Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 32 (2019) 840–847

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

The 12th International Conference Interdisciplinarity in Engineering

A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things

Snehal Deshmukh-Bhosale[a,b,]*, Santosh S. Sonavane[c]

[a] *Asst. Professor, RMD Sinhgad Sinhgad School of Engineering, Warje, Pune,*
[b] *Research Scholar, Raisoni College of Engineering and Management, Pune, India*
[c] *Dr. D. Y. Patil Technical Campus, Lohgaon, Pune, India*

Abstract

Today there is a trend of the Internet of Things (IoT) where many objects are connected to the internet. In future number of objects connected to the internet will be more as compared to people in the world. So providing security to IoT devices is one of the ongoing research issues. Inserting security in IoT devices is challenging because maximum devices involved in IoT are resource constrained in terms of battery power and memory size. In IoT, nodes communicate using insecure internet which makes network exposed to various attacks. RPL (Routing protocol for low power and lossy network) is the protocol specially designed for IoT network is very prone to various security attacks. The proposed work in this paper is an implementation of an intrusion detection system (IDS) for Wormhole attack and attacker. Wormhole attack is one of the most severe attacks taking place at 6LoWPAN adaption layer of RPL network. In this type of attack, a pair of attacker nodes forms a tunnel between two nodes as if they are directly connected to each other to misguide network traffic. The proposed IDS is implemented in Contiki OS, using Cooja Simulator. We have used received signal strength indicator (RSSI) to identify the attack and attacker node.

*Keywords :*IoT; IDS; Wormhole Attack; Contiki OS; RPL; 6LoWPAN

* Corresponding author. Tel.: +91-98-90476048
E-mail address: sa_bhosale@yahoo.com

2351-9789
10.1016/j.promfg.2019.02.292

1. Introduction

Internet of Things (IoT) is the latest trend where many things are connected to internet forming a new infrastructure in existing network system using IPv6 protocol. A wide range of potential applications like smart city, smart home, smart healthcare monitoring system etc. are proposed under IoT technology. It uses RPL (Routing Protocol for Low Power Lossy Network) and 6LoWPAN (IPv6 over Low Power Wireless Private Area Network) protocols which are designed for constrained devices to communicate within a network and connect to the internet. Current research in IoT focuses on the developments of the protocol designed for it. [1]

This paper is organized as follows. Section 1 gives the introduction of IoT and its security challenges. Section 2 discusses about the IoT protocols RPL and 6LoWPAN. Section 3 gives idea about a Wormhole attack. Section 4 gives explanation of proposed system followed by Section 5 which explains about experimental setup of the proposed system. Section 6 concludes the paper.

1.1. Security Challenges in IoT

Unlike traditional human controlled computers, devices in IoT such as smart refrigerator, smart oven, child TV can be easily accessed by an intruder because of its continuous connectivity to the internet. All these appliances cannot afford to add heavy security algorithms in their structure because of small size, portability, low cost etc of the devices. This is the reason which makes addressing security issue very challenging in a IoT network compared to the traditional computer network. Most of the objects are handled by common people and not by skilled engineers hence security must be inbuilt in IoT appliances. [2] [3]

Insecure internet and wireless sensor network are the two major components of IoT which make IoT network vulnerable to various security attacks. There are many attacks which take place over novel protocols solely designed for IoT network. [4]. For example, 6LoWPAN and RPL protocols can undergo Fragmentation attack, Rank Attack, Version number attack, Denial of Service Attack, Wormhole Attack, Sybil attack etc. [5]. To mitigate these kinds of attacks many researchers have proposed prevention and detections schema. The attack detection is done by using an Intrusion Detection System (IDS). While designing the IDS for IoT system, few things must be taken under consideration like IDS is designed for resource-constrained device network hence it must be lightweight system in terms of memory and processing power. Also, devices forming IoT are extremely heterogeneous in nature hence designing IDS for these kinds of devices are very challenging. [6]

2. IoT Protocols

In this topic, the protocols which are mostly affected by the Wormhole attacks are taken into consideration. Those are Routing Protocol for Low Power and Lossy Network (RPL) and IPv6 over Low Power and Wireless Private Area Network (6LoWPAN).

2.1. RPL (Routing Protocol for Low Power and Lossy Network)

Routing Protocol for Low-Power and Lossy Networks (RPL) [7] is a distance-vector protocol that can support a variety of data link protocols [8]. RPL protocol is developed for 6LoWPAN network of IoT. As the name suggests this protocol is designed for low power and lossy network using IPv6. RPL is built on directed tree graphs hence RPL has bidirectional communication. RPL creates a routing topology in form of DODAG (Destination Oriented Directed Acyclic Graphs) which is maintained by DIO (DODAG Information Object) advertised by each node. [9]

The RPL specification defines all four types of control messages as ICMPv6 information messages with a requested type of 155. This new type has been officially confirmed by IANA [10].There are many attacks which are taking place on RPL network like DODAG Version attack,[11], sinkhole attack [12], DIO suppression attack [13].

2.2. 6LoWPAN (IPv6 over Low Power and Wireless Private Area Network)

For connecting devices in IoT, a 6LoWPAN protocol is standardized by IETF workgroup. 6LoWPAN standards enable the efficient use of IPv6 over low-power, low-rate wireless networks on simple embedded devices through an adaptation layer and the optimization of related protocols. A 6LoWPAN is a lightweight protocol designed specifically for constrained devices in IoT network [14]. A 6LoWPAN border router is used to connect sensor nodes to the internet as shown in Fig. 1. The 6LoWPAN protocol is designed by compressing the IPv6 protocol for networking layer.

Major security requirements for the IoT are data confidentiality, authentication, privacy and trust [15]. Cryptography is one of the methods to address the security in IoT but it cannot detect the all attacks especially routing attack. Hence it is necessary to develop IDS which will address many internal attacks taking place in IoT network. Several IDSs are available for WSN but those are directly applicable to in the IoT network. It has been already discussed in this paper that, IoT network is based on 6LoWPAN network which is a novel protocol developed only for resource-constrained devices. Developing an IDS for IoT network is an ongoing research topic. Few IDSs are developed for IoT network as, RIDES [16], SEVLTE [17], IDS against DOS attack [18]. But still, complete security in IoT network is not guaranteed.

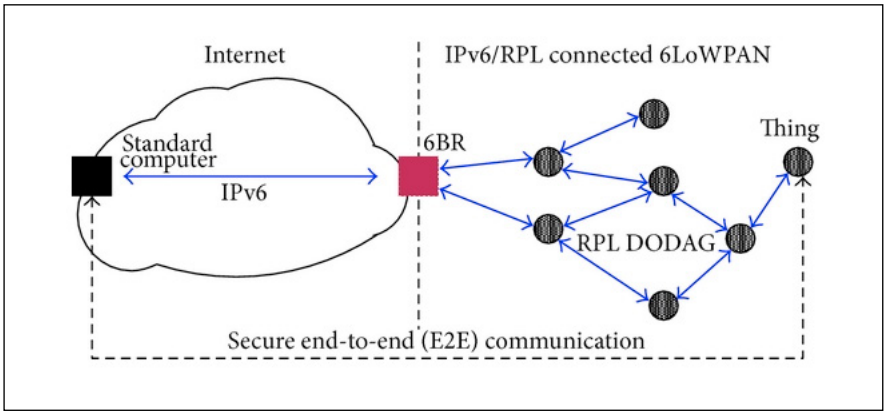

Fig. 1 IoT using 6LBR

3. Wormhole Attack

Marianne Azer et el (2009) have given a full explanation about Wormhole attack in their paper [19]. Wormhole attack is considered to be severe attacks on IoT routing. In this attack a tunnel is established between two nodes and the packet is forwarded among each other. These distant malicious nodes pretend that they are very close to each other so that neighbor nodes forward packets through them. Fig 2 gives the generalized idea of a wormhole attack. [20]

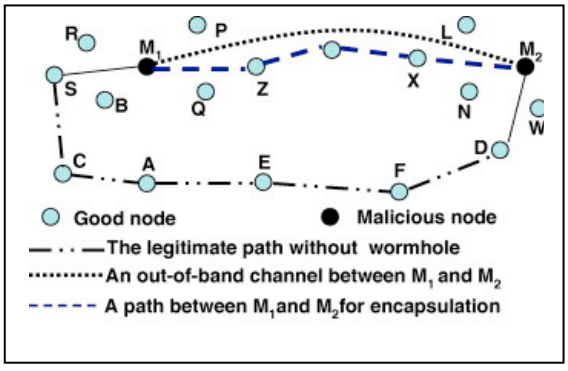

Fig 2 Generalized diagram of Wormhole Attack

We in this paper are focusing on Wormhole Attack taking place at 6LoWPAN/Adaption Layer [21]. It has four modes of operation explained as follows:

1. Encapsulation: In this type of mode, a colluding node of one end of IoT network hears the RREQ (Route Request) packet from another end through which it forms the tunnel and both the nodes pretend that they are nearby and directly connected. By assuming these colluding nodes are directly connected, nearby legitimate nodes transmit their packets through them which may cause a delay in transmission or loss in packets.
2. Packet Relay: In this type, attacker nodes relay packets between two legitimate nodes. In this type of mode, two legitimate nodes which are not in direct range with each other are connected through a malicious node which relays the packet between two valid nodes.
3. Out of Band Channel: In this type of attack mode, wormhole attack uses long wired and a wireless link. This attack requires specialized hardware to launch it. To introduce this attack, an out of band high bandwidth link is established between two attacker nodes. These two end malicious nodes which are physically located at long distance pretend to legitimate nodes that they are closely located by attracting traffic through them which eventually turn as out of band channel mode.
4. High Power Transmission: In this mode, only one malicious node with high transmission capacity can insert the attack in the network. When this node receives RREQ, it rebroadcasts the request with very high-level capability by attracting legitimate nodes to overhear this request and broadcast the packet towards the destination. In this way, a malicious node will be part of the network by creating the attack.

In paper [22] authors have discussed the implementation to evaluate the impact of a wormhole attack on a real RPL network, reasons of attacks and countermeasures

4. Proposed System

The proposed system is the novel Wormhole attack Detection System, basically designed for the IoT environment.

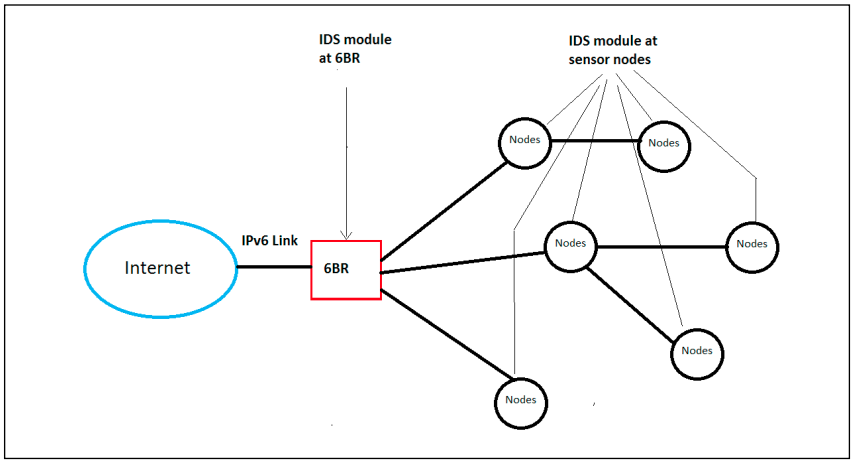

Fig 3: Proposed System

The proposed system's architecture is as shown in Fig 3. In this architecture, sensor nodes are connected to the internet using IPv6 link through the IPv6 Border Router (6BR) [23]. In centralised approach, IDS can be placed at border router and in the distributed approach; it is placed at sensor nodes. In our architecture, we are using hybrid approach of implementation where IDS is placed at border router as well as sensor nodes.

4.1. Distributed Module:

In the distribution module we are proposing following four steps:

i. Neighbour Validation**:** In this step neighbour Information from all sensor nodes is collected which contains destination node ID and neighbour's node ID.
ii. Distance Calculation**:** This step calculates the distance between to nodes using Euclidean distance method for which we are using Received Signal Strength Indicator (RSSI) value. RSSI value will be used to give the distance between two coordinates.
iii. Identification of Attack**:** In this step, RSSI value received from victim node and neighbour node is compared with the threshold value. The RSSI value is converted into distance and vice a versa. In this step, module checks whether the node has connected to valid parent, or it is connected to the parent through a wormhole link. When it confirms that node has parent through a wormhole tunnel, its starts hidden wormhole detection approach. And when it detects the packet dropping violation it starts the exposed kind of wormhole detection method.
iv. Attacker Detection: In this step, a distance between a node and its neighbour is identified using RSSI value. If this distance is more than the transmission range of the node then it is concluded that the concerned node is an attacker node.

4.2. Centralised Module:

i. Topology Construction**:** Client sends rank and ID information of a node, its parent and its children's to 6BR for constriction of network topology and for detection of the attack.
ii. Attack Detection**:** In this module, node cooperates with Detection module at 6BR to detect the hidden and exposed kind of wormhole attack. Also for detection of malicious node producing wormhole tunnel.
iii. Locating Attacker Node**:** By recording the RSSI value of the root node or broadcasting node from where victim packet has been broadcasted further, attacker node can be located.

4.3. Algorithm of the system:

1) Algorithm for wormhole attack detection on node side:

1) For every node N do
   When it selects new parent send new parent info and RSSI value of packet received from parent to 6BR
2) If Ni receives the silent packet then
   It will not forward any packet in threshold time ts (time for silent packet sending to all nodes + time for sending dummy packets between victim nodes)
3) If Ni receives monitoring packet then
   It will start listening channel after ts and records RSSI value for that.
4) If node Ni receives victim packet then
   It will start sending fixed number of packets to another victim node
5) If packet monitoring is done then
   Send RSSI value to 6BR and return to a normal state
6) If continuous packet loss found then
   Broadcast the PathTrace packet, contains the list of nodes in the path

2) Algorithm for detection of the wormhole at the border router (6BR):

Let PL is list of nodes in path,
Let AL is list of nodes sent ACK on processing PathTrace packet
Rmin and Rmax are the minimum and maximum range distance calculated from RSSI value

1) If Parent info received from node Ni then If actual distance between Ni and its parent is more than the range node Ni then
    a) Calculate Rmin and Rmax form RSSI value
    b) Find out suspect nodes in that range
    c) Find out the neighbors of suspect nodes and expected RSSI value to receive the packets.
    d) Send silent packet to all node (except the suspect node, victim nodes)
    e) Send monitoring packet to monitoring nodes Mi
    f) Send victim packet to both parent and Node Ni
2) If receives the packet from monitoring node Mi then If only one packet is received then Suspect node is malicious node, generate alert. Else Choose the suspect node as malicious node whose monitoring node send the most approximate RSSI value.

5. Experimental Setup

Intrusion Detection System for Wormhole attack is implemented in open source operating system Contiki [24]. Contiki supports in built simulator named as Cooja Simulator [25]. It supports various types of sensor nodes for simulation. In our experimentation, we use Cooja simulator to run Tmote sky nodes to get desired output [26]. In Fig. 4 Node 1 will act as a Border Router. We are evaluating a True Positive detection Rate for detecting wormhole attack and attackers. True Positive Detection Rate is defined as a ratio of the number of successful detections to the total number of detections of attack We are using cc 2420 as a radio interface. In our experimental setup, we have taken 8, 16, 24 nodes as shown in Fig 4.

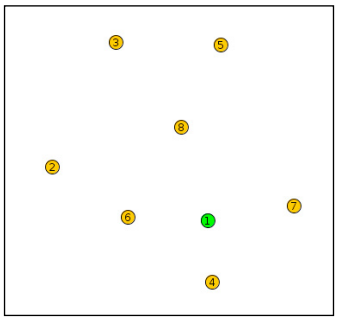

Fig 4 (a): Network Topology N=8

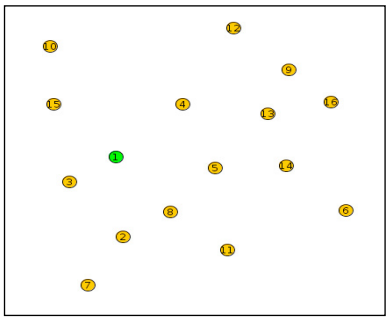

Fig 4 (b): N=16

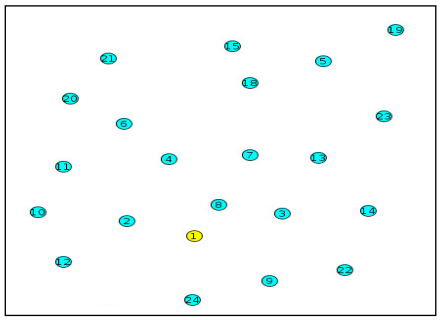

Fig 4 (b): N=24

Initially, we have run the system for 15 minutes for topologies as N=8, 16 and 24 and observed the reading for True Positive Detection Rate. We inserted 12 wormhole attacks in the system. Further, we have run the experiments for 15, 30, 45 and 60 minutes and observed the readings for the detection of the attack. For detection of attack we have referred Received Signal Strength Indicator (RSSI) values. The readings taken for various topologies are as shown in Fig. 5. In Figure 5, Node 1, we have considered as a border router. Second node and last node of all three topologies are acting as attacker nodes.

Table 1, gives the observed values of attack detected for a various time slot and for different topology. From the graph observed in Fig. 5, we have concluded that True Positive Detection Rate is linear with time. We have also concluded that as network size increases, True Positive Detection Rate reduces.

Table 1: Detection of attacks for different topologies

No. of Nodes/Time	15 Mins	30 Mins	45 Mins	60 Mins
No. of Wormhole Attacks taken place	12	12	12	12
No. of Wormhole Attacks detection for N=8	2	5	6	9

No. of Wormhole Attacks detection for N=16	1	3	4	7
No. of Wormhole Attacks detection for N=24	0	3	4	5

$$\text{True Positive Detection rate} = \frac{\text{Total no. of attacks detected successfully}}{\text{Total no.of attacks taken place}} * 100 \quad (1)\ [17]$$

By substituting the values from Table 1, in equation 1, we get a graph as shown in Fig. 5. From graph shown in Fig 5, we can conclude that good linear correlation exists between No. of wormhole attacks taken place and detection of the attack. For small network size (N=8) the correlation is 96.8 %. As network size is increased the correlation value is reduced. It is 92.7% for N=16 and 87.9% for N=24. We are working on the algorithm to get better correlation value for larger network size.

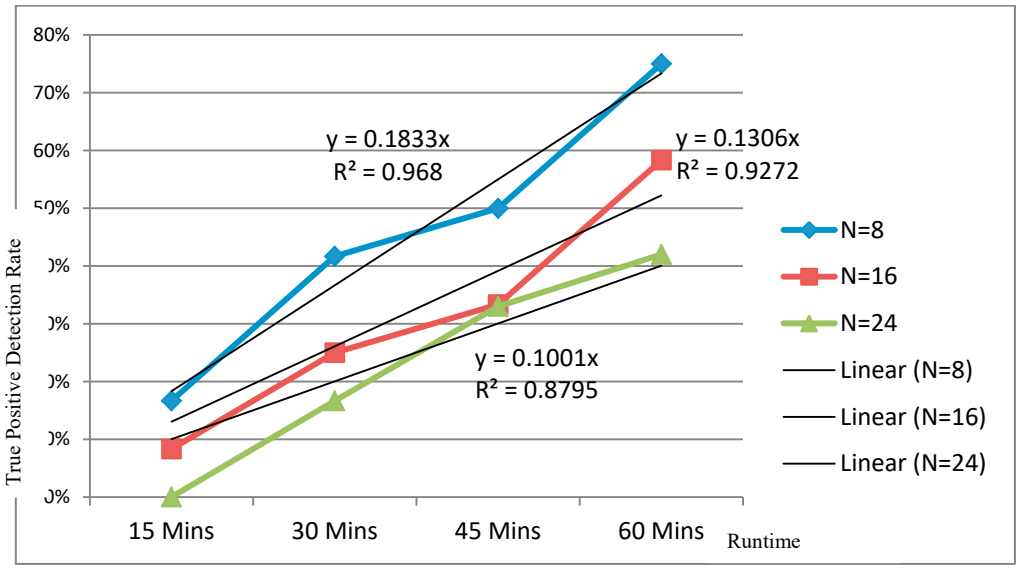

Fig. 5 True Positive Detection Rate

6. Conclusions

Wormhole attack is one of the severe attacks taking place at 6LoWPAN layer of RPL network of IoT. Very less work has been attained till now to detect this attack. We have designed and implemented an intrusion detection system to detect wormhole attack using Contiki OS and Cooja Simulator. After implementing IDS for Wormhole Attack it has been observed that designed IDS has detected the attack with success rate around 90%. It is concluded that true positive detection rate for small network size (N=8) is a higher comparatively bigger network (N=16, 24). Coefficient of correlation between a number of attacks taken place and attacks detected is more than 90% for network size N=8 and 16. This value is below 90% for N=24 which has to be improved. We are working on the improvement of positive detection rate for the network having higher number of nodes.

References:

[1] A. Rghioui, A. Khannous, M. Bouhorma, Denial-of-service attacks on 6LoWPAN- RPL networks: threats and an intrusion detection system proposition, J. Adv. Comput. Sci. Technol. 3 (2014) 143–153, doi: 10.14419/jacst.v3i2.3321.

[2] Davar PISHVA, “Internet of Things: Security and Privacy Issues and Possible Solution”, ICACT Transactions on Advanced Communications Technology (TACT) Vol. 5, Issue 2, March 2016
[3] Ms. Snehal Deshmukh, Dr. S. S. Sonavane, “Security Protocols for Internet of Things: A Survey”, ICNETS2, VIT University, Chennai, 2017, 978-1-5090-5913-3/17/$31.00_c 2017 IEEE. DOI: 10.1109/ICNETS2.2017.8067900
[4] Hamid Bostani a , Mansour Sheikhan, “ Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on Map Reduce approach”, http://dx.doi.org/10.1016/j.comcom.2016.12.001 0140-3664/© 2016 Elsevier B.V.
[5] A. Mayzaud, R. Badonnel, and I. Chrisment, “A taxonomy of attacks in RPL-based Internet of Things,” International Journal of Network Security, vol. 18, no. 3, pp. 459–473, 2016.
[6] Wallgren, Linus, ShahidRaza, and Thiemo Voigt. “Routing Attacks and Countermeasures in the RPL-based Internet of Things.” International Journal of Distributed Sensor Networks, 2013, 2013.
[7] O. Gaddour and A. Koubˆaa, “RPL in a nutshell: A survey,” Computer Networks, vol. 56, no. 14, pp. 3163–3178, 2012.
[8] T. Winter, P. Thubert, A. Brandt et al., “RPL: IPv6 routing protocol for low-power and lossy networks,” RFC 6550, March 2012.
[9] O. Garcia-Morchon, R. Hummen, S. S. Kumar, R. Struik, and S. L. Keoh, “Security Considerations in the IP-based Internet of Things,” March 2012.
[10] P. Perazzo, C. Vallati, A. Arena, G. Anastasi, and G. Dini, “An implementation and evaluation of the security features of RPL,” in ADHOC-NOW’17. Springer, 2017, pp. 63–76.
[11] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Sch¨onw¨alder, “A study of RPL DODAG version attacks,” in AIMS’14. Springer, 2014, pp. 92–104.
[12] A. Dvir, T. Holczer, and L. Buttyan, “VeRA - version number and rank authentication in RPL,” in MASS’11. IEEE, 2011, pp. 709–714.
[13] P. Perazzo, C. Vallati, G. Anastasi, and G. Dini, “DIO suppression attack against routing in the Internet of Things,” IEEE Communications Letters, vol. PP, no. 99, pp. 1–1, 2017.
[14] T. Kushalnagar, G. Montenegro, C. Schumacher, IPv6 over Low-power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem State- ment, and Goals, RFC 4919 (2007).
[15] S. Sicari, A .Rizzardi, L.A .Grieco, A .Coen-Porisini, Security, privacy and trust in Internet of things: the road ahead, Comput. Netw. 76 (2015) 146–164, doi: 10. 1016/j.comnet.2014.11.008 .
[16] Amin, Syed Obaid, et al. "A novel coding scheme to implement signature based IDS in IP based Sensor Networks." *Integrated Network Management-Workshops, 2009. IM'09.IFIP/IEEE InternationalSymposium on*.IEEE, 2009.
[17] S. Raza, L. Wallgren, T. Voigt, SVELTE: real-time intrusion detection in the In- ternet of things, Ad Hoc Netw. 11 (2013) 2661–2674, doi: 10.1016/j.adhoc.2013. 04.014 .
[18] Kasinathan, Prabhakaran, et al. "Denial-of-Service detection in 6LoWPAN based internet of things." *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*. IEEE, 2013.
[19] Marianne Azer, Sherif El-Kassas, Magdy El-Soudani, “A Full Image of the Wormhole Attacks
Towards Introducing Complex Wormhole Attacks, in wireless Ad Hoc Networks”, International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009
[20] Mrs. Snehal Deshmukh-Bhosale , Dr. S. S. Sonavane, “ Wormhole attack detection in Internet of Things”, International Journal of Engineering & Technology, *International Journal of Engineering & Technology, Volume 7 (2.33) (2018) 749-751,March 2018*
[21] Marcus Okunlola Johnson, Arish Siddiqui, Amin Karami, “A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks”, International Journal of Computer Applications (0975 - 8887), Volume 174 - No.4, September 2017
[22] PericlePerazzo, Carlo Vallati, Dario Varano, Giuseppe Anastasi and GianlucaDini, “Implementation of a Wormhole Attack Against a RPL Network: Challenges and Effects”, 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), ISBN 978-3-903176-02-7 © 2018 IFIP 95
[23] Mrs.Snehal Deshmukh-Bhosale, Dr. S. S. Sonavane, “Implementation of 6LoWPAN Border Router (6BR) in Internet of Things”, International Journal of Innovations & Advancement in Computer Science IJIACS, ISSN 2347 – 8616 Volume 7, Issue 3, March 2018
[24] A. Dunkels, B. Grönvall, T. Voigt, Contiki – a lightweight and flexible operating system for tiny networked sensors, in: EMNets’04, Tampa,USA, 2004, pp. 455–462.
[25] Ing PietroGonizzi and Simon Duquennoy. Hands on Contiki OS and Cooja Simulator: Exercises (Part II). https://team.inria.fr/fun/files/2014/04/slides_partI.pdf, 2013. [Online; accessed 10-November-2017].
[26] Texas Instruments. (2016) CC2420 SimpleLink™ Multistandard Wireless MCU l. [Online]. Available: http://www.ti.com/lit/ds/symlink/cc2420.pdf [Online; accessed 13-January-2018].