Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 6, June-2016

A Survey : Locating the Attacker of Wormhole Attack on RPL in IoT

Roshni Patel[1], Rutvik Mehta[2]

[1]*Computer Science and Engineering Department, PIET Vadodara*
[2]*Information Technology Department, PIET Vadodara*

Abstract — Internet of Things (IoTs) offers capabilities to identify and connect worldwide physical objects into a unified system. Internet of Things consists of devices which are limited in resources like battery powered, memory and processing capabilities etc. Due to this a new network layer routing protocol is designed called RPL(Routing Protocol for low power and lossy Network), which is a light weight protocol and its functionality differs from traditional routing protocol. This rank based routing protocol may undergo several kinds of attack as they are connected to the unsecured Internet, limited resources; also the communication links are lossy. This paper focuses on the possible attack carried out on RPL, along with the comparative analysis to mitigate these attacks. Also we have focused on the methods for providing security against wormhole attacks.

Keywords- IoT, IEEE 802.15.4E, ROLL, 6LoWPAN, RPL, DODAG, Wormhole, Honeypot, IDS.

I. INTRODUCTION

IoT the first term introduced by Kevin Ashton in 1998, is a future of Internet and Ubiquitous Computing. This technological revolution represents the future of connectivity and reachability. In IoT, 'things' refer to any object on face of the Earth, whether it is a communicating device or a non-communicating object. The objects become communicating nodes over the Internet, through data communication means, primarily through Radio Frequency Identification (RFID) tags. IoT is not only hardware and software paradigm, but includes interaction and social aspects as well. IoT stands for a "world-wide network of inter-connected objects based on standard communication protocols which are uniquely addressable" [1]

Structurally, the IoT requires software architectures that are able to deal with a large amounts of information, queries, and computation, making use of new data processing paradigms, stream processing, filtering, aggregation and data mining, all of this sustained by communication standards such as Hypertext Transfer Protocol(HTTP) and Internet Protocol (IP). In contrast, due to the nature of IoT objects, very low power consumptions are required so any object can plug into the Internet while being powered by batteries or through energy harvesting. Energy is wasted by transmission of unneeded data, protocol overhead, and non-optimized communication patterns; this needs to be taken into account while plugging objects into the Internet. IoT can be divided into three important layers viz. Perception, Network and Application.

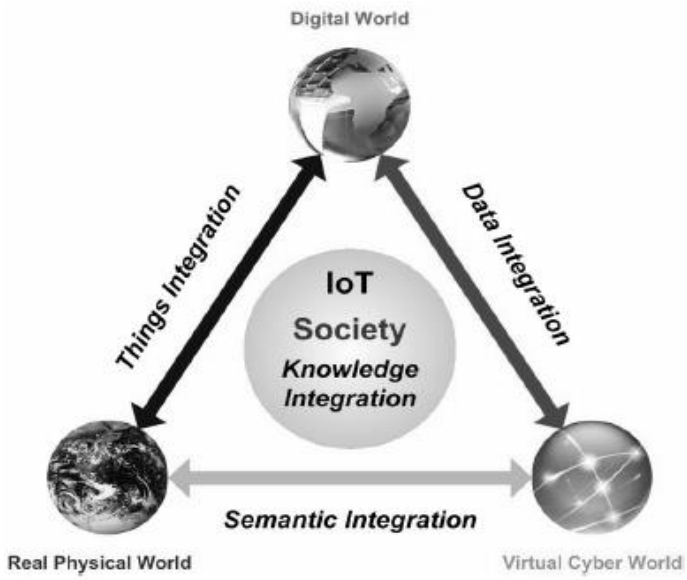

Figure 1. Internet of Things – a symbiotic interaction among the real/physical, the digital, virtual world and society [2].

II. PROTOCOL STACK OF IoT

2.1 Physical Layer

Regarding the IoT Protocol Stack, from a PHY perspective, the current IEEE 802.15.4 -2006 PHY layer(s) suffice in terms of energy efficiency. Given that a large amount of IoT applications however will require only a few bits to be send. It may be advisable to commence looking into a standardized PHY layer which allows ultra-low rate transmission over very narrow frequency bands, with the obvious advantage of enormous link budgets and thus significantly enhanced ranges.

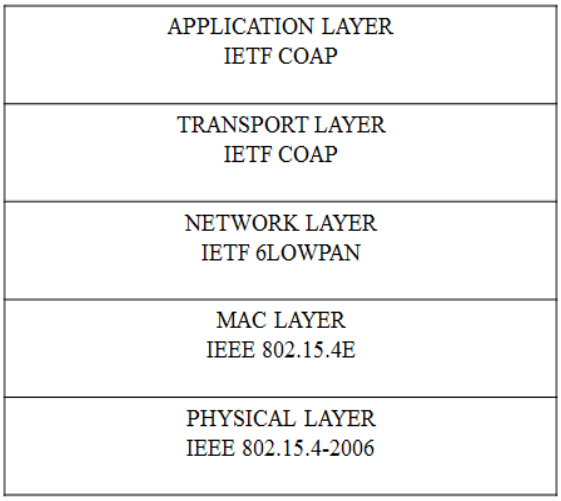

Figure 2. Protocol Stack of IoT [4]

2.2 MAC Layer

2.2.1 IEEE 802.15.4E

IEEE802.15.4e standard is very suitable for IoT because it is latest generation of highly reliable and low-power MAC protocol.

2.3 Network Layer

From a network perspective, the introduction of the IETF 6LoWPAN protocol family has been instrumental in connecting the low power radios to the Internet and the work of the IETF ROLL allowed suitable routing protocols to achieve universal connectivity.

2.3.1 IETF 6LoWPAN

6LoWPAN integrates IP-based infrastructures and WSNs by specifying how IPv6 packets are to be routed in constrained networks such as IEEE802.15.4 networks. Due to the limited size of the link layer in the 6LoWPAN networks, the 6LoWPAN standard also defines fragmentation and reassembly of datagram. The IEEE 802.15.4 frame size may exceed the Maximum Transmission Unit (MTU) size of 127 bytes for big application data; in that case additional fragment(s) are needed.

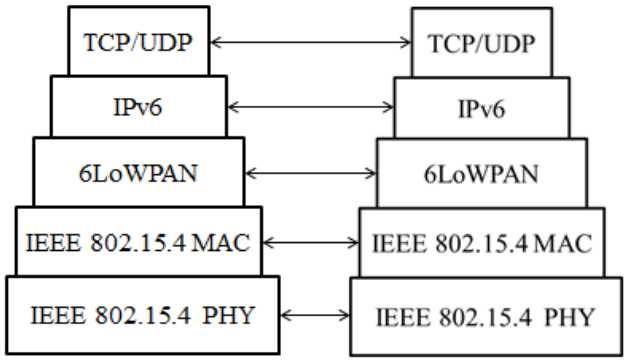

Figure 3. Position of 6LoWPAN in IPv6 [5]

6LoWPAN networks are connected to the Internet through 6BR (6LoWPAN Border Router) that is analogous to a sink in a WSN. The 6BR performs compression/decompression and fragmentation/ assembly of IPv6 datagrams.

2.3.2 IETF RPL

Low-power and Lossy Networks (LLNs) consist largely of constrained nodes (with limited processing power, memory and sometimes energy when they are battery operated or energy scavenging). These routers are interconnected by lossy links, typically supporting only low data rates. Another characteristic of such network is that the traffic patterns are not simply point-to-point, but in many cases point-to-multipoint or multipoint-to-point. Furthermore such networks may comprise upto thousands of nodes. An effective solution is being developed by the IETF "Routing over Low Power and Lossy (ROLL) Network" working group.

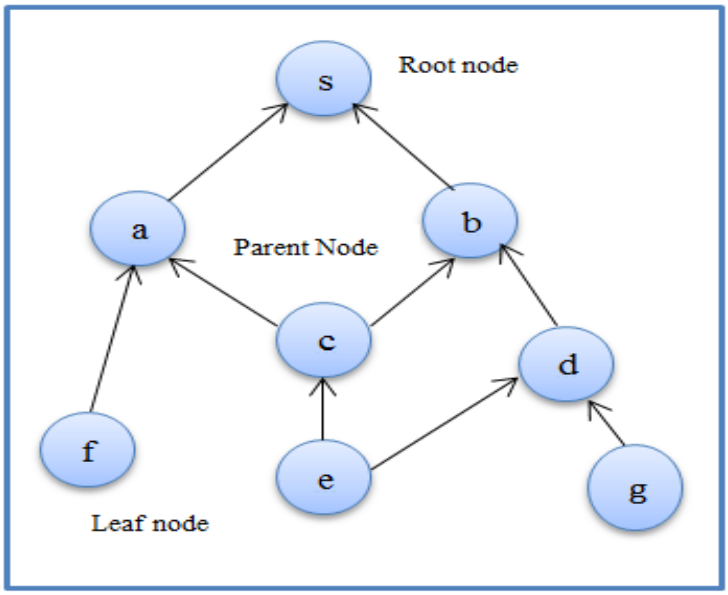

Figure 4. RPL routing tree: DODAG [5]

It basically designed for the multipoint to point communication, but it can also support the point to point and point to multipoint communication. RPL topology forms the DODAG (Destination Oriented Directed Acyclic Graph) tree, which contains only 1 root. The root node is also called as the sink node. Root node starts the formation of the topology by broadcasting the DIO (DODAG Information Object) messages. Node receiving the DIO message selects the parent to sender, with rank value calculated with respect to the parents rank value and other parameters. The rank value may depend on the distance from the root node, energy of link etc. The network owner can decide the rank value calculation parameters. The nodes continue to broadcast the DIO message and form the tree topology.

III. SECURITY THREATS AND CHALLENGES OF IoT

3.1 Security Concerns in IoT

The security of the IoT system has seven major standards viz. privacy protection, access control, user authentication, communication layer security, data integrity, data confidentiality and availability at any time [4].

- Front-end Sensors and Equipment
- Network
- Back-end of IT systems

3.2 Privacy Concerns in IoT

Privacy can be defined as "the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others [4]".

- Privacy in device
- Privacy during Communication
- Privacy in Storage
- Privacy at Processing

To preserve privacy mainly two things should be kept in mind

- Personal data must be treated in a way that it should be simpatico with the intended purpose.
- Without explicit acceptance and the knowledge of the data owner, their personal data should not be disclosed or retained to third party.

IV. APPLICATIONS OF IoTs

Table 1. Applications of IoT [4]

Field of Application	Example of Application
E – health	Patient Monitoring, Doctor tracking, Personnel Tracking, Real-time patient health status monitoring, Predictive expertise information to assist doctors and practitioners.
Retail & Logistics	Supply Chain control, Intelligent Shopping Applications, Smart Product Management
Smart Transportation	Smart Transportation through real-time dynamic on-demand traffic information and shortest-time travel path optimization.
Smart Home	Energy use, Water use, Remote control Application, Intrusion Detection Systems
Environmental Monitoring	Air Pollution, Noise Monitoring, Waterways, Industry Monitoring.
Energy Conservation	Smart Devices, Smart Grid
Green Agriculture	Green Houses, Compost, Irrigation Management, Soil Moisture Management

V. RPL (ROUTING PROTOCOL FOR LOW POWER AND LOSSY NETWORK)

Low Power and Lossy Networks (LLLNs) consist largely of constrained nodes (with limited processing power, memory and sometimes energy when they are battery operated or energy scavenging). These routers are interconnected by lossy links, typically supporting only low data rates that are usually unstable with relatively low packet delivery rates. Another characteristic of such networks is that the traffic patterns are not simply point-to-point, but in many cases point-to-multipoint or multipoint-to-point.

These characteristics offer unique challenges to a routing solution: the IETF "Routing over Low Power and Lossy (ROLL) networks" working group. It has proposed the leading IPv6 Routing Protocol for Low Power and Lossy Networks (LLNs), RPL based on a gradient-based approach.

The four values in RPL which are used to identify and maintains a topology is RPLInstanceID, DODAGID, DODAGVersionNumber, and Rank.

- Multiple Instance of RPL may run concurrently on the network devices and each instance has specific routing optimization objectives, such as the minimization of delay and energy consumption. For this, RPLInstanceID is deployed to identify one of the possible RPL instances running on the same network.
- The RPLInstanceID and DODAGID uniquely identify a single DODAG in the network. A RPL Instance comprises of multiple DODAGs, each of which has a unique DODAGID.
- A DODAG is sometimes reconstructed from the DODAG root, by incrementing the DODAGVersionNumber.
- The topology is set-up based on a Rank metric, which defines individual node position with respect to the DODAG root, as specified by the Objective Function.

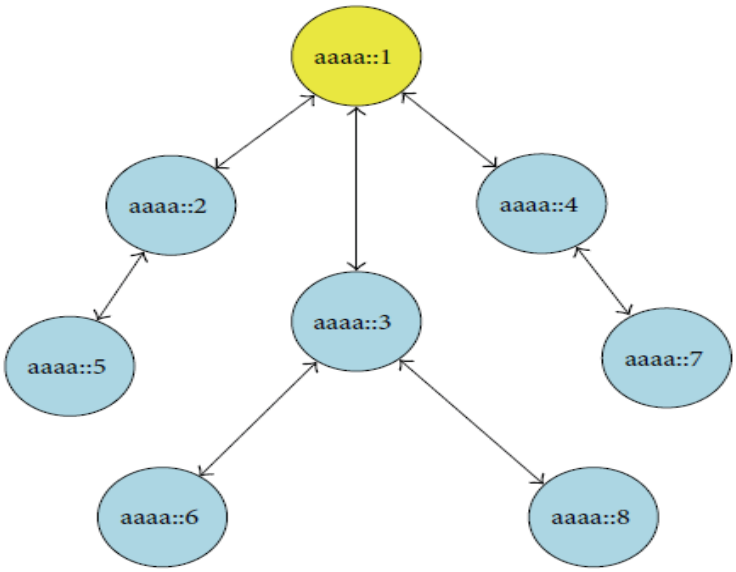

Figure 5. A simple RPL DODAG where each node has a unique IPv6 address [6]

VI. ATTACKS ON RPL TOPOLOGY

The attacks on RPL Topology along with their consequences on network and existing solution for these attack is as follows [6].

6.1 Selective Forwarding Attack

With this attack DoS (Denial of Service) attack can be launched. The purpose of this attack is to disrupt routing paths and filter any protocol by selectively forwarding packets. In RPL attacker could forward all RPL control messages and drop rest of the traffic. Solution for this attack is by creating a disjoint path or dynamic path between parent and children.

6.2 Sinkhole Attack

A Sinkhole occurs when a compromised node performs two malicious acts:

- It attracts legitimate traffic by advertising a favorable route, e.g. through manipulation of the rank field in a Destination Information Object (DIO) message.
- The Sinkhole drops any legitimate data traffic routing through it, degrading the performance of the network

It can be evaluated by two defensive techniques

- Parent fail-over
  Parent failover technique uses UNS (unheard node set) field in DIO message indicating that the nodes are in sinkhole compromised path. If the node receives the DIO message containing its ID in UNS then it adds its parents in local blacklist.
- Rank Authentication
- The Rank Authentication Technique relies on one way hash technique. The root begins to generate hash value by picking random value, and broadcast it in DIO message. All nodes calculate the hash value using previous received one and again broadcast it using DIO message. Each node stores the hash value received by its parents along with number of hops in the path. When root node broadcasts random number securely, then node can verify its parent rank using that intermediate hops number.

6.3 Sybil Attack

The IoT is vulnerable to Sybil attack where attackers can manipulate fake identities or abuse pseudo-identities to compromise the effectiveness of the system. Due to Sybil Attack, the IoT system may generate wrong reports, and user might generate spam reports and lose their privacy [5].

There are 3 types of Sybil Attack: SA-1, SA-2, SA-3.

- SA-1
  The SA-1 exists in sensing domain or social domain. But the capability of building connection with the honest node is not strong.

- SA-2

SA-2 attackers usually exist in social domain; also the number of attack edge is large. The goal of SA-2 is to disseminate spam, advertisements and malware; steal and violate user's privacy and maliciously manipulate the reputation system

- SA-3

SA-3 attackers are in mobile networks (mobile domain). Its main goal is to manipulate the local popularity, disseminate spam in the mobile environment, or violate user's privacy.

Table 2. Summary of Attacks on RPL [6]

Attack	Effect on Network Parameter	Method to countermeasure	Comments on Method
Selective Forwarding	Disrupt Routing Path	Heartbeat Protocol, end-to-end packet loss	Both Technique only detects existence of attack.
Sinkhole	Large traffic flows through attacker nodes	Parent failover, authentication technique	Parent failover detects the attack, Rank Authentication Technique avoids the attack
Hello Flooding Attack	Route formation through attacker node	RPL's Global and Local Repair Mechanism removes attack	This attack cannot exist for longer time in RPL Network
Wormhole	Disrupt the Network Topology	Merkle's Tree Authentication	Prevention Technique
Sybil	Routing traffic unreachable to victim node	Social Graph based Sybil Detection, Behavior Classification based Sybil Detection, Mobile Sybil Defense	It is used to detect all three types of Sybil attack.
Clone ID	Routing Traffic unreachable to victim node	No technique evaluated yet	---
Denial of Service	Make resources unavailable to intended users	IDS based Solution	Not compactable to general architecture
BlackHole	Packet Delay and Control Overhead	No technique evaluated yet	--
Rank	Packet Delay, Delivery Ratio, Generation of un-optimized path and loop	IDS based Solution, VeRA, TRAIL	IDS based solution detects the attack and VerA and TRAIL prevents the Rank Attack
Version	Control overhead, delivery ratio, end to end delay	VeRA	VeRA prevents attack from occuring
DIS attack	Packet Delay	No Techniques evaluated yet	---

6.4 Hello Flooding Attack

For joining the network node broadcast initial message as HELLO message. Attacker can introduce himself as neighbor node to many nodes by sending the Hello message with strong routing metrics and enter in network. In RPL, DIO (Destination Information Object) messages are referred as Hello messages, which are used to advertise information about DODAG.

6.5 Wormhole Attack

The main purpose of this attack is to disrupt the network topology. This attack has two adversaries who are connected through a private line which is not a part of the network. The packets received by one of the attacker are sent to the other attacker through the private line and the other attacker rebroadcast the packets, thereby utilizing the network resources and spreading fake information about routes in the network.

6.6 Clone ID attack

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

6.7 Blackhole Attack

The attacker who is active on a compromised node advertises that the node has the shortest route to the destination node in whose packet he is interested in. Then all the nodes would adjust their routing table accordingly and route all the packets to the particular node through the compromised node only, which may drop or alter the packets.

6.8 Denial of Service Attack

Denial of Service Attack or Distributed Denial of Service attack is attempted to make resources unavailable to its intended user. In RPL this attack can be done by using the IPv6 UDP packet flooding. If many malicious nodes get coordinated, it results in Distributed Denial of Service attack; in this attack it is difficult to identify the malicious nodes.

6.9 Alteration and Spoofing Attack

6.9.1 Rank Attack

RPL has a strict rule about the node rank that "rank strictly increases in downward direction and decreases in upward direction". By changing rank value, an attacker can attract child nodes for selecting as parents or to improve some other metric, and can attract large traffic going towards the root. The consequences after the rank rule is broken are as follows.

- Un-optimized path gets created
- Optimized path may be interrupted, which means they exist but will never be discovered
- A loop can be created without any detection

6.9.2 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 bring inconsistencies in topology. The loop and rank inconsistencies created by the attack is located around the neighborhood of the attacker.

6.9.3 DIS Attack

DIS (DODAG Information Solicitation) is used by new node to receive the topology information before joining the RPL network. In this attack malicious node periodically send the DIS message to its neighbors. Upon receiving the message the receiver resets its DIS Timer assuming something went wrong with the topology around it. Also the receiver sends the DIS message indicating the sender is willing to join the network. Due to both way of sending DIS message leads to increase in end-to-end delay, more control overhead and hence energy harvesting.

VII. WORMHOLE ATTACK

In Wormhole attack there are two adversaries which are connected through a private line which is not part of the network [6]. The packets received by one of the attacker are sent through a private line to the attacker. Later, the attacker can tamper the data, messages or rebroadcast the packets, thereby utilizing the network resources and spreading fake information about route in the network. This type of attack can be launched even if the network uses authentication.

The symptoms of the Wormhole Attack are[10]:

- Packet Travel Time (PTT) is higher than normal
- The Delay per Hop will be higher and a sudden variation can be seen in it
- Round Trip Time of the packet will be higher than the normal
- Previously longer routes will now be reached in less number of hops, and two particular hops always repeat
- Node doesn't broadcast the RREQ received by it
- Node broadcast RREQ which is not received by broadcast
- Node attempts to perform DoS attack by flooding network with data packets.

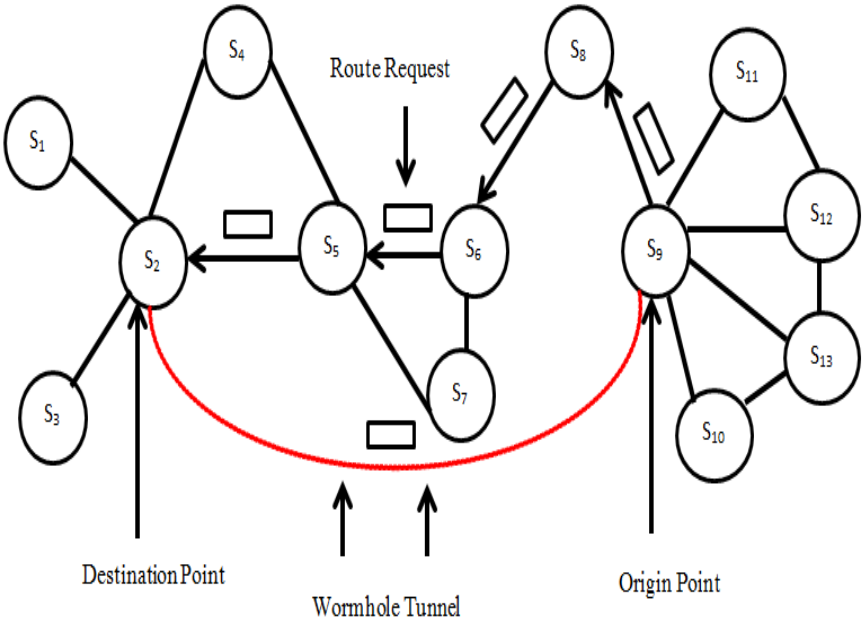

Figure 6. Wormhole attack

Wormhole attacks are of 3 types:

- Closed Wormhole – In closed wormhole the neighbor discovery beacons are tunneled between M1 and M2 without adding any self-information. The malicious nodes are external agents such as simple transceivers that can stay invisible for S and D.
- Half – open Wormhole – In half-open wormhole only one node is comprised node. The other node is simply an external agent. In such a case the beacon of the comprised node M_1 are tunneled towards the external malicious node M_2 and the beacons of the M_2 neighbors are tunneled back towards M_1
- Open Wormhole – In open wormhole both malicious nodes are comprised internal nodes participating to the routing protocol.

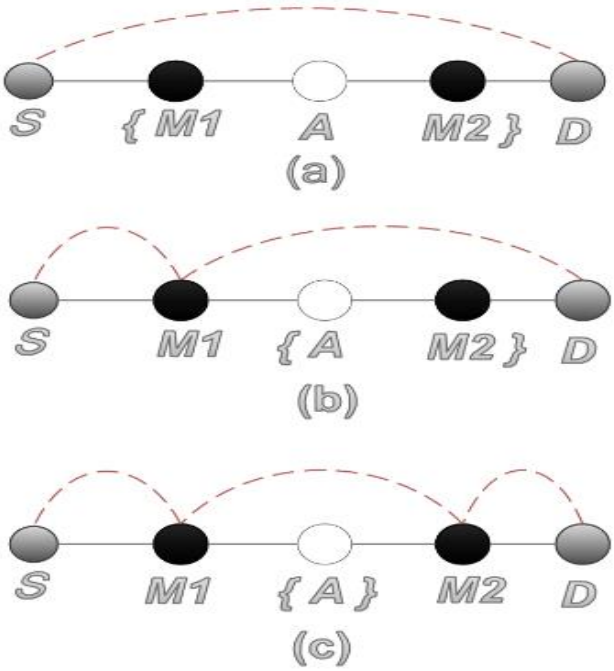

Figure 7. Types of Wormholes (a) closed (b) half open and (c) open wormhole [10]

Table 3. Summary of Attacks on Wormhole

Methods /Techniques	Tools	Protocol	Wormhole Detection	Wormhole Prevention	Accuracy
WIM/DSR [8]	--	--	Yes	Yes	Low false alarm
Merkle tree based authentication protocol[11]	Ns2	--	Yes	Yes	Boost in throughput, reduction in jitter and end-to-end delay
RTT-TC [16]	Ns2	AODV	Yes	No	High Detection Rate, Accuracy of Alarm
Packet Travel Time[17]	--	AODV / DSR	Yes	No	---
WADP [18]	Matlab	AODV	Yes	Yes	Free from false detection
Secure Routing Mechanism against Wormhole attack[19]	---	--	Yes	No	--
AIS using Honeypot [14]	Ns2	AODV/DSR	Yes	Yes	Robust, resilient to error, very little false alarm.

VIII. HONEYPOT METHOD

Honeypot is a trap to detect, capture and misguide the intruders who try to attack the system or gain unauthorized access to it. A honeypot is a highly flexible tool with applications in such area as network forensics and intrusion detection [15].

Honeypots are closely monitored network decoys serving several purposes that include the following

- They can distract attackers from more valuable machines on a network
- They can provide early warning about new attack and exploitation trends.
- They allow in-depth examination of adversaries during and after exploitation of honeypot.

Honeypots are a technology whose value depends on the "bad guys" interacting with it. All honeypot works on the same concept: nobody should be using or interacting with them, therefore any transactions or interactions with a honeypot are, by definition, unauthorized.

Honeypots can be classified based on their purpose (production, research and honeytokens) and level of interaction (low, medium and high).

Purpose of Honeypot

- Research Honeypot
- Production Honeypot

Level of interaction

- Low-Interaction Honeypots
- Medium-Interaction Honeypots
- High-Interaction Honeypots

IX. IDS (INTRUSION DETECTION SYSTEM)

An Intrusion Detection System (IDS) is a tool or mechanism to detect attacks against a system or a network by analyzing the activity in the network or in the system it-self [6]. Once an attack is detected an IDS may log information about it/or report an alarm. Hybrid IDS architecture is mostly suitable in IoT as it contains the resource constrained devices. The IDS system is categorized as follows:

9.1 Signature based IDS

Signature based detection match the current behavior of the network against predefined attack patterns. This approach is static and cannot detect new attacks unless their signature is manually added into the IDS.

9.2 Anomaly based detection

Anomaly based detection tries to detect anomalies in the system by determining the ordinary behavior and using it as a baseline. Any deviation from the baseline is considered as anomaly.

9.3 Host-based Intrusion Detection System (HIDS)

Host-based IDSs examine data held on individual computers that serve as hosts; they are highly effective for detecting insider abuses.

9.4 Network-based Intrusion Detection System (NIDS)

Network based IDS analyze data packets that travel over the actual network. These packets are examined and sometimes compared with empirical data to verify whether they are malicious or benign nature.

X. CONCLUSION

Security is a prime concern in any network. In this paper, we have undergone a survey on IoT, its architecture, protocol stack and its applications. With addition of new routing protocol that is RPL; additional attack came into scenario. Various mechanisms are proposed against the attack on RPL. The attacks need a detection and prevention mechanism. One of the methods Honeypot along with its pros and cons is also discussed in the paper. At last focus on IDS System is done. Future Enhancement is to perform the implementation of the techniques which are not yet evaluated.

REFERENCES

[1] Rita Maria Palattella et al., "Standardized Protocol Stack for the Internet of (Important) Thinngs," in *IEEE Communications Survey & Tutorials, Vol.15, No.3*, 2013, p. 1389.

[2] Mohamed Abomhara and Geir M. Koien, "Security and Privacy in the Internet of Things: Current Status and Open issues".

[3] Jorge Granjal, Edmundo Monterio, and Jorge Sa Silva , "Security for the Intrenet of Things: A Survey of Existing Protocols and Open Research Issues," in *IEEE Communications Survey & Tutorials*, 2015.

[4] Satish J. Kumar and Dhiren R. Patel, "A Survey of Internet of Things: Security and Privacy Issues," in *International Journal of Computer Application(0975-8887)*, March 2014.

[5] Zhengguo Sheng et al., "A Survey on the IETF Protocol Suite for the Internet of Things: Standards, Challenges, and Opportunities," in *IEEE Wireless Communications*, December 2013.

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

[7] Kuan Zhnag, Xiaohui Liang, Rongxing Lu, and Xuemin Shen, "Sybil attacks and their Defenses in the Internet of Things," in *IEEE INTERNET OF THINGS JOURNAL*, October 2014.

[8] Faraz Idris Khan, Taeshik Shon, Lee taekkyuem, and Kihyung Kim, "Wormhole Attack Prevention mechanism for RPL based LLN Network," *IEEE*, vol. 149, 2013.

[9] T Divya Sai Keerthi and Pallapa Venkataram, "Locating the Attacker of Wormhole Attack by using the Honeypot," in *International Conference on Trust, Security and Privacy in Computing an Communication*, 2012, p. 1175.

[10] Luis Fernando Garcia and jean Marc Robert, "Preventing Layer-3 Wormhole Attacks in Ad-hoc Networks with Multipath DSR," in *The 8th IFIP Annual Meiterranean Adhoc networking Workshop 2009*, 2009, p. 09.

[11] Mohammad Rafiqual Alam and Sun King Chan, "RTT-TC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET," *IEEE*, p. 991, 2010.

[12] Adel Saeed Alshamrani, "PTT: Packet Travel Time Algorithm in Mobile Adhoc Network," in *2011 Workshops of International Conference on Advanced Information Networking and Applications*, 2011, p. 561.

[13] Juhi Biswas, Ajay Gupta, and Dayashankar Singh, "WADP: A Wormhole Attack detection And Prevetion Technique in MANET using Modified AODV Routing Protocol," in *IEEE*.

[14] Tao Chen, Haiping Huang, Chen Zhengyu, Yiming Wu, and Hao Jiang, "A Secure Routing Mechanism Against Wormhole Attack in IPv6-based Wireless Sensor Networks," in *2015 Seven International Symposium on Parallel architectures, algorithms and Programming*, 2015, p. 111.

[15] Iyatiti Mokube and Michele Adams, "Honeypots: Concepts, Approaches and Challenges," *ACMSE*, p. 321, March 23-24, 2007.

[16] Dena Aldhobaiban, Khaled Elleithy, and Laiali Almazaydeh, "Prevention of Wormhole Attacks in Wireless Sensor Networks," in *2014 Second International Conference on Artificial Intelligence, Modelling and Simulation*, 2014, p. 287.