91.5	87.1	76.0	33.3	26.5	21.4
Throughput (bps)	30	213.6	126.7	71.5	68.5	62.3	161.5	83.8	60.3	58.2	54.1
	60	670.2	288.2	211.6	200.3	189.6	499.8	233.06	177.8	165.2	148
Normalized Overhead	30	1.339	2.193	3.585	4.12	4.56	0.867	3.146	3.93	4.56	5.6
	60	1.395	2.968	4.260	4.8	4.9	1.830	3.526	4.32	5.23	5.89
Energy Consumption (J)	30	0.764	0.601	0.60	0.58	0.547	0.808	0.766	0.62	0.612	0.598
	60	0.216	0.210	0.197	0.191	0.187	0.264	0.254	0.221	0.215	0.203

Table 6.7 presents the performance results in terms of data interval for the S-MODEST and SecTrust model. In the data interval from 10 to 15 seconds, the detection accuracy of S-MODEST is reduced by 9% when increasing the data interval from 10 to 15 seconds. The proposed scheme has a 28% increase in throughput in a data interval of 50 nodes compared to the SecTrust model. For increasing data interval from 10s to 50 s, the proposed scheme increases from 1.39 to 4.9 in terms of normalized overhead, maintaining a better performance compared to the SecTrust model in 60 node topology. Considering energy consumption, the proposed scheme has an 8.55% decrease compared to the SecTrust model in the network scenario with 60 nodes.

6.2 Future Works

It is a real challenging issue to securely route the data over heterogeneous IoT devices with various routing standards. Some of the future works are described as follows:

- In future work, the trust-based secure RPL routing systems combine the most trustworthy nodes into the IoT network and offer solutions for recouping the batteries of such trustworthy nodes by maintaining battery drained information. Thus, it enhances the routing reliability and prolongs the network lifetime significantly. Further, the proposed works also focus on detecting various types of novel IoT routing attacks.
- In IoT, heterogeneous devices generate a vast amount of data, and it is crucial to forward such data to the desired destination in a secure manner. Instead of designing routing mechanisms with similar data forwarding, it is necessary to design appropriate routing mechanisms with data fusion models.
- The IoT devices are resource-limited, and it is crucial to prolong the network lifetime for various real-time mission-critical applications. Load-balancing is an effective solution to improve the IoT lifetime. Designing an effective load-balancing mechanism through multipath routing diminishes the rapid exhaustive energy conservation of resource-limited IoT devices, especially in parent nodes. Hence, it is essential to handle the topology re-configurations effectively. Furthermore, efficient load-balancing models enhance the quality of data delivery, fault-tolerance, and data reliability.

- Node cooperation is an essential requirement in IoT routing. Most of the IoT devices are heterogeneous, and it is very tedious to achieve better cooperation among such devices to achieve efficient routing. Incentive-based secure routing assists to enhance the node cooperation in RPL routing over IoT.