Improving the Power and EnergyCo-efficient using Load Balancing Routing Protocol in Internet ofThings

Ms. Himanshi Ramani
Research Scholar, Department of Computer Science and Engineering,
Geetanjali Institute of Technical Studies
Udaipur, India
himanshi9511@gmail.co

Dr. Ajay Kumar Sharma
Associate Professor, Department of Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
profsharmaak@gmail.com

Dr. Mayank Patel
Professor, Department of Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
mayank999_udaipur@yahoo.com

Dr. Narendra Singh Rathore
Director, Geetanjali Institute of Technical Studies
Udaipur, India
director@gits.ac.in

Article Info
Page Number: 6928 - 6939
Publication Issue:
Vol 71 No. 4 (2022)

Abstract

Routing Protocol for Low-Power and Lossy Networks (RPL) is an IPv6 routing protocol that is standardized for the Internet of Things (IoT) by Internet-Engineering Task Force (IETF). RPL forms a tree-like topology which is based on different optimizing process called Objective Function (OF). In most cases, IoT has to deal with low power devices and lossy networks. So, the major constraints of the RPL are limited power source, network life time and reliability of the network. OFs depend on different metrics like Expected Transmission Count (ETX), Energy, Received Signal Strength Indicator (RSSI) for route optimization. In this work, the ETX and Energy based OF have been evaluated in terms of energy-efficiency and reliability. For one sink and nine senders, the simulated average power consumption is 1.291 mW and 1.56 mW respectively, for

Article History
Article Received*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

ETX OF and Energy OF. On the other hand, the average hop count for ETX OF is 1.89, which is 3.01 for Energy OF. Thus, ETX OF is more energy-efficient but it is not reliable as it takes fewer hops with long distances. Moreover, it does not take load balancing and link quality into account. However, Energy OF is more reliable due to short hops, but it is not energy efficient and sometimes it might take unnecessary hops.

INTRODUCTION

The Internet of Things (IoT) is a model of modern computing that refers to material devices that are connected to each other. These IoT devices have networking built in so they can connect, talk to each other, and share data. IoT devices are another name for these things that connect to each other. Concerns have been raised about security as the number of Internet of Things devices grows, especially when it comes to sharing sensitive data. Authentication is one of these things to think about when deciding how trustworthy something is. Authentication is a big problem in the Internet of Things because the protocols, devices, and topologies are so complicated. Internet of Things systems that connect to each other need to be able to be trusted so that carelessness doesn't lead to security problems.

Authentication is not only needed for access management to work, but also for communication to be clear. The Internet of Things (IoT) is made up of knots with very few resources. These knots are spread out across the IoT ecosystem in a way that doesn't depend on time or place. The Internet of Things (IoT) is being used in a wide range of places right now, such as hospitals, smart homes, smart factories, and smart cities. Also, a hypertext net age can be used between different handheld terminals. However, it is also possible that most (if not all) of our programmes could be run over a fifth-generation (5G) cellular network, which was just created and is now being made available to the public. Make a link between the information held by different objects or switch the information between objects. By the year 2022, 43 billion devices are expected to be connected to the Internet of Things around the world. When 5G networks become commercially available, this number is likely to grow dramatically.

Routing Information Replay Attacks

An RPL node can also be used to carry out attacks that use routing information replay. It saves control messages from other nodes that are still good, and then sends them to a different part of

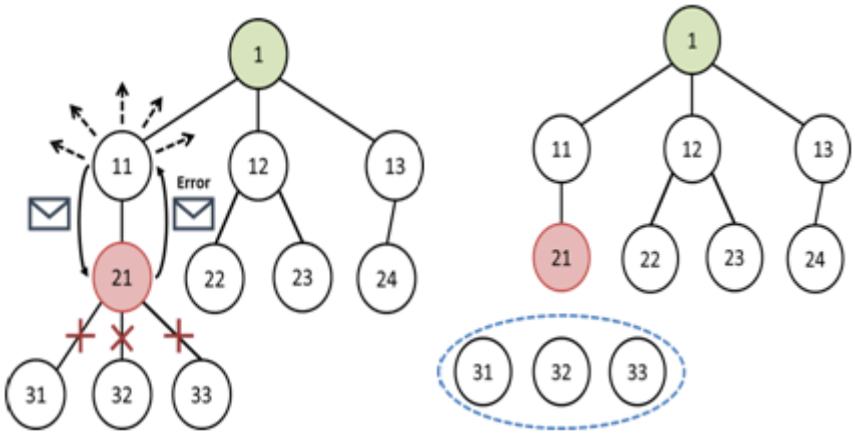
the network at a later time. Because the topology and routing paths of dynamic networks change often, this kind of attack can do a lot of damage to them. Because of replay attacks, nodes will add old information to their routing tables, which will lead to a fake topology. A few sequence counters are used by the RPL protocol to make sure that the routing information is as up to date as possible. The version number for DIO messages and the path sequence number can be found in the transit information option of DAO messages [80]. This attack is talked about in [66], but the authors don't look into its possible effects or explain how it could happen in RPL networks.

Worst Parent Attacks

This method, which is called a "Rank attack" and is explained in involves picking the desired parent who is the least desirable according to the objective function in a methodical way. The result is that the path that is made is not the best one, which means that performance is bad. Because child nodes depend on their parents to route packets and because neighbours can't keep an eye on this attack, it can't easily stop it. But if a security solution is put in place that rebuilds a global view of the network based on information from the nodes, like the method described inthis attack should be found.

DAO Inconsistency Attacks in Storing Mode

DAO inconsistencies happen when a node has a downward route that was learned from a DAO message, but this route is no longer valid in the routing table of the child node [80]. This path was learned from the parent node before. RPL has a way to fix this problem. It's called DAO inconsistency loop recovery in the data path validation. The Forwarding-Error "F" flag in data packets is an optional way for RPL router nodes to delete downward routes that are no longer valid. This flag tells the RPL router nodes that a packet can't be sent by a child node. This is done by the RPL router nodes. Figure 3.4 shows that the data packet with the "F" flag is sent back to the parent so that another neighbour node in the network can be used. Once a packet has been sent in the wrong direction, it should never be sent in that direction again. When this happens, the router sends the packet back to the parent that sent it with the Forwarding-Error "F" bit set and the Down "O" bit left. This means that the packet has been sent on to the next place. When the parent gets the packet with the "F" bit set, it clears the "F" bit and tries to send the packet to another neighbour. This happens because the parent deletes the routing state that is needed. If the condition of the alternative neighbour remains the same, the operation will be done again.



(a)Initial State (b) Final State

Figure 1: Illustration of a DAO inconsistency attack.

In this situation, you need to watch out for Node 21, which is the bad node. It does this by telling RPL routers to get rid of legal downstream routes, which takes nodes out of the DODAG graph. The "F" flag is used to do this. When node 21 gets a packet from node 11, it only changes the RPL "F" flag before sending the message back to node 11. Because of this, the last 31–33 nodes of the network are cut off from the graph.

RPL Security

According to the RPL specifications, the protocol is supposed to have the following security features: On the other hand, the specification says that implementing these security elements (either in part or in full) is "optional": RPL was made so that when link-layer security measures are available, they can be used to protect the transport of messages. RPL has its own security measures, which are mostly provided by the following three security modes:

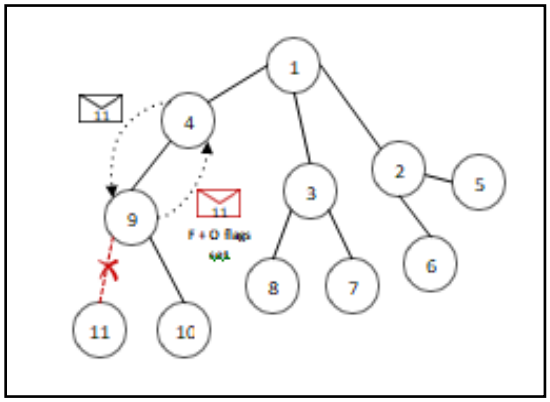


Figure 2: DAO inconsistency loop recovery procedure.

UM: The mode that RPL will automatically switch to whenever it needs to depend on link-layer security. During this mode, no security precautions are used with regard to RPL control messages; instead, they are communicated with one another in plain text.

PSM: On each node, a preinstalled encryption key, also called a symmetrical key, is set up by hand. When nodes join or maintain the DODAG, they use this key to encrypt and decrypt the secure versions of RPL control messages. It is recommended that you use this mode when you need a secure routing solution even though you only have a small number of devices.

ASM: Here, two different encryption keys are used: a preinstalled one (similar to PSM), which allows any node to join the DODAG as a leaf node (a node that doesn't have any children and doesn't do routing), and an authenticated key, which is only used by routing-capable nodes to create and maintain the DODAG. Both of these keys are used together to encrypt information. In this case, routing nodes need both keys to be able to talk to other routing nodes and leaf nodes that already have the preloaded key (using the authenticated key). You can only get these authenticated keys from a trusted authentication authority. How this authority verifies the nodes and gives them their keys, on the other hand, is something that is up to the implementation. The extra "Replay Protection" feature of RPL is called "Consistency Check," and it can be turned on or off as needed. These checks compare a non-repeating value (Counter with CBC-MAC "Cipher Block Chaining-Message Authentication Code" (CCM) Nonce), which is sent in CC secure messages, with the stored status information (the address of the originating node and the CCM nonce value that was most recently received from that node). The goal of this comparison is to find out if the originating node has already used the CCM nonce value that was sent.Both the PSM and the ASM exchange encrypted RPL control messages. RPL uses AES/CCM (Advanced Encryption Standard (AES) in CCM mode) with a 128-bit key to make a 32-bit or 64-bit Message Authentication Code to make sure that the sent messages are private, secure, and true (MAC). By using these MACs, the messages' integrity can be guaranteed. As an added layer of security, RPL uses Rivest-Shamir-Adleman encryption (RSA) and Secure Hash Algorithm (SHA)-256 for digital signatures of the messages to make sure they are private and real (with support for 2048- and 3072-bit signatures, respectively). It's important to note that RPL has only been offered by UM implementations up until now. No RPL implementation, even the most popular ones like Contiki OS [8] and TinyOS [45], has security measures like these. Perazzo et al. [46, 47] proposed a partial implementation of RPL's security features by adding PSM and the replay

protection to ContikiRPL (Contiki OS's implementation of RPL) (Contiki OS implementation of RPL). Simulation tests in Contiki were used to figure out how well the authors' plan worked. They showed that putting RPL in PSM by itself (with no replay protection) won't add much to the time it takes to set up a network, the control overhead of RPL, or the amount of power it uses. But large-scale networks, in particular, will need more power because of the replay prevention system (with more than 25 nodes).

Classification of RPL Attacks and Mitigation Methods

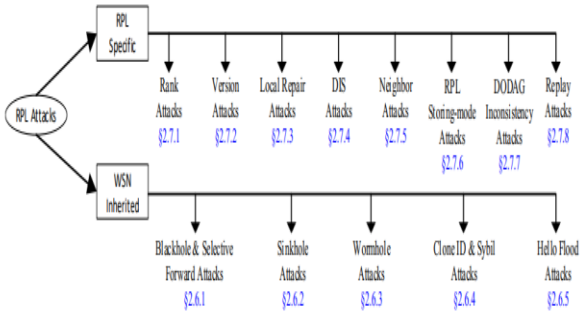


Figure 3: Classification of RPL attacks.

Classification of RPL's Attacks

The Internet of Things is similar to wireless sensor networks (WSNs) in some ways, but it lets objects talk to the Internet all the way down to their own parts. This means that attacks on IoT networks will come from both WSNs and more traditional networks like the Internet [22]. In this chapter, we'll talk about routing attacks that can happen to RPL. Based on where they came from, these attacks can be put into two groups: those that came from WSNs and those that RPL made by taking advantage of its own weaknesses (RPL-specific attacks). Figure shows both of these types of attacks, as well as some examples of common attacks that fit into each category. 2.6. A thorough look at these attacks and the steps that can be taken to stop them

PROPSOED SYSTEMS

TX and Energy are two very important factors for figuring out how well OF is doing. Both ETX and energy-based OF have been tested and evaluated using simulations. Figure 4.1 shows how the sender

nodes are spread out randomly across the network in each of these cases. So that an accurate assessment can be made, the deployed zone has been cut in half so that each half is the same size. The sink is at a distance of 0 metres from the line, and the other sender nodes are between 0 and 100 metres away. Senders that are between 0 and 50 metres from the sink are considered closer nodes because they are closer to the sink. Senders that are between 50 and 100 metres away are called "far nodes" in this show how the average amount of power used by ETX-based OF and Energy-based OF differs for closer and farther nodes, respectively. In RPL, the amount of power that each node uses can be broken down into four groups: I transmit power (also called Tx power), II receive power (also called Rx power), III CPU power, and IV low power mode (LPM) power. In an energy-based OF, a node uses an average of 1.56 milliwatts of power. In an ETX-based OF, a node uses an average of 1.291 milliwatts of power. So, it's clear that the ETX OF has a better rating for energy efficiency than Energy.

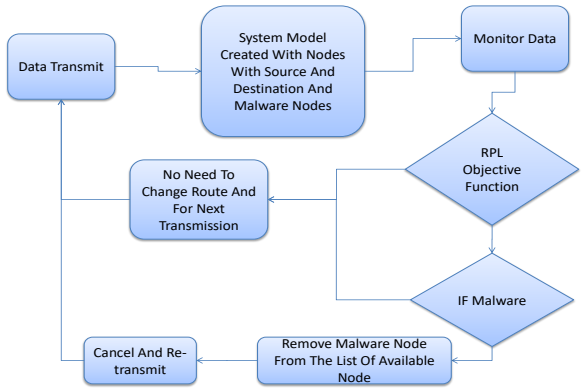


Figure 4flow diagram

A new routing protocol for the Internet of Things called energy-efficient load-balanced RPL (EL-RPL). In this protocol, an algorithm is given as a way to choose parents. It chooses a parent from the parent list to be the next hop node on the path to the destination node based on the highest amount of energy left and the total number of packets the parent has received. This might make it easier for all the parents on the list to do their share of the work. The EL-RPL protocol also makes DODAG creation better by stopping DIO packets from being sent to nodes with lower ranks. This is how it improves the development of DODAG. This will lead to less energy use, which will in turn make the networks last longer. A lot of experiments were done with the MATLAB simulator in order to find out how well the RPL routing protocol works. The results show that the proposed RPL protocol can save energy, cut down on the number of control packets, and make IoT networks last longer than they do with other protocols that are already in use.

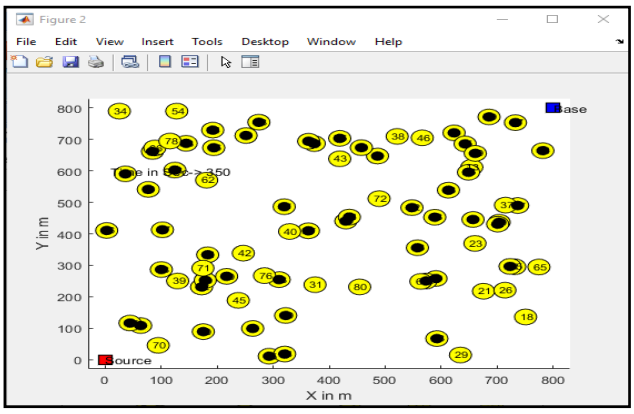


Figure 5 Node deployment

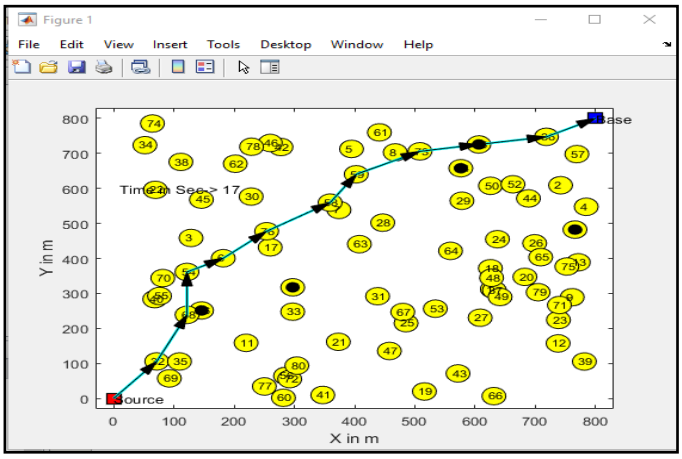


Figure 6 Step 1 The sink/root initialises

Step 1 For DODAG data to start, the root (sink) must send out the first control messages DIO. These messages will include the RPLInstanceID, DODAG identification, version number, rank, and the RPL-supported OF used to calculate the rank.

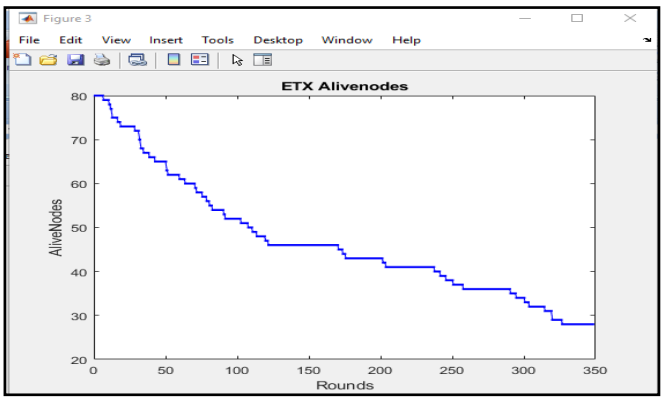


Figure 7 ETX alive node

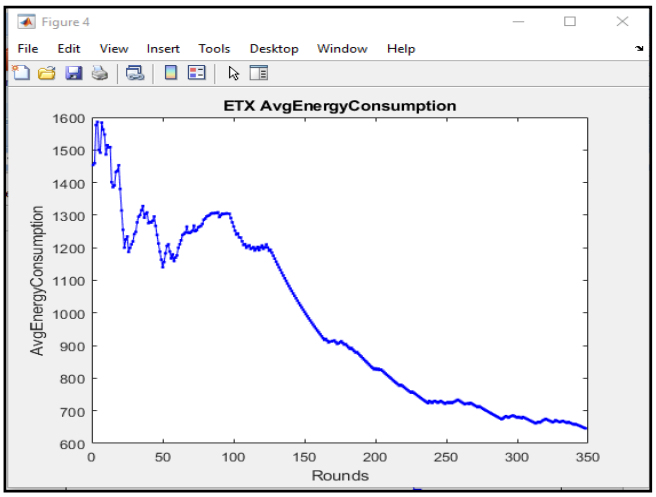


Figure 8 ETXAvg Energy Consumption

An RPL-based Internet of Things network for smart cities can be made reliable by improving the network's performance and making it last longer. Performance metrics can be used to measure how well a network works. Some examples are the convergence time, the amount of power used, the amount of control traffic overhead, and the packet delivery ratio. On the other hand, the reliability of the network can be measured by the node participation metric. Our proposed Multi DODAG architecture tries to make RPL for Smart City IoT work better and be more reliable.

Performance metrics

When analyzing the performance of our protocol and contrasting it with the performance of the standard RPL protocol, we make use of the following metrics.Energy consumption The following calculation is used to determine the average cumulative energy consumption in the network. This is done so that it can be counted.

$$EC \leftarrow \left(1 - \left(\frac{\sum_{j=1}^{P} \frac{\sum_{i=1}^{n} E_i}{n}}{P}\right)\right) * 100$$

where EC is the average value of the energy consumption for each node during each period, n is the "number of nodes" in the network, P is the number of periods, and Ei is the total amount of energy that node I consumed during all of those periods.

Energy consumption

The quantity of energy that is used has a big effect on how long the nodes will last. It has mostly to do with sending and receiving messages, processing on the central processing unit (CPU), and being idle or overhearing. Using the equation, you can figure out the average amount of energy each node used during each period (4).

Table1 ETX OF Proposed System and Existing System

	ETX OF	
	Proposed System	Existing System
TXPower	7.17	7.99
RXPower	50.88	50.07
LPMPower	14.94	11.15
CPUPower	30.57	30.18

Conclusions

Energy savings, which will in turn increase the lifetime of the network. The suggested protocol offers a method for power-efficient routing that helps low-power nodes in local area networks (LLNs) preserve the power of their batteries. The MATLAB simulator was used to conduct a number of experiments in order to evaluate the efficacy of the EL-RPL routing protocol in comparison to two other protocols: RPL and IRPL. The findings demonstrate that our suggested protocol is capable of conserving energy in an effective manner, reducing the number of control packets, and enhancing the IoT network's lifetime in comparison to competing protocols. In the not too distant future, one of our goals is to build a new objective function that may be used for the selection and persistence of routing paths by combining several metrics. Taking into consideration the dependability of routing is one way to make the suggested protocol better. In order to evaluate how effective the improved RPL technique is, one of our goals for the future is going to be to conduct actual tests.

References

1. MingyuPark;GunmoJeong;HeedeokSon;JeongyeupPaekPerformance of RPL Routing Protocol over Multihop Power Line Communication Network2020 International Conference on Information and Communication Technology Convergence (ICTC)Year: 2020 | Conference Paper | Publisher: IEEE
2. SharwariSolapure;HarishKenchannavar;Umakant P. KulkarniAnalysis of Various RPL Protocol Objective Functions for Quality of Service Parameters2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)
3. P. Deepavathi;C. MalaEMR-ESD: Ensure Multicast Routing and Enable Secure Data transmission protocol to perform multicast forwarding in RPL based IoT Networks2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)Year: 2022 | Conference Paper | Publisher: IEEE
4. Pedro David Acevedo;DaladierJabba;PaulSanmartín;SebastiánValle;Elías D. Nino-RuizWRF-RPL: Weighted Random Forward RPL for High Traffic and Energy Demanding ScenariosIEEEAccessYear: 2021 | Volume: 9 | Journal Article | Publisher: IEEE
5. BoonpipobNapasiripakorn;KananbadeeSrisomboon;Wilaiporn LeeComprehensive Study of Parent Selections with Trickle Timers for RPL Protocol in AMI Network2022 37th International Technical Conference onCircuits/Systems, Computers and Communications (ITC-CSCC)Year: 2022 | Conference Paper | Publisher: IEEE
6. IliarRabet;HosseinFotouhi;MaryamVahabi;MárioAlves;MatsBjörkmanRPL-RP: RPL with Route Projection for Transversal Routing2021 IEEE 7th World Forum on Internet of Things (WF-IoT)
7. Rong-GueiTsai;Pei-HsuanTsai;Guan-RongShih;JingxuanTuRPL Based Emergency Routing Protocol for Smart BuildingsIEEEAccessYear: 2022 | Volume: 10 | Journal Article | Publisher: IEEE
8. Patel, M., Choudhary, N. (2017). Designing an Enhanced Simulation Module for Multimedia Transmission Over Wireless Standards. In: Modi, N., Verma, P., Trivedi, B. (eds) Proceedings of International Conference on Communication and Networks. Advances in Intelligent Systems and Computing, vol 508. Springer, Singapore. https://doi.org/10.1007/978-981-10-2750-5_17
9. Mohamed RedhaBouakouk;AbdelkrimAbdelli;LyndaMokdadODM-RPL: Optimized Dual MOP RPL2021 IEEE Symposium on Computers and Communications (ISCC)Year: 2021 | Conference Paper | Publisher: IEEE

10. Patel, Mayank, and Ruksar Sheikh. "Handwritten digit recognition using different dimensionality reduction techniques." International Journal of Recent Technology and Engineering 8.2 (2019): 999-1002.
11. Khalid A. Darabkh;Muna Al-AkhrasRPL over Internet of Things: Challenges, Solutions, and Recommendations2021 IEEE International Conference on Mobile Networks and Wireless Communications(ICMNWC)Year: 2021 | Conference Paper | Publisher: IEEE
12. Mohammad HosseinHomaei;Shahab S. Band;AntonioPescape;AmirMosaviDDSLA-RPL: Dynamic Decision System Based on Learning Automata in the RPL Protocol for Achieving QoSIEEE AccessYear: 2021 | Volume: 9 | Journal Article | Publisher: IEEE
13. Paul Sanmartin;KarenAvila;SebastianValle;JavierGomez;Daladier JabbaSBR: A Novel Architecture of Software Defined Network Using the RPL Protocol for Internet of ThingsIEEEAccessYear: 2021 | Volume: 9 | Journal
14. ShiplaSen, MayankPatel, Ajay Kumar (2021). Software Development Life Cycle Performance Analysis. In: Mathur, R., Gupta, C.P., Katewa, V., Jat, D.S., Yadav, N. (eds) Emerging Trends in Data Driven Computing and Communications. Studies in Autonomic, Data-driven and Industrial Computing. Springer, Singapore. https://doi.org/10.1007/978-981-16-3915-9_27
15. NesrineKhelifi;SoufienJaffali;FatmaMallouli;AyaHellal;HabibYoussefA survey on Mobility Under RPL Routing Protocol2022 IEEE 9th International Conference on Sciences of Electronics, Technologies ofInformationand Telecommunications (SETIT)Year: 2022 | Conference Paper | Publisher: IEEE
16. Shekhawat, V.S., Tiwari, M., Patel, M. (2021). A Secured Steganography Algorithm for Hiding an Image and Data in an Image Using LSB Technique. In: Singh, V., Asari, V.K., Kumar, S., Patel, R.B. (eds) Computational Methods and Data Engineering. Advances in Intelligent Systems and Computing, vol 1257. Springer, Singapore. https://doi.org/10.1007/978-981-15-7907-3_35
17. Syeda Mariam Muzammal;Raja Kumar Murugesan;NoorZamanJhanjhi;Low Tang JungSMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoTApplications2020 International Conference on Computational Intelligence (ICCI)
18. Badis Djamaa;Mustapha Reda Senouci;Hichem Bessas;Boutheina Dahmane;Abdelhamid MelloukEfficient and Stateless P2P Routing Mechanisms for the Internet of Things IEEE Internet of Things Journal Year: 2021 | Volume: 8, Issue: 14 | Journal