RESEARCH REVIEW JOURNALS
Volume-04
Issue-02
February -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Trust Management System for IoT heterogeneous mesh network

*[1]R. Chawngsangpuii and [2]Dr. Prodipto Das

[1]*Asst. Professor, Department of Information Technology, Mizoram University, 796001, India*
[2]*Asst. Professor, Department of Computer Science, Assam University, Silchar, 788011, India*

ARTICLE DETAILS

Article History
Published Online: 20 February 2019

Keywords
Internet of Things, LLN, trust, security, RPL, routing

***Corresponding author**
Email: *sangpuii_77g@hotmail.com*

ABSTRACT

Background/Objectives: The technology offered by IoT is so vast and advanced that the physical objects around us will be able to collect information from anywhere and everywhere. However, the complexities of the IoT system make developing trust management system very intricate. Hence, the objective is to develop an efficient trust management system for IoT heterogeneous network for providing trust to ensure efficiency between devices.

Methods/Statistical analysis: The calculation of both direct and indirect trusts is carried out for finding out whether a node is to be trusted or not. Our proposed trust protocol is evaluated using Cooja simulator in Contiki 2.7. Performance evaluation is done for the new system and compared with two objective functions of RPL.

Findings: Cooja simulator which is dedicated for simulating IoT environment is utilized to evaluate the proposed system with various performance metrics such as energy consumption, packet loss rate and throughput. From the findings, the proposed system has only 17.1 % to 20.1% average packet loss rate while OF0 has between 72.2 % to 78.1 % and MRHOF has between 67.8 % to 74.07 %. The energy consumption rate of the proposed system is also low which is more promising than the other two.

Novelty/Applications: The proposed reliable trust system in this work addressed RPL attacks. As a result, it will be able to preserve stability in the IoT system networks. Hence, it can provide beneficial improvement in securing network routing and performance.

1. Introduction

The IoT can be regarded as an extension of the internet and the communication networks. It creates an era of digital innovation and development by integrating billions of physical objects to collect data and pass on the data to other objects or humans. It makes communication possible between the objects, human and objects, and the objects to the global internet. Due to these possibilities, it has gained wide popularity in different sectors such as academic, government and industrial sectors.

However, the IoT employs different technologies and frameworks from that of the conventional internet. The ability of the small objects to communicate and exchange the data with the other objects as well as to anyone in the internet invites security threats to the data, the objects and even to humans. In addition, the physical objects are not equipped with abundant data storage, battery power and processing power. For these shortcomings, the traditional bulky, energy-consuming security solutions are not suitable for the IoT system. The necessity of developing a strong trust management system arises for establishing trust between the objects and the users for the proper acceptance and wide adoption of the IoT system. When the objects are deployed in hostile surroundings, they are exposed to risks from malicious attacks.

The IoT comprises of many Low-power lossy networks (LLNs) which are able to connect to the internet. Each LLN consists of many networking devices which can be used for many applications [1]. To integrate the LLNs and IoT, the IETF (International Engineering Task Force) standardized RPL"(Routing Protocol for Low-Power and Lossy Network)"and 6LOWPAN for using IPv6 on LLNs [2]. The RPL security mechanisms which are based on cryptography can defend from outsider attacks but is still vulnerable from insider attacks which are studied extensively in [3]. The attacks can also be classified as network traffic attacks, network topology attacks and resource-consuming attacks. Since the RPL is not equipped with self-healing mechanism in the face of attacks except for hello flooding attack, providing security mechanism is essential for smooth functioning [4].

2. Literature Survey

The authors in [5] proposed intrusion detection system which they called IDS, that alleviates attacks such as selective-forwarding, sinkhole, and rank attacks. However, their system suffered from synchronization of DIO and the detection rate was not accurate. The authors in [6] provided an overview and study of RPL, the attacks on the 6LOWPAN and the RPL topology. [7] surveyed on the existing secure mechanisms for routing protocols and also the weakness of the RPL and various defence mechanisms. It also presented research concerns for these challenges. The authors in [8] proposed hybrid IDS system for securing the RPL protocol, which can alleviate from RPL attacks. [9] studied on the concepts and security measures on the RPL. It also mentioned the importance of employing risk management for the attacks.

[10] proposed a selection scheme for secure parent node for excluding malicious nodes based on trust mechanism. The scheme worked well for detecting rank attacks but other attacks were not properly detected by the scheme. [11] proposed trust metric-based scheme for RPL where the highest trust route is calculated. Though the system can help in

mitigating the rank attack but it suffered from network performance due to high overhead in communication as well as energy consumption. [12] proposed VeRA protocol which stands for "Version number and Rank Authentication" for RPL secure routing. However, it degraded the network performance due to high packet loss and less packet delivery. [13] proposed trust-based secure RPL protocol for IoT with the purpose of providing secure IoT routing and detecting the attacks. However, the proposed mechanism assumed that all trust values from the nodes are all trust-worthy, hence did not take into account for the trust calculation. The authentication system proposed in [14] can protect against rank attack but suffered from depletion of network resources. Another trust-based mechanism is put forward in [15] for IoT which considered the reputation of all the nodes but focussed only on direct observations in order to detect malicious nodes.

3. The Concept of Trust

Trust has many connotations in social context as well as with machines. It is a complex concept since there can be many interpretations from different perspectives belonging to different fields. In general, trust can be used to measure confidence level of a person for believing that another person behaves in productive manner.

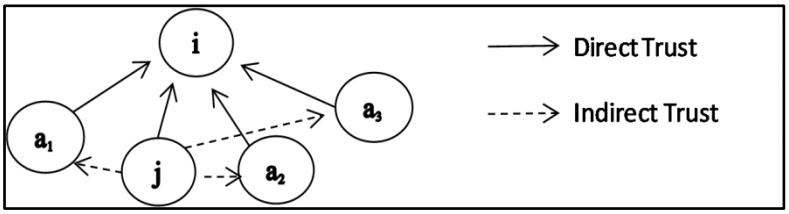

Figure 1.Direct trust and Indirect Trust"

In sensor networks, trust can also be used to quantify a belief from past communication as well as behaviour of the communicating two nodes as shown in Figure 1. Trust played an important role for sensor nodes in selecting future route path and communication [16].

- Direct Trust: Direct trust estimate is taken from the source node and its neighbours. It comes from the direct communication and is more reliable than the indirect trust.
- Indirect Trust: If a node cannot connect directly to source node, the indirect trust estimate is taken from the opinions of other nodes on the source node. It can also be thought of as a recommendation trust from other nodes.

Some of the characteristics of trust which are worth mentioning for enhancing the trust concept [17] are:

- *Trust is context-dependent*:
  In this, the degree of trust is not same for different contexts, and can be applied to one context at a time.
  For example, Mary trusts John for career advice but not for banking advice.
- *Trust is dynamic*:
  Trust may remain same only for a period of time and can change in due course.
  For example, Mary trusts John, but Mary found out that John is not reliable and hence cannot be trusted.
- *Trust is asymmetric*:
  Trust may not be same for different parties which are communicating.
  For example, if Mary trusts John, John may not trust Mary.
- *Trust is not transitive*:
  Trust cannot be assumed to hold true for all communicating parties. A node i trusts j, j trusts k, but i may not trust k.

For example, if Mary is trusting John, and John is trusting Bob, then Mary may not be trusting Bob.

4. The RPL

RPL protocol is using IPv6 and a "distance-vector routing protocol" which decides the best route by the distance a packet has to pass through. It is also a proactive protocol in which all the nodes are maintaining one or multiple routing tables which are updated regularly. A DODAG (Destination Oriented Directed Acyclic) graph is maintaining the topology of RPL that may have tree or mesh topologies based on the arrangements of the IoT devices. The graph starts from the root or border router node which is also called the sink node in the graph as shown in figure 6.2. A DODAG is exclusively recognized by both the RPL Instance Id and the DODAG Id. Many DODAGs may be present in an RPL instance and the traffic can move to the root or downwards.

4.1 The DODAG Formation

The DODAG construction is done in a gradual manner i.e., step-by-step manner as depicted in Figure 2. DIO (DODAG Information Object) message broadcast is done by root or sink node at the initial stage. The DIO message has the necessary information for nodes to locate the RPL topology instance, choose its parent, and preserve the topology.

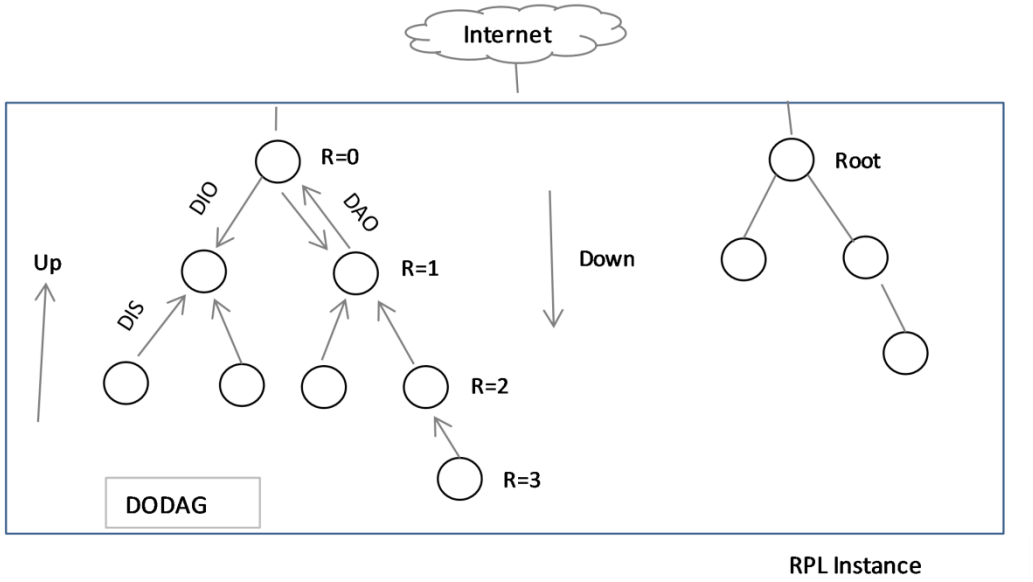

Figure 2. RPL Topology

A node, after receiving the DIO message, finds the RPL instance and selects its parent. A node also attaches the DIO message sender to the list of parents and specifies its own rank by using the OFs (Objective functions) of the RPL [18]. The rank for any node is determined from the location of that node to the root in the graph and is always higher than its parents rank.

After updating the DIO message, it will then be forwarded by the node to all the neighbours. A node sends any data to the root node by its selected chosen parent, which will be by default, the gateway for the node. In the DODAG, all the nodes have upward path towards the root.

To join a network, the node broadcasts DIS message (DODAG Information Solicitation) in order to receive the DIO information message from its neighbours. The DIO information messages are transmitted regularly with the help of the trickle algorithm, which controls the traffic in the network [19]. After joining the network, the node sends a message known as DAO (DODAG Advertisement Object) message to the neighbours for updating the topology in the routing table. The node advertising a DAO message gets DAO-ACK (DAO-Acknowledge) message. In this DAO-ACK message, information such as RPL Instance Id, the sequence of DAO and the status of the network are included.

4.2 Routing Attacks in RPL:

RPL is susceptible to many attacks as behavior of nodes is not considered during routing process. Many RPL attacks are not easy to detect and isolate due to the heterogeneous nature of the networks and nodes. Many security mechanisms proposed are able to solve external attacks like eavesdropping but not the insider attacks. Brief definitions of blackhole and rank attacks, which are addressed in this work, are given below:

- *Blackhole Attack*: A malicious node will act as a route for packets when other node tries to discover network route. As a result, all the packets forwarded using this malicious node will be dropped rather than sending. Blackhole attack becomes more serious when combined with the rank attack, which can lead to low rate in delivery and network instability.
- *Rank Attack:* This attack happens when a malicious node wrongly advertises a low rank to make other nodes choose it as a parent node. To save itself from the wrong rank advertisement, RPL does not have mechanism. This attack may lead to node resource exhaustion, loops generation in the network and network congestion.

5. The Proposed Trust System

The IoT can be regarded as an extension of the internet and the communication networks. It creates an era of digital innovation and development by integrating billions of physical objects to collect data and pass on the data to other objects or humans. It makes communication possible between the objects, human and objects, and the objects to the global internet. Due to these possibilities, it has gained wide popularity in different sectors such as academic, government and industrial sectors.

In the proposed trust system, a calculation of direct and indirect trusts is done for determining whether a node is trustworthy or not. There are phases such as gathering of information by nodes, calculating the trust values, sharing the information and detection of untrustworthy nodes. The RPL utilizes objective functions which are OF0 (Objective Function Zero) and MRHOF"(Minimum Rank with Hysteresis OF)"for node selection and optimization. These two functions are compared with our proposed system and checked for effectiveness. The evaluation of trust comprises of direct as well as indirect trusts which is given below:

5.1 Direct Trust Computation

Direct trust is evaluated by a node named i of its neighbouring node named j from the direct observation i.e., from its 1-hop neighbour at time t, by the equation 1 given below with the trust components.

$$Dir_{ij}(t) = E_{ij}(t) + H_{ij}(t) + U_{ij}(t) \quad (1)$$

where $E_{ij}(t)$ is the belief the node i has on node that it is still having the energy to perform necessary operations. The actual remaining energy can be calculated by the residual and initial energy of a node

$H_{ij}(t)$ is the honesty component, which is the belief the node i has on node j based on direct observation to check whether node j maintains consistency in terms of handling data, retransmission or any delay experienced on the node j

$U_{ij}(t)$ is the unselfish component, which is used by node i to check node j if it follows the same network protocol, which can also be derived based on the rate of data forwarded and data received by the node j.

5.2 Indirect Trust Computation

The indirect trust is computed by the node i for another node from the opinions collected by other neighbouring nodes. These opinions collected can be thought of as recommendations given by the neighbours about a certain node. The indirect trust is calculated from the direct trust of the shared neighbours between the two nodes i and j for reducing the communication overhead.

Indirect trust of i on j is calculated by recommendation of j from the neighbours a_1, a_2 and a_3 as shown in equation 2.

$$IDir_{ij}(t) = Dir_{ia}(t)\ x\ Dir_{aj}(t) \quad (2)$$

where a is common neighbour for both the nodes.

5.3. Total Trust Computation

The total trust among nodes i and j at a time t is computed from both the direct trust and the indirect trust as under in equation 3.

$$TDir_{ij}(t) = Dir_{ij}(t) + IDir_{ij}(t) \quad (3)$$

The trust value is further checked with the trust level calculation for selecting the high ranked nodes as trusted nodes as provided in Table 1. This is carried out for secure communication in the network and for discarding the untrustworthy nodes.

Table 1 Trust Level

Level Meaning	Value
Total	(0.91 – 1)
Good	(0.76 – 0.90)
Low	(0.51 – 0.75)
Poor	(0.26 – 0.50)
No Trust	(0 – 0.25)

5.4 Proposed Algorithm

The proposed trust system algorithm for IoT nodes and isolating blackhole and rank attacks is given below:

Step 1. Let i and j be two nodes
Step 2. Calculate the Total trust TDir using the equation
Step 3. Compare the two nodes based on their path metric and rank
Step 4. Use the value in Step 3 for selecting best parent and detecting malicious nodes
Step 5. If TDir.Node(i) >= Trust_value(threshold) then
Select Node(i) as Parent
else
Blackhole node
Discard (Set TDir.Node(i) = null)
Step6. If DIO_sequence.Node(i) = DIO_sequence.Node(j)
If rank.Node(i) = rank.Node(j) then
Select Node(i) as Parent
else
Rank attack node
Discard (Set TDir.Node(i) = null)
Step 7. Forward trusted nodes for routing
Step 8. Stop

5.5 The Flowchart

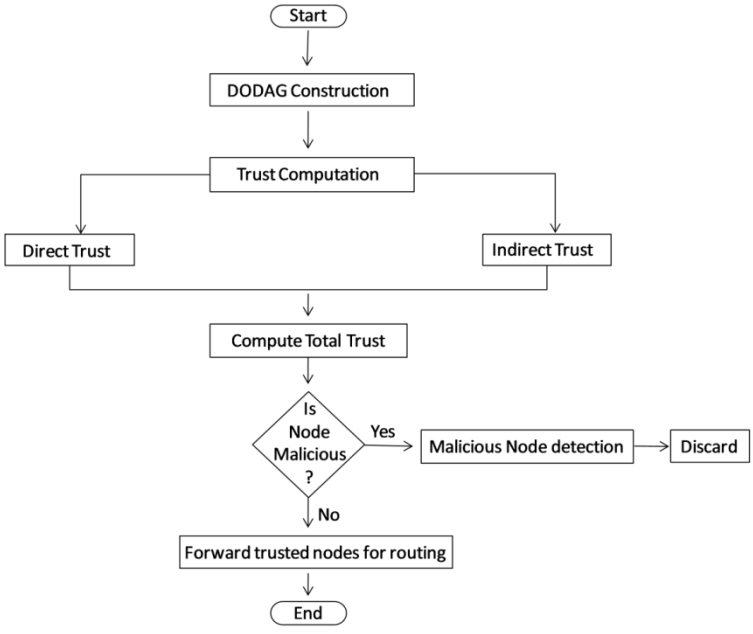

Figure 3. Flowchart of the Proposed Trust System

6. Simulation and Performance Results

The performance study of our proposed trust system is evaluated with the help of Cooja simulator in Contiki 2.7 OS [20]. The various parameters for simulation are given in Table 2. The Cooja simulator allows topologies of small and large networks and is dedicated for simulating IoT environment. The performance metrics used to evaluate the proposed system are packet loss rate, energy consumption and throughput.

Table 2. The Simulation Parameters Used

Parameter	Description
Name of Simulator	Contiki-Cooja 2.7
Node type	Tmote sky
Coverage area	100m x 100m
Number of nodes	30
Transport Layer	UDP
Network Protocol	IP based
Routing Protocol	Proposed, OF0, MRHOF
Simulation time	60 mn
Radio medium model	UDGM with distance loss

6.1 Packet Loss Rate

The loss rate for packets can be determined from the total number of both undeliverable and deliverable packets. The rate can be used to express the reliability of a network. The results from the simulator show that the proposed system has lesser packet loss compared to OF0 and MRHOF as shown from Figure 4 and 5. It is shown that OF0 has the highest packet loss which indicate that packet dropping is highest in OF0 due to network congestion while parent selection. The MRHOF network is also found to have high packet loss due to collision of data packets and congestion in network.

The proposed system has average packet loss rate between 17.1 % to 20.1% while OF0 has between 72.2 % to 78.1 % and MRHOF has between 67.8 % to 74.07 % as shown in Figure 6. Hence, the proposed system has better performance with respect to packet loss rate.

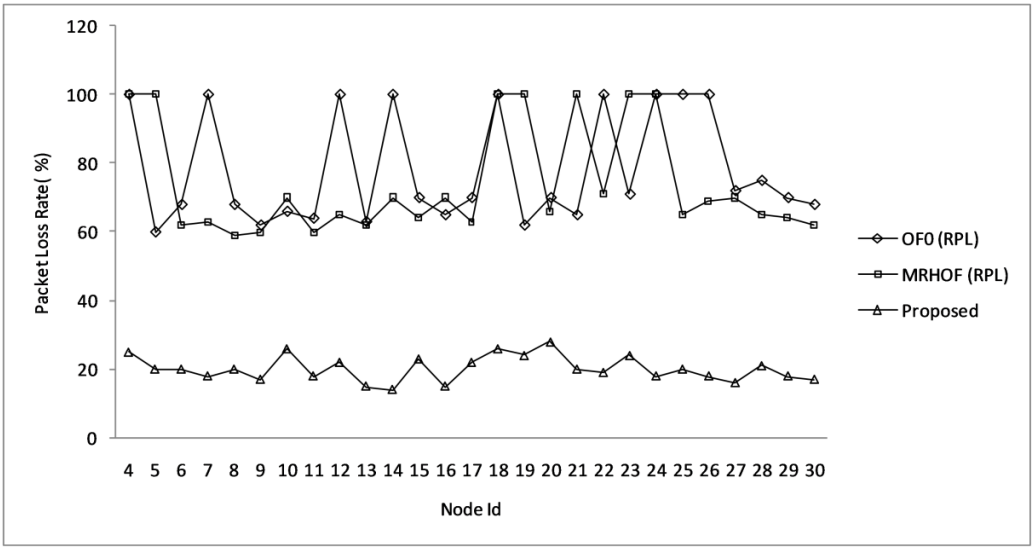

Figure 4. Packet Loss Rate during Blackhole attack

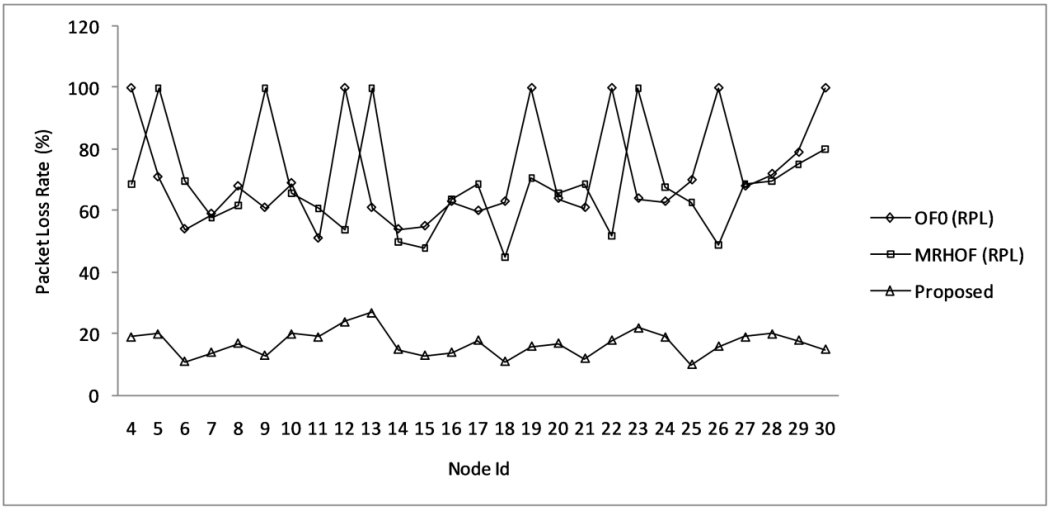

Figure 5. Packet Loss Rate during Rank attack

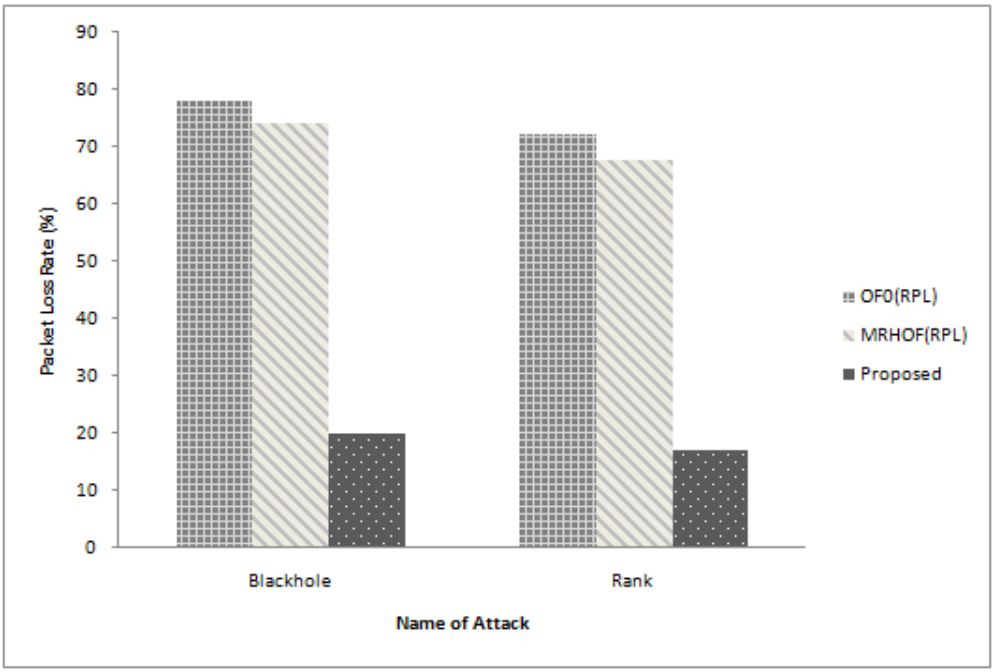

Figure 6. Average Packet Loss Rate during both attacks

6.2 Energy Consumption

Nodes which are more often selected as parents due to low ranks consume more energy than other nodes. When malicious nodes get selected as chosen parents more often in the cases of OF0 and MRHOF networks, they consume more energy due to unstable network topology caused by high rate in rank changes.

It is shown from Figure 7, that the consumption of energy in OF0 and MRHOF in the first 20 minutes is lower than the proposed system. However, after selecting and isolating the attack nodes, the proposed system's network topology became more stable, which results in low rate for energy consumption.

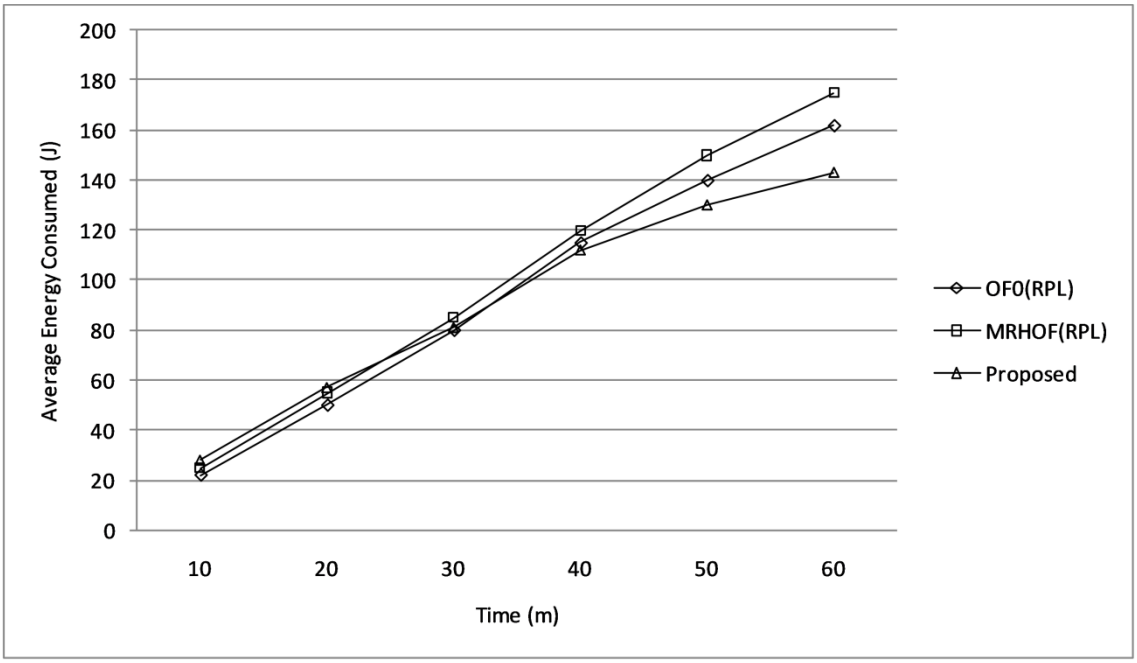

Figure 7. Average Energy Consumed during both attacks

6.3 Throughput

In communication network, throughput is another important performance metric which indicate the rate of successful delivery of data in the network. From the Figure 8, the throughput of the proposed system is better than the other two due to the detection mechanism which provides stable network. While the throughput of the other two networks is relatively low due to the attacks since the packets do not reach the DODAG root.

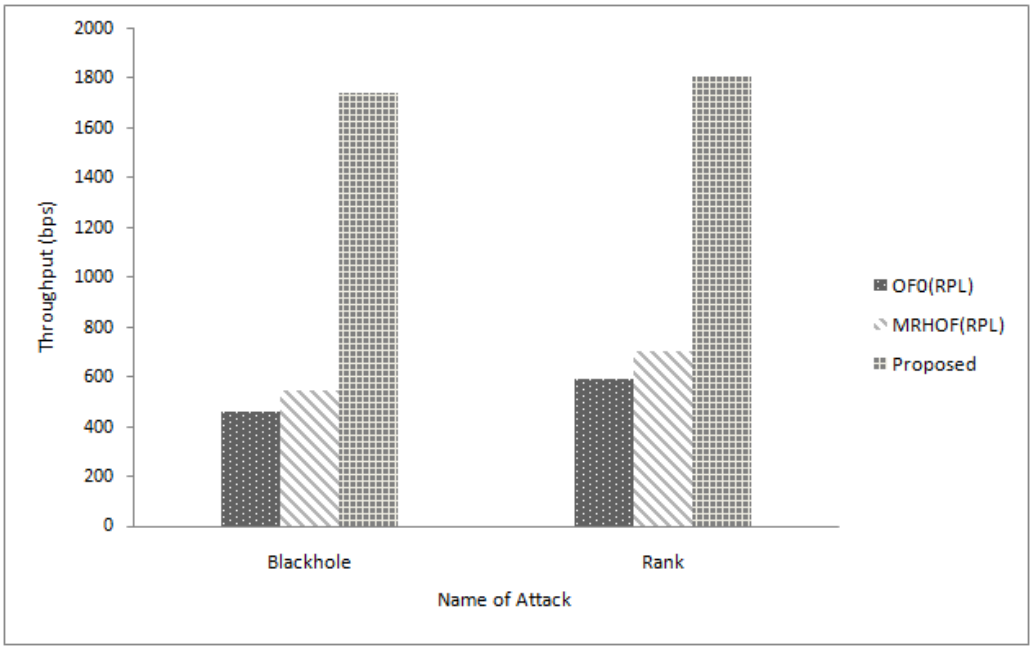

Figure 8. Throughput during both attacks

7. Conclusion

We proposed a reliable trust system in this work by addressing two attacks of RPL, which can cause instability of the IoT system networks. The direct and indirect observations from nodes are used for calculating the level of trust. The trust system is checked and evaluated in a simulator with respect to performance metrics such as packet loss rate, energy consumption and throughput. The evaluation shows that the proposed system is better when compared to the other RPL networks in secure routing and network performance. For future work, we plan to achieve performance evaluation in real-life test-beds and investigate the effectiveness against other routing attacks.

References

1) Kim H, Im H, Lee M, Paek J, Bahk S. A Measurement Study of TCP over RPL in Low-power and Lossy Networks. *Journal of Communications and Networks*. 2015; 17(6), 647-655. DOI: 10.1109/JCN.2015.000111
2) Winter T, Thubert P, Brandt A, Hui J, Kelsey R, Levis P, Pister K, Struik R, Vasseur JP, Alexander R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. *Internet Engineering Task Force (IETF)*, Internet Draft, 2012; RFC 6550:1-157.
3) Tsao T, Alexander R, Dohler M, Daza V, Lozano A, Richardson M. A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL). *Internet Engineering Task Force (IETF)*, Tech. Report. 2015; RFC 7416:1-40.
4) Wallgren L, Raza S, Voigt T. Routing Attacks and Countermeasures in the RPL-Based Internet of Things. *International Journal of Distributed Sensor Networks*. 2013; 2013, 1-11. DOI: 10.1155/2013/794326.
5) Raza S, Wallgren L, Voigt T. SVELTE: Real-time intrusion detection in the Internet of Things. *International Journal of Ad-Hoc Networks*. 2013; 11(8), 2661-2674. DOI: 10.1016/j.adhoc.2013.04.014.
6) Pongle P, Chavan G. Real Time Intrusion and Wormhole Attack Detection in Internet of Things. *International Journal of Computer Applications*. 2015; 121(9), 1–9. DOI: 10.5120/21565-4589.
7) Airehroura D, Gutierreza J, Ray S. K. Secure routing for internet of things: A survey. *Journal of Network and Computer Applications*. 2016; 66, 198-213. DOI: 10.1016/j.jnca.2016.03.006.
8) Le A, Loo J, Chai K, Aiash M. A specification-based IDS for detecting attacks on RPL-based network topology. *Information*. 2016; 7(2), 1-19. DOI: 10.3390/info7020025.
9) Mayzaud A, Badonnel R, Chrisment I, Grand Est –Nancy I. A Taxonomy of Attacks in RPL-based Internet of Things. *International Journal of Network Security*. 2016; 18(3), 459–473. https://hal.inria.fr/hal-01207859
10) Iuchi K, Matsunaga T, Toyoda K, Sasase I. Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network. *Proceedings of 21st IEEE Asia-Pacific Conf. on Communications (APCC)*, Japan. 2015; 299–303.
11) Djedjig N, Tandjaoui D, Medjek F, Romdhani I. New trust metric for the RPL routing protocol. *Proceedings of 8th IEEE International Conference on Information and Communication Systems (ICICS)*, Jordan. 2017; 328–335.
12) Dvir A, Holczer T, Buttyan L. VeRA - Version number and rank authentication in RPL. *Proceedings of 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, Spain. 2011; 709–714.
13) Airehroura D, Gutierreza J, Ray S. K. A Lightweight Trust Design for IoT Routing. *Proceedings of 14th IEEE Intern. Conf. on Dependable, Autonomic and Secure Computing, 14th Intern. Conf. on Pervasive Intelligence and Computing, 2nd Intern. Conf. on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, Auckland. 2016; 552-557.
14) Perrey H, Landsmann M, Ugus O, Schmidt T. C, Wählisch M. TRAIL: Topology Authentication in RPL. *Proceedings of ACM International Conference on Embedded Wireless Systems and Networks (EWSN)*, Austria. 2016; 59 - 64.
15) Khan Z. A, Ullrich J, Voyiatzis A. G, Herr-mann P. A Trust-based Resilient Routing Mechanism for the Internetof Things. *Proceedings of ACM 12th International Conference on Availability, Reliability and Security (ARES)*, Reggio Calabria, Italy. 2017; 1-6.

16) Jøsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. *Decision Support Systems*. 2007; 43(2), 618–644. DOI: 10.1016/j.dss.2005.05.019
17) Pranata I, Skinner G, Athauda R. A Holistic Review on Trust and Reputation Management Systems for Digital Environments. *International Journal of Computer and Information Technology*. 2012; 1(1), 44-53. https://www.ijcit.com/archives/volume1/ issue1/Paper010106.pdf
18) Iova O, Theoleyre F, Noel T. Using multiparent routing in RPL to increase the stability and the lifetime of the network. *International Journal of Ad Hoc Networks*. 2015; 29, 45–62. DOI: 10.1016/j.adhoc.2015.01.020
19) Levis P, Clausen T, Hui J, Gnawali O, Ko J. The trickle algorithm. *Internet Engineering Task Force (IETF)*, Tech. Report. 2011; RFC 6206 : 1-13.
20) Contiki: The Open Source Operating System For The Internet Of Things. [online] Available at: <http://www.contiki-os.org/> Date accessed: 24/11/2016.

