International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Design Of Intrusion Detection System For Dos Attack In 6lowpan And RPL Based IoT Network

Snehal Deshmukh-Bhosale, S. S. Sonavane,

Abstract: ***Internet of Things (IoT) is a network spread globally and accommodates maximum things under it. All these things are connected globally using IPv6 protocol which satisfies the need of connecting maximum devices by supporting 2^128 addresses. Because of heavy-weight nature of IPv6 protocol, a compressed version of it known as IPv6 Low Power Personal Area Network (6LoWPAN) protocol is used for a resource-constrained network that communicates over low power and lossy links. In IoT, devices are resource-constrained in terms of low battery power, less processing power, less transceiver power, etc. Also these devices are directly connected to insecure internet hence it is very challenging to maintain security in IoT network. In this paper, we have discussed various attacks on 6LoWPAN and RPL network along with countermeasures to reduce the attacks. DoS attack is one of the severe attacks in IoT which has various patterns of execution. Out of various attacks we have designed Intrusion Detection System (IDS) for Denial of Service (DOS) attack detection using Contiki OS and Cooja simulator.***

Keywords: IoT, 6LoWPAN, RPL, Contiki, Cooja, IDS, DoS Attack

I. INTRODUCTION

things will be connected to each other through the internet, forming the IoT network. Smart city, smart home, smart parking, etc. concepts are arising through IoT. As devices of day to day activities are connected to internet, providing security to those is the biggest challenge. Many researchers are working hard to find the solution to the attacks on 6LoWPAN and RPL network. In the near future, security will be basic and important factor to deploy and use most of the IoT applications successfully. It has been discussed by many researchers about the need for security in a constrained network in IoT [1][2] [3].

In IoT, end nodes are connected to the internet through IPv4 or IPv6 protocol. Edge router or border router connects the local IEEE 802.15.4 network to internet ie IPV6 network. The structure is as shown in Fig. 1. It also shows the protocols used in communication over IP.

The IoT devices are tightly constrained in resources such as short battery life, short radio range, limited processing capability, etc. A protocol that can manage these conditions is required for IoT implementation. A 6LoWPAN is an adequate solution for lightweight protocol requirement by IoT that integrates IPv6 and IEEE 802.15.4 by adding an adaptation layer in network protocol stack as shown in Fig.2.For 6LoWPAN implementation, maximum IoT security attacks are introduced due to IEEE 802.15.4. Because this protocol has weaker security link compared to IP. Also, resource-constrained devices of IoT have limited support security services hence those can be easily tampered by attackers. From a security point of view 6LoWPAN network is open to attack from its local network i.e. WSN and external network i.e. internet [4][5].

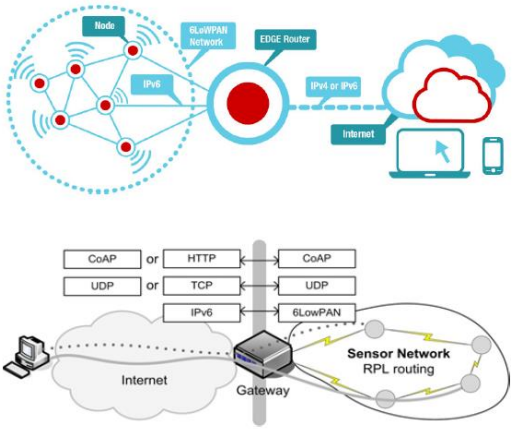

Fig. 1: IoT Architecture

The 6LoWPAN network needs a protocol which should satisfy conditions like, security, support to constrained network, performance, adaptive routing, etc. IETF working group, Routing Over Low Power and Lossy Network (ROLL) proposed Routing Protocol for Low Power and Lossy Network (RPL) for 6LoWPAN network which satisfies its maximum requirement [6].

Many authors have analyzed the existing mitigation techniques for attacks in IoT network. Annas Rghioui et al. have discussed RPL protocol which is designed for 6LoWPAN network. 6LoWPAN is a new IPv6 header compression protocol, specially designed for tightly constrained devices network. IoT devices are very prone to security attacks as they are directly connected to insecure internet. RPL protocol also undergoes security attacks very easily because RPL connects the network which has less processing power and less battery life. Attack like DoS attack affects the processor time, congestion in communication lines and bandwidth or denial of resources to intended users, etc[7].

Manuscript published on 30 September 2019.
*Correspondence Author(s)
Ms. Snehal Deshmukh-Bhosale,*, Research Scholar, Raisoni College of Engg. And Management, Pune, Asst. Professor, RMD Sinhgad School of Engg, Warje, Pune., sa_bhosale@yahoo.com
Dr. S. S. Sonavane, Dean R&D and Professor (E&TC), Indira College of Engineering & Management, Parandwadi, Pune, , Maharashtra, India

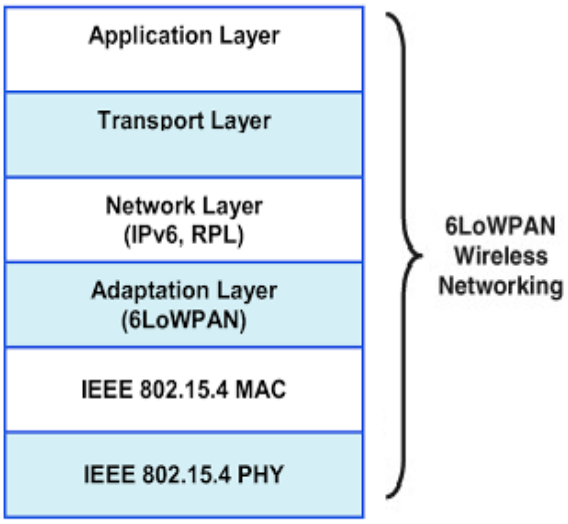

Fig. 2 IoT Protocol stack

The paper is organized as follows: Section II discusses Security attacks on 6LoWPAN and RPL network with mitigation techniques. Section III discusses the Denial of Service attack. Section IV explains the methodology of IDS implementation and Section V concludes the paper.

I. SECURITY ATTACKS ON 6LOWPAN AND RPL AND MITIGATION TECHNIQUES:

A.6LoWPAN:

IPv6 protocol was not the initial choice for IoT network because of its bulkiness. A 6LoWPAN protocol enables communication using IPv6 over the IEEE 802.15.4 protocol. IPv6 headers are not small enough to fit within the small 127 bytes Maximum Transfer Unit (MTU) of the IEEE 802.15.4 standard. Hence to make compatibility fragmentation at the transmitter end and defragmentation of packets at the receiver side is performed by Adaptation layer. To achieve these three essential tasks named as, Header Compression, Fragmentation and Link Layer Forwarding are done on each packet.6LoWPAN connects WSN to the internet so it faces security attacks from both the sides:

i. Security Attacks from the local side (Internal Attack):
In the internal attack, attacker nodes physically capture the legitimate nodes and break the cryptographic security. Internal attacks mainly destroy the network operation hence it is important to detect them in time with predefined IDS. Sybil Attack, Sinkhole attack, Selective forwarding attacks, blackhole attack, etc. are the examples of internal attacks which are discussed next.

ii. Internet Side Attack (External Attack):
End-users can access the data from WSN through 6LoWPAN link. Here authenticity plays a very important role. Attacker nodes can access the information illegally if authentication is not applied properly. In this case, authentication attack comes in picture. It also faces a confidentiality attack where the unauthorized node has access to the resources of IoT devices [8]

iii. Fragmentation Attack:
Fragmentation is required in 6LoWPAN adaptation layer because of different MTU size of IPv6 and IEEE 802.15.4. For compatibility between these two protocols, fragmentation is done at the adaptation layer. When fragmented packets are transmitted, there is no mechanism which will identify the authenticity of the received fragment. Attacker node changes original fragment with duplicate one and put it in fragmented chain. Hmmen Rene et al. have proposed two mechanisms for identifying this attack. (a) Split Buffer Approach where attacker node attacks the receiver buffer before it reassembles al the received fragments. Attacker disrupts buffer allocation. This approach proposes direct communication between an authentic sender and attacker for attack detection.
(b)Content Chaining Scheme approach uses cryptography to verify that the received fragment belongs to the same pocket or not for detecting the attack [9].

iv. Confidentiality Attack:
Confidentiality Attack has many types like Man in Middle attack, Eavesdropping attack, Spoofing attack, etc. 6LoWPAN extension IPSec supports AH and ESP for secure communication between traditional internet and IPv6. Raza et al. have used crypto hardware for maintaining authenticity and confidentiality in IoT communication [10][11].

v. Sinkhole Attack:
In this attack malicious node misguides the shortest path to the communicating nodes which affects the processing and the battery power of nodes which has limited resources. Weekly et al. have implemented techniques named as parent failover and rank authentication techniques to mitigate the sinkhole attack. In their work, they have concluded that the combination of both methods is more effective than a single method [12].

vi. Selective Forwarding Attack:
In this type of attack, attacker forwards or drops selective packets from a particular node or group of nodes. In worst cases, the attacker node doesn't forward any packets and stops communication of the victim node to other networks. Authors developed IDS to detect the said attack successfully using Contiki OS and Cooja Simulator. They have concluded that if attacker node is nearer to the border router it detects the attacker with the highest true positive detection rate [13].

vii. Hello Flooding Attack:
In a normal network, any node can join the IoT network by sending a hello message. An attacker node broadcast hello message by pretending it as a neighbor node. If the attacker node is not in communication range of IoT network then it is difficult to launch this attack. Karlof and Wagner et al. implemented a method for removal of Hello flooding attack by making HELLO message link bidirectional. If no link-layer acknowledgment message is received the path assumed to be suspicious and the packet will be transferred through a different route. Even if the geographical location is known then any packet received from far away node beyond the transmission range is discarded by assuming hello flooding attack [14][15].

viii. Sybil Attack:

In a Sybil attack, attacker node manipulates fake identities and act as a genuine node. It may also have several logical addresses on the same physical node. In this attack, attacker nodes take control over the entire network with logical addresses. J. Newsome et al.
in their work explained the mitigation technique against Sybil attack by introducing an information table of the node with their ID and location which will avoid further consequences of disturbing the network due to Sybil attack [16].

ix. Wormhole Attack:
Wormhole Attack is one of the severe attacks in IoT which misguides the legitimate nodes by changing the routing information. Malicious nodes advertise as the shortest path is through them and attract traffic towards them. In reality, they form a tunnel with a long-distance attacker node. In this attack, packets are delayed and legitimate nodes get involved in the communication unnecessarily by draining their battery power. Deshmukh-Bhosale et al. have developed an IDS to detect the attack and attacker nodes. They have used hop count and signal strength to identify the attacker. Border router in the system maintains the shortest path using signal strength and hop count in the routing table. When any packet doesn't follow the predefined path and new nodes are identified in the path which is not in the transmission range of sender and receiver then the attack is detected [17].

II. DENIAL OF SERVICE (DOS) ATTACK

Annas et al. have discussed the DoS attack on 6LoWPAN network. This attack makes network unavailable for an indefinite period, which affects the performance of the network by damaging the network. It is difficult to design the IDS to detect the DoS attack because it has various patterns of attack insertion. Authors have elaborated; IoT standards like IPv6 and IEEE 802.15.4 have their own security solutions. But IPv6 security protocols are heavy in nature which is not desirable for IoT network which has less processing power. IEEE 802.15.4 security solutions are not compatible with IPv6 communication stack. It shows that traditional solutions for wireless communication cannot be used directly for IoT network security [7].

A. Countermeasures for Security Attacks

For various attacks discussed so far, no mitigation technique is available which will remove any of the discussed attacks completely and permanently. As it is known that IoT is a network of constrained devices where many attacks target the scarcity of resources and energy for data processing. The main purpose of the attacker is to disrupt the entire network and flood the network with useless data.
Detection of attack is known as intrusion detection where any abnormal activity in the network is detected and tried to remove from network. IDS analyze the data traveling through the network and take the corrective action if it detects the symptoms of security threats. While designing the IDS for 6LoWPAN network, one must consider characteristics of 6LoWPAN network because 6LoWPAN network is an ad-hoc network which is infrastructure less and also heterogeneous and distributed in the hostile environment [18].

The IETF RFC 4944 have addressed various security threats in RPL and 6LoWPAN network, still, there is no 100% security implementation in this network. David Airehrour et al. have summarized the various research challenges in 6LoWPAN as well as in RPL in their paper. They have analyzed the latest routing protocols and existing security mechanism in IoT. They have also discussed the open research challenges [19].

III. IMPLEMENTATION OF THE IDS

For experimentation, we have used Contiki OS with inbuilt Cooja simulator. We have used Tmote Sky nodes for simulation purpose. Designed IDS detects the DoS attack in IoT network. As it has been already discussed, DoS attacks manipulate the network connection and make it unavailable to its intended users. It denies clients asset on a system by presenting undesirable movements. DoS attack is also introduced in-network by flooding the target with traffic. This is a very popular attack where victims of DoS attack are often the web servers of commercial website.

For the implementation of the IDS using Contiki OS following files are used 1. border-router.c, 2. UDP-server.c (UDP-client.c can also be used), 3. slip-bridge.c (It contains callback function for processing a SLIP connection request), 4. https-simple.c (A simple web server forwarding page generation to a protothread). UDP-server nodes will form a DAG with the border router set as the root. The border router will receive the prefix through a Serial Line Interface Protocol (SLIP) connection and it will be communicated to the rest of the nodes in the RPL network.

Simulation Result:

In our experimentation, we have considered the topology of N=16 and N=24 as shown in Fig 3 (a), (b) respectively. Border Router is shown in a different color. In our work data packets of the same size are transmitted from sensor nodes to the Border Router. Various metrics like hop count, the total number of packets transmitted, energy consumption by each node and transmission energy are considered by proposed IDS. In our work, we have considered packet loss type of DoS attack.

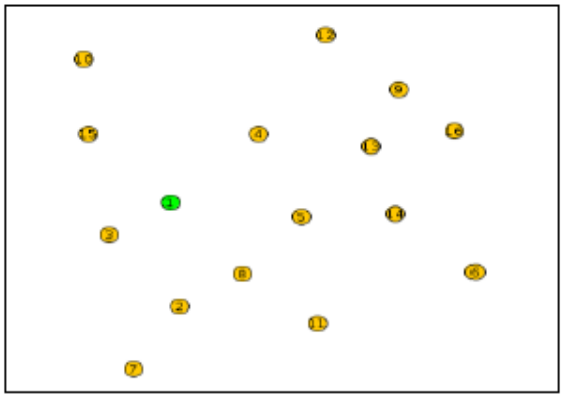

Fig 3(a): Topology N=16

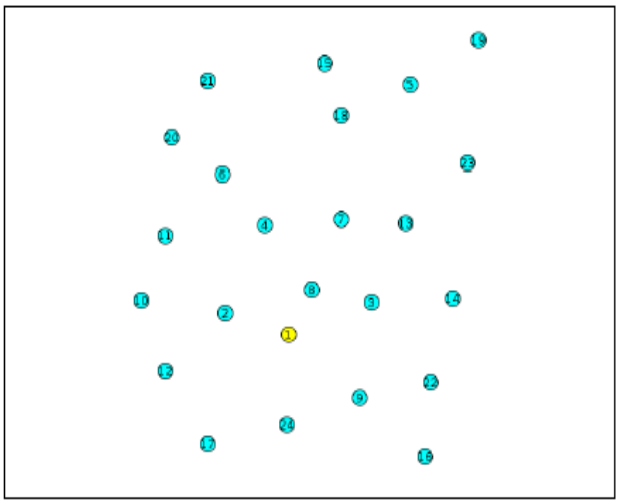

Fig 3(b): Topology N=24

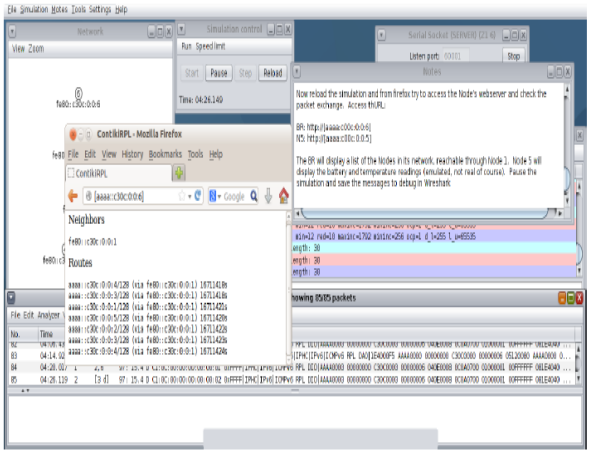

Fig. 4: IoT Network setup

In our implementation, we have checked for the condition without attack and with an attack. When no attack is present, no packet loss is detected as shown in Fig 4. After inserting the attack it has been observed the loss of transmitted packets by showing packet loss as shown in Fig 5. This method has given 93% of the correct detected rate.

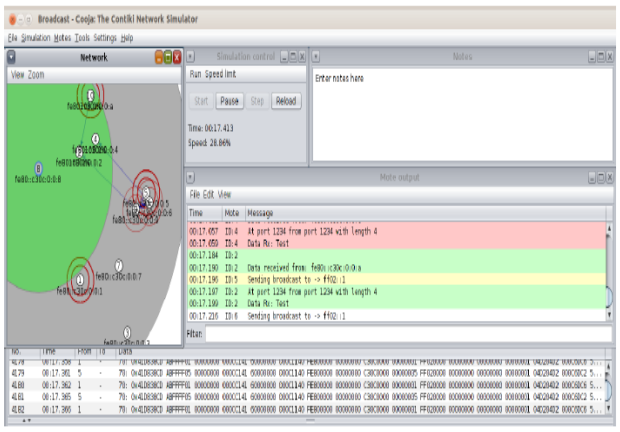

Fig. 5: Cooja simulation for DoS Attack

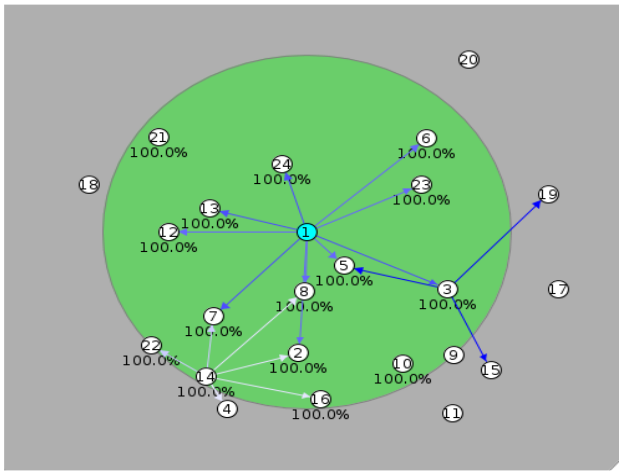

Fig. 6: Transmission of packets

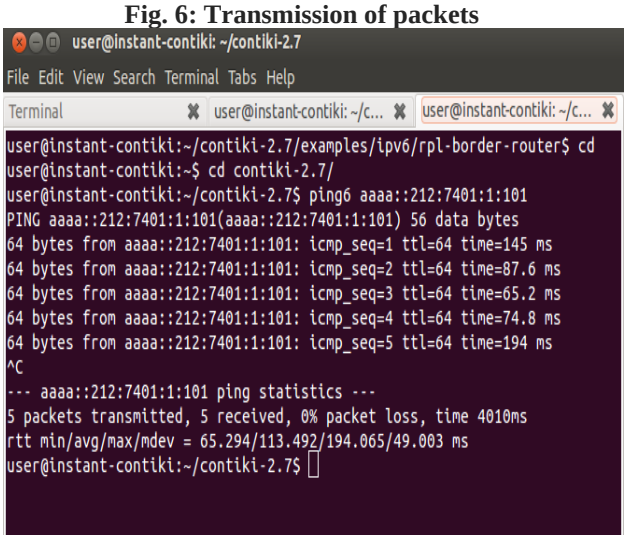

Fig 7: No loss of packets when no attack

Fig 8: Packet loss due to DoS Attack

IV. CONCLUSION

IoT network is constrained network in terms of battery, processing power, memory, etc. hence it is very susceptible to the security attacks. In this paper, we have discussed many attacks which affect the quality of communication in IoT. We have also discussed the mitigation techniques for various security attacks in IoT. We have also analyzed mitigation techniques designed by researchers.

As attack pattern is not the same in IoT because of its heterogeneous nature and hence it is difficult to design an IDS which will remove the attack completely and permanently. We have observed that there are many attacks which are unaddressed until now where a lot of research work is expected to be done. In this paper, we have designed IDS for DoS attack using Contiki OS and Cooja simulator. Attack pattern of DoS is not constant in IoT because of its heterogeneous nature hence it is difficult to design IDS against DoS attack. The developed IDS have given 93% of detection rate which is highest for IoT network. This IDS consumes less energy which is important requirement for resource-constrained network. After detecting the DoS attack successfully, we are working to define IDS which will detect more than two attacks using same IDS configurations.

REFERENCES:

1. Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha, "Survey on secure communication protocols for the Internet of Things", http://dx.doi.org/10.1016/j.adhoc.2015.01.006, 1570-8705/_ 2015 Elsevier B.V., journal homepage: www.elsevier.com/locate/adhoc
2. J. Gubbi, R .Buyya, S. Marusic, M.Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener.Comput.Syst.29 (7)(2013)1645–1660.
3. 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
4. David Airehroura, Jairo Gutierreza and Sayan Kumar Ray, Secure Routing for Internet of Things: A Survey Journal of Network and Computer Applications, 2016.
5. Linus Wallgren, Shahid Raza, Thiemo Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things", International Journal of Distributed Sensor Networks Volume 2013, http://dx.doi.org/10.1155/2013/794326
6. Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Published 26 January 2017, Journal of Electrical and Computer Engineering Volume 2017, Article ID 9324035, https://doi.org/10.1155/2017/9324035
7. Anass Rghioui, Anass Khannous, Mohammed Bouhorma, "Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition", Journal of Advanced Computer Science and Technology, 3 (2) (2014) 143-153, Science Publishing Corporation, www.sciencepubco.com/index.php/JACST, doi: 10.14419/jacst.v3i2.3321
8. Anhtuan Le, Jonathan Loo, AboubakerLasebae, Mahdi Aiash and Yuan Luo, "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach", INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, *Int. J. Commun. Syst.* (2012), Published online in Wiley Online Library. DOI: 10.1002/dac.2356
9. Hummen, René, Jens Hiller, Hanno Wirtz, Martin Henze, "6LoWPAN fragmentation attacks and mitigation mechanisms.", Proceedings of the Sixth ACM Conference on Security and privacy in wireless and mobile networks.ACM, 2013.
10. Shahid Raza, Simon Duquennoy, Tony Chungogan Yazar, Thiemo Voigtandv Utz Roedig, "Securing Communication in 6LoWPAN with Compressed IPsec.", distributed computing in Sensor Systems and Workshops (DCOSS), IEEE,2011.
11. Shahid Raza, Simon Duquennoy1, Joel Höglund1, Utz Roedig2 and Thiemo Voigt1 "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN." SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2014; 7:2654–2668 Published online 18 January 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.406
12. Weekly, Kevin, and Kristofer Pister. "Evaluating sinkhole defense techniques in RPL networks." Network Protocols (ICNP), 2012 20th IEEE International Conference on. IEEE, 2012.
13. Suricata- The Next Generation Intrusion Detection System." [Online] http://www.openinfosecfoundation.org, Accessed Jan 2019
14. Wallgren, Linus, Shahid Raza, and Thiemo Voigt."Routing Attacks and Countermeasures in the RPL-based Internet of Things."International Journal of Distributed Sensor Networks 2013.
15. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2, pp. 293–315, 2003.
16. J. Newsome, E. Shi, D. Song, and A. Perrig, "Sybil Attack in IoT: Modelling and Defenses: Sybil attack in sensor networks: analysis & defenses," in Proceeding of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN '04), pp. 259 –268, ACM, April 2004
17. Mrs.Snehal Deshmukh-Bhosale, Dr. S. S. Sonavane, "A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things", www.elsevier.com/locate/procedia, ScienceDirect, Procedia Manufacturing 32 (2019) 840–847,10.1016/j.promfg.2019.02.292
18. Leonel Santos, Carlos Rabadao, Ramiro Gonçalve, "Intrusion Detection Systems in Internet of Things", Publisher: IEEE, DOI: 10.23919/CISTI.2018.8399291
19. David Airehrour, Jairo Gutierrezand Sayan Kumar Ray, "Secure Routing for Internet of Things: A Survey", Journal of Network and Computer Applications, 2016.
20. Texas Instruments CC2420 Simple Link™ Multi standard Wireless MCUl. [Online]. Available: http://www.ti.com/lit/ds/symlink/cc2420.pdf [Online; accessed February-2019].
21. 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.
22. Ing Pietro Gonizzi 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 December 2018].

AUTHORS PROFILE

Mrs. Snehal Deshmukh-Bhosale, Persuing PhD in SPPU, Pune, Asst. Professor, E&TC Dept, RMDSSOE, Pune, Published more than 30 reesarch papers in international journals, Published two patents on current research work, Received best paper award twice for current research work. Having more than 18 years of experience in the field of education, To fulfill the work of PhD Mrs. Bhosale with her guide have developed an Intrusion Detection System (IDS), using Contiki OS and Cooja Simulator. They have got the optimum result in terms of throughput, delay and attack detection in terms of positive and negative attack detection. For hardware implementation we have used Raspberry Pi and node nRT52 nodes.

Dr. S. S. Sonavane, Dean R&D and Professor (E&TC), Indira College of Engineering & Management, Parandwadi, Pune, , Maharashtra, India, He is having20 years of experience in educational field and served in many well-known organizations. He has a successful academia and published 2 books at International level (Austria and one in Germany). He had more than 75 International and National publications on his name in reputed peer Reviewed Journals. Published more than 5 patents on his name. He is the registered PhD guide in SPPU, Pune.He is also Reviewer of many Electronics International Journals including IEEE Sensor Journal and IEEE Communication Letters. He had successfully completed two Research Projects funded by University of Pune. Research Areas: Wireless Sensor Network, Internet of Things