Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.8 No.S3, 2019, pp. 100-104

Acknowledgement Based Technique for Detection of the Wormhole Attack in RPL Based Internet of Things Networks

Vikram Neerugatti[1] and A. Rama Mohan Reddy[2]
[1]Research scholar, [2]Professor
[1&2]Department of Computer Science and Engineering, Sri Venkateswara University, Andhra Pradesh, India
E-Mail: vikramneerugatti@gmail.com, ramamohansvu@yahoo.com

Abstract **- Internet of Things (IoT) is the advanced technology, were the constrained nodes/things (all the objects around us such as chair, home, car, keys, etc.) will be connected to the internet to form a network, for sharing and monitoring the data, remotely. RPL (IPv6 Routing Protocol for Low Power and Lossy networks) is a routing protocol particularly designed for the constrained (low powered, low computation, less size, etc.) networks with the protocol 6LoWPAN (IPv6 Low Powered wireless Personal Area Networks). Due to the constrained behaviour of the RPL protocol, it will leads to many RPL routing attacks such as Sinkhole, Black hole, Wormhole, Selective forwarding, rank attacks, etc. This paper was focused on the Wormhole attack. The Wormhole attack will select the packets from one location and drops those packets in some other location (malicious) by forming the Tunnelling. To detect this attack here proposed andimplemented a novel approach called (ADWA). Acknowledgement based technique for detection of the wormhole attack in RPL based Internet of Things networks. This approach was shown efficient results with the Telosb sky emulator nodes in the Contiki Cooja simulator, in terms of the Packet delivery ratio, delay and detection of wormhole attack.**
Keywords: **IoT, RPL, 6LoWPAN, Attacks, Detection Technique, Security**

I. INTRODUCTION

IoT can be defined as in Fig.1. IoT is an emerging research area, where the market value is very and it is the recent trend in the computing. Here everything around us can be connected to the internet with the unique IP address. By connecting the things to the internet every persons at every time from every place can monitor and share the data. This technology leads to the communications like thing to thing communication, thing to person communication and person to person communication globally.

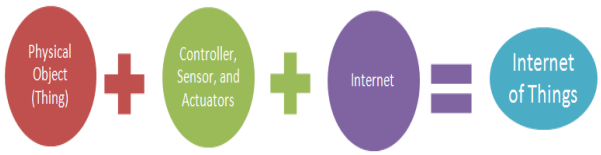

Fig. 1 IoT

The enabling technologies for this techno are wireless networks, Cloud computing, cheap data rates, mobile devices (such as Smart phone), sensors, actuators, embedded devices (microcontrollers, microprocessors, etc.), etc. it has vast applications in almost every fields like smart healthcare, smart agriculture, smart home, smart chair, smart utilities, etc. The Cisco IT Company predicted that, the connected devices will be increased more than the human beings in the world. The prediction was shown in Fig.2. This prediction concludes that there is a huge demand in developing the technology IoT.

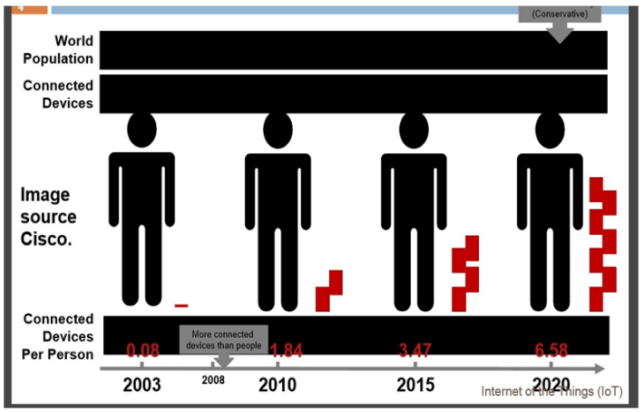

Fig. 2 Connected devices will be increased more than the human population in the word (Source: Cisco white paper)

During the stages of developing IoT technology new protocols was developed such as RPL, 6LoWPAN, CoAP, MQTT, etc.

A. RPL

This RPL was formed by the IETF working group [1]. RPL is a Routing protocol for low power and lossy networks, particularly designed for the internet of things networks with the protocol 6LoWPAN.6LoWPAN is the header compression protocol of the IPv6 protocol, where it enables to connect the things to Internet by providing the unique IP to everything. In 6LoWPAN protocol the routing will be done with the help of the RPL protocol. The RPL is a distance vector routing protocol. The routing will be established by routing discovery in two processes. In first process the gateway node will send the broadcast message to all the other nodes and in second process all other nodes will send the unicast message to the gateway node. As shown in the Fig.3 the RPL will work in the Things part of Connectivity in Internet of Things. The RPL control messages [2] are tabulated in Table I.

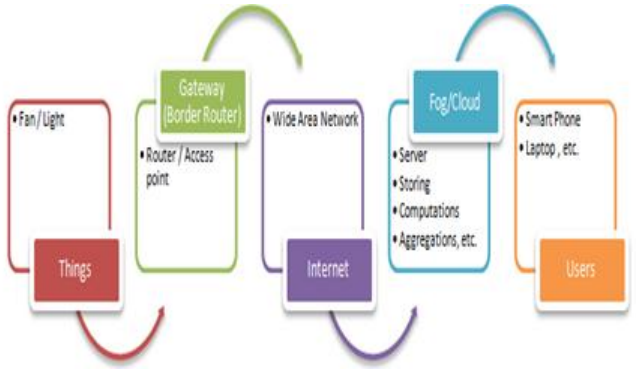

Fig. 3 Connectivity in Internet of Things

Generally the RPL topology is the DODAG (Destination oriented directed acyclic graph), where no loops will be formed and all the nodes will be directed towards the gateway node. Gateway node is responsible for creation of the DODAG for sending the packets. DODAG was created with the help of the RPL control messages. The Control messages DIO will broadcasted by the gateway node to all the neighbour nodes, to join the DODAG.

TABLE I RPL CONTROL MESSAGES

DIO	DODAG Information Object
DAO	Destination Advertisement Object
DAO-ACK	Destination Advertisement Object-Acknowledgement
DIS	DODAG Information Solicitation

The neighbour nodes after receiving the DIO message, it will send the DAO control message to the gateway node, based upon the DAO, the gateway node will multicast the DAO-ACK, which is to join the DODAG or not to join the DODAG. If new node wants to join the existing DODAG, then the new node will send the DIS control message to the gateway node. Then based upon the acknowledgement from the gateway node it can join or cannot join the DODAG.

The RPL will work in the two modes of the operation, to maintain the downward routes in the DODAG called as Storing mode and Non-storing mode. In the DODAG the gateway will be always storing mode, other nodes may be a storing or non-storing, but should be either one mode. In storing mode the control messages will be stored, various in the non-storing mode the control messages will not store [2]. As the RPL is a constrained protocol, it leads to many attacks, as discussed in the next sub-section.

B. RPL Attacks

Due to the weak links of the RPL protocol leads to the many routing attacks like in the Table 2. As shown in the Table II IoT had different layers [3], and in each layer has the variety of the attacks. Current paper was focused on the Network layer protocol RPL (IPv6 routing protocol for low power and lossy networks) attacks. The RPL has different attacks like Blackhole, Hello flood, sinkhole, wormhole, killerbee, selective forwarding, rank attack, etc [3-6].

TABLE II SECURITY THREATS FROM EACH PROTOCOL LAYER

Layer	Protocols	Threats & Attack Framework
Application	CoAP, XMPP, MQTT	XMPPloit(Framework)
Transport	TCP, UDP	UDP Flooding, TCP SYN Flooding, De-synchronization
Network	MPL, RPL, 6LoWPAN	KillerBee(Framework), Black-hole Attack, Change Rounting Information, Packet Capture & Injection, Selective-Forwarding, Sinkhole, Hello Flood, Wormhole, Sybil, Tiny Fragmentation
Data Link	802.15.4, 802.11, 802.15.1	KillerBee(Framework), GTS Attack, Back-off manipulation, ACK attack
Physical	802.15.4, 802.11, 802.15.1	Jamming, Tampering

Source: Changmin Lee, *et al.*,

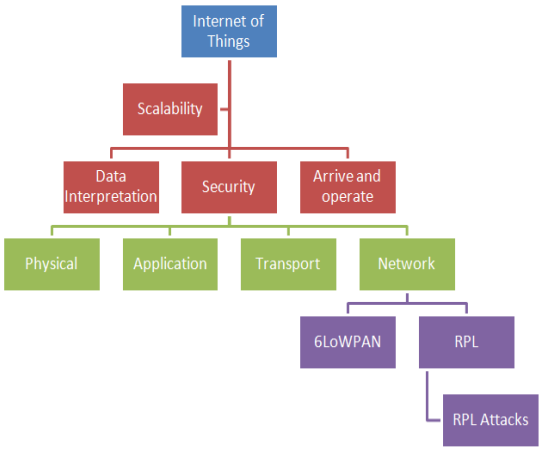

Fig .4 Taxonomy of the RPL attacks

In Black hole attack [7], the malicious nodes will drop the packets. Here one malicious node may collude with the other node and can become more powerful. In the selective forwarding attack the malicious node will selectively forward the packets and remaining packets will be dropped. Where as in the, Sybil attack or clone attacks duplicate nodes will be created to disrupt the traffic. In the sinkhole attack the malicious node will attract the neighbour nodes by advertising towards it. In the rank attack the malicious node will communicate the wrong rank to establish the DODAG, etc. This paper focused on the wormhole attack, about it was discussed in next sub-section.

C. *Wormhole Attack*

In Wormhole attack the malicious node will send packets to the other malicious node by creating the tunnelling [3-7]. It

will transfer the packet from one location to the different location [8].It will disrupt the network very largely. The tunnel has more power to transmit the packets compared to the normal routing. It can combine with the other attacks like the sinkhole attack and cause serious damage to the network. Wormhole attack can be a various forms such as [8]

1. Wormhole by using the Encapsulation.
2. Wormhole by using the High quality channel / out of band
3. Wormhole using the high Power transmission capability
4. Worm hole using the Packet relay
5. Wormhole using the Protocol deviation or distortion.

In the wormhole encapsulation attack the data packets will be encapsulated and the hop counts will not increase, but the attack will have the impact. With the help of the high data rate / good quality channel the packets can be transferred very fast and thus the worm hole will be occurred from long distances. Due to the authentication problems, two are more malicious nodes will made authenticate possible and this called as the packet relay wormhole attack. The malicious node tries to attack the network traffic during the communication called as the protocol deviation wormhole attack.

The next sections were organized as follows. In the section II related work was discussed, in the Section III the proposed work was discussed, the implementation part was discussed in the section IV, in Section V results was discussed, finally in section VI the conclusion and future work was discussed.

II. RELATED WORKS

The [9] authors proposed a mechanism i.e. cryptographic system depend on neighbourhood communication to avoid wormholes. But the solution does not need time synchronization or time measurement, that requires only a small fraction of the nodes to know their location, and is decentralized.

The [10] authors proposed a lightweight countermeasure for the wormhole attack known as LITEWORP, it does not require any specialized hardware. LITEWORP is particularly suitable for resource constrained multi-hop wireless networks such as a sensor network.

In [11] authors discussed a countermeasure for the wormhole attack, known as MOBIWORP, which mitigate the wormhole attack in mobile networks. MOBIWORP uses a secure CA (central authority) for global tracking of node positions. Local monitoring is used to detect and also isolate malicious nodes locally. The effect of MOBIWORP on the data traffic and the fidelity of detection are brought out through extensive simulation using NS-2.

In [12] authors proposed a new mechanism known as packet leashes, for detecting and defending against wormhole attacks, and presents a specific protocol called TIK, that implements leashes.

In [13] authors discussed the protocols that require an authentication mechanism which is also known as True Link. True Link is virtually independent of the routing protocol that used. The performance evaluation shows that true link provides effective protection against potentially devastating wormhole attack.

The [14] authors proposed SAM to detect attacks and to identify malicious nodes, Comparing to the previous approaches; no special requirements are needed in these scheme. Whenever, SAM may act as a module in local detection agents in an intrusion system for wireless ad hoc networks.

In [15] author discussed particular severe security attack that affects the ad hoc networks routing protocol is called the wormhole attack. The wormhole attack is two phase process launched by one or several malicious nodes.

In [16] author presents a secure routing mechanism against wormhole attack in IPv6 based WSN. The design of this routing mechanism can be classified in to two phases' wormhole defence and detection, which is based on the average distance per hop in the network and the TTL of IP header.

In [17] author discussed subtlest security attack in RPL WSANs is the wormhole attack. In which a malicious actor establishes and controls an out of band channel between two distant nodes of the network. Due to its convenience RPL is induced to use such a channel to forward the traffic.

In [18] authors proposed a new scheme that monitors the signal strength of nodes, if distance found greater than default distance then the attack is detected. Both techniques act as backup of each other such that if one method fails other will detect the attack. This scheme doesn't require excessive power or specialized hardware equipment which is quite useful in resource constrained environment

In [19] author proposed Merkle tree based authentication protocol which runs on the notation of constructing a tree of hashed security information. The approach by formulating the wormhole problem as graph theoretic problem and also shows effectiveness of the Merkle tree based approach for authenticating communication.

In [20] author proposed Merkle tree based approach to prevent from disrupting the links, and observe better throughput reduction in jitter, and end to end delay as compared with wormhole attack and no avoidance mechanism. The mechanism with the traversal algorithm assists in managing the authentication in a huge network,

which is broken down into many trees avoiding wormhole attacks in the networking.

III. PROPOSED SYSTEM

To detect the wormhole attack, the Acknowledgement based technique (ADWA) was proposed. It works based on the acknowledgments sent by the nodes in DODAG to the gateway node (root node of the DODAG). The acknowledgement consists of the neighbours nodes of each node in a DODAG of the RPL protocol. Based on the neighbours of each node the malicious node of the wormhole attack can be detected. The algorithm was shown in the Algorithm 1.

Algorithm 1: Proposed detection technique of the Wormhole attack

/* where 'A' is the gateway node, 'B' is the other nodes,'C' is white node (normal node), 'D' is black node (malicious node)*/

1. start
2. Gateway node 'A' broadcast the DIO control message (objective function) to all other nodes.
3. other nodes 'B' receives the DIO
4. Other nodes 'B' send the DAO to the gateway node 'A'
5. Gateway node 'A' then multicast the DAO-ACK to nodes 'B'
   i) If
   Can join the DODAG
   ii) Else
   Cannot join the DODAG
6. The DODAG will be constructed by repeating the Steps 2-5.
7. The node 'A' sends the DIO (to collect the neighbors of each node)
8. Nodes 'B' will send the DAO (neighbor's information)
9. node 'A' sends the DAO-ACK
10. if wrong Neighbors
11. malicious node detected (make as black node 'D')
12. else
13. normal nodes (make as white node 'C')
14. end

IV. IMPLEMENTATION

The proposed system was implemented in the ContikiCooja Simulator with the parameters tabulated in the Table III. Here 30 sky motes was created, one node among 30 will act as a gateway node, 2 nodes among 29 will act as a wormhole nodes and remaining will act as a normal nodes. In the gateway node border router code with the proposed detection technique code was injected, in the two nodes worm hole code (in one nodes collects the packet and in other node to receive the packets) was injected. In remaining nodes the normal code will be injected. The results were shown in the next section.

TABLE III SIMULATOR PARAMETERS

Parameter	Value
Simulator	Cooja Simulator
Radio medium model	Unit disk graph medium (USGM)
Range of nodes	RX and TX : 100m
Mote type	sky motes
Number of nodes	10, 20,30, 40, 50
Number of sinks	1
Number of malicious nodes	10 to 25%
Physical layer	IEE 802.15.4
Network layer	Contiki RPL
Objective function	Hop count and ETX

V. RESULTS

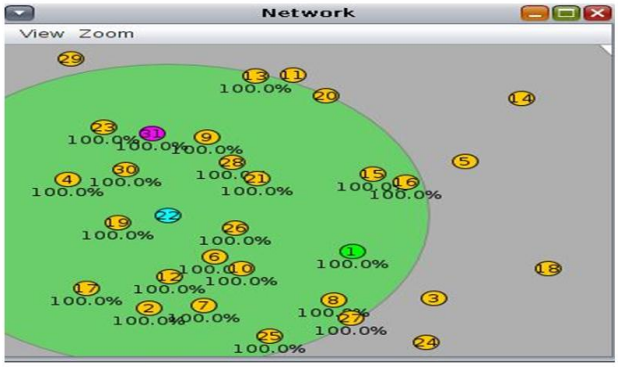

Fig. 5 30 Sky motes in the cooja simulator

Fig.5 shows the sky motes with the code that injected in it as discussed in the section implementation. Fig. 6 shows the packet delivery ratio and Fig.7 shows the End to End delay with the different no of nodes like the 5, 10, 15, 20, 25, 30, etc. with the parameters that indicated in the Table III. Here the packet delivery rate and the End to End delay was shown and proved that the proposed system was high when compare to the attack scenario. The results proved that the detection rate of the proposed system was efficient in detecting the wormhole attack.

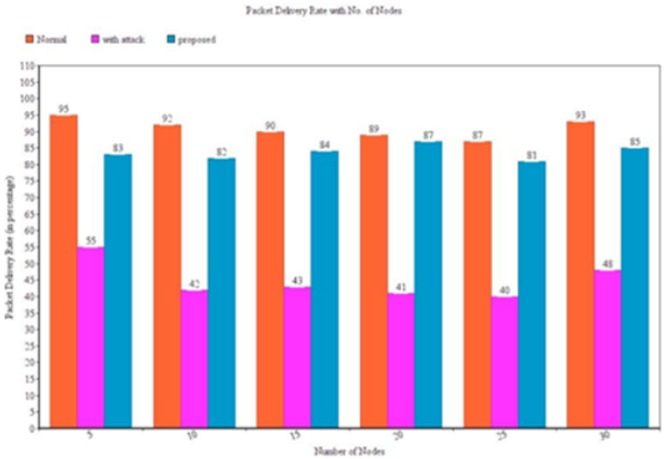

Fig. 6 Packet delivery ratio with No. of Node

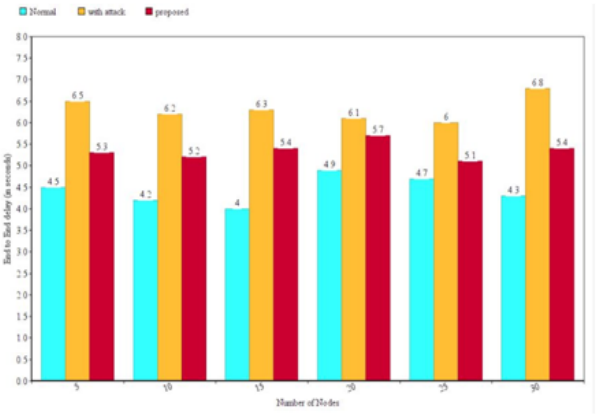

Fig.7 End to End delay with No. of Nodes

V. CONCLUSION AND FUTURE WORKS

Internet of Things was the emerging area in the computing technology. IoT was the constrained networks so the routing was done by the RPL protocol. So, here the RPL protocol was discussed clearly. As RPL was constrained which leads to the many attacks. The various attacks in the RPL were discussed. Particularly the wormhole attack was discussed clearly. The detection technique for the wormhole attack was proposed and implemented in the cooja simulator. The proposed technique was based on the acknowledgements of the each node in the DODAG of the RPL. The results proved the efficiency of the proposed system in terms of the Packet delivery ratio, end to end delay and the attack detection rate.

REFERENCES

[1] Granjal, Jorge, EdmundoMonteiro, and Jorge Sá Silva, "Security for the internet of things: a survey of existing protocols and open research issues", *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 3, pp. 1294-1312, 2015.

[2] Gaddour, Olfa, and AnisKoubaa, "RPL in a nutshell: A survey", *Computer Networks*, Vol. 56, No. 14, pp. 3163-3178, 2012.

[3] Mosenia, Arsalan, and Niraj K. Jha, "A comprehensive study of security of internet-of-things", *IEEE Transactions on Emerging Topics in Computing*, Vol. 5, No. 4, pp. 586-602, 2017

[4] Wallgren, Linus, ShahidRaza, and Thiemo Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things", *International Journal of Distributed Sensor Networks*, Vol. 9, No. 8, pp. 794326, 2013.

[5] Pongle, Pavan, and GurunathChavan, "A survey: Attacks on RPL and 6LoWPAN in IoT", *Pervasive Computing (ICPC), 2015 International Conference on* IEEE, 2015.

[6] Raza, Shahid, Linus Wallgren, and Thiemo Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", *Ad hoc networks*, Vol. 11, No. 8, pp. 2661-2674, 2013.

[7] Ahmed, Firoz, and Young BaeKo. "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks", *Security and Communication Networks*, Vol. 9, No. 18, pp. 5143-5154, 2016.

[8] Khandare, Pravin, Yogesh Sharma, and S. R. Sakhare, "Countermeasures for selective forwarding and wormhole attack in WSN", *Inventive Systems and Control (ICISC), 2017 International Conference on* IEEE, 2017.

[9] Khalil, Issa, SaurabhBagchi, and Ness B. Shroff, "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks", *Dependable Systems and Networks, 2005, DSN 2005 Proceedings, International Conference on*. IEEE, 2005.

[10] Khalil, Issa, SaurabhBagchi, and Ness B. Shroff, "MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks", *Ad Hoc Networks*, Vol. 6, No. 3, pp. 344-362, 2008.

[11] Hu, Y-C., Adrian Perrig, and David B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks", *INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, Vol. 3, 2003.

[12] Eriksson, Jakob, Srikanth V. Krishnamurthy, and MichalisFaloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks", *Network Protocols 2006, ICNP'06 Proceedings of the 2006 14th IEEE International Conference on IEEE*, 2006.

[13] Song, Ning, LijunQian, and Xiangfang Li, "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach", *Parallel and distributed processing symposium 2005, Proceedings, 19th IEEE international*, 2005.

[14] Azer, Marianne, Sherif El-Kassas, and Magdy El-Soudani, "A full image of the wormhole attacks-towards introducing complex wormhole attacks in wireless ad hoc networks", *arXiv preprint arXiv:0906, 1245*, 2009.

[15] Chen, Tao, *et al.*, "A secure routing mechanism against wormhole attack in IPv6-based wireless sensor networks", *Parallel Architectures, Algorithms and Programming (PAAP), 2015 Seventh International Symposium on* IEEE, 2015.

[16] Perazzo, Pericle, *et al.*, "Implementation of a wormhole attack against arpl network: Challenges and effects", *Wireless On-demand Network Systems and Services (WONS), 2018 14th Annual Conference on IEEE*, 2018.

[17] Ahsan, Muhammad Saad, Muhammad NasirMumtazBhutta, and MoazamMaqsood, "Wormhole attack detection in routing protocol for low power lossy networks", *Information and Communication Technologies (ICICT), 2017 International Conference on IEEE*, 2017.

[18] Khan, FarazIdris, *et al.*,"Wormhole attack prevention mechanism for RPL based LLN network", *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on IEEE*, 2013.

[19] Idris Khan, Faraz, *et al.*, "Merkle tree based wormhole attack avoidance mechanism in low power and lossy network based networks", *Security and Communication Networks*, Vol. 7, No. 8, pp. 1292-1309, 2014.

[20] Poovendran, Radha, and LoukasLazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks", *Wireless Networks*, Vol. 13, No. 1, pp.27-59, 2007.