V. Chandra Sekhar Reddy *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 7, July- 2018, pg. 63-77 **ISSN: 2321-8363**
UGC Approved Journal
Impact Factor: 5.515

Implementation of Wormhole Attack on RPL Protocol in Internet of Things

V. Chandra Sekhar Reddy[1], Dr. K. Ramesh Reddy[2]
[1]Research Scholar, Dept. Of Computer Science, Rayalasema University, Kurnool, A.P, India
Email: vcsreddy7@gmail.com
[2]Asst. Professor, Dept. Of Computer Science, V S University, Nellore – 524320, A.P, India
Email: drkrreddy05@gmail.com

Abstract: ***The Internet of Things has the potential to change the world, just as the Internet did. May be even more so" [19].The IoT does not transfigure our lives or field of computing, but we can consider it as another footstep in the maturity of the Internet that we already have taken. The aim of IoT is develop an enhanced surrounding for the mankind which will automatically comprehend the requirements of human beings and will perform in view of that. But the communication of these many number of devices is a challenging task for that Routing Protocol for Low-Power and Lossy Networks (RPL) is a novel routing protocol standardized for constrained environments such as 6LoWPAN networks. Providing security in IPv6/RPL connected 6LoWPANs is challenging because the devices are connected to the untrusted Internet and are resource constrained, the communication links are lossy, and the devices use a set of novel IoT technologies such as RPL, 6LoWPAN, and CoAP/CoAPs. In this paper we provide a comprehensive analysis of IoT technologies and their new security capabilities that can be exploited by attackers or IDSs. One of the major contributions in this paper is our implementation and demonstration of well-known routing attacks against 6LoWPAN networks running RPLas a routing protocol. Particularly, we implemented the wormhole attack and its devotion on IoT with the help of contact operating system.***
Keywords: DODAG, Attacks on RPL, RPL Implementation

1. Introduction:

The Internet of Things has the potential to change the world, just as the Internet did. May be even more so" [19].The IoT does not transfigure our lives or field of computing, but we can consider it as another footstep in the maturity of the Internet that we already have taken. The aim of IoT is develop an enhanced surrounding for the mankind which will automatically comprehend the requirements of human beings and will perform in view of that. From the private users point of view the most apparent effect of the introduction of IoT will be seen in both working and domestic fields. IoT bundles several different technologies together to build its vision [2]. The integration of these enabling technologies, along with Internet based and context aware services facilitate a dynamic platform for IoT [4]. Due to the capabilities that can be offered by IoT, it has gained major attention from the industry as well as

 ISSN: 2321-8363
UGC Approved Journal
Impact Factor: 5.515

academia since the past decade [20] [21]. IoT promises to build the globe where all the objects around us will be connected to the Internet and will be communicate with each other with bare minimum human intervention [23]. IoT is going to offer huge number of applications in various environments for improving the quality of our lives. These applications will generate enormous amount of data. One of the key upshots of this rising field is the creation of an unprecedented amount of data, its storage, ownership, security, expiry and it's routing to a desired destination for generating some intelligence out of it that can be further used to build a smart environment. The routing issues become more and more challenging for low-power and lossy radio-links, multi-hop mesh topologies, the battery supplied nodes and frequently changed network topologies. One misconception related to IoT is that, a significant pool of protocols previously developed for the functionality of the Internet would migrate into IoT [4], but this is not the case. As IoT contains a set of moving as well as stationary components, multiple issues arise in the development of routing protocols where these devices will inter communicate with each other. As various factors shown in table I are dominant in the operation of routing protocol, so it becomes difficult to devise a single protocol which will achieve all these objectives that are inherently paradoxical. Due to it routing becomes a notorious NFL (no free lunch) class of algorithm. According to Oladayo Bello et al. [3] an intelligent routing protocol can unleash the intrinsic power of any heterogeneous, dynamic, and complex network that is characterized by multiple dynamic factors such as changing topology and flow. Thus to achieve the full functionality of IoT, intelligent protocols are needed for D2Dcommunication in IoT. Efficient and scalable routing protocols adaptable to different scenarios and network size variations, capable to find optimal routes are required. Another major issue with the IOT routing protocol is that security.

ISSN: 2321-8363
UGC Approved Journal
Impact Factor: 5.515

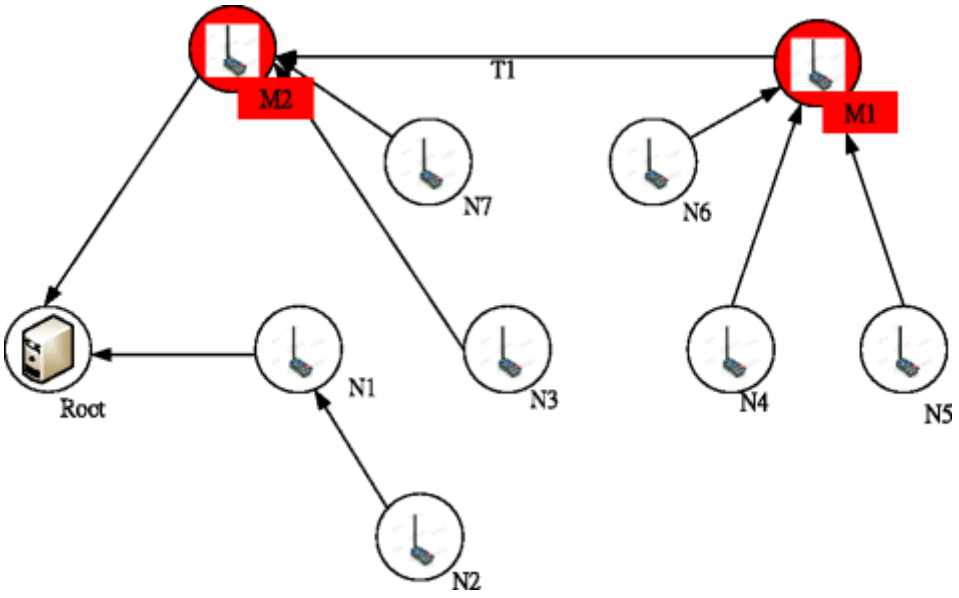

Figure-1: wormhole attack on RPL

RPL facing lot many number of routing issues here we present an overview of the security issues. And the most divesting attack on IOT RPL routing protocol is wormhole attack here we give and tailed view of wormhole attack on RPL and its variants. Here figure-1 shows the wormhole attack on RPl. The two nodes M1 and M2 are communicated with each other and form wormhole.

2. INTERNET OF THINGS

IoT is widely used term but because of the large amount of concepts included in it but its definition is still fuzzy. Although the definition of 'Things' has changed as technology evolved, the main goal of making a computer to sense information without the help of human intervention remains the same[12]. Many researchers have attempted to define IoT.

2.1 Routing protocol over low power and lossy networks (RPL):

Routing is very challenging for 6LoWPAN networks due to the low power and lossy radio links, the battery supplied nodes, multi hop mesh topologies and frequent topology changes due to mobility. This protocol is developed by International Engineering Task Force (IETF) for low power and lossy networks and it is considered as a de facto routing standard for Internet of Things having the aim to optimize the routing scheme for converge cast traffic pattern. RPL is a distance vector protocol. Starting from a border router, RPL constructs a Destination-Oriented Directed Acyclic Graph (DODAG) using one or several metrics. The

 ISSN: 2321-8363
UGC Approved Journal
Impact Factor: 5.515

DODAG is generated by considering the link costs, node attributes and an objective function. Rank generation for every node on the DODAG is done by the objective function. It supports various types of traffic such as multipoint to point, point to multipoint and point to point. For having loop-free topology, the rank must strictly monotonically increase from the root towards the leaves of the DODAG. In complex scenarios lossy link network is divided into many partitions depending on the applications context. So in situations it may form multiple uncoordinated DODAG's with independent roots. Multiple instances of RPL can run concurrently on the network devices. RPL Instance ID is used for the unique identification of the instance. The formation and maintenance of the network topologies is done by DODAG Information Option (DIO) messages which are multi casted periodically and link locally by each node for establishing path towards the root node. DIO messages contain the information such as the DODAG identifier, the objective function, the rank of the node, or the metrics used for the path calculation. After receiving the DIO message, the neighbouring node can set its own rank based on its neighbor's rank. Thus the DODAG construction is done in widening wave fashion. Destination Advertisement Object (DAO) messages are used to back propagate the routing information from leaf nodes to the roots.

Benefit of RPL:

i. This is end to end IP based solution which does not require translation gateways for accessing the nodes within the network from outside world.

ii. It dynamically adapts the sending rate of the routing control messages which will be generated frequently only if the network is in unstable condition.

iii. It allows optimization of network for different application scenarios and deployment.

Shortcomings:

i. Does not support multipath routing.

ii. Energy balancing and load balancing are not taken into consideration.

E. Multi parent routing in RPL:

Lifetime of the network is considered as the time period before the death of the first node of the network due to run out of the energy. The purpose behind designing this routing protocol is to maximize the overall lifetime of the network by taking care of most energy constrained nodes i.e. bottlenecks. OanaIova et al. proposed the Expected Lifetime (ELT) metric for denoting the residual time of the node [17].They constructed a DODAG based on ELT metric for accurately estimating the lifetime of all the routes towards the border router and designed a mechanism for detecting bottlenecks for spreading the traffic load to several parents. A node exploits all its parents, assigning a weight of traffic to each of them and distributes fairly the energy consumption among all the paths towards the border router. As only a part of its traffic will finally arrive at a specific bottleneck, energy consumption is well balanced.

Virtue:

i. Supports multipath routing to improve the fault tolerance, congestion avoidance and QoS.

ii. It also increases the network lifetime by balancing the traffic load amongst multiple parents.

2.2 Attacks on RPL Routing protocol

A. Selective Forwarding Attack:

This attack takes place by selectively forwarding packets. With this attacks DoS (Denial of Service) attack can be launched. The purpose of attack is to disrupt routing paths and filter any protocol. In RPL attacker could forward all RPL control messages and drop the rest of the traffic.

B. Sinkhole Attack:

In sinkhole attacks attacker node advertises beneficial path to attract many nearby nodes to route traffic through it. This attack does not disrupt the network operation but it can become very powerful when combined with another attacks.

C. Sybil Attack:

Sybil attack is similar to a clone ID attack; malicious node uses several identities on the same physical node. Using this attack large parts of a network can be taken under control without deploying physical nodes. Author [4] in his work categorized Sybil attacks in social domain of Internet of Things and stated defence against these attack. Sybil attack on RPL is not evaluated yet.

D. Hello Flooding Attack:

For joining the network node broadcast initial message as HELLO message. Attacker can introduce himself as neighbour node to many node by broadcasting Hello message with strong routing metrics and enter in network. In RPL, DIO messages refereed as Hello message, which is used to advertise information about DODAG.

E. Wormhole Attack:

RPL can undergo the wormhole attack [1]. The main purpose of this attack is Disrupt the network topology and traffic flow. This attack can takes place by creating tunnel between the two attackers and transmitting the selective of all traffic through it. Wormhole attack can be prevented using the construction of Markle tree authentication [5].

F. Clone ID Attack:

Attacker node clones the identity of other node to gain access to traffic destined to victim node or through victim node. Clone ID attack is possible in RPL network.

G. Black hole Attack:

In the Black Hole attack, similar to a hole which sucks in everything, attacker node drops all data packets silently. In this way, all packets in the network routing through that node are dropped. Author [6] in his work tested the Black hole attack on 6LoWPAN network.

H. Denial of Service Attack:

Denial of service or Distributed denial of service attack is attempt to make resources unavailable to its intended user. In RPL this attack can be bring using the IPv6 UDP packet flooding. Many malicious nodes by coordinating can bring the Distributed denial of service attack, in this attack it is difficult to identify the malicious nodes. However IDS system in [7] proposed the framework for detection of DOS attack in 6LoWPAN. The architecture

integrates the IDS into the network framework developed within the EU FP7 project ebbits. At the security layer of ebbits Dos protection module is added. IDS probe nodes located in the network which sends periodically the traffic in 6LoWPAN through wired connection to IDS system. Dos protection manager receives the alerts from IDS system. It takes the network related information from other modules of network manager layer to confirm the attack. IDS sends the jamming information of attack to Dos protection manager. The presence of jamming information at the modules of network manager of ebbits indicated the presence of attack.

Alteration and Spoofing Attack Rank attack:

In RPL rank value increases from root to child node. By changing Rank value, an attacker can attract child node for selecting as parents or improve some other metric, and can attract large traffic going toward the root.

Version Attack:

This attack takes place by publishing the higher version number of DODAG tree. When nodes receive the new higher version number DIO message they start the formation of new DODAG tree. This can cause the generation of new un-optimized topology and brings inconsistencies in topology. **Local Repair Attack:** In local repair attack, attacker without any problem with link quality periodically sends the local repair message. This causes the local repair around the nodes which hears the local repair message. Local repair attack creates more impact on delivery ratio than any other kind of attack [10], generates more control packets and increases the end to end delay. While constructing the packet dropping occurs from previous topology. Also exhaust the energy of node unnecessarily.

Neighber Attack:

In this attack the malicious node broadcast DIO messages that it received without adding information of himself. The node who receives this type of messages may think that new neighbor node send this DIO message. The victim nodes try to select the node which is not in range as parent node and change the route to the out range neighbors. This attack is similar to the wormhole attack with special case of selective forwarding of DIO message only.

DIS Attack:

DIS (DODAG Information Solicitation) message used by new node to get the topology information before joining the RPL network. In this attack malicious nodes periodically sends the DIS messages to its neighbors.

3. Wormhole attack

Wormhole attack is one of the attacks on networking layer which affects the RPL protocol. This attack can even be launched if the network uses cryptographic techniques this attack is also not dependent on MAC (Medium Access Control) protocol layer. The attacker nodes only replays the messages in the network they do not produce new packets, which is due to this reason they easily bypass the cryptographic techniques. Mainly Wormhole attack is classified into three techniques [21][22] which are as follows: Hidden Wormhole attack Exposed Wormhole attack Half open Wormhole attack

a. Hidden Wormhole Attack

In hidden attack the malicious nodes do not change or modify the headers of packet. This attack is also called close Wormhole. They simply forward the packet through tunnel from one point to another point by replaying them in the network. As mentioned in Fig I node A transmits the packet to node K where the malicious node M 1 captures the packet and transfers to malicious node M 2 through tunnel and then replays them to nodes L and B. Through this tunnel nodes L and B becomes neighbors of nodes A and K but in reality the wormhole link makes them false neighbors to each other and Wormhole attack is hidden in the network. The nodes do not know about malicious nodes existence.

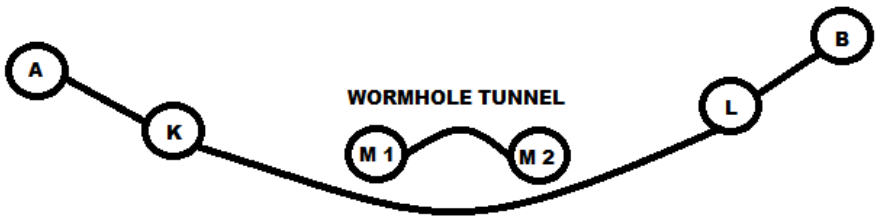

Fig-2: Hidden Wormhole Attack

b. Exposed Wormhole Attack:

The exposed Wormhole attack is also called open Wormhole attack. In this attack the malicious nodes do not alter the packet head but modify them using their identities in those packets during the route set up and other nodes will know that Wormhole attack is being taking place but they do not know the malicious node location. The scenario developed in Fig 2 will be such that node A send packet to node K from where malicious node M 1 will tunnel the packets through tunnel to malicious node M 2 from where it is forwarded to nodes L and B making them as false neighbors of node A and K but in this attack the network will know that wormhole attack is taking place but the location of malicious nodes will be unknown to network.

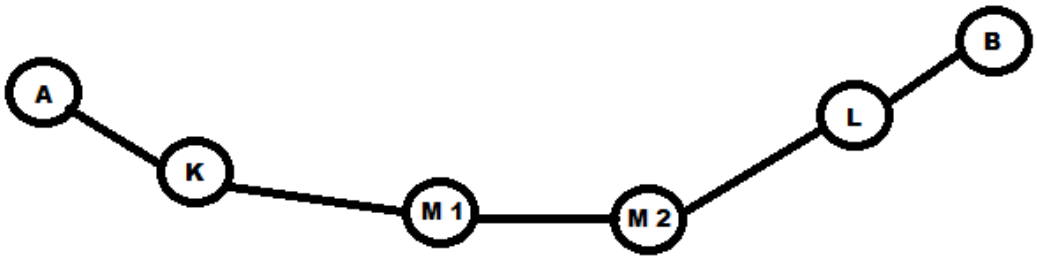

Fig-3: Exposed Wormhole Attack

c. Half Open Wormhole Attack:

In half open Wormhole attack one side of network modifies the packet header but other side of network does not change it. One side acts as open and other side acts as close Wormhole attack.

Methods to Launch Wormhole Attack:

There are number of ways wormhole attack can be generated [20]. Following methods are as:

I.) Encapsulation Technique

In this technique the legitimate node send route request RREQ to the network. The malicious node detects the RREQ packets and tunnels them to another malicious node present inside the network. After the packet is received second malicious node broadcast the request to its neighbors and neighbors detect that this is shortest path having less hop count through tunnel

and neglect the RREQ send by legitimate node which is more than two hops. This technique prevents the nodes to detect the original path send by legitimate node.

II.) Out of Band Channel

Out of band channel method is difficult to generate because it uses specialized hardware. In this attack high quality, low latency, single hop wireless link is created between nodes having high bandwidth by using directional antennas or using wired medium to create link. Due to this long out of band channel the malicious nodes miss guides the nodes as wrong neighbors.

III.) High Power transmission

This technique generates the attack using high power transmission. This attack can also be launched by only packets with high power as compared to other nodes present in the network. When malicious node detects the RREQ packet it broadcast it over the network and other nodes hear the high transmission they rebroadcast back to malicious node. Using this way attacker node creates the path between nodes even without the help of other attacker nodes.

IV.) Packet Relay

Packet relay is another type of technique used by Wormhole to attack the nodes. In this method Wormhole creates private link wired or wireless between two distant nodes which are not in range of one another but they are at the range of malicious nodes. The attacker nodes display the victim nodes as they are neighbors of one another starts replaying packet between them by tunnel and control traffic between distant nodes through this way they can also control the traffic between the tunnel. This attack can be launched by one to many malicious nodes.

V.) Protocol Deviations

Wormhole attack can also be launched by using protocol deviation method. In this technique to reduce or limit the MAC layer collision legitimate nodes step back for a moment of time before forwarding the RREQ through network but the malicious node do not back off and consistently broadcast the RREQ messages to nodes. By doing so attacker nodes RREQ will arrive first at the nodes by showing them as their neighbors.

4. Wormhole attack on RPL

A wormhole is an out of band connection between two nodes using wired or wireless links. Wormholes can be used to forward packets faster than via normal paths. A wormhole in itself is not necessarily a

Breach security; for example, a wormhole can be used to forward mission critical messages where high throughput is important, and the rest of the traffic follows the normal path. However, a wormhole created by an attacker and combined with another attacks, such as sinkhole, is a serious security threat.

As we discussed in Section 4.1, an IDS for the IoT could place processing intensive modules and a firewall in the 6BR.An attacker can create a wormhole between a compromised constrained node in a 6LoWPAN network and a typical device on the Internet and can bypass the 6BR. Such a wormhole can become a very serious security breach and is very hard to detect especially when the wormhole is systematically switched on and off. Ways to prevent or at least detect such a wormhole in the IoT are a research challenge that needs to be addressed. It is comparatively easy to detect wormholes created within an RPLDODAG. One approach is to use separate link layer keys for different segments of the network. This can counteract the wormhole attack as no communication will be possible between nodes in two separate segments. Also, by binding geographic information to the neighbour hoods it is possible to overcome a wormhole [20]. As wormholes are usually coupled with other attacks, detecting the other attack and removing/avoiding the malicious node will ultimately overcome wormhole attacks.

5. Implementation:

Implementing Wormhole Attacks against RPL. We simulate a wormhole attack by using the network simulator Coojaand set up a physical medium where two nodes on opposite sides of the network have a very good connection. Subjected to a wormhole attack, they form a high quality route, and the neighboring nodes connect through the malicious nodes 2 and 5. We run this simulation for 24 hours to allow RPL inherent mechanisms to self-heal the RPL DODAG. However, the network state has shown that the attack is still there after 24 hours

which means that RPL does not provide any specific mechanisms to counter wormhole attacks.

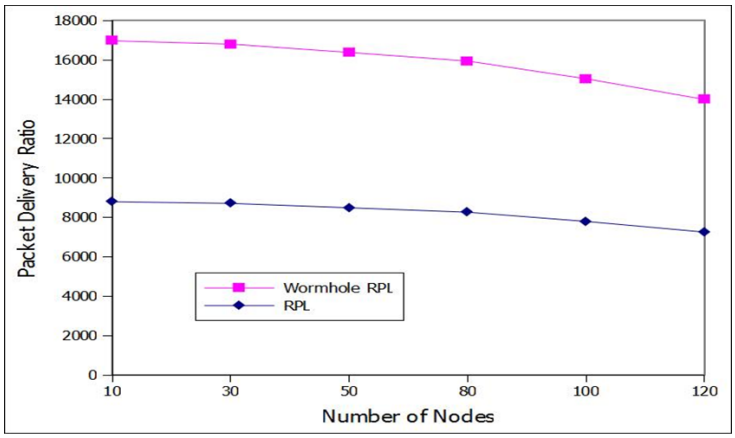

Figure-4: Packet Delivery Ratio

Here figure-4 shows the comparison of packet delivery ratio of normal RPL to the Wormhole RPL. PDF is the number of packets delivered to the total number of packets. Wormhole RPL have the Low PDF ratio compared to normal RPL.

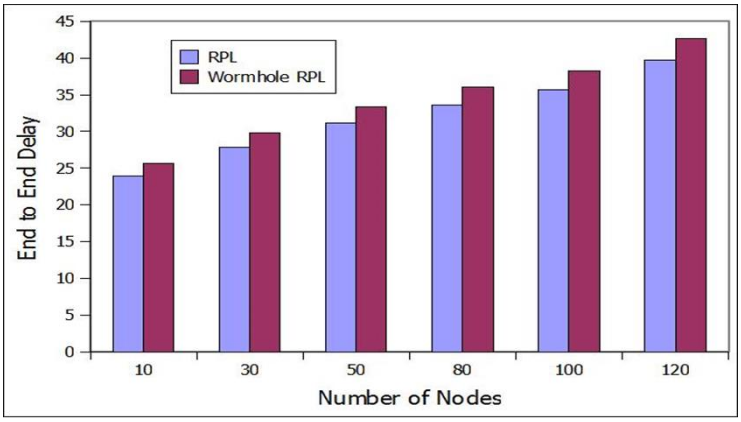

Figure-5: End to End Delay

Here figure-5 shows the comparison of End to End Delay of normal RPL to the Wormhole RPL. E2E delay is the amount of delay done by a packet to transfer from source to destination. Wormhole RPL have the High E2E delay compared to normal RPL.

ISSN: 2321-8363
UGC Approved Journal
Impact Factor: 5.515

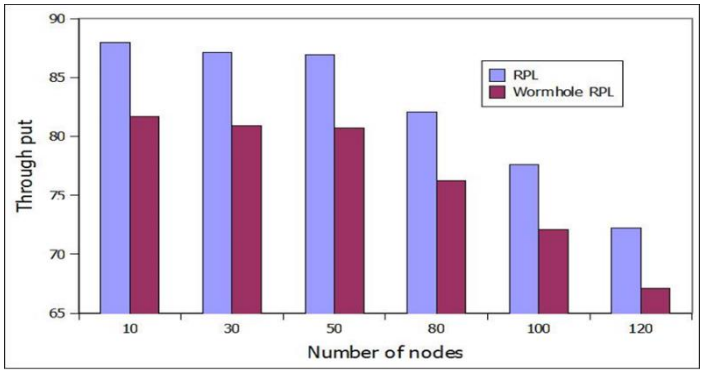

Figure-6: Through put

Here figure-6 shows the comparison of through put of normal RPL to the Wormhole RPL. Through put is the number of packets delivered within the period of time. Wormhole RPL have the Low Through put compared to normal RPL.

6. Conclusion:

In this paper we have reviewed novel IoT protocols and highlighted their strengths and weaknesses. We have shown that, while the RPL protocol is vulnerable to different routing attacks, it has inherent mechanisms to counter HELLO flood attacks and mitigate the effects of sinkhole attacks. The aim of this paper is to highlight the importance of security in the RPL-based IoT. Particularly, we shown the wormhole attack and its impact on the IOT network. The simulation results shows that the effect of wormhole with respect to the performance metrics.

Future work: As a future work needs to propose and implement a novel secure RPL protocol which can able to mitigate the wormhole attack in IOT RPL.

 ISSN: 2321-8363
UGC Approved Journal
Impact Factor: 5.515

References:

[1]. 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 (2013).
[2]. Raza, Shahid, Linus Wallgren, and Thiemo Voigt. "SVELTE: Real-time intrusion detection in the Internet of Things." Ad hoc networks 11.8 (2013): 2661-2674.
[3]. Weekly, Kevin, and Kristofer Pister. "Evaluating sinkhole defense techniques in RPL networks." Network Protocols (ICNP), 2012 20th IEEE International Conference on. IEEE, 2012.
[4]. Zhang, Kuan, et al. "Sybil Attacks and Their Defenses in the Internet of Things."
[5]. Khan, Faraz Idris, et al. "Wormhole attack prevention mechanism for RPL based LLN network." Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on. IEEE, 2013.
[6]. Chugh, Karishma, AboubakerLasebae, and Jonathan Loo. "Case Study of a Black Hole Attack on 6LoWPAN-RPL." SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies. 2012.
[7]. Kasinathan, Prabhakaran, et al. "Denial-of-Service detection in 6LoWPAN based internet of things." Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on. IEEE, 2013.
[8]. Le, Anhtuan, et al. "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks." (2013): 1-1.
[9]. Le, Anhtuan, et al. "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach." International Journal of Communication Systems 25.9 (2012): 1189-1212.
[10]. Le, Anhtuan, et al. "The impacts of internal threats towards Routing Protocol for Low power and lossy network performance." Computers and Communications (ISCC), 2013 IEEE Symposium on. IEEE, 2013.
[11]. Dvir, Amit, TámasHolczer, and LeventeButtyan. "VeRA-version number and rank authentication in rpl." Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on. IEEE, 2011.
[12]. Perrey, Heiner, et al. "TRAIL: Topology Authentication in RPL." arXiv preprint arXiv: 1312.0984 (2013).
[13]. Mayzaud, Anthéa, et al. "A Study of RPL DODAG Version Attacks.", 2013
[14]. Kasinathan, Prabhakaran, et al. "DEMO: An IDS framework for internet of things empowered by 6LoWPAN." Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013.
[15]. Jun, Chen, and Chen Chi. "Design of Complex Event-Processing IDS in Internet of Things." Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on. IEEE, 2014.
[16]. Amin, Syed Obaid, et al. "A novel coding scheme to implement signature based IDS in IP based Sensor Networks." Integrated Network Management-Workshops, 2009. IM'09. IFIP/IEEE International Symposium on. IEEE, 2009.

 ISSN: 2321-8363
UGC Approved Journal
Impact Factor: 5.515

[17]. Le, Anhtuan, et al. "Specification-based IDS for securing RPL from topology attacks." Wireless Days (WD), 2011 IFIP. IEEE, 2011.
[18]. Hummen, René, et al. "6LoWPAN fragmentation attacks and mitigation mechanisms." Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks. ACM, 2013.
[19]. Oliveira, Luis ML, et al. "Network admission control solution for 6LoWPAN networks." Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on. IEEE, 2013.
[20]. Raza, Shahid, et al. "Securing communication in 6LoWPAN with compressed IPsec." Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on. IEEE, 2011.
[21]. Raza, Shahid, et al. "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN." Security and Communication Networks (2012).
[22]. Sherburne, Matthew, Randy Marchany, and Joseph Tront. "Implementing moving target IPv6 defense to secure 6LoWPAN in the internet of things and smart grid." Proceedings of the 9th Annual Cyber and Information Security Research Conference. ACM, 2014.
[23]. Khan, Zubair A., Saeed U. Rehman, and M. Hasan Islam. "An analytical survey of state of the art wormhole detection and prevention techniques." International Journal of Science and Engineering REsearch 4.6 (2013): 1723-1731.

