# Directed Acyclic Graph Inherited Attacks and Mitigation Methods in RPL: A Review

P. S. Nandhini[1,2](✉) and B. M. Mehtre[2]

[1] Department of CSE, Kongu Engineering College, Perundurai, India
nandhinisvl@gmail.com
[2] Centre of Excellence in Cyber Security (COECS), IDRBT,
Established by RBI, Hyderabad, India
bmmehtre@idrbt.ac.in

**Abstract.** RPL (Routing Protocol for Low Power and Lossy Network) is designed for Low Power and Lossy Network (LLN). In RPL, both the nodes and links have resource constraints. There will be many RPL instances in the network. The operation of RPL requires bidirectional links that exhibits asymmetric properties. LLNs do not have predefined network topology. Directed Acyclic Graph (DAG) is organised as a topology by RPL. It uses control packets for associating the data packets with a RPL instance and for validating the routing states. The manipulation done in the control packets and constrained resource of RPL leads to various attacks such as rank attack, DIS attack, Version attack, etc., In this paper, we have discussed the operation of RPL, classification of attacks and various mitigation methods. We have also concentrated on DAG inherited attacks because it degrades the overall performance of the network.

**Keywords:** RPL · Bidirectional · Asymmetric · DAG · LLN · Instance · Rank attack · Version attack · Control packets

## 1 Introduction

Internet of Things (IoT) is a collection of heterogeneous devices or things that are uniquely identified and connected to the Internet. The smart devices can be a wide variety of devices such as smart phones, RFID tags, actuators and sensors. The origin of IoT has led to the connection of devices, people, services and many objects [1]. It plays a major role in security sensitive areas also. The IoT has transformed traditional things or objects to smart device with the help of enabling technologies such as embedded devices and softwares, communication technologies, wireless sensor network, Internet protocols and applications [2].

The devices are heterogeneous in IoT network and so they use various standards. There are various protocols for IoT. IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) is one of the protocols. It is a simple low-cost communication network. It allows connectivity in applications where throughput is relaxed and the resource is constrained [3]. LoWPAN include devices that co-ordinate together for connecting the physical devices to real time applications. The architecture of 6LoWPAN is shown in Fig. 1.

P. Karrupusamy et al. (Eds.): ICSCN 2019, LNDECT 39, pp. 242–252, 2020.
https://doi.org/10.1007/978-3-030-34515-0_25

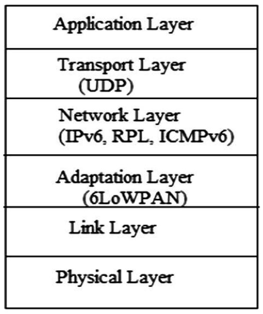

**Fig. 1.** Architecture of 6LoWPAN

The inclusion of a new layer called Adaptation Layer in between the Link layer and the Network Layer is the major difference regarding the architecture [4]. The functions of the adaptation layer [5] are compression and decompression of UDP and IPv6 header, fragmentation and reassembly of packets and routing of packets.

The paper is organized as follows: Sect. 2 overviews the operation of RPL protocol and the control packets used for the construction of DAG. In Sect. 3, the DAG inherited attacks and the mitigation methods are discussed. In Sect. 4, we have provided the concerns, challenges and opportunities related to RPL. The conclusion is in Sect. 5

## 2 RPL Overview

RPL is designed for resource constrained networks. It is a Distance Vector Routing protocol. The LLNs like Radio Networks don't have predefined topologies i.e., wires between nodes. So, RPL protocol has to find links and select nodes efficiently which is done with the help of control packets [6]. It is a source routing [7] protocol.

### 2.1 RPL - Control Messages

If the value of the type field in ICMPv6 message is 155 then it signifies the RPL control message. There are five RPL control messages. The control message of RPL can be identified from the code field. The control message has the base field that depends on the code.

**DODAG Information Solicitation (DIS):** This is used for soliciting DIO control message from nodes in RPL. It is similar to the router solicitation which is used in the neighbor discovery in IPv6. A node explore its neighbor with the help of DIS message to identify the nearby DODAGs.

**DODAG Information Object (DIO):** It holds the information that are needed by the node to identify an instance of RPL, learn the configuration parameters, selection of the DODAG parents and the maintenance of the DODAG. This is used by the root of the DODAG for the construction of a new DAG. It is multi-casted in the DODAG. The base object fields of this message are RPLInstanceID, Version number, Rank, Destination Advertisement Trigger sequence number (DTSN), grounded flag, mode of operation, DODAG preference. DTSN is used for the maintenance of downward routes.

**Destination Advertisement Object (DAO):** This is used for the propagating the information about the destination in the upward direction. In the storing mode of RPL, for the selection of the parent DAO message will be unicasted by the child. In the non-storing mode of RPL, the DAO control packet is sent to the root of the DODAG. DAO message is acknowledged by (DAO-ACK) message to the sender.

**Destination Advertisement Object Acknowledgement (DAO-ACK):** This control packet is delivered as a response to an unicast DAO message. The response is also unicasted. The message of recipient could be a parent of DAO or root of the DODAG.

**Consistency Check (CC):** It is delivered as a secured message. It is used for checking and synchronising the message counters or timestamps between each pair of nodes. It is used for issuing challenge-response.

### 2.2 DODAG Construction and Maintenance

DODAG construction consists of two steps: (i) DIO control message is broadcasted from the root down to the client to construct routes in the downward direction. (ii) DAO message is unicasted for constructing routes in the upward direction. It is issued by the client to the DODAG root. The construction of DODAG is depicted in Fig. 2.

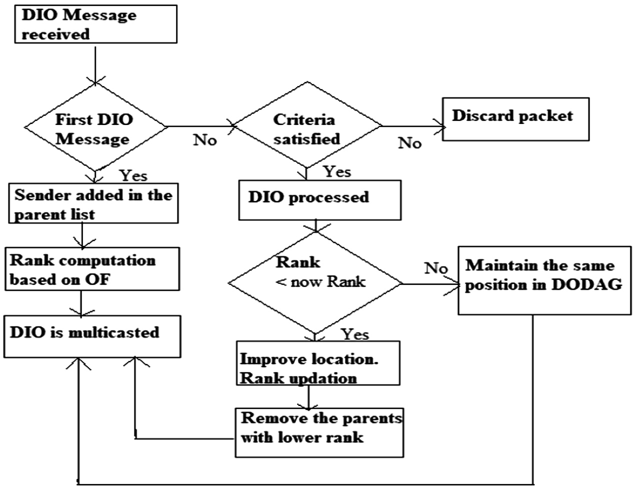
DIO Message received
First DIO Message
No
Criteria satisfied
No
Discard packet
Yes
Sender added in the parent list
Yes
DIO processed
Rank computation based on OF
Rank < now Rank
No
Maintain the same position in DODAG
DIO is multicasted
Yes
Improve location. Rank updation
Remove the parents with lower rank

**Fig. 2.** Construction of DODAG

For the construction of the DODAG: (i) DIO message is broadcasted. It contains DODAGID, rank information [8], Object Function [9, 10]. (ii) DIO message can be received by a node which is willing or not willing to join the DODAG (It may also be a member of DODAG already). If a node wants to get added in the DODAG: (i) Adds the address of the sender of the DIO message to the parent list (ii) Calculate rank based on OF (iii) Forwards the updated rank in DIO.

The node then chooses a node as a parent from the parent list, through which the traffic passes. If a node is already a DODAG member and if it obtains another DIO message, it can be processed in different ways: (i) Based on the criteria of RPL, it can discard the DIO message (ii) Process the DIO message to retain its location in the DODAG where it is a member already (iii) If the computed rank is lower then it churns its location. If a rank of the node is changed, it must remove all the nodes in the parent list to avoid loops.

Grounded DODAG will offer connectivity to the nodes that are needed for obtaining the goal of the application. Floated DODAG will not satisfy the goal but it provides the routes to nodes in the DODAG (Example: During repair, it is used to maintain interconnectivity). The DODAG is maintained by the trickle timer. It is used for optimizing the frequency of message transmission depending on the condition of the network. The duration of the timer increases exponentially whenever the timer is fired.

### 2.3 Repairing DODAG

The repairing of the DODAG can be done in two ways: (i) Global Repair: The root of the DODAG performs a global repair by increasing DODAG version which leads to a new version of DODAG. The nodes can take a new position in the newly formed DODAG. (ii) Local Repair: This is performed within the DODAG version. The parameters necessary for configuration are specified in the DIO message. DODAG loops occur when a node gets detached from the DODAG and tries to reattach to a device in its sub-DODAG where its attached. If DIO message is missing, then loop is encountered. Mostly, this looping problem occurs during local repair.

## 3 Classifiaction of RPL Attacks

Due to resource constraints and manipulation of RPL control packets, RPL is prone to various attacks such as wormhole attack, blackhole attack, rank attack, version attack, etc. The attacks can be classified as address based attacks and DAG based attacks. The classification of attacks is depicted in Fig. 3. Since there are huge number of attacks, DAG inherited attacks and its countermeasures have been reviewed.

### 3.1 Rank Attack

In RPL, the rank of a node gets incremented from DODAG root to the child node. If the value is altered, the attacker (i) Attracts the child node for selecting the parent (ii) Improve the metrics (iii) Attract large amount of traffic to flow through the attacker.

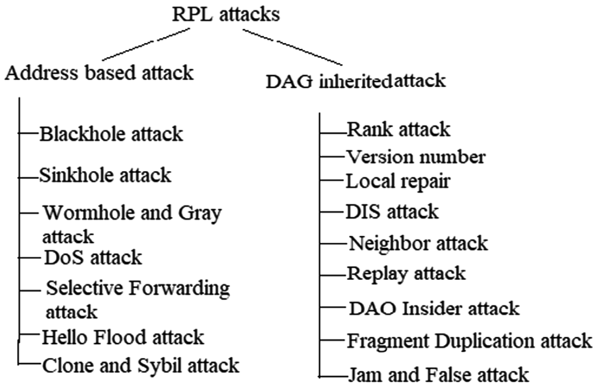

**Fig. 3.** Classification of RPL attacks

In Fig. 4, the black color node is an attacker. Its rank is 3 but it manipulates its rank to be 1 and tries to attract the neighbor nodes which are blue in color. According to [11], the child node will receive the information about parent through the control messages. If there is an attacker, it takes a bad quality route. There are different types of rank attack. It will degrade QoS parameters. If rank attackers are deployed in crowded area, the performance of the network is degraded.

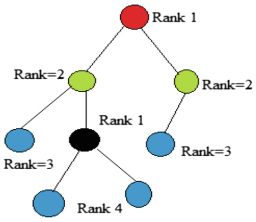

**Fig. 4.** Rank attack

According to authors [12], the attack aimed at rank property will have various effect on the RPL performance. The authors have depicted that the rank of node has increased to the maximum rank of its neighbors after running the simulation for particular time. The consequences of this is that (i) There are loops between root nodes and its child (ii) The network is not stable and many control packets are generated for optimizing the topology. According to [13], the rank attack is done to attract and manipulate the traffic in the network. The rank attack is done by compromising rank information. The node will not change itself.

Kamble et al. [14] proposed three types of rank attacks. They are (i) Increased Rank attack (ii) Decreased Rank attack (iii) Worst parent attack.

**Mitigation Methods:**

Airehrour et al. [15] proposed SecTrust-RPL. It is a secure trust-aware RPL for IoT. SecTrust -RPL is used for the detection of Sybil and Rank attack. It isolates the attacker from the network. The trust system is incorporated in the RPL protocol. It evaluates trust by examining the successful delivery of packets between the nodes. The computed trust value is used for making optimal routing decision, while isolating the attacker from the network. No re-integration of battery drained pre-trusted nodes after the recovery of battery power.

Shafique et al. [16] proposed SBIDS. It is Sink based Intrusion Detection System. It provides high detection of rank attacker. All the detection processes are carried out in the sink node and so less computational overhead. More routing metrics including energy, throughput, ETX, etc., can be included along with rank in the proposed algorithm for enhancing the detection rate of the rank attacker.

Semedo et al. [17] proposed Vulnerability Assessment of Objective Function of RPL Protocol for IoT. In this paper, the authors have induced the rank attack by altering the objective function (OF0 and MRHOF). The effect of energy depletion and delivery ratio of packet in the presence and absence of attacker is analysed. The rank attack removes a node completely from the network. The recent advancement techniques such as Machine Learning, Artificial intelligence can be deployed to detect the rank attack.

Stephen et al. [18] proposed Energy based Validation and Verification (E2V). It is a technique for detecting and identifying Rank Inconsistency Attack (RInA) in IoT. E2V detects the inconsistency in the rank based on the node's energy level. The calculation of rank, identification and elimination of malicious node are the mechanism integrated for providing a secured communication in IoT networks. The E2 V mechanism is included in the root node for the identifying the attacker. The energy of the root node gets depleted quickly.

Sahay et al. [19] proposed Attack Graph - based Vulnerability Assessment of Rank Property in RPL-6LoWPAN in IoT. The consequences of violation of the properties of rank also results in various attacks. More energy consumption and high traffic overhead are the consequences of Increased Rank attack. Large interruption in the network and DODAG formation is the consequence of decreased attack. Increased end-to-end delay and the network sub-optimization are the consequences of worst parent selection.

## 3.2 Version Number Attack

Version number is one of the fields in each DIO message. When there is a global repair, it is increased by the DODAG root. If the value is not updated, then the older value signifies that it can't be used as a parent. The attacker node can modify the version number, when DIO message is forwarded to its neighbors. This will lead to the rebuilding of DODAG unnecessarily. The consequence of this attack is that (i) Many loops are created (ii) Loss of data packets (iii) Overhead of control message (iv) Congestion in network.

**Mitigation Methods**

Mayzaud et al. [20] performed the version attack to identify the effects of it on the performance of the networks. It is identified that there is 18 times increase in overhead. The attack has doubled the delay and the delivery ratio is reduced by 30%. The attacker position is the main concern that determines the network performance.

Perrey et al. [21] proposed TRAIL (Topology Authentication for RPL). The proposed method relies on (i) DAG root is the trust node (ii) The nodes interconnect to the root in a hierarchy. The strong cryptographic mechanism is used for the detection of topology attacker. TRAIL is scalable and reliable.

Luchi et al. [22] proposed a scheme for selection of parent node in construction of route. The scheme will exclude the attacker node from the network. If there are multiple parents for a node then the node will choose a parent after denying the best candidate. The attacker will publish the lower rank than the good ones. From the simulation, it is found that the attackers had no effect in parent selection of node in the proposed scheme. It is achieved by reducing the total number of child nodes attached to the attacker.

## 3.3 Local Repair Attack

The attacker node will periodically send local repair message. When the node near to it, it hears this message, it starts its local repair message. On comparing with other attacks, local repair attack has more effect on the packet delivery ratio. It generates more control packet. The delay is also increased. The node energy will get exhausted due to this attack.

**Mitigation Methods**

TRAIL [21] discussed in the mitigation method of version number attack can be extended to local repair attack. The IDS is the best solution for mitigating local repair attack.

## 3.4 DIS Attack

DIS control packet is used by a node to obtain the topology information. During this attack, the attacker sends DIS message periodically. On receiving this message, the neighbor nodes will reset the DIO timer. This happens because the node assumes that there is some disruption in the topology. If the attacker node unicasts the DIS control packet, the destined neighbor node provides response to it by sending DIO. This implies that the receiver is ready to join the network. There is no impact on delivery ratio. It is a multicast attack and the delay is increased. This attack creates overhead due to control packets. The energy of the node gets depleted.

**Mitigation Methods:**

There is no specific mitigation method for this attack. Specification based IDS is a good solution for mitigating DIS attack.

### 3.5 Neighbor Attack

In this attack, the DIO control packet which is received by the attackers is broadcasted to its neighbors without any manipulation. If the sender is not in the transmission range, the attackers try to create an image that the sender is also in the transmission range. The victim node could select the parent that is not in its range. It is identical to the wormhole attack. This attack is created by forwarding the DIO control packets selectively. The consequences of this attack are: (i) QoS parameter is affected (ii) Packet delivery ratio has no effect (iii) End-to-end delay is slightly increased (iv) Slight topology disruption. If this is combined with other attacks, it is difficult to mitigate.

**Mitigation Methods:**
According to [3, 23], there is no specific method to mitigate this attack. It is hard to identify this kind of attack. Location based mitigation method can be used to detect this kind of attacks. Some IDS can also be extended to mitigate this kind of attack.

### 3.6 Replay Attack

This attack is created by replaying the routing information. The malicious node saves the routing information from other nodes and forwards it later. The receiver node will update their routing table. Thus, the table is updated using outdated routing information. The topology gets altered. This will lead to the disruption of topology and routing paths. The DIO VersionNumber or DAO message path sequence is used to confirm the freshness of the routing information.

**Mitigation Methods:**
According to [6], Winter suggested that integrating MIC (Message Integrity Code) is not sufficient to prevent this kind of attack.

Perazzo et al. [24] proposed that MAC layer encryption can be used to distinguish DIO message from other routing messages and data messages. This alone is not sufficient to prevent this kind of attack. Along with this, the replay protection mechanism can be used. Replay protection mechanism allows the good nodes to detect the false DIO message. So, replay protection technique can also be used for mitigation of this kind of attack. For dynamic RPL network, there is no specific mechanism for mitigation so far.

### 3.7 DAO Insıder Attack

To build the routes in downward direction, DAO message is used. The RPL specification does not reveal when and how the DAO messages are transmitted. The attacker transmits the DAO message repeatedly to create overhead in the network. According to [25], DAO message is transmitted based on DIO trickle timer. The child unicasts the DAO message to its parent on three situations (i) On receiving a DIO message from its preferred parents (ii) On changing the parents (iii) On detecting specific errors.

**Mitigation Method:**

Ghaleb et al. [26] proposed SecRPL for addressing the DAO Insider attack. SecRPL limits the DAOs forwarded by a parent. The restrictions are applied in 2 ways: (1) Restricting the number of forwarded DAO messages regardless of the node that sent the DAO message intially. (2) Restricting the number of forwarded DAO control messages for each destination. The deployed malicious node triggers the DAO attack by sending DAO control message to its parent. The DAO attack varies from DIS attack because DAO packets are broadcasted from end to end. This type of attack is implemented without the need for compromising the security keys from legitimate nodes (Table 1).

**Table 1.** Review of the mitigation methods of DAG Inherited Attacks

| Attacks | Effects on network performance | Mitigation methods | Review on the mitigation methods |
|---|---|---|---|
| Rank attack | Formation of loops, less packet delivery ratio, generation of unstable paths, packet delay. It affects the performance of the network | SecTrust-RPL, SBIDS, Vulnerability Assessment of Objective Function, E2 V, Graph – based Vulnerability Assessment | The attack aimed at rank property will create multiple impact on performance of RPL. In all the proposed mechanism the resource constraints of the nodes are considered |
| Version number attack | Control packet overhead is increased, less delivery of packets, more delay | Topology Authentication for RPL, Secure Scheme for parent selection | The control packet overhead is reduced and the delivery ratio is increased |
| Local Repair attack | Topology formation disruption due to overhead in control packets | TRAIL and IDS | It is a reliable and scalable mechanism |
| DIS attack | More resource consumption | Specification based IDS | Not implemented so far |
| Neighbor attacks | False route, route disruption, more resource consumption | Location based mitigation method | Not implemented so far |
| Replay attacks | Routing and topology disruption | Replay protection technique | No specific mechanism for dynamic RPL |
| DAO insider attack | Overhead in the network due to large number of DAO messages | SecRPL | It limits the number of DAO message sent by the parents |

## 4 Issues, Concerns and Challenges

From the review, it is clear that vast number of researches have been conducted for preventing and detecting attacks in RPL. There are certain challenges that need to be addressed. They are

- The security features of RPL remains unexplored
- Many options are available in RPL that remains unused. This can be explored to provide security
- IDS is one of the mitigation methods for encountering the attacks. The resource constraint nature of the node should be considered while implementing IDS
- Cooja is the most widely used simulation for evaluation. Many tools and testbeds can be explored for evaluation

## 5 Conclusion

In this paper, DAG inherited attacks and their mitigation methods are reviewed. The performance of the network is degraded significantly, due to the manipulation of RPL control packets. The attacks, effects of the attacks on the RPL, mitigation methods and the significance of mitigation methods are tabulated. Thus, this review will provide a platform for the future researches who conduct research on RPL based attacks and mitigation methods.

## References

1. Conti, M., et al.: Internet of Things security and forensics: challenges and opportunities, pp. 544–546 (2018)
2. Al-Fuqaha, A., et al.: Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutorials **17**(4), 2347–2376 (2015)
3. Pongle, P., Chavan, A.: A survey: attacks on RPL and 6LoWPAN in IoT. In: 2015 International Conference on Pervasive Computing (ICPC). IEEE (2015)
4. Pai, V., Shenoy, U.K.K.: 6LowPan—performance analysis on low power networks. In: International Conference on Computer Networks and Communication Technologies. Springer, Singapore (2019)
5. Garg, R., Sharma, S.: A study on need of adaptation layer in 6LoWPAN protocol stack. Int. J. Wirel. Microwave Technol. (IJWMT) **7**(3), 49–57 (2017)
6. Winter, T., et al.: RPL: IPv6 routing protocol for low-power and lossy networks. No. RFC 6550 (2012)
7. Clausen, T., Herberg, U., Philipp, M.: A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL). In: 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE (2011)
8. Vasseur, J.P.: Terms used in routing for low-power and lossy networks. No. RFC 7102 (2014)
9. Deshmukh-Bhosale, S., Sonavane, S.S.: A real-time ıntrusion detection system for wormhole attack in the RPL based Internet of Things. Proc. Manuf. **32**, 840–847 (2019)

10. Verma, A., Ranga, V.: Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT. Wirel. Pers. Commun. 1–24 (2019)
11. Le, A., et al.: The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sens. J. **13**(10) 3685–3692 (2013)
12. Xie, W., et al.: Routing loops in dag-based low power and lossy networks. In: 2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE (2010)
13. Dvir, A., Buttyan, L.: VeRA-version number and rank authentication in rpl. In: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems. IEEE (2011)
14. Kamble, A., Malemath, V.S., Patil, D.: Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. In: 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI). IEEE (2017)
15. Airehrour, D., Gutierrez, J.A., Ray, S.K.: SecTrust-RPL: a secure trust-aware RPL routing protocol for Internet of Things. Future Gener. Comput. Syst. **93** 860–876 (2019)
16. Shafique, U., et al.: Detection of rank attack in routing protocol for Low Power and Lossy Networks. Ann. Telecommun. **73**(7–8) 429–438 (2018)
17. Semedo, F., Moradpoor, N., Rafiq, M.: Vulnerability assessment of objective function of RPL protocol for Internet of Things. In: Proceedings of the 11th International Conference on Security of Information and Networks. ACM (2018)
18. Stephen, R., Arockiam, L.: E2 V: techniques for detecting and mitigating rank inconsistency attack (RInA) in RPL based Internet of Things. J. Phys.: Conf. Ser. **1142**(1) (2018). IOP Publishing
19. Sahay, R., Geethakumari, G., Modugu, K.: Attack graph—based vulnerability assessment of rank property in RPL-6LOWPAN in IoT. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE (2018)
20. Mayzaud, A., et al.: A study of RPL DODAG version attacks. In: IFIP International Conference on Autonomous Infrastructure, Management and Security. Springer, Heidelberg (2014)
21. Perrey, H., et al.: TRAIL: topology authentication in RPL. arXiv preprint arXiv:1312.0984 (2013)
22. Iuchi, K., et al.: Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network. In: 2015 21st Asia-Pacific Conference on Communications (APCC). IEEE (2015)
23. Le, A., et al.: Specification-based IDS for securing RPL from topology attacks. In: 2011 IFIP Wireless Days (WD). IEEE (2011)
24. Perazzo, P., et al.: DIO suppression attack against routing in the Internet of Things. IEEE Commun. Lett. **21**(11), 2524–2527 (2017)
25. Dunkels, A., et al.: Contiki: the open source OS for the Internet of Things. 13 October 2012 (2015)
26. Ghaleb, B., et al.: Addressing the DAO Insider Attack in RPL's Internet of Things networks. IEEE Commun. Lett. **23**(1) 68–71 (2019)