

Attacks and Security Issues in IoT Communication: A Survey

Apeksha Gajbhiye, Professor Devkant Sen

Department of Electronic and Communication
Technocrats Institute of Science and Technology
Bhopal, M.P. , India
apekshagajbhiye01@gmail.com

Abstract – Internet of Things influence our lives to go in a straightforward and simpler way, yet it additionally goes over numerous security issues. The security issues are likewise that this device once made can't be refreshed, the equipment changes are impossible after the execution we need to think before the usage anyway we can roll out improvements in the software field.. They form an Internet of Things (IoT) that will lead to a completely new set of applications revolutionizing the use of Information and Communication technology in various areas of our living. In this survey of attacks and security scheme some of the solution for different attacks is discuss with including cross layer routing attack in IoT. This paper presents the survey of different challenges and attacker effect. The routing procedure of RPL and security issues is discussed. The interconnectedness of the IoT networks, however, poses a significant risk since the systems will be subject to malicious attacks. An example is denial of service attacks precluding the devices from communicating with other stations. Therefore, security issues must be considered for the engineering and deployment of IoT networks. Security is required in WSN because attacker is consumes the useful energy of nodes i.e. necessary for communication in network. The cross layer attack is flooding the huge amount of packets in network and every node in network is capture and forwards these packets to next neighbor. The packets sending and receiving is consumes the lot of energy. The different previous security scheme function is to detect the attacker on the basis of attacker malicious activities and identified the routing misbehavior in network.

Keywords– Routing ,Attack, Security, Survey, IoT.

I. INTRODUCTION

IoT network is comprised of a suite of low power devices, the processing power and routing functions for data are limited. In addition, the routing protocol for an IoT network has to be modified to support mobile connectivity. The use of Internet of Things (IoT) enabled devices for military operations have gained traction in recent years due to its rapid speed to market and cost effectiveness [1]. From the smart homes and healthcare to wearable, the IoT connects almost all the facets of everyone's life. Different utilities can communicate and interact to provide different services.

This smart nature of things lead to the many applications like smart cities, smart agriculture, home automation, healthcare, military surveillance security etc[2]. RPL is a routing protocol based on distance vector, which is specially designed for low power, resource constrained network. The entire routing protocol is built through the interaction of ICMPv6 control messages across smart devices. The optimal path selection of RPL routing protocol is constrained by functions, different functions

can be designed for different scenarios to make the structure more flexible, the network more efficient and the network communication more stable. The RPL routing protocol can meet the rapidly fields changing of the network topology in a fixed state at a certain point, the whole network construct is a destination oriented directed acyclic graph (DODAG). The attacker in the network is not only degrades the routing performance but also injected the fake information or deliver unwanted packets continuously in network [3]. The RPL implementations do not enable secure operation modes. This leaves the door open to multiple attacks wherein a malicious node can manipulate contents of packets to adversely affect the network operation.

Existing routing protocols are not suitable to deal with these requirements [4]. The main RPL focus is to make the routing topology to be auto-optimized, while prevent any loops from happening. The loop prevention mechanism is based on the Rank concept to show the node relationship. Routing Protocol for Lowpower and Lossy Networks (RPL) is an open routing protocol standardized by the IETF ROLL [5].



Fig.1. Example of IoT.

The example of IoT is shown in figure 1 where the number of devices is controlled by single sensor or sensors are sharing the information among them to deliver receiver. The IoT is a system of inter-related computing devices, mechanical and digital machines, objects, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

A thing, in the Internet of Things, can be person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low. Any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. An increase in the number of smart nodes as well as the amount of upstream data the nodes generates, is expected to raise new concerns about data privacy, data sovereignty and security.

Practical applications of IoT technology can be found in many industries today, including precision agriculture, building management, healthcare, energy and transportation. Hatchedman attack [3] is that the malicious node manipulates the source route header of the received packets, and then generates and sends a large number of invalid packets with error route to legitimate nodes, which cause the legitimate nodes to drop the received packets and reply an excessive number of Error messages back to the DODAG root.

1. Network Characteristics

The traditional wireless networks like Sensor Network in IoT is comparable to devices that forming networks have the subsequent distinctive characteristics[6, 7] and constraints:-

2. Densely deployment

Sometimes IoT nodes are densely deployed and might be many orders of magnitude on top of that in a network. The densely deployed network is reliable but required more resources and constraint.

3. Battery-powered sensing element nodes:

The battery power is consumed for every activity done by sensor. Sensors are unit sometimes hopped up by battery and are deployed during a callous setting wherever it's very sturdy to alter or recharge the batteries. Strict energy utilization, calculation, and storage constraints: The battery utilization based communication is the critical task in sensor network. Sensors have extremely restricted energy, computation, and storage capabilities.

4. Self-configurable

Sensors are independently communicated with each other. Sensing nodes are sometimes arbitrarily deployed and separately section themselves into a communication network.

5. Unreliable sensor nodes

The sensors are unreliable in term of communication. If the node is participating in routing then they're out of range is break the communication and second is energy depletion. Since sensing element nodes are at risk of physical damages or failures because of its readying in harsh or hostile setting.

6. Data redundancy:

The sensor nodes in network collect huge amount of data and the nodes possible to deliver data same information that will to already evaluate. Thus, the data detected by multiple sensing element nodes usually have a particular level of correlation or redundancy.

7. Application specific

A sensors in network is typically designed and deployed for a particular application or a multiple tasks. The planning necessities of sensors in network modified with its application. The each sensor node energy time collect the information and complete their task.

8. Many-to-one communication manner

The collected by sensor nodes must be possible to deliver through the single sensor due to not identified the another sensor in range. In most sensor network applications, the data detected by sensing element nodes be due multiple supply sensor nodes to a selected single sink, exhibiting a many-to-one manner.

9. Frequent topology change

The sensor network is dynamic that means the topology changes frequently because of the node failures, damage, addition, energy depletion, or channel fading.

II. CHALLENGES IN IOT

There are various challenges [8, 9] that have to be considered while designing any protocol or architecture for the IoT. Some of them are described below:-

1. Massive Scaling:-

The smart devices being deployed in the network are large in number so, we need to give authentication, maintaining, protecting, use and support of such large things are major problems. Many of things in network will require their own energy source will energy scavenging and enormously low power circuits eliminate the need for batteries. Collection of data and its storing and usage of it may concern in massive scaling.

2. Architecture and Dependencies:-

As many things are connected to internet it is necessary to have an adequate architecture that permits easy connectivity, control, communications and useful applications. Coming to dependencies how will these objects interact in and across applications? Many things or set of things must be disjoint and protected from other devices. At other times it makes sense to share devices and information. One possible approach is to borrow ideas from smart phone world.

3. Big Data generated:-

In IoT there will exist a vast amount of raw data being continuously collected. It will necessary to develop techniques to convert raw data into usable knowledge. For example this can be more helpful in medical stream by monitoring the person heart rate, pulse, blood pressure and that raw data should be converted into usable knowledge by giving precautions to person or doctor like medical streams it can be implemented in many fields like industrial, home appliances.

4. Robustness

In IoT applications works on the basis of sensing, automation and computation platform. In this deployment it is common for devices to know their locations, have synchronized clocks, know their neighbour devices when cooperating and have coherent set of parameter settings such as consistency, sleep, awake schedules, appropriate power levels for communication.

5. Privacy and Security

Privacy is the most concern in IoT, the data which storing in cloud using big data should not be seen by any other person. To solve these problems privacy policies for each system should be specified. Once specified either the individual IoT applications must enforce privacy. Security attacks are problematic for the IoT because of the minimal capacity of things be used, the physical accessibility sensors, actuators and objects and the openness of the system, including the fact that most devices will communicate wirelessly. Identifying and naming of the object is also an important thing in IoT and use of wireless sensor networks plays a crucial role in IoT which may leads to security issues.

III. SECURITY ISSUES IN IOT

The security is the major concern in any network. Without security it is not possible to protect the data and useful information. The some of the security issues [10, 11] are:-

1. IoT Security-Data Encryption

Internet of things applications collect tons of data. Data retrieval and processing is integral part of the whole IoT environment. Most of this data is personal and needs to be protected through encryption. To address this IoT security issue you can use Secure Sockets Layer protocol or SSL wherever your data is present online. Websites already use SSL certification to encrypt and protect the user's data online. This is only half part of the equation other half is to protect the wireless protocol side. While data is being transferred wirelessly it needs encryption as well. Sensitive data like locations need to be available to be concerned user and no one else. Therefore make sure you use a wireless protocol with inbuilt encryption.

2. IoT Security- Data Authentication

After successful encryption of data chances of device itself being hacked still exist. If there is no way to establish the authenticity of the data being communicated to and from an IoT device, security is compromised. For instance, say you built a temperature sensor for smart homes. Even though you encrypt the data it transfers is there is no way to authenticate the source of data then anyone can make up fake data and send it to your sensor instructing it to cool the room even when its freezing or vice versa. Authentication issues may not be upfront but they definitely pose a security risk.

3. IoT Security-Side-channel Attacks

Encryption and authentication both in place still leave scope for side channel attacks. Such attacks focus less on the information and more on how that information is being presented. For instance if someone can access data like timing information, power consumption or electromagnetic leak, all of this information can be used for side channel attacks.

IV. ROUTING OVER LOW POWER AND LOSSY PROTOCOLS IN IOT

A Routing protocol is a communication system tasked with the responsibility of making intelligent routing decision during for forwarding of routing data among nodes. In sensor, there are two types of routing namely: Proactive and Reactive routing and protocols developed are based on any of these two systems. The Internet Engineering Task Force (IETF) quickly recognized the need to form a new Working group to standardize an IPv6-based routing solution for IP smart object networks, which led to the formation of a new Working Group called ROLL (Routing Over Low power and Lossy) networks in 2008[12]. The protocol was designed as a

standard for low power and lossy network, which includes all IoT sensor nodes. It is basically designed for the multipoint to point communication, but it can also support the point to point and point to multipoint communication. RPL is a proactive routing protocol, which operates by discovering routes as soon as the RPL network is started. The ROLL Working Group conducted a detailed analysis of the routing requirements focusing on several applications: urban networks including smart grid, industrial automation, home and building automation.

This set of applications has been recognized to be sufficiently wide to cover most of the applications of the Internet of Things. The objective of the WG was to design a routing protocol for LLNs, supporting a variety of link layers, sharing the common characteristics of being low bandwidth, lossy and low power. Thus the routing protocol should make no specific assessment on the link layer, which could either be wireless such as IEEE 802.15.4, IEEE 802.15.4g, (low power) Wifi or Powerline Communication (PLC) using IEEE 802.15.4

RPL is a Distance Vector IPv6 routing protocol for LLNs that specifies how to build a Destination Oriented Directed Acyclic Graph (DODAG sometimes referred to as a graph in the rest of this document) using an objective function and a set of metrics/constraints[13]. DAG—Directed Acyclic Graph. A directed graph having the property that, all the edges are oriented in such a way that no cycles exist. All edges are contained in paths oriented toward and terminating at one or more root nodes.

The objective function operates on a combination of metrics and constraints to compute the 'best' path. RPL forms a tree-like topology known as Destination Oriented Directed Acyclic Graph (DODAG), which contains only 1 root. The root node is also called as the sink node. Root node starts the formation of the topology broadcasting the DIO (DODAG Information Object) message. Node receiving the DIO message selects a preferred parent. Based on some metrics, rank value is calculated with respect to the parent rank value and other parameters. The preferred parent acts like a gateway for that node. If a node wants to forward a packet for which it does not have a path in its routing table, it simply forward it to its parent preferred parent who has a path either to the destination or its own parent for forward transmission until it gets to the final destination in the tree. Path selection is an important factor for RPL and hence uses multiple metrics for this purpose.

V. LITERATURE SURVEY

The previous work is done in field of secure IoT communication is mentioned in this section. The security from attacks is provides by each author and each reach is contribute to resolve this issue:-

In this paper [14], they have investigated how the attack on RPL Routing protocol degrades the end-to-end throughput of the application. We have exploited the Rank system of the RPL protocol to implement the attacks. We manipulated the rank of in RPL protocol, so our node in some manner modified the network topology. IoT sensor uses RPL protocol, and when the sensor node wants to transmit sensed information to its 6LowPAN gateway, it uses the RPL protocol to find the best route available to the destination. RPL protocol uses control messages to find the nearest neighbor who is having minimum hop count and rank concerning 6LowPAN gateway and makes a path between sender and receiver.

This approach centers on Intrusion Detection Systems (IDS) that help to retrieve various forms of network attacks for distributed systems, e.g., the denial of service attacks mentioned above [15]. IDS can be signature-based such that they check the network traffic for certain attack patterns. In contrast, anomaly based IDS try to find abnormalities in the overall behavior which may be an indication for attacks. Thus, unlike the signature-based IDS they can also detect previously unknown attacks but are often subject to "false positives", i.e., reports about incidents that are not attacks. Of course, a good IDS shall minimize the number of false positives but, one the other hand, detect as many real attacks as possible. Unfortunately, many IDS tend to demand a lot of communication overhead to coordinate the different nodes in a network. Moreover, the comparison with known signatures as well as the analysis of anomalies often afford complex computations that may exceed the abilities of smaller devices.

In this paper [16], they present the DIO (degradation-of-service) attack suppression attack, which can severely degrade the routing service in RPL. The DIO suppression attack induces victim nodes to suppress the transmission of DIO messages, which are the RPL messages necessary to build the routing topology.

This causes a general degradation of the routes' quality that can lead, eventually, to network partitions. Unlike other RPL attacks in the literature, the DIO suppression attack does not require the adversary to forge bogus RPL messages. It is sufficient that she periodically replays previously heard messages. The attack can thus be mounted without stealing cryptographic keys from legitimate nodes. The DIO suppression attack uses the replay technique, which is a classic attack technique, for a radically different purpose. Indeed, the replay technique is usually used to make a victim accept old information as new. On the other hand, in the DIO suppression attack it is used to make a victim believe that the routing information it is about to send is already being transmitted many times by other nodes. We show that the attack severely degrades the routing service, and it is far less energy expensive than a jamming attack.

In this paper [17], they propose a novel lightweight authentication scheme for heterogeneous WSNs in the context of IoT. The scheme authenticates each object and establishes a secure channel between the sensor node and the remote user. Our scheme uses once and keyed-hash message authentication (HMAC). It provides authentication with less energy consumption, protects the sensor node identity from disclosure, and terminates with a session key agreement between a sensor node and a remote user. The scheme provides also mutual authentication and a high security level against several attacks. When developing our novel lightweight mutual authentication and key agreement scheme for heterogeneous WSNs, we focused on the resource constrained architecture of WSNs and security requirements. We use the fifth authentication model. This model is the only one which initiates the authentication scheme by firstly contacting the specific object.

VI. CONCLUSION

The "things" of IoT refers to the intelligent devices that have communication and access to the internet, the equipment has the characteristics of large quantity, frequent switching and limited resource. Special routing protocol is need to manage and organize these smart devices for efficient and secure networks and to integrate it with the traditional internet. This survey of attacks and preventions is extremely helpful in field of engineering to gauge the network performance just in case of attack Wireless device network may be a quite in network. There a brand new quite internal attack known as hatchetman attack drain the energy of every device within the network, during this planned work a evil spirit attack is investigated and applicable methodology is planned for implementation for rising security and performance in network by distinguishing and removing suspicious node from the network. supported the recently developed techniques a replacement security technique is meant and enforced for simulating the impact of attack preparation and therefore the performance improvement once security theme implementation. In addition, for justifying the answer and their increased performance ancient routing protocol is needed to check with the developed routing protocol.

VII. EXPECTED OUTCOME

In future we tend to implement our planned Technique in NS-2 [18] and find malicious node that causes cross layer attack and take away the malicious node from the network. We have a tendency to conjointly compare our planned work with normal routing performance. We will detect cross layer attack on the basis of heavy flooding of packets and these packets are consumes the un-necessary resources like bandwidth and energy of other normal nodes because in every action perform by node is required

coordination of other nodes which is not possible w/o communication.

REFERENCES

- [1]. DOD's Environmental Research Programs, "Internet of things (IoT): Opportunities and challenges for implementation on dod installations," 2017.
- [2]. R. Benabdessalem, M. Hamdi, Tai-Hoon Kim, "A Survey on Security Models, Techniques, and Tools for the Internet of Things", IEEE. 7th International Conference on Advanced Software Engineering & Its Applications, 978-1-4799-7761-1/14 2014.
- [3]. Cong Pu, Tianyi Song, "Hatchetman Attack: A Denial of Service Attack Against Routing in Low Power and Lossy Networks", 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2018.
- [4]. T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, RPL: IPv6 routing protocol for low-power and lossy networks, RFC 6550, IETF, 2012.
- [5]. P. J. Vasseur and D. Culler, "Routing over Low Power and Lossy Networks (ROLL)," Internet Engineering Task Force (IETF), Tech. Rep., 2010.
- [6]. S. Li, L. Da Xu, and S. Zhao, "The Internet of Things: A Survey," in [Information Systems Frontiers], ©[Springer]. doi: [10.1007/s10796-014-9492-7], pp.243-299, 2014,.
- [7]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
- [8]. S.Singh and N.Singh, "Internet of Things (IoT):Security Challenges, Business Opportunities & Reference Architecture for E-Commerce," in Green Computing and Internet of Things (GCIoT), 2015 International Conference on. IEEE, 2015, pp.1577-1581.
- [9]. E. Alsaadi and A. Tubaishat, "Internet of Things : Features , Challenges , and," vol. 4, no. 1, pp. 1–13, 2015.
- [10]. S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security,privacy and Trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
- [11]. C Suchitra , C.P Vandana, "Internet of Things and Security Issues", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.1, pg. 133-139, January- 2016.
- [12]. J. Hui and J. Vasseur, The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams, RFC 6553 (Proposed Standard), Internet Engineering Task Force, Mar. 2012.
- [13]. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Sch• onw• alder, "Addressing DODDAG

- inconsistency attacks in RPL networks," in Proceedings of Global Information Infrastructure and Networking Symposium (GIIS'14), pp. 1-8, 2014.
- [14]. Vivek Kumar Asati, Emmanuel S. Pilli, S. K. Vipparthi, Shailesh Garg, Shubham Singhal, and Shubham Pancholi, "RMDD: Cross Layer Attack in Internet of Things," IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018
- [15]. Zeeshan Ali Khan and Peter Herrmann" A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things, IEEE 31st International Conference on Advanced Information Networking and Applications, 2017.
- [16]. Pericle Perazzo, Carlo Vallati, Giuseppe Anastasi, and Gianluca Dini DIO Suppression Attack Against Routing in the Internet of Things, IEEE Communications Letters (Volume: 21 , Issue: 11 , November 2017.
- [17]. Hamza Khemissa, Djamel Tandjaoui A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things, Wireless Telecommunications Symposium (WTS), 2016.
- [18]. The CMU Monarch Project, The CMU Monarch Extensions to the NS Simulator, URL: <http://www.monarch.cs.cmu.edu/>. Page accessed on February 20th, 2018.