Machine Learning Based Technique for Detection of Rank Attack in RPL based Internet of Things Networks

Vikram Neerugatti, A. Rama Mohan Reddy

Abstract*: Internet of Things (IoT) is a new Paradiagram in the network technology. It has the vast application in almost every field like retail, industries, and healthcare etc. It has challenges like security and privacy, robustness, weak links, less power, etc. A major challenge among these is security. Due to the weak connectivity links, these Internet of Things network leads to many attacks in the network layer. RPL is a routing protocol which establishes a path particularly for the constrained nodes in Internet of Things based networks. These RPL based network is exposed to many attacks like black hole attack, wormhole attack, sinkhole attack, rank attack, etc. This paper proposed a detection technique for rank attack based on the machine learning approach called MLTKNN, based on K-nearest neighbor algorithm. The proposed technique was simulated in the Cooja simulation with 30 motes and calculated the true positive rate and false positive rate of the proposed detection mechanism. Finally proved that, the performance of the proposed technique was efficient in terms of the delay, packet delivery rate and in detection of the rank attack.

Index Terms: Internet of Things, RPL, rank attack, KNN, security

I. INTRODUCTION

The Internet of Things (IoT) is a new technology which makes the computing ubiquitous [1]. The enabling technologies for Internet of Things is wireless sensor networks, cloud computing, mobile devices, etc. with the advent of this technology any object around us can be connected to the internet with unique identity. In 1999, Kevin Ashton coined the term Internet of Things (IoT) [2]. By 2020, the Internet of Things devices will create about $ 1.1-$2.5 trillion market value by connecting 2.12 million things to the internet [3]. It has vast applications in different fields like transportations and logistics, healthcare, smart environment, personal and social, etc. [4]. Internet of Things has research challenges like massive scaling, architecture and dependences, creating knowledge and big data, robustness, security, privacy, etc. [5].

The characteristics of IoT are, low size, low power, less capacity devices, etc. so it is called as constrained devices. It says that the Internet of Things devices are low powered, less computing power and small in size. Due to this constrained behavior of Internet of Things devices, most of these devices were vulnerable to security and privacy issues. Most of the attacks [6] are shown in the Figure 2.

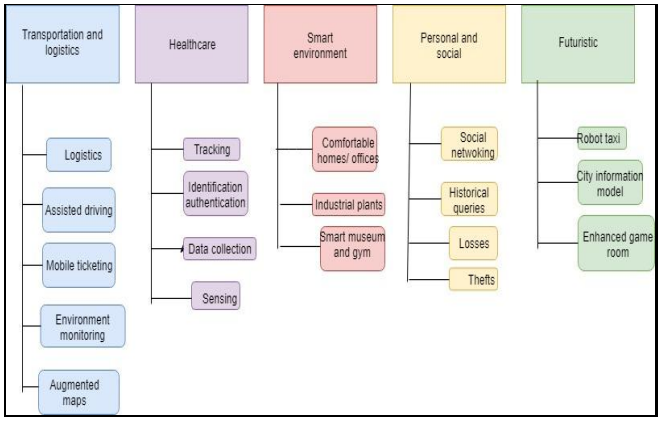

Figure 1: Various applications in Internet of Things

This paper focused on the rank attack in the routing protocol for low power lossy networks (RPL) protocol in the network layer of the Internet of Things. The layers in Internet of Things were shown in Figure 3.

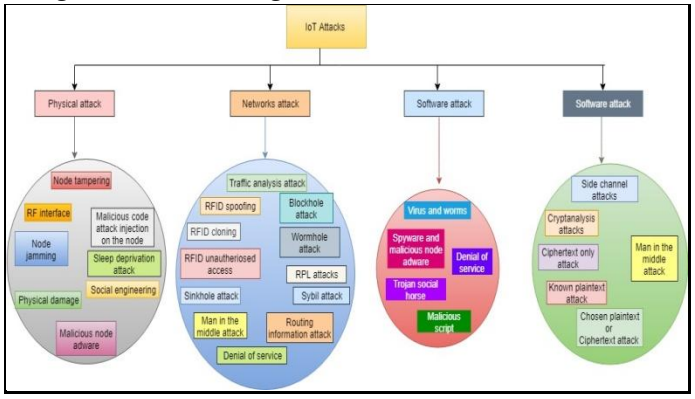

Figure 2: Attacks in Internet of Things

The RPL is a routing protocol in the 6LoWPAN (IPv6 low power wireless personal area networks). In this networks due to the less security features this whole network suffer from various routing attacks like rank attack, wormhole attack, block hole attack [8]. The rank in RPL protocol is the physical position of the node with respect to the border router and neighbor nodes. Border router is a node which connects the 6LoWPAN Internet of Things network and IPv6 traditional network. In the rank attack the attacker will attracts other nodes to establish route through it by advertising with false rank. This paper proposed a machine learning based technique (MLTKNN) for detection of these rank attack.

Revised Manuscript Received on July 22, 2019.

Vikram Neerugatti, Research scholar, Department of CSE. Sri Venkateswara University Tirupati, Andhra Pradesh, India

Dr. A. Rama Mohan Reddy, Professor, Department of CSE. Sri Venkateswara University Tirupati, Andhra Pradesh, India

Retrieval Number: I30440789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3044.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

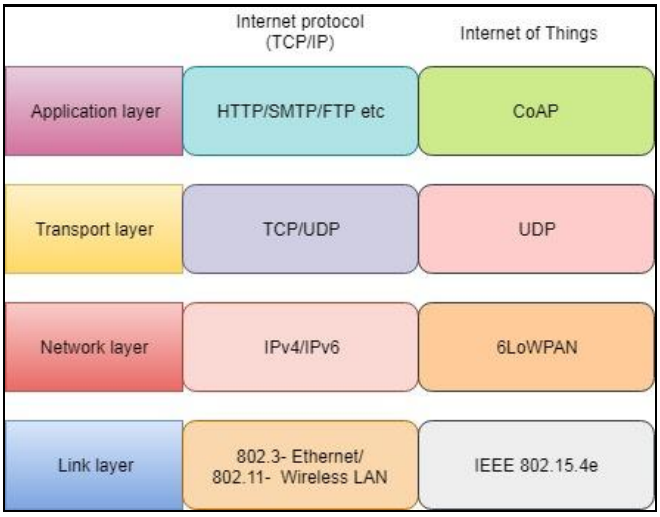

Figure 3: Layered architecture in Internet of Things

Figure 4 shows the IoT setup, which shows the general connections between the Traditional network and the IoT network. The Gateway/Border Router connects the both the traditional network and IoT network with the internet connection. The IoT network is purely Things network with 6LoWPAN protocol where the Things around us will be connected. In the traditional network, the Fog/Cloud/Servers/Computers/Smart mobiles will be connected. Users will be communicated via Web/Applications thought Computers/Mobile Phones, etc.

The current work was focused in the IoT network in the RPL Routing protocol of the 6LowPAN network in the network layer of the IoT network. The RPL is the distance based routing protocol which creates Destination oriented directed acyclic graph (DODAG). It creates a Spanning tree (no cycles) and all nodes in the tree by default will point towards the root node. The packets can be transfer toward the root or away from the root. RPL will work based on the control messages like the DODAG Information Object (DIO), DODAG Advertisement object (DAO), DODAG Advertisement object Acknowledgement (DAO-ACK), DODAG Information Solicitation (DIS).

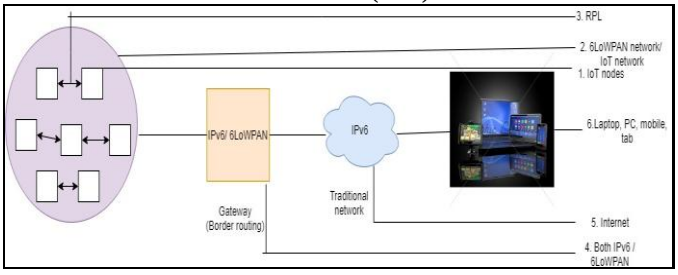

Figure 4: IoT setup: that shows the connection between IoT network and traditional network by using gateway

The DODAG construction will start from the root node. It sends the DIO message to all the other nodes for construction of the DODAG, other nodes will send the DAO message that willing to form DODAG, root node based on the willing will send the DAO-ACK message that you can join to form the DODAG based on the Objective function in the RPL (default/user choice). With this the DODAG will be formed, if any new node want to join the existing DODAG then it sends the DIS message. This process will be continues till the task accomplished. By default the RPL has the security mechanism to mitigate the External attack but it can't mitigate the internal attacks. The internal attack means the existing node in the DODAG will act as the attack node. The current work is focused on the mitigation of the internal attacks.

This paper is organized as follows, in next section discussed about the related work, in section III discussed about the proposed system, implementation procedure was discussed in the section IV, in section V results were produced and finally conclusion and future work was discussed in the section VI.

II. RELATED WORK

Raza, et.al. proposed a secure communication technique, between the sensor networks and the traditional network. Here the encryption and decryption mechanisms were used for the authentication of the networks [7]. Abdual, et.al. Proposed a rank attack based on the objective function in RPL and perform the simulation. The simulation result shows the wrong route, which enable to decrease the throughput and increases the delay [9]. Anhtuan, et.al. Analyses the various types of threats in the perspective of rank attack and provided knowledge for mitigating the rank attack [10]. Linus, et.al. has done a RPL comprehensive analysis in security of the Internet of Things devices. Here various RPL routing attacks here implemented and demonstrated in cooja simulator [11].

III. PROPOSED SYSTEM

This paper proposed a K-nearest neighbor based technique for detection of the rank attack in RPL protocol for IoT based networks. The rank attack in the RPL protocol is the physical position of the node with respect to the border router (root node) on the neighbor nodes. While formation of the DODAG in the RPL protocol the attacker node may attracts the border router for establishing a routing path with wrong rank. For detection of this wrong node here proposed and implemented a technique called MLTKNN based on the Machine learning approach KNN algorithm. The step by step algorithm is as follow.

To find the rank among the nodes in the proposed System the metric used is the distance based matric, i.e

$$\text{Distance (Rd) (X, Y)} = \sqrt{\frac{\sum_{i=1}^{n}(x_i - y_i)^2}{n}}$$

By using the above formula we can find the exact distance between the nodes in the RPL protocol. So that enables to send the packets in the shortest distance with less time delay.

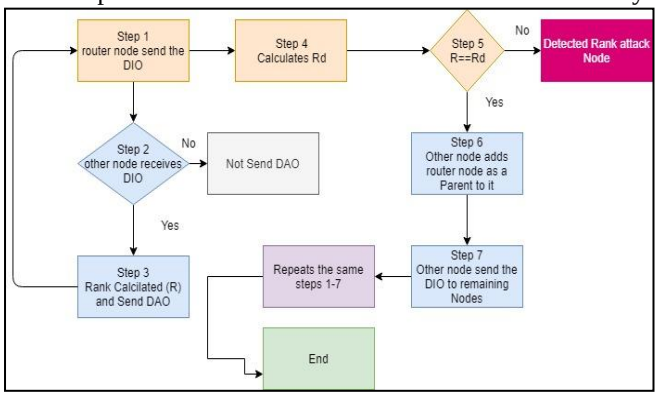

Figure 5: working procedure of the proposed system

Retrieval Number: I30440789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3044.0789S319
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Algorithm: Proposed Detection process of the Rank Attack

/* where 'X' is Border router node, 'y' is other nodes, 'Z' is Rank attack node 'Rd' is a distance between the parent node and child node, 'R' is the Rank of the individual node ,

Rd (X, Y) = $\sqrt{\frac{\sum_{i=1}^{n}(x_i-y_i)^2}{n}}$ */

0: Start
1: root node 'X' broad cast DIO (DODAG ID, Objective Function, rank=0)
2: other node 'Y' receives the message DIO
3: calculates rank 'R' based on DIO
4 nodes 'Y' sends (unicast) the DAO to node 'X'
3: node 'X' performs
4: calculates Rank 'Rd' for node 'y'
5: if Rd = = R
6: node 'X' sends DAO-ACK to 'Y'
7: else
8: node 'X' removes the node (rank attack node 'y'=='Z')
9: then node 'Y' adds the node 'X' as it parent
10: Node 'Y' multicasts the DIO message to other nodes.

The working nature of the algorithm is shown in the Figure 6.

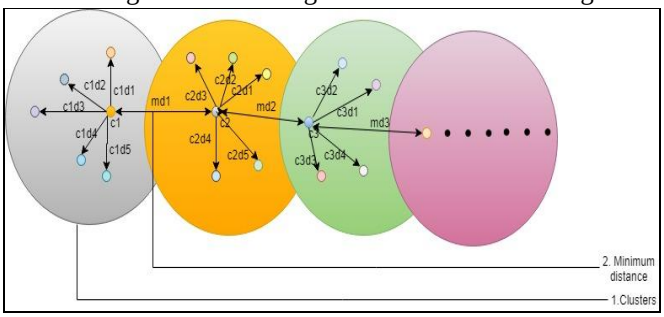

Figure 6: Rank calculation in RPL routing

IV. IMPLEMENTATION

The proposed system was implemented in cooja simulator based on the contiki operating system which is designed particularly for the constrained devices. The proposed algorithm is implemented in the border router node. The border router node will check the distance of every node physically within the radio range from the node to node based on the distance metric. Then the calculated distance is compared with the rank of the corresponding node. After comparison of both the values based on the obtained value the malicious node will be detected. Once the malicious node detected it will be removed from DODAG.

In the cooja 30 sky motes are used. Among 30 sky motes one sky mote is considered as RPL border router node. Where the proposed algorithm was injected in one of the node and it considered as RPL border router node. Other few nodes among 29 nodes were considered as the malicious nodes with rank attack (rank attack code was injected) and remaining nodes has normal nodes (normal code without attacks). After simulating with this setup the results are shown in next section.

V. RESULTS

The results were drawn in the contiki based Cooja Simulators with the 30 nodes in the Network with 28 normal motes and 1 with rank attack (malicious), 1 general border router mote. And the results that shown in Figures(7-14), was drawn from the simulation setup with the 20% rank attack nodes among 30 notes network. The Simulation Setup is shown in Table 1. The figure 7 shows the Initial setup of the cooja simulator after adding the require motes. The figure 8 shows screen shot at the time of the detection of the rank attack, the figure 9 shows the average power consumption of each node during the simulation, the figure 10 shows the neighbors nodes of each node. Figure 11 shows the End to End delay and Figure 12 shows the Packet delivery ratio of the nodes with normal, attack and proposed system and it shows that the proposed has an effective result compared with the attack nodes alone. Finally the figure 13 shows the True positive rate and figure 14 shows the true negative rate effectively.

Table 1: Simulation Setup

Parameter	value
Simulator	Contiki Cooja Simulator
Radio medium model medium (USGM) distance loss	Unit disk graph
Range of nodes.	R× and T× : 50m
Mote type	sky motes
Duty cycle	contikiMAC
Size of deployment area	100×100m
Number of nodes	30
Number of sinks.	1
Number of malicious nodes	5 to 20%
Physical layer.	IEE 802.15.4
MAC layer.	ContikiMAC, lpv6
Network layer	contikiRPL
Transport layer.	UDP
Objective function.	Hop count and ETX, proposed

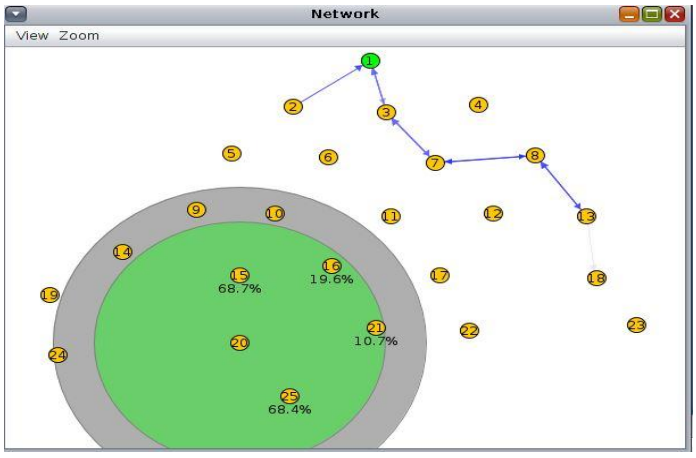

Figure.7 Proposed setup i.e. 30 sky motes with the Normal, attack and proposed Detection Mechanism

Retrieval Number: I30440789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3044.0789S319
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

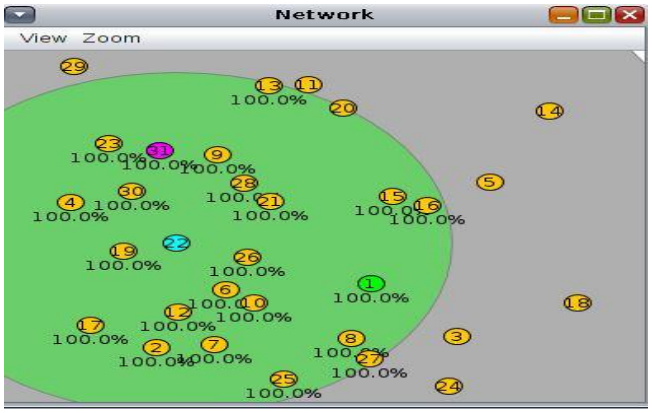

Figure 8: Node 1 is Border router node with the proposed algorithm, node 31 is the rank attack node and remaining are the normal nodes.

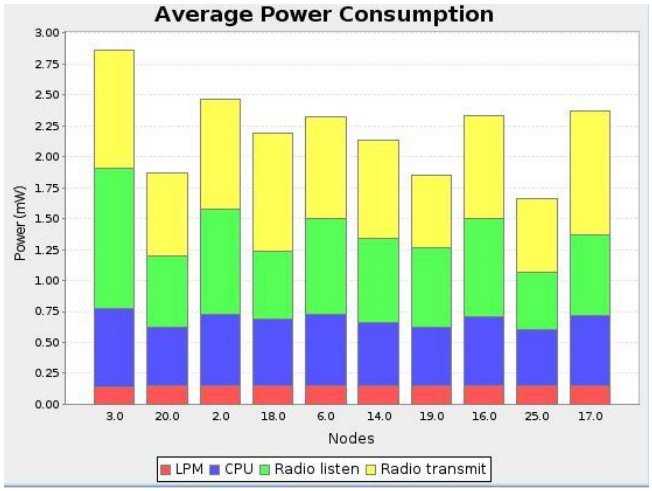

Figure 9: Average Power Consumption of Nodes in IoT network

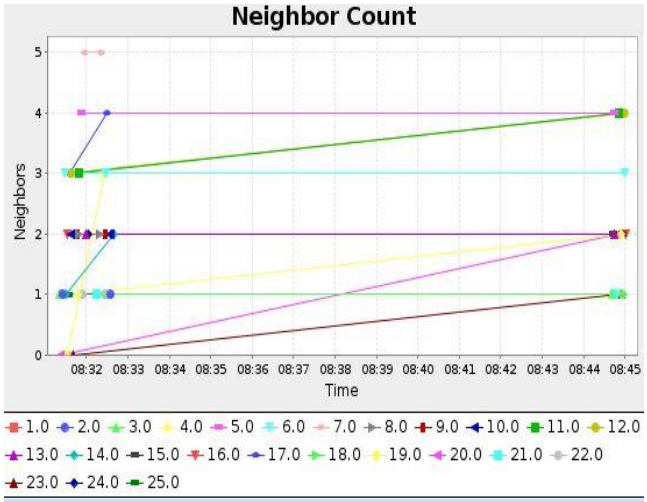

Figure 10: Neighbors Count of the Nodes

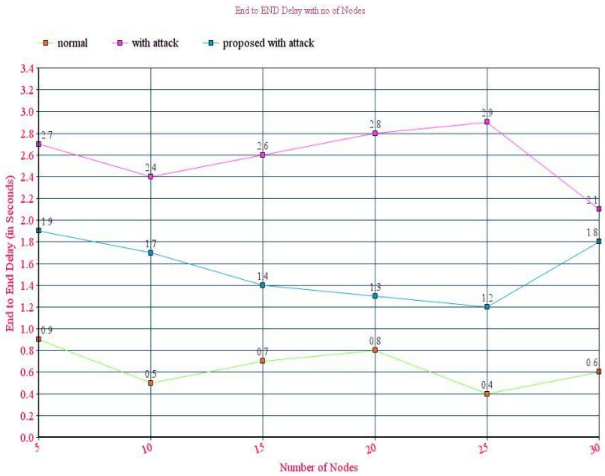

Figure 11: End to End delay

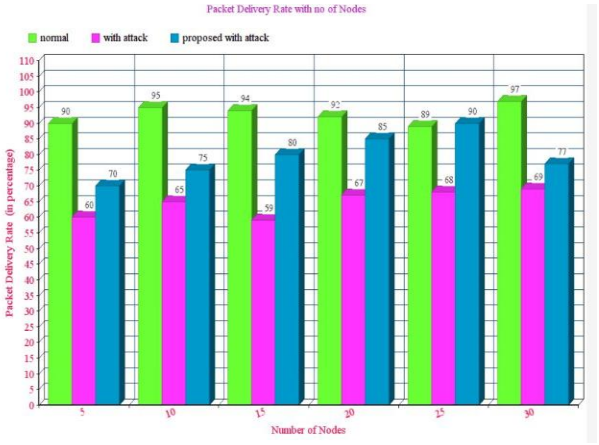

Figure 12: Packet Delivery Ratio

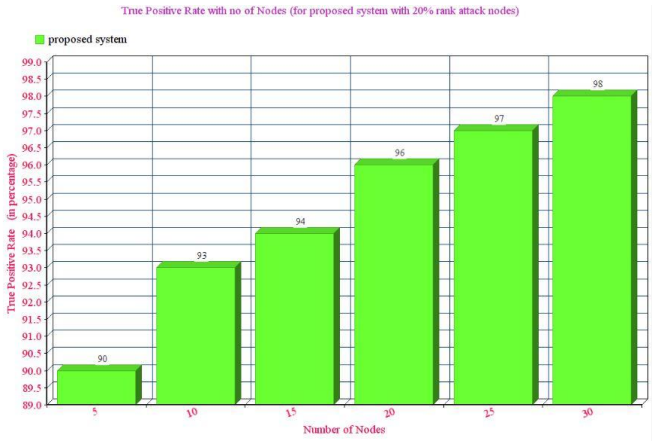

Figure 13: True Positive Rate

Retrieval Number: I30440789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3044.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

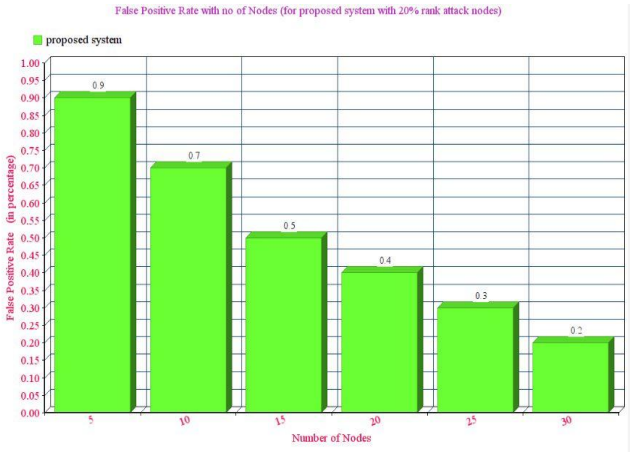

Figure 14: False Positive Rate

VI. CONCLUSION & FUTURE WORK

An efficient technique was proposed for detection of the rank attack in the RPL based Internet of Things networks. The proposed method will detect the malicious node (rank attack) based on the distance calculations among the nodes with respect to the border router. By verifying the calculated rank and the original rank of a node, the malicious node was detected. The proposed technique was proved that the node detection rate is high in 30 nodes network and the performance was high in terms of delivery rate and delay. In future work the detection mechanisms for other RPL attacks like, Worm hole and black hole attacks will be proposed and implemented in contiki cooja simulator.

REFERENCES

1. Mattern, Friedemann, and Christian Floerkemeier. "From the Internet of Computers to the Internet of Things." From active data management to event-based systems and more. Springer, Berlin, Heidelberg, 2010. 242-259.
2. Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660.
3. Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE Communications Surveys & Tutorials 17.4 (2015): 2347-2376.
4. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.
5. Stankovic, John A. "Research directions for the internet of things." IEEE Internet of Things Journal 1.1 (2014): 3-9.
6. Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: a survey." I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on. IEEE, 2017.
7. Yang, Yuchen, et al. "A survey on security and privacy issues in internet-of-things." IEEE Internet of Things Journal 4.5 (2017): 1250-1258.
8. Le, Anhtuan, et al. "Specification-based IDS for securing RPL from topology attacks." Wireless Days (WD), 2011 IFIP. IEEE, 2011.
9. Rehman, Abdul, et al. "Rank attack using objective function in RPL for low power and lossy networks." Industrial Informatics and Computer Systems (CIICS), 2016 International Conference on. IEEE, 2016.
10. 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.
11. Wallgren, Linus, Shahid Raza, and Thiemo Voigt. "Routing Attacks and Countermeasures in the RPL-based Internet of Things." International Journal of Distributed Sensor Networks9.8 (2013): 794326.

AUTHORS PROFILE

Mr Vikram Neerugatti, Research Scholar, Department of Computer Science and Engineering, Sri Venkateswara University, Tirupati. Mr. Vikram Neerugatti, is Working on Internet of Things on IoT at Sri Venkateswara University, Tirupati. He Pursuing his PhD in the area of Internet of Things (IoT) and his research Contributes are to provide detection and prevention mechanisms for RPL attacks like Sinkhole, Black hole, Wormhole, Rank attack, etc in IoT. He completed his Bachelors (B.Tech) & Master's (M.Tech) Degree in the Specialization of Computer Science and Engineering at JNTUA. He has M.S Degree from Brain wells University, London, UK. He has more than 10 years teaching experience from various Institutions like NIT, Goa, Sri Vidyanikhethan, A. Rangampeta, Sri Venkateswara University, Tirupati and Sri Venkateswara College of Engineering, Chittoor. He has more than 5 years of Research Experience form NIT Goa and S. V University, Tirupati. He has attended more than 50 Workshops specifically in the area of IoT. He has published 15+ National and International Conferences and Journals. He got 6 best research paper awards. Recently he got Dr. B.R. Ambedkar Research Fellowship award for his innovative research contributions. His research areas are Internet of Things, Fog Computing, Cloud Computing, etc. He acted as a Resource person for more than 20 workshops specifically in the domain of the IoT & Fog Computing in various institutions like Sri Venkateswara University, Sri Padmavathi Mahila Viswavidyalam, Tirupati, Chdalavada Venkata subbamma engineering college, Tirupati, Sir Vidyanekithan Engineering College, etc.

Dr. A. Rama Mohan Reddy He **r**eceived his B.Tech Degree from JNT University Anantapur in 1986, Masters in Computer Science and Engineering from NIT, Warangal in 1991 and Ph.D. in Computer Science and Engineering from Sri Venkateswara University, Tirupati in 2007. He is currently working as a Professor of Computer Science and Engineering, SV University College of Engineering, Tirupati, India. His research interests are Software Engineering, Software Architecture, Cloud Computing, Operating System and Data Mining. He is life member of ISTE, IETE, ISC and CSI. He has more than 30 years of experience in teaching, 7 scholars completed Phd.'s under his guidance. He has 100+ publications and presented 78+ papers in National and International conferences.

Retrieval Number: I30440789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3044.0789S319
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication