ISSN 2347 - 3983
Volume 8. No. 8, August 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter86882020.pdf
https://doi.org/10.30534/ijeter/2020/86882020

Trust Based Technique for the Multicasting in IoT

Jaspreet Kaur[1], Navpreet Kaur[2]
[1]M.tech Student, ECE Department, BBSBEC Fatehgarh Sahib, India, jaspreetkaura20587@gmail.com
[2]Assistant Professor, ECE Department, BBSBEC Fatehgarh Sahib, India, navpreet.kaur@bbsbec.ac.in

ABSTRACT

A network is defined as the collected information such as systems and organization that collectively form a group, this group is utilized to share information with one another. According, to computer terminology it is defined as the combinations of the computers that has been utilized to share the information or services through internet connection. There are two types of networks exists such as wired and wireless networks. The route is maintained within a local region, in this protocol and is termed as the routing zone. This research work is based on the multicasting for the path establishment from source to destination. The technique of multicasting is applied in the RPL routing protocol for the path establishment from source to destination. The multicasting technique will be based on the trust calculation. The path will be established from source to destination through nodes which have maximum trust. The trust based multicasting technique is implemented in network simulator version 2 and compared with RPL routing protocol in terms of delay, packet loss and throughput.

Key words: RPL, IoT, Routing, Trust, Multicasting.

1. INTRODUCTION

The Internet of Things (IoT) is defined as a network through which multiple devices, smart nodes and artifacts are linked to each other to conduct communication without requiring any human intervention. The objects act autonomously, based on the relation between objects. Analysis of gathered data for decision taking, the creation of lightweight data and the retrieval of data through accessing and approving cloud-based services are some of the behavior of IoT nodes. Users, services, sensors, and artifacts are very tightly related to each other via IoT. IoTs are implemented inside the applications spanning from smart grid healthcare services to autonomous transport networks. The amount of connected devices and intelligent services delivered by IoT networks has been outgrowing, due to the tremendous market possibilities offered in the IoT scenarios [2].

There are many IP-based network apps and IoT applications that provide connectivity using TCP and UDP. In certain IoT applications [16], however, there are few widely used functions for the delivery of messages. Various systems enforce these features in regular interoperable ways [6]. A publication / subscribe network architecture which is named MQTT (Message Queue Telemetry Transport) is built very similar to the client / server interface. MQTT protocol is considered to be of tremendous value due to its easy structure and capacity to prevent heavy CPU and memory usage. Another protocol which is built from the finance industry is the Advanced Message Queuing Protocol (AMQP). The encryption is handled using the TLS / SSL protocols. For connectivity purposes, CoAP is implemented to insure that less power and processing embedded modules are used.

Various network layer protocols were also developed. The most widely recognized IoT interface for MAC is the IEEE 802.15.4 [15]. Throughout this protocol a frame structure is specified where the source and destination addresses are described in headers along with the way nodes will communicate. Low power multi-hop networking has recently been implemented in IoT, because it is not appropriate to use frame formats previously used in conventional networks because they create overhead in these structures. Channel hoping and time synchronization are used to maintain high efficiency, fewer expenses and satisfy IoT connectivity requirements [5].

Understand the expectations of network administrator, the routing protocols for each network have to be well defined and configured [14]. The IPv6 Routing Protocol for Low power and Lossy networks (RPL) is a standardized remote vector routing protocol. Because of the way the devices are connected, the protocol has no cycle, and thus has no loop. Cycles are avoided by the DODAG with the border routers that are connected to internet. All devices connected to DODAG are connected to the Internet via that border router. When calculating the position of a node in relation to the root node, the protocol avoids loops [18]. This position with respect to root node is called the rank and the rank increases as you move away from the border router. Loops are avoided by ignoring messages from a child node traveling down. A node has a parent, which sends data from the nodes to the border router and can have several children. The node is responsible for forwarding the packages of children to the border router.

Trust and Reputation is a security mechanism in environments where different entities communicate and interact. Firstly, there are different definitions of trust, but compared to the Trust and Reputation systems, the definition of Gambetta fits better "Trust (or symmetrically, mistrust) is a specific level of reasonable likelihood in which an agent assesses whether

another agent or group of agents may carry out a certain behavior, both before and in a capacity to control that activity (or in his ability to track it at all times) and in a context in which it influences his behavior."As a result of this definition, trustworthiness can be described as the probability that an entity behaves as expected. Reputation in general is an estimate of how an agent will behave in the future based on observations of his past behavior. Reputation is used because it offers an additional source on which agents can rely when they make reliable decisions [13].

The world is already computerized and the data protection from attackers is a very important task. Many unauthorized networks are joining the approved network [10]. Trust as a soft security mechanism is especially important to service-oriented IoT networks as IoT devices operated by human beings are fundamentally malicious for their own benefit. To design a trust model for the IoT, that is capable of handling the challenges and attacks such as Bad-mouthing attack, ballot-stuffing threats, and On-Off attack, several IoT trust management systems were generated, and the calculation of trust almost falls into the classification based on five design dimensions: propagation of trust, composition of trust, updating of trust, aggregation of trust and formation of trust [7].

2. LITERATURE REVIEW

Guo, J. *et al.* [7], proposed a method for classifying up-to - date trust computing models for IoT applications. The method is to identify current trust computing models based on five dimensions of the design: trust structure, trust dissemination, trust aggregation, trust upgrade and trust construction. This work outlines the benefits and disadvantages of the solutions in each aspect, and illustrates the efficacy in protection strategies against hostile attacks. Finally, it outlined the limitations in IoT trust computing research and suggested future avenues for study.

Mayzaud, A. *et al*. [12], presented a novel method to classifying attacks contained beyond the RPL. Mostly three groups of attacks were listed for that strategy. The network's longevity has been shortened by resource invasions. Such attacks produced a great deal of false contact or created a series of loops. The RPL design methodology didn't address the installation and management of the protection modes. Therefore it was established that a significant obstacle to the agreed framework of RPL networks was the interaction between various protection levels.

Aris, A. *et al*. [4], presented a detailed analysis of the attacks on RPL version number. There was also an analysis of the attacks that was focused on various scenarios. The theoretical work was focused on the specifications for IETF routing. It also measured the impact of version number invasions on node energy consumption. A probabilistic method was used to measure the probabilities for the attacks. The simulation findings revealed that the output of the mobile attackers and remote nodes had exactly the same impact on the network. An analysis will be conducted in the future on the coming actions of DIO information in order to understand the potential role of virtual number threat.

Khan, Z. A. *et al*. [9], proposes several modern IDS solutions that were really suitable to the tiny devices. The suggested solution used the trust management technique to handle the status details regarding the neighbors. The method suggested proved to be very effective in singling out nastily acting groups. In a control driven network this phase was completed. The primary purpose of the arbitrary theory of trust management was to identify the intruder nodes identified in the network. Various algorithms for controlling reputation were considered in this paper, namely Neighbor Based Trust Dissemination (NBTD), Clustered Neighbor Based Trust Dissemination (CNTD) and Tree Based Trust Dissemination (TTD).

Ma, G. *et al.* [11], Analyzing RPL security issues, setting up a test network to test RPL network security, and introducing an M-RPL security routing protocol based on RPL. The routing protocol defines a hierarchical clustering network topology, the network's intelligent system determines the backup path during the route discovery process in various clusters, enables backup paths to ensure data routing when a network is breached. The test results demonstrate the M-RPL network can avoid the routing attacks effectively. M-RPL offers a way to maintain protection over the Internet of Things (IoT).

Santiago, S. *et al.* [17], suggested the concept and implementation of energy intensive IoT routing. The routing parameters are combined to maximize network performance. The suggested methodology uses fuzzy inference method to merge energy-conscious metrics to choose the preferred direction and extend the networks' lifespan. The results are derived using MATLAB and for the specified scenario the output performance is 63.4 percent.

Abdo, H. *et al*. [1], proposed an innovative method to guarantee the security and protection of occupational hazard inquiries. To this purpose, the newly created version of the protection framework was paired with a conventionally utilized safety investigation method named bowtie analysis. The updated variant was named for study of the assault list. A new approach was proposed for the risk spectrum assessment based on two word related pieces. The one part was for protection and the other part was for defense. The findings checked indicated that the solution presented had done well. In the future the researchers will establish a more accurate and difficult technique for estimating the probability.

Hampiholi, A. S. *et al*. [3], proposed an updated GA named as MEGA (Maximum Enhanced Genetic Algorithm) utilizing the method of Local Search and Sleep-Wake-up. It optimizes the Wireless Sensor Network in such a way that there is robust energy saving and extension of network lifespan. Design and performance review of ad-hoc networking protocols is carried out utilizing software-based modeling techniques and device functionality is tested with increased energy saving and routing

capacity for various networking situations and WSN conditions.

Jaiswal, K. *et al*. [8], an Optimal QoS-aware multi-path routing protocol has been proposed for IoT-based Wireless Sensor Network. The proposed protocol defines the route from source to destination by measuring the optimum cost factor, where two factors, i.e. lifetime and congestion in a node, are taken into consideration. This provides fewer energy usage and greater QoS, given the fact that the protocol adopts two kinds of packet control. Extensive simulation was done and another routing algorithm compared to current state of the art to help improved performance of the protocol proposed.

3. PROBLEM FORMULATION

In the previous research work, the RPL routing protocol is using the broadcasting nature for the path establishment to source to destination. In the technique of broadcasting, the path establishment process using broadcasting protocol is called DODAG. In the DODAG routing protocol, if the path already exists from source to destination then the data will be directly transmitted through that path. The source flood route request packets in the network to establish path to destination. The source route request messages are flood in the network. The nodes which are adjacent to destination will reply back with the route reply messages to source node. The source select best path to destination based on hop count and sequence number.
The path which has least hop count and maximum sequence number will be selected as the best path for the data transmission from source to destination. Due to broadcasting nature of RPL routing protocol, the network bandwidth is very high and also delay for path establishment is high. In this research work, the technique of multicasting is proposed for the path establishment from source to destination because the multicasting technique is based on the trust mechanism for the path establishment from source to destination. So, it is reducing the bandwidth consumption and delay in the network.

4. RESEARCH METHODOLOGY

During this research work, the technique of multicasting is used for the path establishment from source to destination. The multicasting technique are going to be supported the trust mechanism for the path establishment from source to destination. The multicasting technique is reducing the bandwidth consumption and delay within the network.
In the trust based routing technique, trust of every node within the network is going to be calculated. The trust of every node within the network is calculated supported the amount of packets forwarded by any sensor node. The node which forward maximum number of packets within the network is considered to be as the cluster head node. The cluster head node will receive the route request messages and nodes which are responsible to established path to destination.
The path from source to destination are established which have minimum hop count and maximum sequence number. The trust of every node within the network is calculated supported the amount of packets forwarded by any sensor node within the network. The node which forward maximum number of packets within the network had maximum trust. The Trust describes the sensor node's reliability. The sensor node which is maximum reliable through that node path data is transmitted from source to destination.

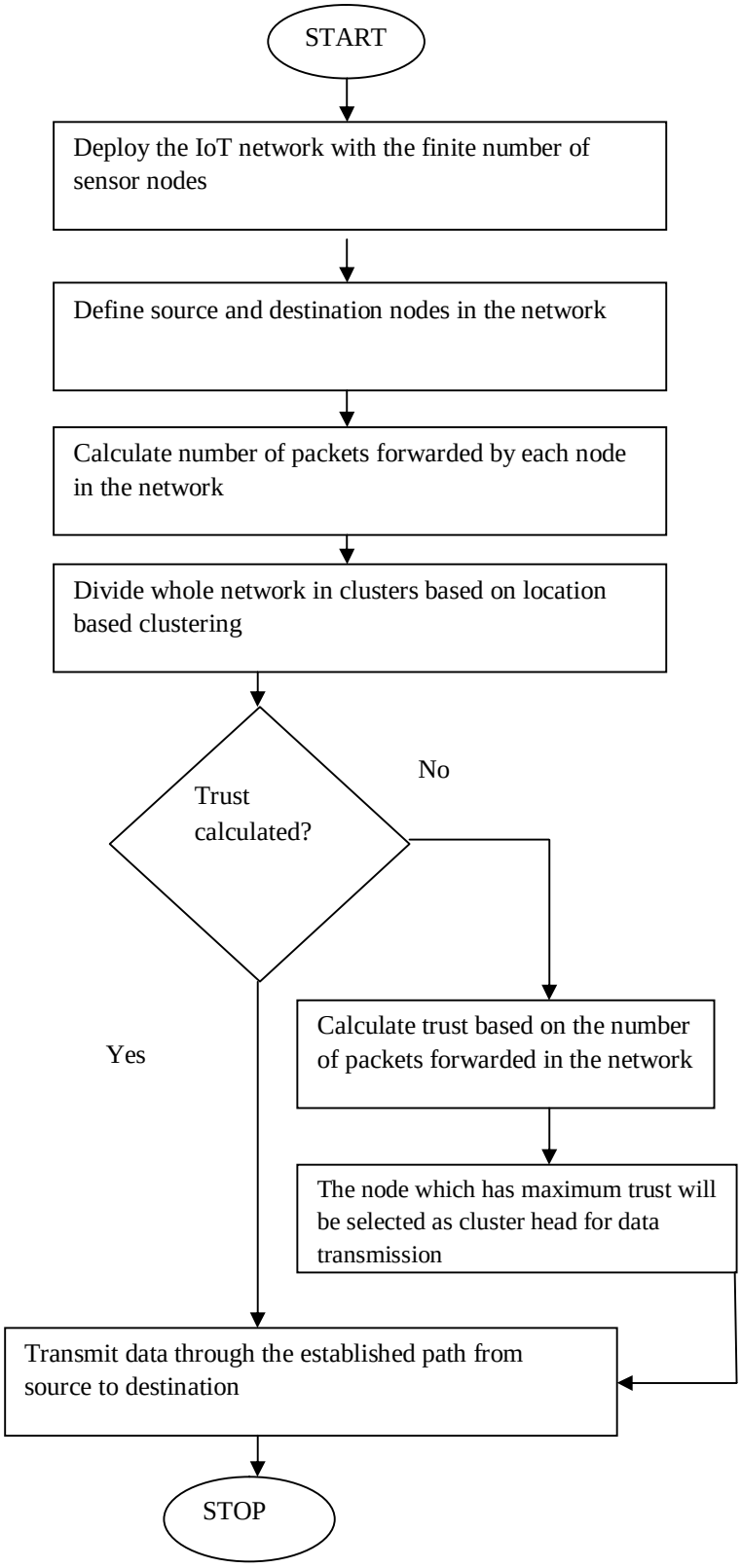

Figure 1: Proposed Flowchart

As shown in Figure 1, the network is implemented with the limited number of sensor nodes. The source nodes and destination nodes are defined within the network. The data is forwarded from source to destination. The whole network is divided up into clusters with the location based clustering. Every node's trust is calculated based on the amount of packets sent over to the network. The sensor node forwarding maximum amount of packets would have highest trust value. The sensor nodes that have the most trust value is chosen as the cluster head. The cluster head is forward details to base station.

5. RESULT AND DISCUSSION

To simulate the real moving behaviors of the nodes in a mobile ad hoc network a simulation .The evaluation will be conducted with some specific number of nodes that will be randomly scattered in a specific region with specific number of connections. To implement this proposed solution we used Network Simulator 2. The network setup is defined below in table 1.

Table 1: Simulation Parameters

Parameters	Values
No. of nodes	22
Routing protocol	RPL
Antenna type	Omni directional
Standard	802.11
Queue	Pri queue
Packet size	1000
Interval	0.05m second
No of packets in queue	50

Table 2: Delay Analysis

Simulation Time	RPL Routing Protocol	Multicasting RPL Protocol
10 second	20 packets	17 packets
14 second	22 packets	19 packets
18 second	24 packets	21 packets
22 second	27 packets	24 packets

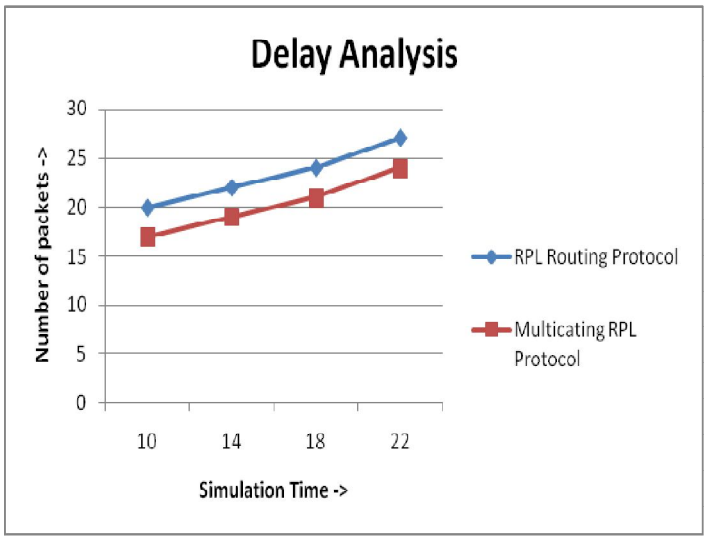

Figure 2: Delay Analysis

As shown in figure 2, delay of the proposed and existing technique is compared for the performance analysis. It is analyzed that delay of the proposed technique is less as compared to existing technique

Table 3: Packet loss Analysis

Simulation Time	RPL Routing Protocol	Multicasting RPL Protocol
10 second	26 packets	17 packets
14 second	28 packets	20 packets
18 second	30 packets	21 packets
22 second	27 packets	24 packets

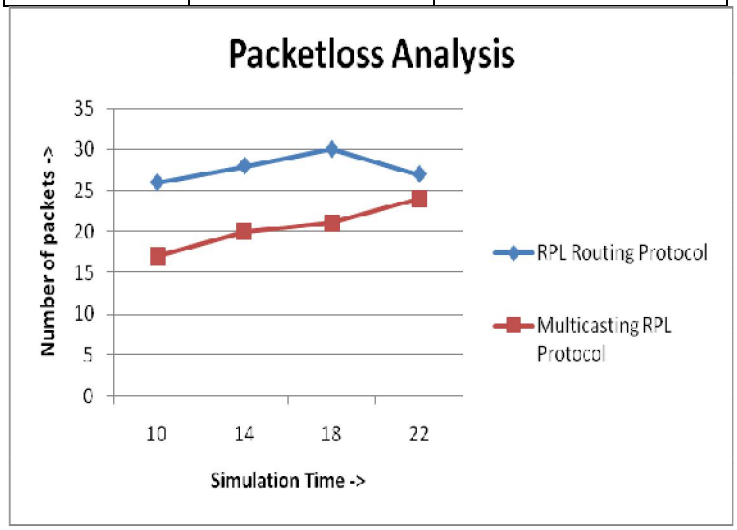

Figure 3: Packet loss Analysis

As shown in figure 3, the packet loss of the proposed technique is compared with the existing technique. The proposed technique has less packet loss as compared to existing technique.

Table 4: Throughput Analysis

Simulation Time	RPL Routing Protocol	Multicasting RPL Protocol
10 second	16 packets	27 packets
14 second	18 packets	28 packets
18 second	20 packets	31 packets
22 second	21 packets	34 packets

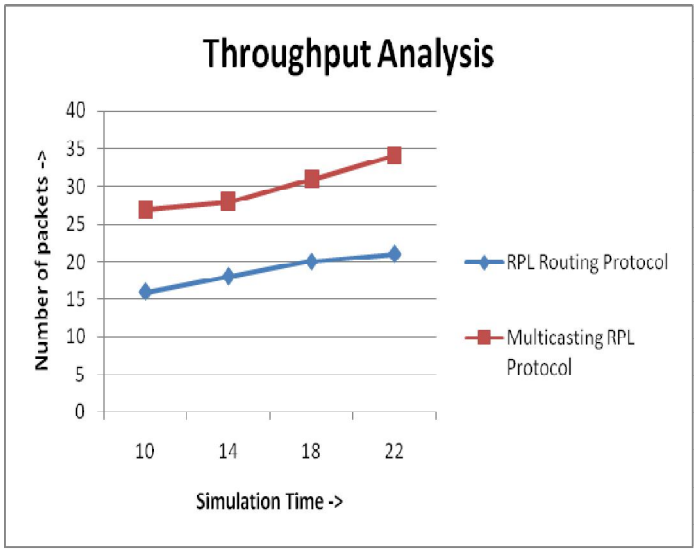

Figure 4: Throughput Analysis

As shown in figure 4, the throughput of RPL routing protocol is compared with multicasting RPL routing protocol. It is analyzed that multicasting routing protocol has high throughput as compared to RPL routing protocol.

6. CONCLUSION AND FUTURE SCOPE

It is the type of the hybrid routing protocol in which the localization of the nodes is done into sub-networks. The merits of the on-demand and proactive routing protocols are integrated using this protocol. In order to speed up communication among neighbors a proactive routing is utilized, within each zone. In order to reduce the unnecessary communication, on-demand routing is utilized by the inter-zone communication. On the basis of the distance between the mobile nodes, network is divided into various routing zones. It is analyzed when the multicasting approach is used for the path establishment then throughput, packet loss, and delay get improved as compared to broadcasting approach for the path establishment. In future multicasting approach can be improved to increase security of the network. The proposed technique can also be compared with other multicasting techniques to test reliability of the model.

REFERENCES

[1] Abdo, H. Kaouk, M. Flaus, J. M. and Masse, F. "A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis," Comput. Secur., vol. 72, pp. 175–195, 2018.

[2] Abdul-Qawy, A. S. Pramod, M. P. E. and Srinivasulu, T. "The Internet of Things (IoT): An Overview," J. Eng. Res. Appl. , vol. 5, no. 12, pp. 71–82, 2015.

[3] Aishwarya, S. Hampiholi, B. P. Kumar, V. "Efficient routing protocol in IoT using modified Genetic algorithm and its comparison with existing protocols", 2018 3rd International Conference on Circuits, Control, Communication and Computing (I4C)

[4] Aris, A. Oktug, S. F. and Yalcin, S. B. O. "RPL version number attacks: In-depth study," Proc. NOMS 2016 - 2016 IEEE/IFIP Netw. Oper. Manag. Symp., no. Noms, pp. 776–779, 2016.

[5] Baccelli, E. Philipp, M. and Goyal, M. "The P2P-RPL Routing Protocol for Ipv6 Sensor Networks: Testbed Experiments," SoftCOM 2011, 19th Int. Conf. Software, Telecommun. Comput. Networks, Split, vol. 1, pp. 1–6, 2011.

[6] Chakrabarti, A. "Emerging Open and Standard Protocol Stack for IoT," AVP Digital Practice, vol. 1, no. 1, pp. 2–6, 2015.

[7] Guo, J. Chen, I.-R. "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems", 2015 IEEE International Conference on Services Computing

[8] Jaiswal, K. Anand, V. "An Optimal QoS-aware multipath routing protocol for IoT based Wireless Sensor Networks", 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)

[9] Khan Z. A. and Herrmann, P. "A trust based distributed intrusion detection mechanism for internet of things," Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA, pp. 1169–1176, 2017.

[10] Lakshmi, N.V.V.N.J.S. Akram P.S. Bharagvi V. M. Harshika, G. Sravani, A, Study and Analysis of Defense Techniques for Various Network Topologies, International Journal of Emerging Trends in Engineering Research, vol.7, no.11, pp. 481-486, 2019.
https://doi.org/10.30534/ijeter/2019/137112019

[11] Ma, G. Li, X. Pei, Q. Li, Z. "A Security Routing Protocol for Internet of Things Based on RPL", 2017 International Conference on Networking and Network Applications (NaNA)

[12] Mayzaud, A. Badonnel, R. and Chrisment, I. "Detecting version number attacks in RPL-based networks using a distributed monitoring architecture," 2016 12th Int. Conf. Netw. Serv. Manag. CNSM 2016 Work. 3rd Int. Work. Manag. SDN NFV, ManSDN/NFV 2016, Int. Work. Green ICT Smart Networking, GISN 2016, pp. 127–135.

[13] Posegga, J. Eder, T. Nachtmann, D. Parra, D. and Schreckling, D. "Real Life Security (5827HS) Trust and Reputation in the Internet of Things Trust and Reputation in the

Internet of Things," Conference Seminar SS2013, pp. 1–19, 2013.
[14] Reddy, P.S. Akram, P.S. Sharma, M.A. Ram, P.A.S. Raj, R.P, Study and Analysis of Routing Protocols, International Journal of Emerging Trends in Engineering Research, vol.7, no.11, pp. 434 – 440, 2019.
https://doi.org/10.30534/ijeter/2019/067112019
[15] Ren, W. "QoS-aware and compromise-resilient key management scheme for heterogeneous wireless Internet of Things," International Journal of Network Management, vol. 21, no. 4, pp. 284- 299, 2011.
[16] Salman T. and Jain, R. "Networking protocols and standards for internet of things," Internet Things Data Anal. Handb., vol. 1, no. 1, pp. 215–238, 2017.
[17] Santiago, S. Arockiam, L. "A novel fuzzy based energy efficient routing for Internet of Things", 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET).
[18] Zhang T. and Li, X. "Evaluating and analyzing the performance of RPL in contiki," Proc. first Int. Work. Mob. sensing, Comput. Commun. - MSCC '14, pp. 19–24, 2014.