International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

A Novel Method for Secure RPL for Resource Based attacks in Internet of Things

P.Silpa Chaitanya, B.Renuka Devi, K.Siva Kumar

***Abstract**: The Routing protocol for low power lossy networks (RPL) was evolved by IETF by considering various conditions of constrained networks. This protocol was aimed in order to encourage several routing topologies known DODAGs which were built under different objective functions to improve the routing using different routing measures. There were billions of devices which were connected all over the world because of which the security is the major concern of routing in IoT devices, where different attacks takes place during the routing. Variety of attacks happens while routing, some on network topology others on network traffic and some other attacks on network resources. This paper studies about resource based attacks which targets at consuming the energy of node, memory, processing power by making malicious nodes to perform unnecessary processing actions and these attacks also effect the network availability and reduce the lifetime of the topology. This paper introduces an allied nodes follow up technique where some allied nodes are staked in the DODAG topology in order to detect the resource based attacks in RPL like version number, neighbour, worst parent, rank attacks. These allied nodes follow up and monitors each and every node and based on proposed constraints not only detects these resource attacks in RPL and also updates the information to the root node about malicious node in order to eradicate it from DODAG. The performance of proposed model was compared with previous attack detection models regarding to the measures like packet delivery ratio, end to end delay and throughput.*

***Keywords** : RPL, DODAG, allied node, resource attacks.*

I. INTRODUCTION

A standardized routing protocol for IoT was RPL which was a distance vector and a source routing protocol for LLN's (Low power Lossy networks), specially designed by IETF [1]. The structure of RPL is a mixture of various DODAG (Destination Oriented Acyclic Graph) that has numerous wireless sensor appliances that are linked to DODAG root as shown in figure 1.

The control messages of RPL [2] are DIO (DODAG Information Object) advertise the data used for maintaining and building DODAG. The DIO base object consist of DODAG ID, RPL instance ID, DODAG version, Objective function, Rank, Mode of operation, next is DAO (DODAG advertisement Object) follows downward traffic and comes from child nodes as an acceptance about their parents, DIS (DODAG Information Solicitation) a node to join an existing topology uses DIS.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

P.Silpa Chaitanya*, Asst. Professor, Department of Computer Science and Engineering, Vignan's Nirula Institute of Technology Science and Women, AP, India

Dr.B.Renuka Devi, Professor, Department of Computer Science and Engineering, Vignan's Nirula Institute of Technology Science and Women, AP, India

K.Siva Kumar, Assoc.professor, Department of Computer Science and Engineering, Vignan's Nirula Institute of Technology Science and Women, AP, India

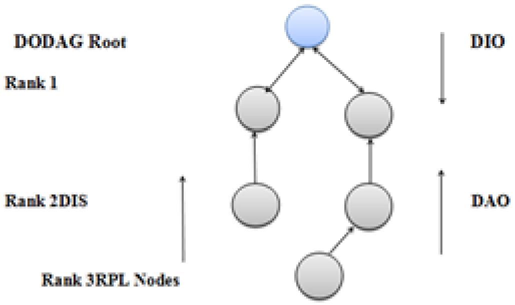

Fig. 1. Wireless sensor appliances linked to DODAG root.

The construction of DODAG was initiated by root by multicasting DIO messages. After getting a DIO message, a node chooses its preferred parent based on the rank of the node. 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].

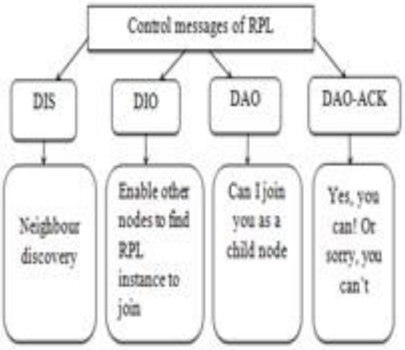
Control messages of RPL
DIS
DIO
DAO
DAO-ACK
Neighbour discovery
Enable other nodes to find RPL instance to join
Can I join you as a child node
Yes, you can! Or sorry, you can't

Fig. 2. Control Messages of RPL

In order to preserve the topology RPL uses some main values related within RPL control messages 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.

DOI: 10.35940/ijitee.B9074.129219

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.

Table. 1. Important terminology related to DODAG

DODAG ID	A value to identify the DODAG
DODAG Version number	Each new shape of DODAG is a new version, a sequential counter incremented by the root to form a new version
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	Defines how routing metrics and some related functions are used to calculate rank

RPL trigger the repair mechanisms when inconsistencies are detected means when a node disappeared from a network due to lack of battery power those mechanisms are local repair mechanism where another path to route the packets is chosen if the preferred parent is not available or can transfer the packet via the sibling nodes, when this mechanism fails there is another mechanism called global repair when the entire DODAG is built by incrementing the version number of DODAG graph

There is a need to protect the routing protocols from the attacks and to provide the security for protecting the data. As seen RPL comes with many built in security modes, but they were not sufficient to overcome all types of attacks. Form which sources the chances of the attacks can be happened are known as shown below:

a) Threat Sources: Threat sources are from the other parties who attack the network and counter measures are suggested only if we came to know the attack patterns, ability and status of the attacker.

b) Outsiders: In this the attackers are the outsiders and they are not genuine nodes, they were duplicate nodes which corrupt the system and steal the data.

c) Insiders: In this the attackers are genuine nodes in the system but they are involved in some fraud activities and also make some changes in the IoT device in order to pilfer the data.

However there are many attacks that will take place in order to steal the data or to destroy the topology. The Resource based attacks are the one among all those which mainly aims to consume more energy of a node and also to drop the life time of the topology. A node which is fake modifies the version number, rank, selects worst parent itself and also advertises the false ranks to neighbor nodes related to a topology and make to rebuild the entire topology which consumes lot of energy and decreases the duration of the network. The version number and rank in DIO base object, there is no means given by the standardized protocol to ensure the honesty of the given version number and ranks and to select only preferred parents [6]. The rebuild of topology causes increase in overhead, loops in topology. Past studies show that attacks on RPL have an huge effect on the networks and also previous studies discussed about addressing those attacks and proposed solutions for some types of attacks even though which contain drawbacks. 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.

II. Related Work

Winter, T., Ed., et.al [1] A security threat examination 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.

Sarumathi Muraliet.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.

Baraq 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 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.

VeRA the Version Number [9,11] and Rank Authentication[13]approach many aim is to remove the nodes which are malicious from pretending the root from receiving the fake version numbers to disrupt or to recreate its entire topology to do this the proposed method provides the authentication for version and rank within base object of DIS through hash and signature methods but there were two problems with VeRA [10], the computational complexity is more and it can be vulnerable to replay attack and hash chain forgery.

Another mechanism called TRAIL [12] which has an advantage that the complexity is less compared to VeRA in which there is no need for each node to transmit neighbor nodes data to DODAG root. However, TRAIL has a drawback that a child node could choose an malicious node as its parent that leads to another attack named worst parent attack.

Several intrusion detection systems [16] finds the intruders that only if a node that does not follow a specific behavior referred to the routing protocol, but this detects well the topology attacks it fails to detect any version number attacks, it only sort 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 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 Mayzaud 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 analyzed the execution considering different metrics and shown that it can detect version number attacks 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.

III. 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.

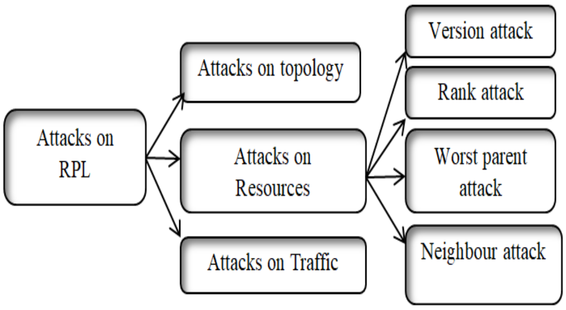

Fig. 3. Resource based attacks in RPL

A. **Version number attacks:** In every DIO format an important field known as version number is present, a fake node increases its version to send DIO to other nodes with fake version number which leads to rebuild the entire topology and also leads to overhead of control messages and reduces 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.

Table. 2. Attack description and Goal of attacks.

Type of attack	Attack description	Goal of attack
Rank attack	The packets were not send 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

IV. PROPOSED METHOD

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.

A. DODAG formation and allied node identification:

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

B. Allied Node follow up procedure:

A root node multicast DIO messages to the available nodes with its nearest allied node id in order 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 initializes 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 neighbor 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.

C. 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
```

D. Advantages of allied node follow up procedure:

1. Helps to maintain the great life time of the network
2. Works efficiently to find number of attacking nodes within the network
3. By detecting all the resource based attacks the energy, memory and processing power of the nodes can be saved
4. Works efficiently for the network with many number of nodes
5. Both detection and isolation is done, shows better performance than standard RPL and improves security.

E. Flowcharts for allied node follow up technique:

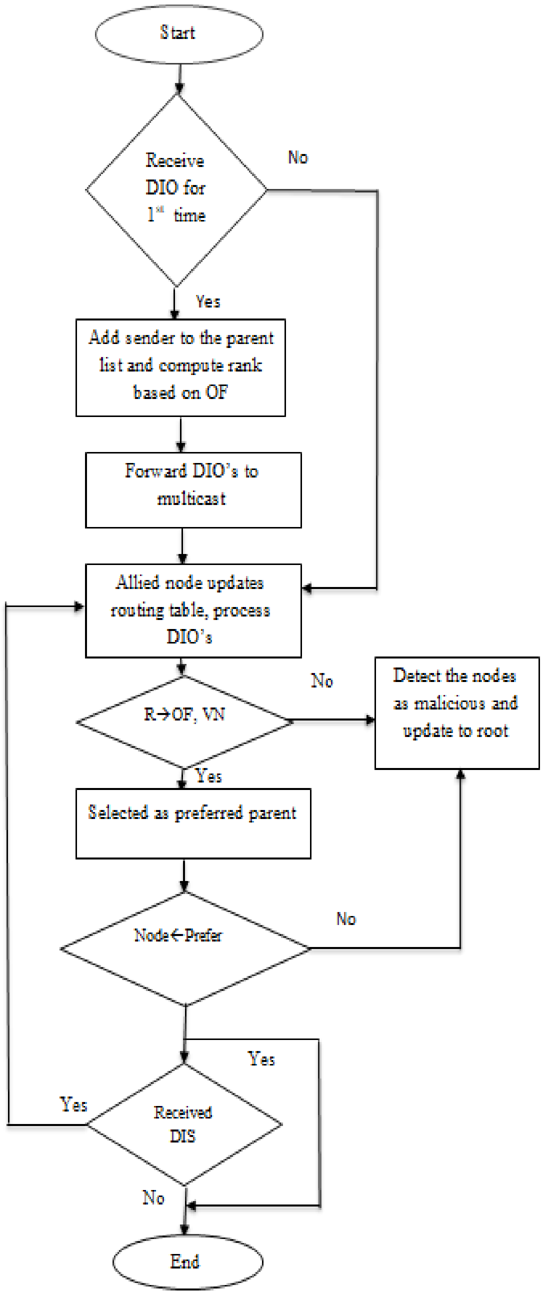
Start
Receive DIO for 1st time
No
Yes
Add sender to the parent list and compute rank based on OF
Forward DIO's to multicast
Allied node updates routing table, process DIO's
R→OF, VN
No
Detect the nodes as malicious and update to root
Yes
Selected as preferred parent
Node←Prefer
No
Yes
Yes
Received DIS
No
End

Fig. 4. Flow chart for proposed model.

V. Experimental Evolution

The behavior and performance of RPL can be defined by considering some of the measures as the parameters. The measures may vary like for example, energy consumption, Packet delivery rate, end to end delay, convergence time, throughput etc. Here in the study, three major metrics were considered they are throughput, packet delivery ratio and End to end delay.

Performance measures:

A. Throughput:

Rate at which packets were successfully delivered through a network channel is known as network throughput. So, for the calculation of the value for the small networks we can sum the packets received by all nodes. There are several ways to measure throughput (instantaneous or average) in a wired or wireless network using network simulators.

Formula:

Throughput = sum (Total count of true packets)*(average size of the packet))/Total time sent to deliver that amount of data.

B. Packet Delivery Ratio:

PDR is simply defined as the percentage among the packets that were generated by the source and received by the destination.

Formula:

Algebraically, it can be defined as:

PDR= N1÷ N2

Where, N1 is the sum of packets received by the destination and N2 is the sum of packets generated by the source.

C. End To End Delay:

Divergence in time at which the sender generated the packet and the receiver received the packet. The E2Edelay is also known as one way delay which was being referred to period taken for the packet to transmit throughout the network from sender to receiver.

Formula:

E2E Delay = Sum of (Delay at sender + Delay at receiver + Delay at intermediate nodes)

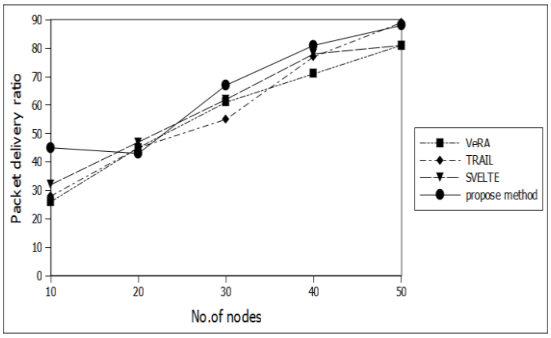

Fig. 5. PDR of RPL for 10 to 50 nodes

Figure 5 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, neighbor 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.

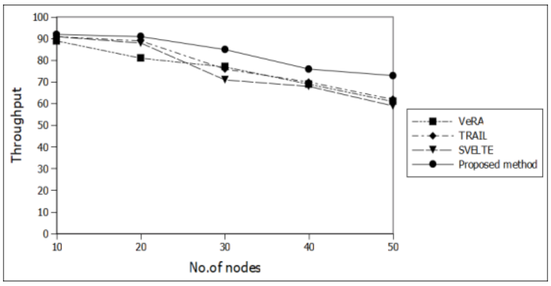

Fig. 6. Throughput of RPL for 10 to 50 nodes

Figure 6 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, neighbor 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.

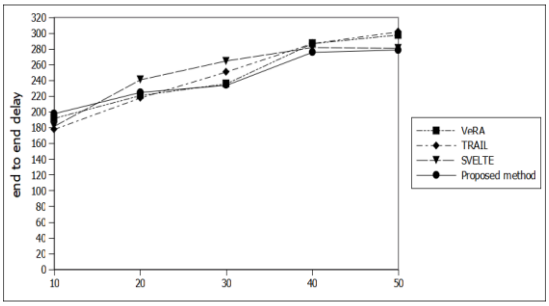

Fig. 7. End to end delay of RPL for 10 to 50 nodes

Figure 7 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 outcomeE2E 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.

VI. CONCLUSION

RPL is a network, in which many devices are connected to this network, but it is suffered from secure communication due to attacks on network topology, network resources, network traffic. In this paper a new attack eradication technique was proposed where the resource based attacks in RPL can be completely removed through an associated node which inspects the entire topology in order to remove the resource based threats like version number attacks, rank attacks, neighbor attacks and worst parent attack. This allied node will be available to each and every node in the RPL topology in order to communicate with each node and to select the best preferred parent to them and also find the attacking node to improve the life time of topology and to decrease the energy consumption of the node, to enhance the packet delivery ratio and to decrease end to end delay. Obtained results shown that the work of proposed model is improved under the defined metrics compared to previous studies. Hence the allied node method protects the RPL topology from different threats and improves its packet delivery ratio, throughput and also to improve the life spanof the network and decreases delay and energy consumption of the nodes.

REFERENCES

1. Winter, Tim. "RPL: IPv6 routing protocol for low-power and lossy networks." (2012).
2. Kamgueu, Patrick Olivier, Emmanuel Nataf, and Thomas DjotioNdie. "Survey on RPL enhancements: A focus on topology, security and mobility." Computer Communications120 (2018): 10-21.
3. Gaddour, Olfa, and AnisKoubâa. "RPL in a nutshell: A survey." Computer Networks 56.14 (2012): 3163-3178.
4. Ghaleb, Baraq, et al. "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 (2018): 1607-1635.
5. Kechiche, Ines, InèsBousnina, and AbdelazizSamet. "A comparative study of RPL objective functions." 2017 Sixth International Conference on Communications and Networking (ComNet). IEEE, 2017.
6. Raoof, Ahmed, Ashraf Matrawy, and Chung-Horng Lung. "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things." IEEE Communications Surveys & Tutorials21.2 (2018): 1582-1606.
7. Murali, Sarumathi, and Abbas Jamalipour. "Mobility-aware energy-efficient parent selection algorithm for low power and lossy networks." IEEE Internet of Things Journal 6.2 (2018): 2593-2601.
8. Ghaleb, Baraq, et al. "A novel adaptive and efficient routing update scheme for low-power lossy networks in IoT." IEEE Internet of Things Journal 5.6 (2018): 5177-5189.
9. Aris, Ahmet, Sema F. Oktug, and S. Berna OrsYalcin. "RPL version number attacks: In-depth study." NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2016.
10. Dvir, Amit, and LeventeButtyan. "VeRA-version number and rank authentication in rpl." 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems. IEEE, 2011.
11. Mayzaud, Anthéa, et al. "A study of RPL DODAG version attacks." IFIP international conference on autonomous infrastructure, management and security. Springer, Berlin, Heidelberg, 2014.
12. Perrey, Heiner, et al. "TRAIL: Topology authentication in RPL." arXiv preprint arXiv:1312.0984 (2013).
13. Le, Anhtuan, et al. "The impact of rank attack on network topology of routing protocol for low-power and lossy networks." IEEE Sensors Journal 13.10 (2013): 3685-3692.
14. Raza, Shahid et al. "SVELTE: Real-time intrusion detection in the Internet of Things." Ad Hoc Networks 11 (2013): 2661-2674.
15. Choudhary, Sarika, and NishthaKesswani. "Detection and Prevention of Routing Attacks in Internet of Things." 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018.
16. Deshmukh-Bhosale, Snehal, and Santosh S. Sonavane. "A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things." Procedia Manufacturing 32 (2019): 840-847.
17. Mayzaud, Anthéa, RémiBadonnel, and Isabelle Chrisment. "A distributed monitoring strategy for detecting version number attacks in RPL-based networks." IEEE Transactions on Network and Service Management 14.2 (2017): 472-486.
18. Shabbir, Ghulam, et al. "Network performance enhancement of multi-sink enabled low power lossy networks in SDN based Internet of Things." International Journal of Parallel Programming (2018): 1-32.
19. Airehrour, David, Jairo A. Gutierrez, and Sayan Kumar Ray. "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things." Future Generation Computer Systems 93 (2019): 860-876.
20. Iova, Oana, et al. "Rpl: The routing standard for the internet of things... or is it?." IEEE Communications Magazine 54.12 (2016): 16-22.

AUTHORS PROFILE

P.Silpa Chaitanya, working as Assistant Professor in Vignan's Nirula Institute of Technology and science for women, having 12 years of experience, doing PHD at Vignan University in the area of Big Data Analytics. Areas of interest are Data Mining, Big Data and IOT.