Analysis of IoT Security at Network Layer

Rahul Sharma[1], Nitin Pandey[2], Sunil Kumar Khatri[3]

[1,2,3]*Amity Institute of Information technology, Amity University Uttar Pradesh, Noida, India*
[1]*rasha5400@gmail.com*, [2]*npandey@amity.edu*, [3]*skkhatri@amity.edu*, [4]*sunilkkhatri@gmail.com*

***Abstract*--The new future for the connectivity to the world are the IoT devices which interconnect heterogeneous object with each other. These IoT devices will make an autonomous world which will have the ability to exchange information and make decisions at the real time. But since these devices are very small therefore they have constrained to memory, processing, battery powered and resources due to which chances of an attack on IoT devices are more than normal devices. To overcome this these IoT devices use lightweight protocols and standards at each layer. At the network layer, 6LoWPAN and RPL are the two main protocols which transfer the data from one device to another. This paper focuses on analyzing different types of attack on the 6LoWPAN and RPL and a new solution for the increased rank attack which helps to stop the loop and resource depletion.**

***Keywords* -- Internet of Things, Network layer, 6LoWPAN, RPL, Increased Rank Attack.**

I. INTRODUCTION

The World has changed a lot with the new emerging technologies. And one of the most talked, researched and used technology these days is IoT. IoT technology has changed the world from senses to sensors which gather and process the data. This concept of IoT includes in Machine-to-Machine (M2M) communications, Wireless Sensor Networks (WSN) and Low-power Wireless Personal Area Networks(LoWPAN). Many applications have been developed in IoT like smart cities, smart manufacturing, health care, automotive, wearables, building and home automation. IoT technology has made our life easy and comfortable but with so many benefits there are some drawbacks and one of the major drawbacks is the security vulnerability that has to be considered.IoT devices are connected using different communication protocols at different layers and each protocol is responsible to transmit the data based on its role and specification. Figure 1 illustrates different layers of communication in IoT with their corresponding.

Application	CoAP
Network/Routing	RPL
Adoptation	6LoWPAN
MAC	IEEE 802.15.4
PHY	IEEE 802.15.4

Fig. 1. Layers and their Protocols [1]

As shown in the figure 1 Application layer uses CoAP protocol. Network or Routing layer use RPL protocol. Adoptation layer have 6LoWPAN protocol, MAC and PHY layer have IEEE 802.15.4 protocol. All these layer help IoT devices to transmit data to other devices in a very secured way.

The communication between the IoT devices is different than other devices on the internet because it is not restricted to machine to human or vice-versa. It has an extra feature that is machine to machine communication. Though IoT has this extra feature of heterogeneity between the network, it raises the issue of compatibility between devices. Therefore, current protocols cannot be used on the IoT devices as it will use more resources. Due to which new protocols have to be developed and testedso that they are efficient security wise and resource wise. Since, new IoT protocols are not so powerful as compared to existing protocols, attackers can easily attack and gain the information about the users or the machine and use it for the criminal activities [2]. In IoT it is important to protect the network and objects equally because objects have the ability to know the network state and protecting them from any attacks. All this can be achieved by using strong protocols and software that enables objects to be responsive to any situations and behaviours that may be abnormal or affect the security.

Given below are some of the different security principles that should be considered for protecting the data from the end-user to the sensor network for achieving a secure communication

A.Confidentiality

Confidentiality ensures data security. It is very important to ensure that the data is secure and only available to authorized users. In IoT it is important that sensors don't reveal the collected data to neighbouring nodes [2].

B. Authentication

Authentication involves to identify and authenticate devices or users which are interacting with each other so that it is known the data is being generated from a trusted source [11].

C. Integrity

Integrity ensures the data that is exchanged between different IoT devices is not altered by any unauthorized device or person while transmission.

D. Availability

Availability ensures the data or resources are available whenever required by the devices or users so that expectations of IoT can be achieved [2].

978-1-5090-3012-5/17/$31.00 ©2017 IEEE

E. Robustness

Robustness ensures that node is able to withstand in abnormal conditions like errors while execution or errors in input but does not degrade its performance.

F. Resiliency

Resiliency ensures the node is able to recover its performance after an abnormal condition.

II. RELATED WORK

Broadly in networks there are two of attacks that are taken place:external attacks and internal attacks
To cope up with these two types of attacks cryptography and IDS are used

A. Cryptography

Cryptography is considered the first line for solving some of the security principles i.e. confidentiality, authentication, and integrity. But, it cannot availability, robustness, and resiliency.

Therefore, it needs to cooperate with the Intrusion Detection System (IDS), which can monitor and detect malicious sources from the early phase to eliminate further damage of the attacks.

Cryptography techniques
In cryptography technique message is encrypted before transmitting. Cryptography aims at threefold protection i.e. authentication should be only given to the authenticated user, who has the right key which decrypts and read the message; integrity message should not be altered during transmission; and confidentiality. The message cannot be decrypted without the key [4].

Cryptography is very strong and helpful for protecting from the external attacks, but it lacks the ability in detecting and eliminating internal attacks. It's because cryptography cannot detect attackers who have legal keys but they behave maliciously.

For example, cryptography in network security is weak under attacks which aim at network performance such as DoS and resource attack like jamming.
Therefore, cryptography alone cannot provide total security in the network. It needs Intrusion detection system to monitor any malicious behavior in the network and prevent it early so that there is a decrease in attacks [10].

B. IDS

IDS is therefore the second line of defence that secures the network from almost all of the internal threats.
The concept behind the IDS is to analyse all the network data collected in order to detect signs of any attacks or intrusion and raise or trigger an alarm and discover the anomaly.

IDS techniques
IDS monitor the data on the basis of time taken between two consecutive messages, repetition, sender identification, high delay, changes in payload, modified packets, lost packets, amount of energy consumed etc.

There are different kinds of IDS which are divided in 3 types of intrusion detection:

1) *Misuse IDS:* Misuse IDS work on the concept of pattern match. Firstly, it defines patterns of each type of internal attack that IDS should detect. If a suspicious behaviour match the pattern it will trigger an alarm.
2) *Anomaly-based IDS:*Anomaly-based IDS works on the principle of gathering the information about the normal behaviour of the monitored network. After gathering it determines a threshold and if normal network exceeded the threshold, the IDS raise an alarm.
3) *Specification-based IDS:* Specification-based IDS is similar to anomaly-based IDS, but the main difference is that its threshold is defined a priori.

III. PROTOCOLS OF NETWORK LAYER

A. 6LoWPAN

6LoWPAN was defined by Internet Engineering Task Force(IETF) as a set of standards which enable the use of IPv6

over Low powered devices in Wireless Personal Network. Therefore, 6LoWPAN is currently the key technology that support internet communications in the IoT devices as IPv6 was impractical for the constrained low energy wireless communication environments [3].

In IoT 6LoWPAN is a protocol which is at the network layer and allows to have connection to internet using open standards. 6LoWPAN can work at multiple frequency band at physical layer due to which it can perform on multiple communication platform [1].

Since IoT devices are resource constrained devices therefore here every bit is very important and should be used very carefully. For example, in IoT MTU size is 127 bytes compares to IPv6 1280 bytes [12].

In 6LoWPAN there are different types of attacks as shown in figure 2

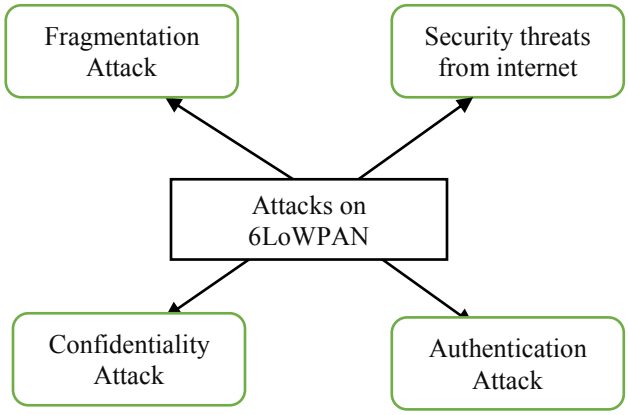

Fig. 2 Attacks on 6LoWPAN [5]

Types of Attacks on 6LoWPAN

1) Confidentiality Attack: 6LoWPAN uses IPsec to have end-to-end secure communication channel between sensor's which are IP enables and the internet. 6LoWPAN have confidentiality of data by using encryption mechanism which helps the IoT devices to be safe from most of all the external attacks like man in middle, eavesdropping etc [5].*2)Authentication Attack:* IoT devices having 6LoWPAN as network topology can join the network without any authentication. Due to this a attacker can join any network very easily. To prevent this type of attack, administrative approval mechanism can be used to first authenticate the node than only a node can be in a particular network topology. Because of this mechanism any node which is in that topology cannot communicate to any third-party nodes. For an example, when a node wants to communicate to another node it will first check its routing table that whether that particular node is in the table or not. If not than it will ask the border router node for that particular node authentication existence. Border router node will check its table for the list of nodes which are authenticated and see if that particular node is there or not. If node is there in the list it will send the message to the node that outside node is authenticated [9]. The node will than updates its routing table and will communicate to that node will be done otherwise the communication will not happen [5].

*3)Fragmentation Attack:*In IoT, when a node sends the fragment to another node there is no mechanism at receiving point to check whether the received fragment is spoofed or duplicated [5]. So, an attacker can easily put his/her own fragments in the fragment chain.

To stop this type of attack, we can use content chaining scheme. In this it uses cryptography mechanism to check whether the received fragments are from same packet or not [8].

*4)Security threats from internet:*The chances of attack from the internet to the 6LoWPAN is very high because of malicious packet present here. So, to avoid such attacks from the internet an firewall can be installed on 6BR so that all the nodes under it are safe from the attack.

B. RPL

RPL stands for Routing Protocol for Low-Power and Lossy Networks and was defined by IETF. It is a network layer protocol which is mainly designed for the wireless devices with small battery and to provide reliable performance in lossy environments. It uses a distance vector routing protocol for Low Power and Lossy Networks(LLNs) using IPv6. RPL protocol are based on Directed Acyclic Graphs (DAG) and is better than tree because it allows node to select multiple neighbour nodes as its parent. In DAG node ranks is always higher than its parent node [6].

RPL has three basic security modes.

- Unsecured: It is the default mode in RPL in which control message is send without using any additional security.
- Preinstalled: It uses key to have confidentiality, integrity and authentication. So, therefore nodes which have devices with pre-configured symmetric keys only join the RPL instance.
- Authenticated: In it, when a node wants to join the network with a pre-installed key than key authority will authenticate and then authorize the devices [1].

There are three broad types of attack on RPL: -

*A. Attack on Topology*These attacks are those which are performed on the network topology which are further classified in Sinkhole attack, Wormhole attack, Blackhole attack as shown in the figure 3.

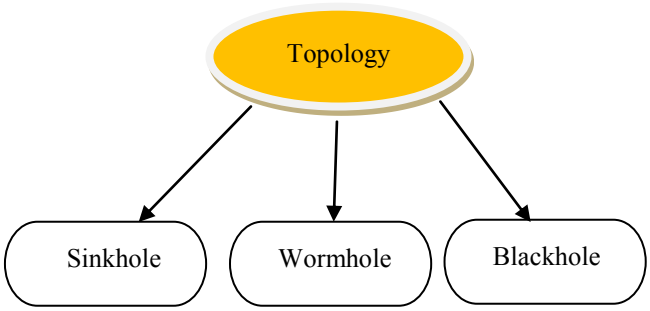

Fig. 3. Topology Attack [4]

1) *Sinkhole Attacks:*In sinkhole attack, a malicious node attracts its nearby neighbour nodes to route the packets through it by advertising it as a beneficial path. This attack makes the node to use a lot of resource and degrade the network performance. This attack become more powerful when combined with other attacks. To defend this attack, we can use rank authentication attack [4], [5], [13].

2) *Wormhole Attack:*Wormhole attack, is produced by at least two of the malicious node communicating directly with each other at different frequency than in the network which they are. When one of the malicious node gets packet [6], it sends directly to other without transiting it through the normal path. To defend from this attack, we can use Markle Tree authentication [4].

3) *Blackhole Attack:* In blackhole attack, a malicious node which receives packets from other nodes to transmit to further drops the packet there itself. This attack becomes more dangerous when combined with sinkhole attack because it will cause great loss of traffic [4], [5].

B. Attacks on Resource

Attacks on resources makes the malicious nodes to perform unnecessary certain actions which leads them to exhaust their resources like consuming more energy, processing power and memory utilization. Due to this it impacts the whole network

by congesting the available links which make the network lifetime shortened. The resource attack is further classified into flooding attack, version attack, increased rank attack and local repair attack as shown in figure 4

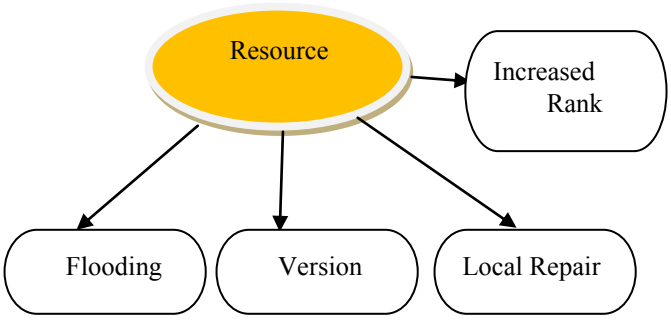

Fig. 4 Resource Attack [4]

1)Flooding: To join a network a malicious node has to broadcast a message as HELLO message to all its neighbour. This node with strong routing metrics enter in network and send HELLO message again and again to others node at given short period of time. perform this attack. This attack generates a large amount of traffic in the network and makes the nodes and links unavailable to others nodes. This causes other nodes to exhaust their resources like consuming more energy, processing power and memory utilization[4].

*2)Increased Rank:*In RPL a rank is increased is downward direction to have the acyclic nature of DODAG and to optimize the routing cost. When a node wants to change its rank, its new rank should be greater than its parent rank. But, a malicious node advertises a higher rank than its supposed rank [5]. And because of this loop are formed as its new parent was in its sub-DODAG.

3)Version: Version attack happens when a higher version number is published in DODAG tree. This leads to have a DIO message to all the other nodes of having higher version number. Due to which it generates a new network topology which is un-optimized and brings in consistencies in the rank order. This attack is very powerful as it increases overhead 18 times and double the time delay in network. A malicious node which is located at large distance from the root causes the increase in overhead, and the loss of packet [4].

*4)Local Repair:*In this attack, an attacker with the help of malicious node sends the repair message locally to all its neighbour in the network. This makes repairmen in all the nodes which hear repair message. This attack has more impact than any other attacks and because of this it affects the delivery ratio of the packets. This attack also leads to generate extra control packets and have an influence on end to end delay of the packets [6]. Due to this, it exhausts the energy resource very drastically.

C. Attack on Traffic

Attack on traffic basically make the congestion in the traffic or over load of packets in the network. This attack is further classified into sniffing attack and decreased attack as shown in figure 5

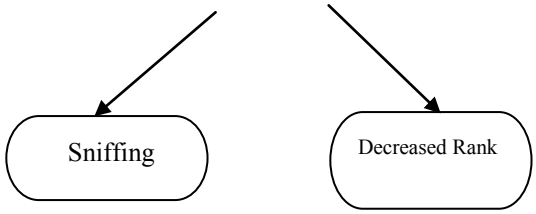

Fig. 5 Traffic Attack[4]

1)Sniffing: Sniffing attack listen to packets over the network which are transmitted from one node to another. If a node is attacked by sniffing attack than an attacker can obtain information like content of the data, routing information and DODAG configuration. This attack is very difficult to be detected because of its passive nature.

*2)Decreased Rank:*In DODAG, if a node has a lower rank than it means it is closer to the root node and has to manage more traffic than compared to the nodes which have higher ranks. When a malicious node advertises a lower rank value than it overclaims its performance. Because of this large part of traffic is attracted towards it [4][14][15].

IV. PROPOSED MODEL FOR PREVENTING INCREASED RANK ATTACK

When a packet has to be transferred to another node, firstly the source node will check its routing table for the existence of the destination address. If itexists, then each of the packets that have to reach at that particular destination address will be assigned nodeCount value (number of nodes, packets have to go through to reach its destination node) in $PACKET_{count}$. After this, when packets go to the next node their $PACKET_{count}$ value will get decremented by 1 at each node. This decrement of $PACKET_{count}$value will continue till it becomes 0. When $PACKET_{count}$ value becomes 0 it will check whether destination node address is equal to current node address. If yes, it means packets has reached its destination address else a trigger will be raised regarding some malicious activity or the packets are in the loop.

If destination address does not exist in the routing table of the source node then a request will be sent to the DODAG regarding existence of the destination address and nodeCount. DODAG will check its routing table to see whether destination address is present or not. If present it will assign nodeCount value in a count variable and send it to the source node. Source node will update its routing table with the destination address.It will assign count value to the nodeCount of that particular destination address. After this, all the packets who have to go to that destination node will be assigned the

nodeCount value in $PACKET_{count}$and the whole process will go on till the packets reach its destination node address or there is an alarm raised regarding packets in the loop or some malicious activity.An algorithm to stop increased rank attack is given below

Algorithm

Step 1: Source node checks routing table
if ($Destination_{Address} == InRouting_{Table}$) then
Step 2: DO
while(packets)
$PACKET_{count=}$ nodeCount
Step 3: send $PACKET_{count}$ to next node
Step 4: Decrement $PACKET_{count}$at each node till
$PACKET_{count} == 0$
Step 5: if ($DestinationMAC_{address} == CurrentMAC_{address}$) then
packets reached its destination
STOP
Step 6: else
DO:
Trigger an alarm
Step 7: else
Do: Send request to DODAG for nodeCount
Step 8: DODAG checks its routing table
if ($Destination_{Address} == InRouting_{Table}$) then
Do count=nodeCount
Step 9: Send count to Source node
Step 10: Source node update its routing table and
nodeCount=count
Step 11: Repeat step 3, 4, 5, 6 and 7
Step 12: Else send message to the source node regarding non-existence of the destination address
Step 12: STOP

A flow diagram of the algorithm isgiven in figure 6

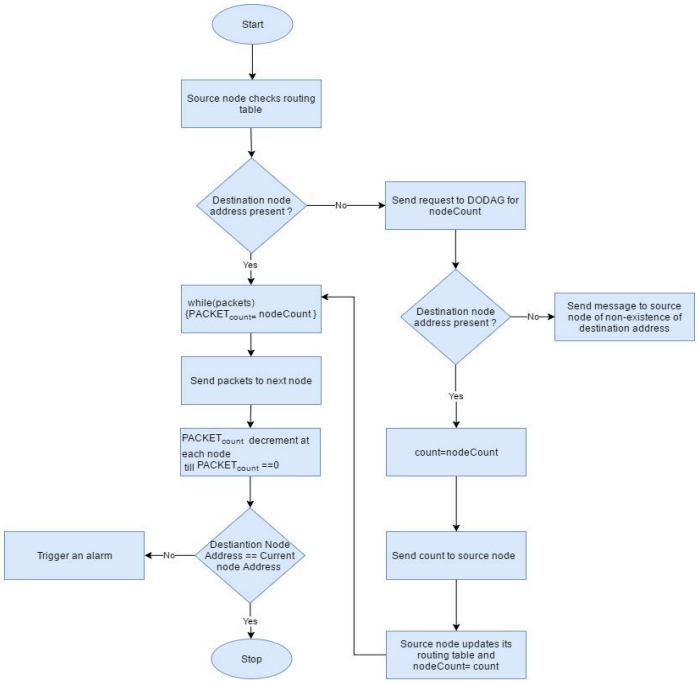

Fig. 6. Flow diagram

VeRa is an existing security mechanism that is used to stop increased rank attack. But node count method is much more beneficial than VeRa because of the following reasons shown in table 1

TABLE 1: Comparison between VeRA and Node Count

Security Mechanism	VeRA	Node Count
Version Number	Check version number from is modified by root or not	Neither It use this mechanism nor it check version number from the root
Rank Authentication	When a node increases, it ranks t does rank authentication	It does not do rank authentication when a node increases it rank
Node Count	It does not use number of nodes requires to reach the destination address	It uses the number of node required to reach at the destination address
MAC Address	It does not use MAC Address for validation	It uses MAC Address for validation
Hash Operation	It uses hash operation for authentication	It uses node count for the authentication

V. CONCLUSION

In this research paper, various types of attacks are described which happens at the network layer that is at the 6LoWPAN and RPL. These two protocol helps to send the packets from source to destination through different nodes. But the chances of attack on network layer is more than compared to other layers. This paper also tells about a new security mechanism which uses the concept of node count to prevent from the increased rank attack. Increased rank attack leads to loop formation between the nodes which exhaust their resources like energy, memory, processing, and make the traffic congested in the network. It also decreases the lifespan of the IoT device and affects the other nodes also in the topology. More research can be done in this new security mechanism to make the IoT devices much secured and energy beneficent.

VI. ACKNOWLEDGEMENT

Authors of this research paper express their deep sense of gratitude to The Founder President of Amity Group, Dr. Ashok K. Chauhan, and Dr. Sunil Kumar Khatri for his keen interest in promoting research in Amity University and have always been an inspiration for achieving great heights.

REFERENCES

[1] Reem Abdul Rahman, and Babar Shah, "Security analysis of IoT protocols: A focus in CoAP", Big Data and Smart City (ICBDSC) 3rd MEC International Conference 15-16 March, 2016.

[2] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures", 10th International Conference for Internet Technology and Secured Transactions (ICITST) 14-16 Dec, 2015.

[3] Seema Nath, Subhranil Som (2017), "Security and Privacy Challenges: Internet of Things", Indian Journal of Science and Technology, Scopus Indexed, included in 'Web of Science' and included in the list of journal recommended by UGC, Vol 10(3), DOI: 10.17485/ijst/2017/v10i3/110642, ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645, January 2017.

[4] Jorge Granjal, Edmundo Monteiro, and Jorge Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communications Survey & Tutorials, Vol. 17, no. 3, pp. 1294-1312, Jan 09, 2015.

[5] Anthea Mayzaud, Remi Badonnel, and Isabelle 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] S. Som, S. Sinha, R. Kataria (2016) "Study On SQL Injection Attacks: Mode, Detection And Prevention", International Journal of Engineering Applied Sciences and Technology, Indexed in Google Scholar, ICI etc., Impact Factor: 1.494, Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 23-29, June - July 2016.

[7] Phul S., Som S., (2016) "Symmetric Cryptography using Multiple Access Circular Queues (MACQ)", 2nd International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2016), Conference Proceedings by ACM – ICPS Proceedings Volume ISBN No 978-1-4503-3962-9, 4 – 5 March, 2016.

[8] Pavan Pongle, and Gurunath Chavan, "A Survey: Attacks on RPL and 6LoWPAN in IoT", International Conference on Pervasive Computing (ICPC), Jan 8-10, 2015.

[9] Anass Rghioui, Anass Khannous, and Mohammed Bouhorma, "Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition", Journal of Advance Computer Science and Technology, vol. 3, pp. 143-153, 2014.

[10] T. Winter, P.Thubert, A Brandt, J.Hui, R. Kelsey, P. Levis, K.Pister, R. Struik, JP. Vasseur, and R. Alexander, "RPL: IPv6 Protocol for Low-Power and Lossy Networks", IETF-6550, 2012.

[11] Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Griece, Gennaro Boggia, and Mischa Dohler, "Standarized Protocol Stack for the Internet of (Important) Things", IEEE Communications Survey & Tutorials, vol. 15, no. 3, pp. 1389-1406, December 12, 2012.

[12] Weigao Xie, Mukul Goyal, Hossein Hosseini, Jerald Martocci, Yusuf Bashir, Emmanuel Baccelli, and Arjan Durresi, "Routing Loops in DAG-based Low Power and Lossy Networks", 24thIEEE International Conference on Advanced Information Networking and Applications, April 20-23, 2010.

[13] Krishnakanth Gupta and Sapna Shukla, "Internt of Things: Security for next Generation Networks", International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Feb 3-5, 2016.

[14] Tariqahmad Sherasiya, Hardik Upadhyay and Hiren B Patel," A Survey: Intrusion Detection System for Internet of Things", International journal of Computer Science and Engineering, vol.5, no. 2, pp. 91-98, Feb-Mar 2016.

[15] Christine Hennebert and Jessye Dos Santos, "Security and Privacy Issues into 6LoWPAN Stack: A Synthesis", IEEE Internet of Things Journal, vol. 1, no. 5, pp. 384-398, September, 2014

[16] Anhtuan Le, Jonathan Loo, Kok Keong Chai, and Mahdi Aiash, "A Specification-Based IDS for Detecting Attacks on RPL-bAsed Network Topology", MDPI, 12 May, 2016.

[17] Fatma Al Shuhaimi; Manju Jose; Ajay Vikram Singh, "Software defined network as solution to overcome security challenges in IoT", 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) at AUUP, NOIDA, India, September 07-09, Year: 2016 Pages: 491 – 496.

[18] Ajay Vikram Singh, Jas Singh Basin, "Variable Speed Limit (VSL) based Model for Advanced Traffic Management through VANETs", 30th IEEE International Conference on Advanced Information Networking and Applications (AINA), Crans Montana, Switzerland, 23-25 March, 2016, Pages 533 – 538.