Ingénierie des Systèmes d'Information
Vol. 27, No. 1, February, 2022, pp. 165-170
Journal homepage: http://iieta.org/journals/isi

Resource Based Attacks Security Using RPL Protocol in Internet of Things

RatnaKumari Challa[1], Kanusu Srinivasa Rao[2*]

[1] Department of Computer Science and Engineering, RGUKT-AP, IIIT - Rk Valley, Kadapa 516330, Andhrapradesh, India
[2] Department of Computer Science and Technology, Yogi Vemana University, Kadapa 516005, Andhrapradesh, India

Corresponding Author Email: kanususrinivas@gmail.com

https://doi.org/10.18280/isi.270120

Received: 15 October 2021
Accepted: 12 January 2022

Keywords:
RPL, IoT, resource-based attacks, security, allied parent

ABSTRACT

The (IETF) shaped the Protocol for low-power lossy networks, which is now known as the LLN routing protocol (RPL) by taking into consideration different circumstances of restricted networks. This protocol was designed to promote the use of numerous direction-finding topologies recognized as DODAGs, which remained developed below a variety of dissimilar goal purposes to enhance routing via the use of various routing techniques. Because there were billions of devices that were linked all over the globe, security is a significant issue when routing in Internet of Things devices, and many assaults take occur throughout the routing process. While routing, a variety of assaults may occur, some targeting network architecture, others targeting network traffic, and still others targeting network resources. This paper investigates resource-based dos attack, which are designed to consume node energy, memory, by forcing hostile nodes to undertake unnecessary processing activities, as well as processing power. These attacks also have an impact on network accessibility and the lifetime of the configuration, as well as on the accessibility of the network. Following up and monitoring each node, these allied nodes use the suggested restrictions to not only identify resource assaults in RPL, but also to update the root node's information about the malevolent bulge in instruction to eliminate it from the DODAG network. The suggested model's results are compared to that of prior attack detection replicas in relationships of system of measurement such as packet drop, final latency, and throughput.

1. INTRODUCTION

RPL was a distance vector and a source steering mechanism for long-range networks (LLNs) that was developed by the Internet Engineering Task Force (IETF) primarily for the Internet of Things [1, 2].

They are DIO (DODAG Information Object) control messages, which advertise the data needed for maintaining and developing DODAG, and they are sent by RPL [2]. The creation of DODAG was started by root, who sent out DIO messages in a multicast fashion. Nodes select their preferred parent depending on the rank of the node they received when they received a DIO message. After completion of establishment process of DODAG each node has default route to root node with their preferred parents. If a node wants to sends any message, then it first approaches the preferred parent if the conveyance fails then it chooses the non-preferred parent by turns. Within RPL every node in the network can decide either the packets to be forwarded in any routing either up or down [3]. Figure 1 explain the DODAG formation in RPL protocol.

To preserve the topology RPL uses some main values related within RPL control messages explained in Table 1 like DIO, DIS, DAO, DAO-ACK.

In RPL to avoid the loops it uses a concept called rank rule, the rank implies the place of the node relevant to remaining nodes regarding to DODAG root. Rank rule determines that the parent node should always hold the lower rank compared to its child [4]. Each DODAG consist of version number, if new node joins the existing topology the version number changes. A node's rank, version number, objective function [5] can be determined in DIO control message.

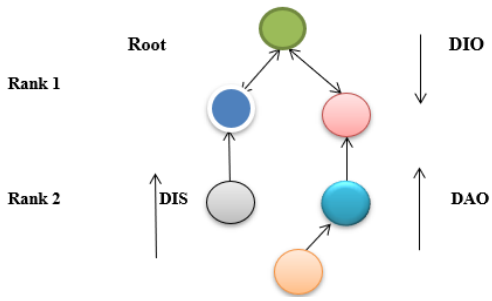

Figure 1. DODAG formation in RPL

Table 1. Important terminology related to DODAG

DODAG ID	A value to identify the DODAG
DODAG Version number	Each new shape of DODAG represents a new edition, which is represented by a sequential counter that has been increased by the root to create a new variant.
RPL instance ID	A DAG comprises of several DODAGs which are identified by RPL instance ID, set of one or more DODAGs share same ID
Rank	It helps for identifying the position of a node
Objective function	Determines how routing metrics, as well as certain associated functions, are utilized to determine rank in the system.

There is an essential to safeguard direction-finding procedures against assaults and to offer safety aimed at the means of defending data. As previously shown, RPL has a number of built-in security features, however they were not adequate to protect against all kinds of assaults. These are the sources from which the odds of an assault occurring are known as indicated in the Table 2 below:

Table 2. Attack description and goal of attacks

Type of attack	Attack description	Goal of attack
Rank attack	The packets were not sent to preferred parent by attacker	Route disruption, node energy consumption
Version attack	Alters the version number which is associated to topology	Less packet delivery ratio, disrupt the entire topology
Neighbour attack	DIO message will be forwarded to neighbour by the attacker without updating	Route disruption, resource consumption
Worst parent attack	An attacker node itself selects the worst parent	Less packet delivery ratio, node energy consumption

Attack patterns, capabilities, and state of the attacker are only known if we are able to identify the threat sources attacking the network. Security measures are only recommended if we are able to identify the intentionally or negligently attacking the network.

Threats and attacks are referred to as outsiders in this scenario, because they are not real nodes; rather, they are duplicate nodes that damage the system and steal the data.

However, there will be many assaults in order to steal the data or to demolish the topology, which will be discussed more below. The Resource-based assaults are the ones among all of them that are primarily concerned with increasing the amount of energy used by a node while simultaneously decreasing the life duration of the topology. A fake node modifies the version number, rank, and selects the worst parent for itself. It also advertises the false ranks to neighbour nodes associated with a topology, causing the entire topology to be rebuilt, consuming a significant amount of energy and shortening the network's lifespan and lifespan of the network. When it comes to the version number and rank in the DIO base object, there is no way provided by the standardized protocol to ensure the honesty of the given version number and rank and to select only preferred parents [6]. Moreover, there is no way provided by the standardized protocol to ensure the integrity of the given version number and rank. The rebuilding of topology results in an increase in overhead as well as loops in the topology. Past research has shown that assaults on RPL have a significant impact on networks, and prior studies have explored strategies for countering such attacks and offered solutions for certain kinds of attacks, despite the fact that these solutions have disadvantages.

In this paper we proposed an allied parent follow up technique in which these allied parent nodes are deployed in the network to detect all these resource based attacks in RPL by following each and every node and detecting the malicious node and informing to the root node. Through this technique the resource based attacks can be found easily and eliminated in RPL networks through which there will be decrease in control overhead and increase in life time of topology. The main contributions are (1) the structure of a removal strategy of attacks and its related algorithm, (2) the placement of allied node into the topology through simulation (3) the performance assessment of our solution via experimental evaluation. The remaining work is sectioned as follows section 2 characterizes the relate work, section 3 characterizes the resource based threats in RPL and their goals and section 4 characterizes about proposed work and its working with algorithm and flow chart and section 5 about test results and section 6 terminates the paper.

2. LITERATURE SURVEY

A security threat examination [1] was performed by IETF RoLL working group for RPL in which the security issues were identified in RPL and also addressed those issues, also classified the identified threats into four categories those are authentication, integrity, confidentiality, availability.

Murali et al. [7] introduced an energy efficient parent selection algorithm in which node selects the best parent which is energy efficient and to reduce the loss of packets a concept called D trickle timer and the results shown the outcome with respect to PDR and energy consumption was good in proposed algorithm but with respect to end to end delay it shows less delay but not complete decrease in the delay while maintain the network consistency during the stage of mobility by establishing a strong path towards destination.

Ghaleb et al. [8] an algorithm named drizzle algorithm was introduced as a new routing primitive for LLNs. Drizzle reduces the delay problems for mitigating the negative effect on the transmission delay problems and also achieve better results than standard RPL [9] with respect to decreasing the delaying and increments the power of the node and it also shows the better results than as compared with normal RPL regarding packet delivery ratio and less delay and also consumes less energy of nodes.

Dvir et al. [10] VeRA has two major drawbacks: it has a greater computing cost and it is potentially prone to attacks. Mayzaud et al. [11] proposed method, on the other hand, provides authentication for version and rank within the DIS base object through hash and signature methods, preventing malicious nodes from pretending to be the root and receiving fake version numbers, which could cause the entire topology to be disrupted or recreated entirely.

However, Perrey, Heiner et al. proposed a model TRAIL [12] has the benefit of being less complicated than VeRA since nodes don't have to send data from neighboring nodes to DODAG root. Although TRAIL offers many advantages, it does have a flaw in that a child node may choose a malicious node as its parent, resulting in an attack known as the worst parent attack.

Several intrusion detection systems [13] finds the intruders that only if a node that does not follow a specific behaviour referred to the routing protocol, but this detects well the topology attacks it fails to detect any version number attacks, it only sorts out where the fake node can violate the rules. Another intrusion detection system is SVELTE [14] which consists of three phase. One for reconstructing the DODAG by intrusion detection, the second one maintains the process of intrusion detection and final one was a mini distributed firewall, but no one of these is used to identify version number attacks. However, SVELTE [15] has two problems where the false detection is high and other is the root of the DODAG [16] has to give intruder information to all other nodes but there is a problem that this information cannot be correctly spread

under the influence of attacking nodes. In order to provide a security based supervision solution, a distributed monitoring structure was introduced, because none of these intrusion detection system address resource based attack properties.

Anth´ea et al. [17] To detect the malicious node a monitoring node was executed in which positioning procedure is done by root node after assembling the data about detection from the monitoring node and the study evaluated the proposed method through trails and also analysed the execution considering different metrics and shown that it can detect version number attacks [18-20] effectively but this monitoring node doesn't work well for any other attack except the version number it identifies the increase in version number and then informs to the root node where the malicious node located and the proposed method cannot be able to find if many malicious nodes are present in the network.

2.1 Resource based attacks in RPL

The main perspective of resource based attacks in RPL is to consume energy of a node and memory of a node or making the fake node perform unnecessary processing. The resource based attacks effects the network availability and also shortened the life time of the network. Below Figure 2 explains the Resource based attacks in RPL.

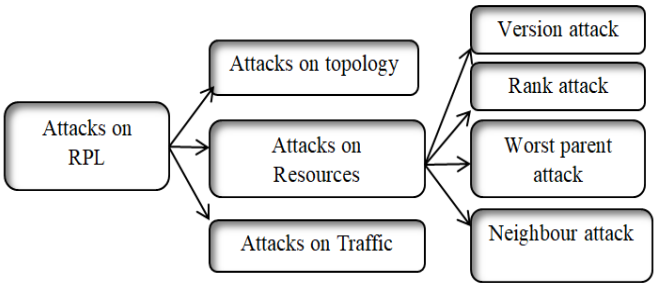

Figure 2. Resource based attacks in RPL

A) Version number attacks: There is an important field in every DIO format known as version number, and it is possible for a rogue node to increase its version number in order to send DIO to other nodes with fake version numbers, causing the entire topology to be rebuilt, as well as increasing the overhead of control messages and reducing the lifetime of the network.

B) Neighbor attack: This takes place when a fake node forwards an unmodified DIO to other nodes to better creating a delusion that true sender of the message is within the range of neighboring nodes but actually it is not within the broad range of the neighboring nodes. The worst situation is the neighbor node chooses one node with a good rank as preferred parent node but actually it is much far away from the node or it may be out of their range.

C) Worst parent attack: This attack is very difficult to detect because a malicious node itself chooses the worst parent and advertises its actual rank to all other nodes and uses this rank technique which attracts others to choose it as parent node, and using the worst path while forwarding the packets can lead to increasing in delays and loops in routing.

D) Rank attack: The range of rank increments from root to child nodes, the malicious node changes its rank to the better rank value and attract the child nodes to select it as a preferred parent node by advertising better rank; the main idea behind the rank attack is to disrupt entire routing topology and to introduce delays.

3. PROPOSED MODEL

In this section we introduced a new allied parent follow up technique which helps to detect and eradicate all the above mentioned resource based attacks in RPL network. The algorithm for formation of DODAG and allied node identification is shown below where the topology is formed in which the root multicast DIOs to the available nodes and root maintains all the id's of the nodes and allied nodes, along with DIO control message the root send nearest allied node id to node, from where a node identifies the allied nodes and communicate with it, later the node communicate with allied node in order to make a node either as node's preferred parent or child.

DODAG formation and allied node identification:

1. Start // for number of nodes n
2. Pn Nodes not in DODAG
3. Qn Nodes in DODAG
4. Set hop count for all nodes i in Pn as 0
5. Combaine root node in DODAG and eliminate it from Pn
6. Now root belongs to Qn
7. Repeat
8. For every node in Qn do
9. {
10. Root (node id, allied node id)
11. R a node in a DODAG, S allied node in DODAG
12. Qn Qn U {R,S}
13. Multicast DIO (VN, R, OF, nearest allied node id)
14. Receive DAO messages from nodes
15. Construct DODAG
16. }
17. End

Allied Node follow up procedure:

A root node multicast DIO messages to the available nodes with its nearest allied node id to join the DODAG and to form a topology. The nodes who were willing to join the DODAG sends DAO replay to root node and then root node validates the rank of the nodes based on objective function and sends DAO ACK, the node choose the parent which rank is less than that to establish the network and allied nodes updates their routing table. The parent nodes multicast DIO's to choose them as preferred parents to the remaining available nodes which are not joined or to the nodes which rank is far greater than root. By receiving DIO's the nodes initialize the path discovery, n receives j possible paths towards the root and validates the path and send some preferred parents data to available allied node before processing DIO's in order to detect if any malicious node is there.

The allied node on receiving DIO's checks preferred parent version number and Validates ranks based on objective function, here if any rank attacker node is present it can be detected because here a node modifies the rank as a better rank but allied node calculates its correct rank based on objective function ETX (Expected transmission count) and also checks Version number (preferred parent)=Version number (root), here Version number attacks can be detected here, if a node changes its version number and send fake updates to child node it can be detected by allied node and informs to root node. If node is malicious then sends message to root and informs to node which sends request to join as a child. The neighbour attack can also be detected here because on receiving a DIO

message every node sends data to allied node, if any node with unmodified DIO is seen it is a malicious node. If not, a malicious node allied node selects the best parent, if a node doesn't accept the best parent selected by allied node, then the node is malicious, worst parent attack is detected here a node itself selects a worst parent, if not node changes its path to preferred parent.

Algorithm for allied parent follow up mechanism:

Step 1: Begin
Root node multicast DIO's to the available nodes
Parent=i;
Rank(i) < Rank(node)
Choose Parent and allied node updates its routing table
Step 2: Received a DIO
then
node initializes the path discovery
node receives j possible paths towards the root
validate path();
Rank (Preferred parent) < Rank (Parent)
Step 3: node allied node
allied node preferred parent (Version number, Rank)
if
Rank Objective function, Version number (Preferred Parent) = Version number (Root)
Go to step 4
else
node is detected as malicious
end for
Step 4: allied node selects the best parent based on rank
if
node preferred parent
node is not malicious
else
node is malicious
}
Step 5: End

Advantages of allied node follow up procedure:

- Helps to maintain the great lifetime of the network
- Works efficiently to find number of attacking nodes within the network
- By detecting all the resource-based attacks the energy, memory and processing power of the nodes can be saved
- Works efficiently for the network with many numbers of nodes
- Both detection and isolation are done, shows better performance than standard RPL and improves security.

4. EXPERIMENTAL RESULTS AND DISCUSSION

Experimental setup:

Used 4GB RAM and intel processor as hardware, Instant Contiki is a finished Contiki advancement condition running inside an Ubuntu Linux virtual machine (Ubuntu 14.04 LTS) that has every one of the compilers, improvement instruments and simulators expected to the examination.

Results and discussion:

Some of the metrics may be used as parameters to determine RPL's behavior and performance. Energy consumption, Packet delivery rate, end-to-end latency, convergence time, and throughput are only a few examples of variables. Throughput, packet delivery ratio, and end-to-end latency were all taken into account in the research.

Measuring results:

a) Network throughput measures the speed at which data packets are successfully delivered across a network connection. As a result, we may total the packets received by all nodes to arrive at the value for small networks. In a wired or wireless network, network simulators may be used to evaluate throughput (either instantaneously or on average).

Formula: Throughput is equal to the sum of the total number of true packets times the average packet size times the whole length of time it takes to send that many packets.

b) Packet Delivery Ratio (PDR) is the proportion of packets sent by the source that were received by the destination. b) Packet Delivery Ratio.

PDR is defined algebraically as: N1 / N2.

When the total number of packets received by the destination equals N1, then the total number of packets produced by the source equals N2.

c) End-to-end delay is the time difference between when a packet is produced and when it is received. It's also called a one-way delay since it refers to the time it takes a packet to go from its originator all the way to its recipient across the network.

E2E Delay is calculated as the sum of the delays experienced at the sender, receiver, and intermediate nodes.

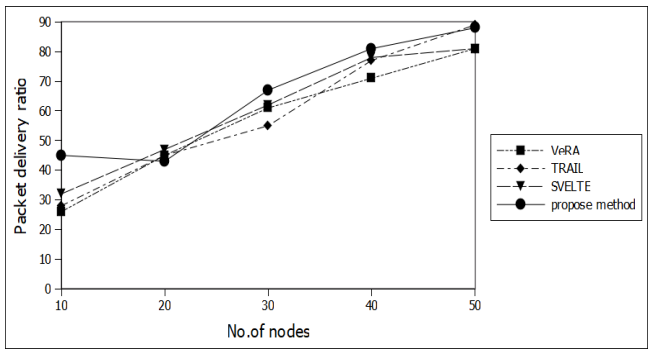

Figure 3. PDR of RPL for 10 to 50 nodes

Figure 3 shows PDR of RPL under 10 to 50 node, graph shows PDR of RPL protocol of the proposed system is high when compared to previous studies where they evaluated version, rank, neighbour and worst parent attacks. By obtained outcome we can see the PDR is good in the proposed system and it somewhat decreases and there is less ratio when compared to present method.

Figure 4 shows throughput of RPL under 10 to 50 node and the graph shows throughput of RPL protocol of the proposed system is high means the rate at which the packet delivery is good when compared to previous studies where they evaluated version, rank, neighbour and worst parent attacks. By obtained outcome we can see the throughput is good in the proposed system and it somewhat decreases and there is less ratio when compared to present method.

Figure 5 shows end to end delay of RPL under 10 to 50 node and the graph shows delay of RPL protocol of the proposed system is low means the difference of time for packet generation between sender and is less at which end to end delay is less when compared to previous studies where they evaluated version, rank, neighbor and worst parent attacks. By

obtained outcome E2E delay is less in the proposed system and it somewhat increases when compared to present method.

Hence the obtained results shown for the important metrics we considered like PDR, throughput, end to end delay the proposed model shown the better results with respect to these three metrics than compared to the previous works.

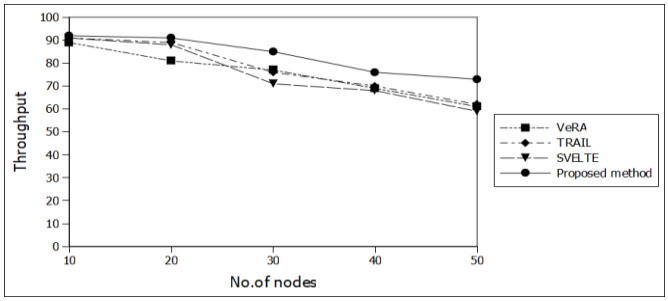

Figure 4. Throughput of RPL for 10 to 50 nodes

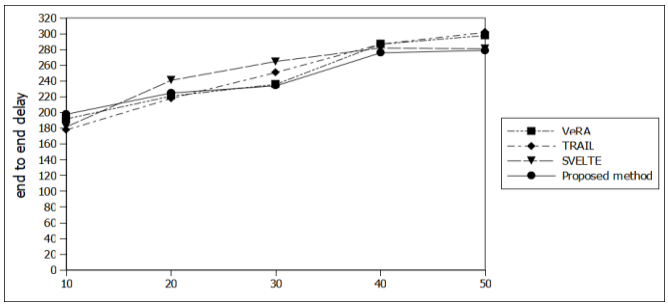

Figure 5. End to end delay of RPL for 10 to 50 nodes

5. CONCLUSIONS

In the RPL network, numerous devices are linked, but secure communication is hampered by assaults on the topology, resources, and traffic of the network. These attacks may be eliminated by using an associated node that inspects the entire topology and removes resource-based threats including variety quantity bouts, vigorous occurrences, foreigner occurrences, and the nastiest parental attack. This novel attack eradication method was presented in this article. Each bulge in the RPL topology will have access to this ally node, which will help them communicate with one another, select the best favoured parental for them, and find the aggressive bulge. This will extend the lifetime of the topology, reduce node energy consumption, improve packet delivery ratios, and shorten end-to-end delays throughout the network. The obtained findings indicate that the proposed model's work is better than in prior research when measured according to the specified criteria. As a result, the allied node approach protects the RPL topology from various threats, increases its packet delivery ratio and amount, and also helps to extend the network's life by reducing latency and node energy consumption.

REFERENCES

[1] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J.P., Alexander, A. (2012). RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks.

[2] Kamgueu, P.O., Nataf, E., Ndie, T.D. (2018). Survey on RPL enhancements: A focus on topology, security and mobility. Computer Communications, 120: 10-21. https://doi.org/10.1016/j.comcom.2018.02.011

[3] Gaddour, O., Koubâa, A. (2012). RPL in a nutshell: A survey. Computer Networks, 56(14): 3163-3178. https://doi.org/10.1016/j.comnet.2012.06.016

[4] Ghaleb, B., Al-Dubai, A.Y., Ekonomou, E., Alsarhan, A., Nasser, Y., Mackenzie, L.M., Boukerche, A. (2018). A survey of limitations and enhancements of the ipv6 routing protocol for low-power and lossy networks: A focus on core operations. IEEE Communications Surveys & Tutorials, 21(2): 1607-1635. https://doi.org/10.1109/COMST.2018.2874356

[5] Kechiche, I., Bousnina, I., Samet, A. (2017). A comparative study of RPL objective functions. 2017 Sixth International Conference on Communications and Networking (ComNet). IEEE, pp. 1-6. https://doi.org/10.1109/COMNET.2017.8285595

[6] Raoof, A., Matrawy, A., Lung, C.H. (2018). Routing attacks and mitigation methods for RPL-based internet of things. IEEE Communications Surveys & Tutorials, 21(2): 1582-1606. https://doi.org/10.1109/COMST.2018.2885894

[7] Murali, S., Jamalipour, A. (2018). Mobility-aware energy-efficient parent selection algorithm for low power and lossy networks. IEEE Internet of Things Journal, 6(2): 2593-2601. https://doi.org/10.1109/JIOT.2018.2872443

[8] Ghaleb, B., Al-Dubai, A.Y., Ekonomou, E., Romdhani, I., Nasser, Y., Boukerche, A. (2018). A novel adaptive and efficient routing update scheme for low-power lossy networks in IoT. IEEE Internet of Things Journal, 5(6): 5177-5189. https://doi.org/10.1109/JIOT.2018.2862364

[9] Aris, A., Oktug, S.F., Yalcin, S.B.O. (2016). RPL version number attacks: In-depth study. In NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, pp. 776-779. https://doi.org/10.1109/NOMS.2016.7502897

[10] Dvir, A., Buttyan, L. (2011). VeRA-version number and rank authentication in RPL. 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems. IEEE, pp. 709-714. https://doi.org/10.1109/MASS.2011.76

[11] Mayzaud, A., Sehgal, A., Badonnel, R., Chrisment, I., Schönwälder, J. (2014). A study of RPL DODAG version attacks. In IFIP International Conference on Autonomous Infrastructure, Management and Security, Springer, Berlin, Heidelberg, pp. 92-104. https://doi.org/10.1007/978-3-662-43862-6_12

[12] Perrey, H., Landsmann, M., Ugus, O., Schmidt, T.C., Wählisch, M. (2013). TRAIL: Topology authentication in RPL. arXiv preprint arXiv:1312.0984.

[13] Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sensors Journal, 13(10): 3685-3692. https://doi.org/10.1109/JSEN.2013.2266399

[14] Raza, S., Wallgren, L., Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8): 2661-2674. https://doi.org/10.1016/j.adhoc.2013.04.014

[15] Gopi, A., Babu, E.S., Raju, C.N., Kumar, S.A. (2015). Designing an adversarial model against reactive and

proactive routing protocols in MANETS: A comparative performance study. International Journal of Electrical & Computer Engineering, 5(5): 2088-8708. http://dx.doi.org/10.11591/ijece.v5i5.pp1111-1118

[16] Deshmukh-Bhosale, S., Sonavane, S.S. (2019). A real-time intrusion detection system for wormhole attack in the RPL based internet of things. Procedia Manufacturing, 32: 840-847. https://doi.org/10.1016/j.promfg.2019.02.292

[17] Mayzaud, A., Badonnel, R., Chrisment, I. (2017). A distributed monitoring strategy for detecting version number attacks in RPL-based networks. IEEE Transactions on Network and Service Management, 14(2): 472-486. https://doi.org/10.1109/TNSM.2017.2705290

[18] Arepalli, G., Erukula, S.B. (2016). Secure multicast routing protocol in MANETs using efficient ECGDH algorithm. International Journal of Electrical and Computer Engineering, 6(4): 1857. http://doi.org/10.11591/ijece.v6i4.pp1857-1865

[19] Airehrour, D., Gutierrez, J.A., Ray, S.K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems, 93: 860-876. https://doi.org/10.1016/j.future.2018.03.021

[20] IIova, O., Picco, P., Istomin, T., Kiraly, C. (2016). Rpl: The routing standard for the internet of things... or is it? IEEE Communications Magazine, 54(12): 16-22. https://doi.org/10.1109/MCOM.2016.1600397CM