International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072

Intrusion Detection for Wormhole Attack

Monica A R[1], Sanchana S[2], Usha Kiran[3], Vaishnavi T S[4], Jagruthi H[5]

[1,2,3,4]UG Student, Dept. of Information Science and Engineering, BNM Institute of Technology, Karnataka, India.

[5]Assisstant Professor Jagruthi H, Dept. of Information Science and Engineering, BNM Institute of Technlogy, Karnataka, India

---

Abstract - *Number of devices that are going to be connected to the internet will be increasing in the near future because of increase in the number of applications in Internet of Things (IoT). Security in IoT devices is one of the major area of concern for us. Providing security to IoT devices is challenging and tough because most of the devices involved in IoT have the characteristics of being resource constrained in terms of battery and processing power and will not be able to bear the extreme stress. In IoT, nodes (also devices) communicate using the internet which makes it insecure and vulnerable to create various attacks and as there exists communication between lot of devices is a challenging task The Routing Protocol for Low-Power and Lossy Networks (RPL) which is a distance vector routing protocol. Providing security for the IPv6/RPL connected and the 6LoWPANs network is challenging and insecure as the devices are connected to the untrusted Internet, which makes the communication links lossy and prone for attacks. The devices use a set of IoT protocols such as RPL, 6LoWPAN. The proposed work in this paper is an implementation of an intrusion detection system (IDS) for Wormhole attack. Wormhole attack is one of the most severe attacks taking place at 6LoWPAN adaption layer of RPL network mostly in the weak IoT devices . In this type of attack, a pair of attacker nodes forms a tunnel between two nodes and behave like they are directly connected to each other to misguide network traffic and the communication of the devices. The proposed IDS is implemented in Contiki OS, using Cooja Simulator.*

Key Words: IoT, RPL, 6LoWPAN, Intrusion Detection, Wormhole Attack, Contiki OS, Cooja Simulator

1. INTRODUCTION

The scope and trend of the internet in IoT is going to be expanded beyond computing and computers, which are being connected. Internet of Things can connect devices which are embedded in various systems to the internet for communication and task performance. When the devices/objects can represent themselves digitally, they can be controlled from anywhere as it is a growing network of smart objects. It refers that the physical objects are capable of exchanging information with other ones in the network. The connected smart devices or objects use the data that they have collected without any help from a human beings and then they transfer it to each other using the internet. It is going to interconnect different things such as physical objects that we see around us, like different objects such as the lighting system in a room, the lights and the bulbs, the fans, the air conditioners and anything and everything including things and objects such as the toothbrush(Wi-FI enabled ones), the microwave oven, the refrigerator and not only in our homes, but also in our business space such as internet enabled working of different machines, internet enabled working of different type of equipments etc. So, each and everything that we see around us that we use at our home in business places, in workplaces, everything being internet driven. So, this is the whole vision of internet driven working of things, or also called internet of things. It enables various smart devices to connect to existing network in a very short duration of time. This purpose is achieved because of IPv6 support provided by IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), a standard which allows the devices which are heavily resource constrained to get connected to the IPv6 network in IoT. 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 help them to communicate within the network and also with the external network by connecting to the internet. The IoT requires security solution where the communication is able to happen securely with integrity, confidentiality and authentication services. The network is being protected against intrusions and disruptions. Also, the data inside a sensor node is stored in an encrypted form. Therefore, the challenge of ensuring secure communication in the IoT network needs to be addressed.Insecure internet and wireless sensor network are the two major components of IoT which make IoT network vulnerable and insecure to various security attacks.

The attack detection is done by using an Intrusion Detection System (IDS). While designing the IDS for IoT system, few points are to be taken into consideration like IDS is designed for resource-constrained devices in the network.

Hence, it must be lightweight system in terms of memory and processing power to be easy on the devices. Also, devices in IoT are extremely heterogeneous in nature which makes designing IDS for these kinds of devices are very challenging and tough.

IoT uses RPL protocol in its network layer which is vulnerable to the routing attacks against the IoT as well as to the attacks against the Wireless Sensor Network (WSN). Routing Protocol for Low power and Lossy Networks (RPL) is a distance vector routing protocol, where the routing is

based on Destination oriented Acyclic graphs or DODAGs which are the Heart and soul of this Routing Protocol. This is a special kind of DAG in which each node wants to reach a single destination. RPL operates with the nodes that have constraints on processing power, memory, and energy (battery power). It is basically designed for high loss rates, low data rates and instability network such as Wireless Sensor Networks (WSN) and also optimized for collection networks with infrequent and inconsistent communication from the collection point to individual nodes.

2. Related work

A. Wormhole Attack

Wormhole attack is an attack in which two attackers nodes locate themselves strategically in the network. Then, the attackers keep on listening to the network, and record the wireless information and steal them which can be made using the tunnel formation between the two nodes.

Wormhole attack can be in various forms such as

1) Using the Encapsulation.
2) Using the High quality channel / out of Band.
3) Using the high Power transmission capability
4) Using the Packet relay
5) Using the Protocol distortion.

Vikram Neerugatti et al. [1] has proposed the elaboration of different control messages and uses in wormhole attacks. The attacker nodes receives the packets at some point in the network of nodes and tunnels them to some other part or nodes of the network and replays (re-transfers the packets) them into the network from that point or stage onwards. With the case of reactive protocols like the DSR and the AODV, the attacks can or could be launched by tunnelling every other requests to the target destination node with direct approaches. When the destination neighbour node finds this request, then they will provide a normal protocol operation to re-broadcast the requested packet and then remove or discard any other requests if in the same route. Thus, this prevents discovery of any other routes. This places the attacker in such a position from where any attack can be launched on the network as it practically controls all the routes discovered. The two continous sensor nodes tunnels the control and data packets between each other, with the intention of creating a shortcut route in the WSN so that it can capture the data. Such a low-latency tunnel between the two conniving nodes will be more in help to increase the probability of it being selected as an active path in the network. This type of attack is closely related to the sinkhole attack, because one of the conniving nodes could fake advertise to be the sink node and to the other nodes and thereby attract more traffic and capture the data than usual. [2].

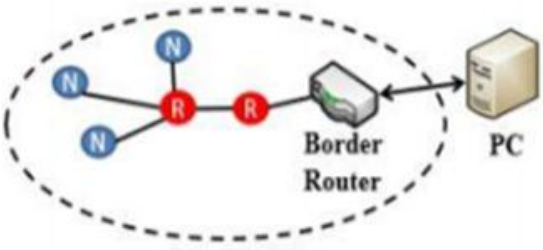

Fig.1 Architecture of the system

Swetha Palacharla, M.Chandan, K.GnanaSuryaTeja, G.Varshitha has proposed a novel model where by assuming the nodes as the sensors in a wireless sensor network (WSN) that are administered through a base station. It's started with briefing about IoT and then briefing on the IoT layer models. After this, they discuss the attacks namely Sinkhole attack, Sybil attack, Hello flood attack, Acknowledgement spoofing attack and their respective detection methods and their vulnerabilities. This paper is a systematic review of the existing mechanism for the detection of wormhole attack and a new method is proposed. Major security concerns are discussed and focus is laid on Wormhole attack. The efficient algorithm is proposed to detect the wormhole attack which not only discloses the wormhole attack but also lists the nodes under this attack dynamically. The security issues that are presently bothering are discussed and there may be vulnerabilities which can occur with the increasing technology which may be due hardware or software [3].

B. IoT and IDS

1) The Internet of Things (IoT)

The IOT or speaking of the IP-connected IoT is a heterogeneous network that consists of the conventional Internet and networks of constrained devices (also known a nodes) connected together using IP protocol. The network of constrained devices in the IoT, called 6LoWPAN networks or an IP-connected WSN, are connected to the conventional Internet using 6LoWPAN Border Routers (6BR). Figure 1 shows the connection of things in a 6LoWPAN network with the Internet using the 6BR. Things in the IoT are uniquely identifiable objects that sense the physical environment and the host devices and then communicate this data to the Internet. An IoT device (a thing) can be a light bulb, a thermostat, an home appliance, an inventory item, a smartphone, a personal computer, or potentially anything. IPv6 with its potentially unlimited address space can connect billion or even trillion of these devices with the IoT.[4]

2) Intrusion Detection Systems.

An Intrusion Detection System (IDS) analyzes activities and processes in a network or in a device in the network and then detects attacks, reports them, and mitigates the harmful effect of the detected attacks and segregates the malicious nodes. Due to the unpredictable behaviour of novel attacks,

IDSs are subjected to false positives which is to raise an alarm when there is no attack and the false negatives which is to not raising an alarm when there is an attack. Generally, there are two categories of IDSs that is signature based and anomaly based. Signature based detection compares the current activities in a network or in a device against predefined and stored attack patterns called signatures. This approach cannot detect new attacks, needs specific knowledge of each attack which is data trained, that has a significant storage cost incorporated that grows with the number of attacks, and has a high false negative rate but low false positive rate. Anomaly based detections determine the ordinary behavior of a network or a device, use it as a baseline or a symptom, and then detect anomalies when there are deviations from the baseline or the natural behaviour of the network. The table 1 shows a difference between different IDS. This approach can detect new attacks but has comparatively high false positive and false negative rates because it may raise false alarms and cannot detect attack when attacks only show small deviations or symptoms from the baseline. [4]

C. Mode of attacks

Packet Relay: In this mode of attack, replay of the packet between the 2 distant nodes and thus succeeds in convincing that they are the neighbour nodes and also helps in tunnelling. Essentially when there is a direct link between two nodes, through a wireline or a long-range wireless transmission, or an optical link that will perform eavesdrop at the origin point and then tunnels them through the link, replaying them in a timely matter at the destination point.

Out of Band channel: In this type of attack the malicious nodes creates a direct connection between them and then passes packets from one side of the network to another side of the network and thus leakage of the packets occur that is out of the channel.

High Power Transmission mode: In this, a single malicious node gets a RREQ, and broadcasts the request at a high power level which cannot be done by other nodes in the network and thus will be successful in leaking of the packet.

Packet Encapsulation: In this mode of attack several malicious nodes exist between the source and destination and thus packets gets encapsulated with the malicious nodes and then receives a RPEQ.

Protocol deviation: In RREQ forwarding, the nodes will back off or withhold for a random amount of time before forwarding reduces the MAC layer collisions.

D. Contiki OS

Contiki is an operating system for networked, memory-constrained systems with a focus on lowpower wireless for devices in Internet of Things. Contiki provides network mechanisms: the uIP TCP/IPstack,which provides IPv4 networking, the uIPv6 stack, which provides IPv6 networking, and the Rime stack, which is a set of custom lightweight networking protocols designed for low-power wireless networks. The IPv6 stack was contributed by Cisco and was, when released, the smallest IPv6 stack to receive the IPv6 Ready certification. The IPv6 stack also contains the Routing Protocol for Low power and Lossy Networks (RPL) routing protocol for low-power lossy IPv6 networks and the 6LoWPAN header compression and adaptation layer for IEEE 802.15.4 links. Contiki provides a set of mechanisms to reduce the power consumption of systems on which it runs. The default mechanism for attaining low-power operation of the radio is called ContikiMAC. With ContikiMAC, nodes can be running in low-power mode and still be able to receive and relay radio messages.[8]

E. Cooja Simulator

COOJA is a network simulator which permits the emulation of real hardware platforms. COOJA is the application of Contiki OS concentrating on network behavior. COOJA is capable of simulating wireless sensor network without any particular mote. Cooja supports the following set of standards; TR 1100, TI CC2420, Contiki-RPL, IEEE 802.15.4, uIPv6 stack and uIPv4 stack.[9]

3. PROPOSED SYSTEM

In the proposed system there is 2 main parts . One is the part where the DODAG is formed through the usage of an algorithm and the second is the usage of the an algorithm to launch the attack and then the detection is done and the network is secured.

A. System architecture

In this type of architecture, the building of the system happens in a 2 stage modular approach where the entire system is broken into 2modules which are further broken into smaller modules and each module has a set of functions to be performed.

The stage 1 is the building of the network and then allocating the client and server motes and also marking a border router and then start the normal flow of packets. Since the project is implemented using the Cooja simulator on Contiki OS. So the type of mote is selected (in this case it's the Sky mote and then placed within the proper radio bandwidth and range is specified and then the motes are placed accordingly.

The next step is the set up of protocol in the network that is the RPL and 6LoWPAN such that there are easy and secured flow of the packets in the network. RPL is the most used with respect to IoT network for security. 6LoWPAN is used for proper transferring of the IPV6 packets. Later part of this module is to start the client and the server process and also execution of the Trickle algorithm for DODAG formation and ranking of nodes.

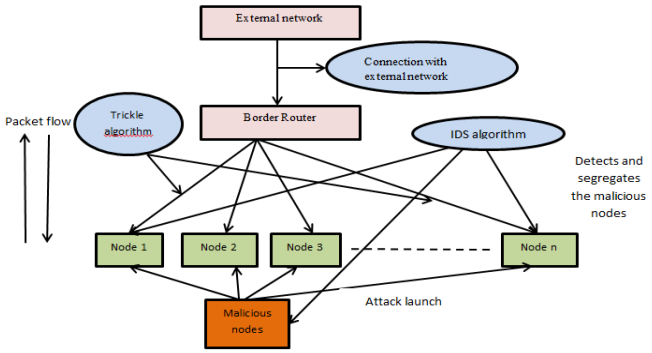

Fig 2 System architecture

Trickle algorithm

Trickle algorithm is the one that helps in inconsistency of the nodes communication between neighbours by performing the ranking and DODAG formation in the network. Trickle works on interval based timer that clicks and uses a DODAG formation.
Trickle works on interval based timer that clicks and uses a constant value do determine the ranking and the DODAG formation. The constant is kept constant depending on the type of the network, topology and the bandwidth.

Algorithm

1. When the algorithm starts execution, it sets I to a value in the range of [Imin, Imax], greater than or equal to Imin value and less than or equal to Imax value.

2. When an interval begins, Trickle resets c (counter) to 0 and sets t to a random point in the interval, taken from the range [I/2, I), that is, values greater than or equal to I/2 and less than I.

3. Whenever Trickle hears a transmission that is "consistent", it increments the counter c.At time t, Trickle transmits if and only if the counter c is less than the redundancy constant k.

4. When the interval I expires, Trickle doubles the interval length. If the new interval length would be longer than the time specified by Imax, Trickle sets the interval length I to be the time specified by Imax.

5. If Trickle hears a transmission that is "inconsistent" and I is greater than Imin, it resets the Trickle timer. To reset the timer, Trickle sets I to Imin and starts a new interval as in step 2. If I is equal to Imin when Trickle hears an "inconsistent" transmission, Trickle does nothing. Trickle can also reset its timer in response to external "events".

This results the consistent DAG formation and ranking of nodes. The second module starts with the concept of the attack launching and the detection of the attack.

The attack formation starts with and uses the RSSI value of the packet flow to segregate the nodes into 2 lists that is the trusted neighbour list and then the untrusted neighbour list.

The attack starts such that it will intrude the network using the RSSI of one of the nodes in the network and then broadcasts its messages and replays the broadcast message such that it will create an illusion to all the nodes in that it's a trusted node and closer to the router for faster transmission of the packets. Thus attack starts by sneaking the packets and changes its RSSI value so that it indicates as symptom for the system that something is wrong and there is an attack.

After that the IDS algorithm starts and then segregates the malicious nodes are the untrusted node and then changes the RSSI value so that secure information transmission and then recovers the network. Thus for further transmission of the packets the network can refer to the 2 lists that is trusted neighbour list and untrusted neighbour list as obtained. This stage 2 repeats on a loop until the network is secure.

Algorithm

Step 1: The DODAG graph obtained from Trickle algorithm provides a list of neighbours to each node in the network.
Step 2: The malicious nodes gets and placed in the network depending on the seeking the neighbour lists from the nodes.
Step 3: The attacker nodes in the networks changes the RSSI value of each session of packet exchange.
Step 4: Then comes the non-malicious node with the attack detection algorithm that will see the change is RSSI value as the symptom of the attack.
Repeat till N number of motes
Step 5: Inspecting each node of the loop such that the affected node gets separated to the trusted neighbour list and untrusted neighbour list.
Step 6: Thus the border router only sends the packets and receives the packets from the nodes in the trusted neighbour list.
Step 7: Thus the network gets secured.

Thus the system function in such a way such that it will launch the attack on loops and inspects the network and each mote such that it will recover the network at a constant rate and the time varies with respect to the number of nodes and the number of malicious nodes.

RESULTS AND DISCUSSIONS

The following section consists of the total evaluation of the proposed system in terms of efficiency of attack, power consumption, analysis of the network, memory consumption.

A. Experimental Setup

The operating system which is used on IOT objects is Contiki OS which is used for networked, memory-constrained systems with a focus on low-power wireless

Internet of Things devices.It has an built-in simulator called cooja which simulates of Contiki nodes.The nodes belong to one of the three following classes emulated Cooja nodes, Contiki code compiled and executed on the simulation host, or Java nodes, where the behavior of the node must be re implemented as a Java class. One Cooja simulation may contain a mix of sensor nodes from any of the three classes.

B. Topologies of nodes

In this experimentation let us consider the 7 , 14 node topology to analyse the attack and the network and node topology to analyse the attack and the network. As shown in fig 3,

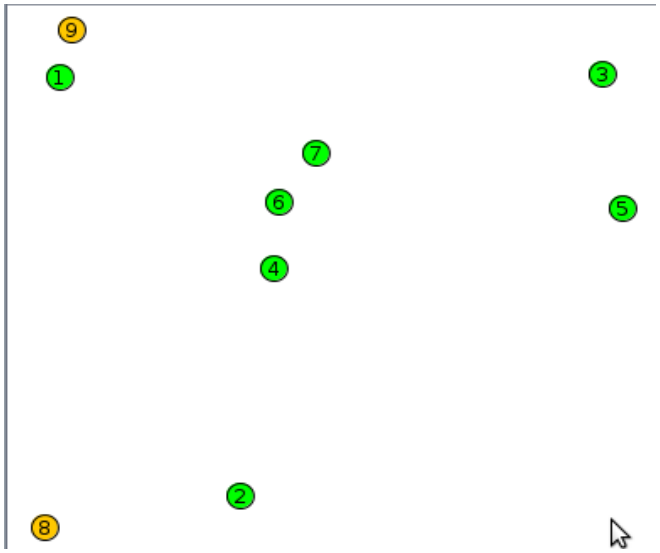

Fig 3: 7 node topology with 2 attacker nodes

This shows a network with 7 nodes named appropriately and the nodes 8 and 9 are attacker nodes respectively. The next network image shows the further processes.

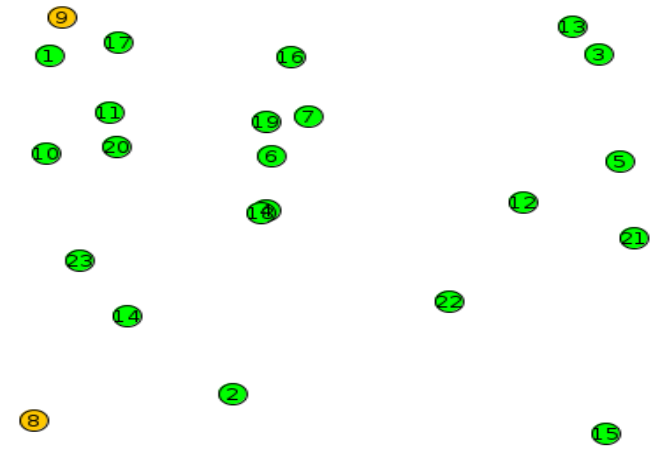

Fig 4: 24 node topology with 2 attacker nodes

This shows a network with 24 nodes named appropriately with 2 attacker nodes 8 and 9.

C. Attack Detection

The attack is initiated in the beginning stage after running the code in simulation. After the attack is started it checks on all the neighbour nodes if they are the victim nodes and gets detected immediately mentioning if the neighbour node is victim node. Fig 5 shows the output of the simulation when attack is initiated.

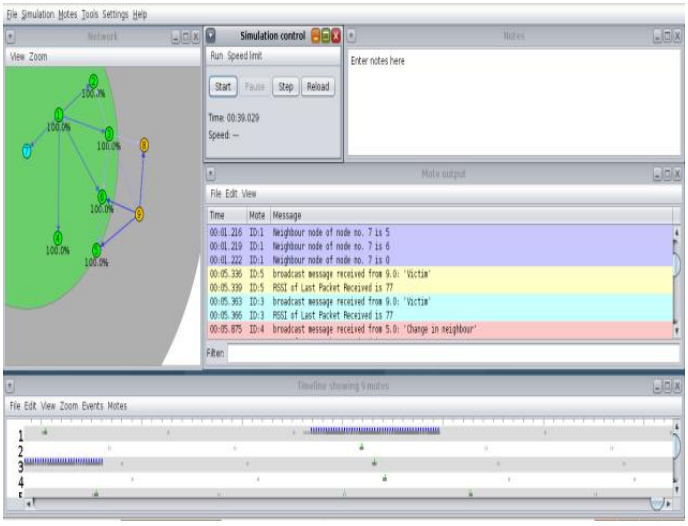

Fig 5: Identifying the victim nodes after attack is initiated.

D. Node Information

This includes all the information of the node such as sent , received, hops, power consumption, average inter packet time , duty cycle, payload. This gives the complete node information which is required for detection of the attacker nodes as shown in the Fig 6,

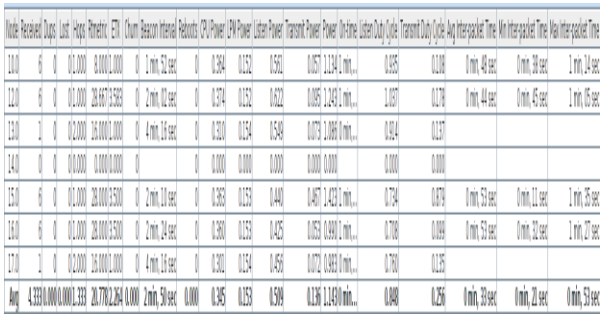

Fig 6: Node Information

The CPU power consumption of the whole attack is reduced by 60% compared to other detection algorithms which increases the efficiency and many nodes can be connected to the network. This also gives other useful information such as hop counts which calculates the distance of the neighbour nodes, average inter packet time is the average time between transmission of the packets between nodes.

E. DODAG Network graph

The DODAG network graph is formed as the nodes get added into the network for transmission of the packets and the detection algorithm is implemented at the very beginning phase which analyses the network and rank them appropriately. Fig 7 shows the network graph.

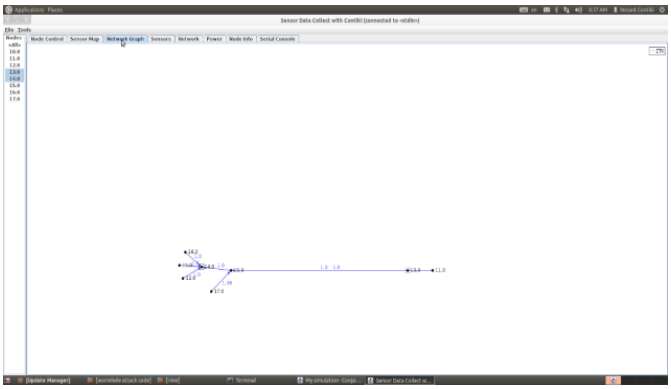

Fig 7: Formation of the DODAG network

The formation of the DODAG network is slower compared to others because the attack and the detection algorithm is implemented at the very beginning phase which analyses the network and checks for the attacker and the victim nodes in the network this is found out in the collect view of the simulator.

F. Instantaneous Power Consumption

After running the simulation for 10 minutes the attack here is launched at 6th second and is detected at the 36th sec. The total instantaneous power consumption graph of project is given in below graph. This is 4 times faster than other algorithms for detection hence consumes more of the cpu where other processes might slow down while running our simulation

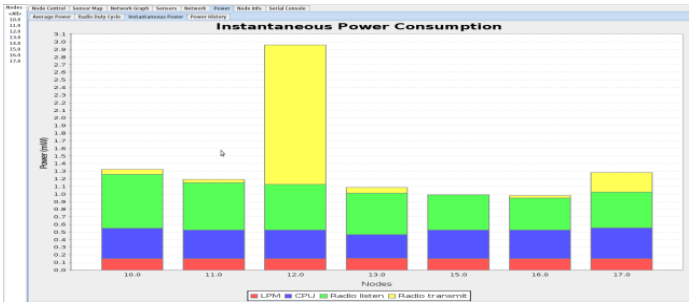

Fig 8: Instantaneous power consumption graph

It can be observed that at the node 12 the traffic was very high and it has made the higher number of transmission of packets.

4. CONCLUSION

We know that with the time many devices around the world are getting connected and this number is exponentially increasing every year so it becomes necessary to secure these devices which are more vulnerable since they work on low power and lossy networks. The method proposed provides 97% of success in the attack detection rate which is higher than any intrusion detection algorithm since the approach is to start detection algorithm at the early stage instead of detecting after the whole network is formed. The advantages of the proposed system is that since it analyses each node and the network it can detect sink - hole attack also with the wormhole attack. The nodes can be increased to any number which was the drawback of many techniques where the number of nodes connected to the network was restricted. It can be observed that at the node 12 the traffic was very high and it has made the higher number of transmission of packets.

REFERENCES

[1] Vikram Neerugatti and A Rama Mohan Reddy, “Acknowledgement based technique for detection of the wormhole attack in RPL based internet of things networks”, Asian journal of computer science and technology.

[2] V Chandra Sekhar Reddy, Dr K Ramesh Reddy, ”Implementation of wormhole attack on RPL protocol in Internet of Things”, V Chandra Sekhar Reddy et al, International Journal of Computer Science and Mobile Applications, Vol.6 Issue.

[3] Swetha Palacharla, M Chandan, K Gnana Surya Teja, G Varshitha, “Wormhole Attack: a Major Security Concern in Internet of Things (Iot)”, International Journal of Engineering & Technology

[4] Linus Wallgreen,Shahid Raza, and Thiemo Voigt,”Routing Attacks and Countermeasures in the RPL-Based Internet of Things”,Hindawi Publishing corporation,International Journal of Distributed Sensor Networks.

[5] Yih-Chun Hu, A. Perrig and D. B. Johnson, "Wormhole attacks in wireless networks," in IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370-380, Feb. 2006, doi: 10.1109/JSAC.2005.861394.

[6] Suchitra C,Vandana C P,” Internet of Things and Security Issues”, Suchitra.C et al, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.1.

[7] Adam Dunkels, Bj¨orn Gr¨onvall, Thiemo Voigt, “Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors”.

[8] Tayyab Mehmood, “COOJA Network Simulator: Exploring the Infinite Possible Ways to Compute the Performance Metrics of IOT Based Smart Devices to Understand the Working of IOT Based Compression & Routing Protocols”.