Internet of Things Security

Apurva Bansal
(1310110069)
CSD 404 - Internet of Things
Shiv Nadar University

***Abstract*—This document is a study of most common security threats in Internet of Things and defense mechanism that can be used to prevent the network from these attacks. As Internet of Things provides greater insights to our increasingly connected lives it is not prone to the attacks that are happening in the world o f networks.**

Keywords—IoT (Internet of Things); Security; Defenses; Threats

I. INTRODUCTION

The Internet of Things (IoT) is a centralized structure which is moving towards a decentralized complex structure of smart devices.This is due to the fact that these changes promise new, improved and improved services and opportunities for business and market. The connections are day by day increasing and we can witness these changes or connections as developments for home automation and others are already taking place. These development will result in growing networking and enable cloud for all sorts of physical entities or devices from machines.The manufacturing is also been transforming as we are moving towards "fourth Industrial Revolution".This level of industrial development will lead to the establishment of smart factories which are powered and secured by smart semiconductor solutions capable of sharing information and optimizing processes across the entire value chain.

Since IoT provides greater insight in our increasingly connected lives , Iot emerges when threats to our data and systems have never been greater. In this paper we will discuss about the IT attacks and defenses that can be applied.

I. SECURITY

By security in the field of IT we mean a secure network such that it concerns with the safeguarding of connected devices and networks. Since keeping the network available 24 hours and its intended use is essential.Denial-of-service (DoS) attacks against such networks may permit real-world damage to the health and safety of people.

Although we usually use the term Security to refer to an adversary's attempt to disrupt, subvert, or destroy a network, a DoS attack is any event that diminishes or eliminates a network's capacity to perform its expected function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS.

Although attackers commonly use the Internet to exploit software bugs when making DoS attacks, here we consider primarily protocol- or design-level vulnerabilities.

An intrusion-detection system monitors a host or network for suspicious activity patterns such as those that match some pre-programmed or possibly learned rules about what constitutes normal or abnormal behavior.An adversary may possess a broad range of attack capabilities. A physically damaged or manipulated node used for attack may be less powerful than a normally functioning node. Subverted nodes that interact with the network only through software are as powerful as other nodes.

A layered network architecture can improve robustness by circumscribing layer interactions and interfaces. A clean division of layers may be sacrificed for performance in sensor networks, however, reducing robustness. Each layer is vulnerable to different DoS attacks and has different options available for its defense. Some attacks crosscut multiple layers or exploit interactions between them.

II. PHYSICAL LAYER

Nodes in a sensor network use wireless communication because the network's ad hoc, large-scale deployment makes anything else impractical. Base stations or uplink nodes can use wired or satellite communication, but limitations on their mobility and energy make them more scarce.

A. Jamming

It is a well known attack on wireless communication. Jamming of a node interferes with it's radio frequencies. Jamming also prevents the node to send or receive data to the remote hub station.

An adversary can disrupt the entire network with k randomly distributed jamming nodes, putting n nodes out of service where k is much less than n. For single frequency networks this attack is simple and effective.

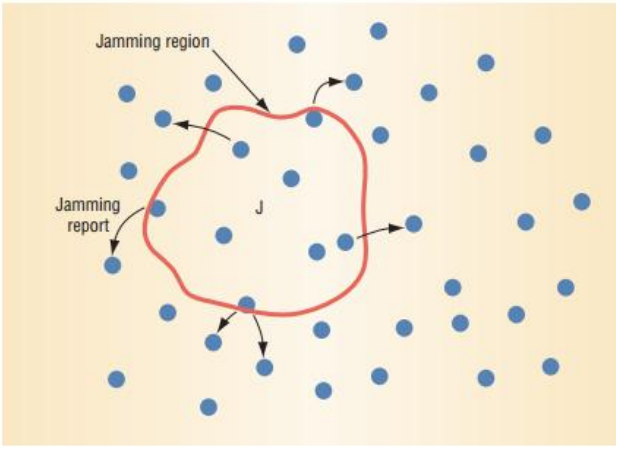

Fig: Nodes along the edge of a jammed region reports the attack to the neighboring nodes.

The defense mechanisms that can be used against jamming are *spread-spectrum* communication. Also the nodes can have a *low duty cycle* such that the problem of jamming could be avoided.

B. *Tampering*

An attacker can also tamper the nodes. By tampering we mean physically interfere with the node and interrogate it to retrieve the data like cryptographic keys to gain higher level access or to send false data.

One of the defenses against the problem of Tampering is *Tamper Proofing.* The second defense can be the use of effective *key management schemes*. These key management services are further classified into three categories. These are *trusted server schemes, self - enforcing schemes and pre - distribution scheme.*

III. LINK LAYER

The link or media access control (MAC) layer provides channel arbitration for neighbor-to-neighbor communication. Cooperative schemes that rely on carrier sense, which let nodes detect if other nodes are transmitting, are particularly vulnerable to DoS.

A. Collision

Adversaries may only need to induce a collision in one octet of a transmission to disrupt an entire packet. A change in the data portion would cause a check sum mismatch at some other receiver. A corrupted ACK control message could induce costly exponential back-off in some MAC protocols.

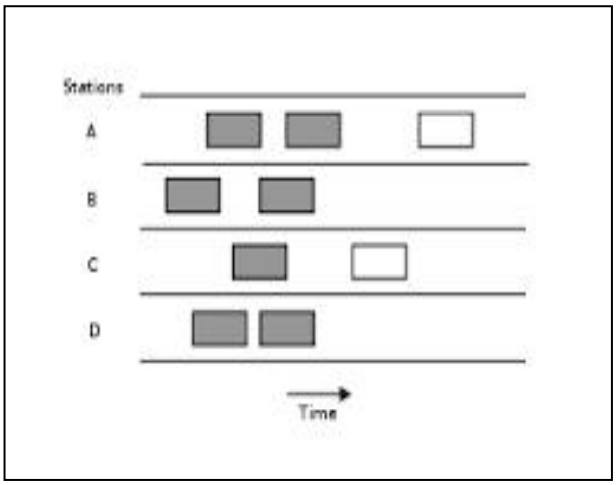

Figure : shows the collision of packets during the transmission.

One of the defenses against the problem of Collegian is *Error Correcting Codes.* For error correcting codes, methods of check sum or hamming distances can be used.

B. Exhaustion

A naive link-layer implementation may attempt re transmission repeatedly, even when triggered by an unusually late collision, such as a collision induced near the end of the frame. This active DoS attack could culminate in the exhaustion of battery resources in nearby nodes. This attack would compromise availability even if the adversary expended no further effort.

One solution makes the MAC admission control *rate limiting*, so that the network can ignore excessive requests without sending expensive radio transmissions. This limit cannot drop below the expected maximum data rate the network supports, though.

IV. NETWORK LAYER

The absence of pre-existing infrastructure in sensor networks means that most if not all the nodes will serve as routers for through traffic. Since every node is potentially a router, this adds new vulnerabilities to the network-layer problems experienced on the Internet. Routing protocols must be simple enough to scale up to large networks, yet robust enough to cope with failures that occur many hops away from a source.

A. Manipulation of routing Information

A more active attack, *misdirection*, forwards messages along wrong paths, perhaps by fabricating malicious route advertisements. As a mechanism for diverting traffic away from its intended destination, this DoS attack targets the sender. By misdirecting many traffic flows in one direction, the DoS attack can target an arbitrary victim.

One of the defenses against the problem of manipulating the router information is *Authentication.* The second defense can be Encryption.Encryption basically means that the data can be encoded and route through the network. Even though, the packet gets to a wrong routing path, the attacker cannot easily be able to decode the information.

B. Selective Forwarding

Selective forwarding means that the compromised node is behaving selectively in the network. For example, there are four nodes in the network. The odes are A,B,C and D. Node A is receiving the packets from the network and is now sending to node B, C and D. In selective forwarding, the compromised node lets say here node A, will behave differently for different node. There may be a case where node A sends all packets to node C. There maybe a case where node A sends a few packets to node B.

One of the defenses against the problem of selective forwarding is *Redundancy.*Redundancy can lessen the probability of encountering a malicious node. The network can send duplicate messages along the same path to protect against intermittent routing failure or random malice. The second defense can be Probing. Networks can use knowledge of the physical topology to detect black holes by periodically sending probes that cross the network's diameter.

C. Sybil Attack

Sybil attack can be described as a security attack where a node takes multiple identities at a time. This will send different values of the parameters in each duty cycle. This kind of attack can happen in location providing application sending multiple locations for a user in a small time interval.

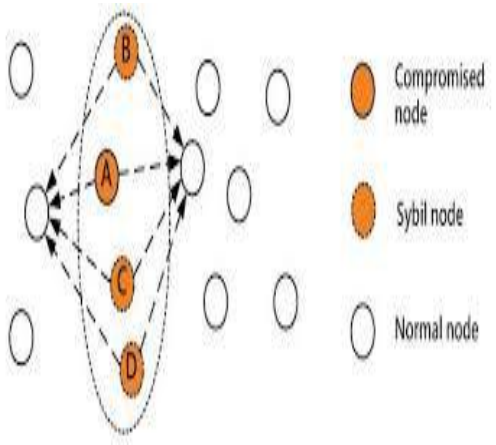

Figure : shows the compromised nodes due to a Sybil node.

The defense mechanisms that can be used against Sybil attack is *Authentication*. The process of authentication provides security in a sense. It does not give access to the sensors directly. It adds a sort of protection layer to it.

D. Sink Hole attack

Sinkhole attack can be described as a security attack where a node acts as a sink. This compromised node will create a region around it equivalent to its transmission region. All the nodes or sensors in or nearby region of this circle will get affected. This compromised node will extract the information from all those nodes or sensors and sink it. Thus leaving the network in an incomplete state.s

The defense mechanisms that can be used against the Sybil attack is *Authentication*. The process of authentication provides security in a sense. It does not give access to the sensors directly. It adds a sort of protection layer to it.

V. TRANSPORT LAYER

This layer manages end-to-end connections. The service the layer provides can be as simple as an unreliable area-to-area any cast, or as complex and costly as a reliable sequenced-multicast byte stream. Sensor networks tend to use simple protocols to minimize the communication overhead of acknowledgments and re transmissions. Protocols that provide sequencing share many DoS vulnerabilities with the Internet transmission control protocol.

A.Flooding

Protocols that must maintain state at either end are vulnerable to memory exhaustion through *flooding*. As in the classic TCP SYN flood,15 an adversary sends many connection establishment requests to the victim. Each request causes the victim to allocate resources that maintain state for that connection.

Limiting the number of connections prevents complete resource exhaustion, which would interfere with all other processes at the victim. However, this solution also prevents legitimate clients from connecting to the victim, as queues and tables fill with abandoned connections. Protocols that are connection-less, and therefore stateless, can naturally resist this type of attack somewhat, but they may not provide adequate transport-level services for the network.

The defense mechanisms that can be used against the problem of flooding is Client puzzle.This defense requires clients to demonstrate the commitment of their own resources to each connection by solving *client puzzles*.16 The server can create and verify the puzzles easily, and storage of client-specific information is not required while clients are solving the puzzles. Servers distribute the puzzle, and clients wishing to connect must solve and present the puzzle to the server

before receiving a connection. An adversary must therefore be able to commit far more computational resources per unit time to flood the server with valid connections. Under heavy load, the server could scale the puzzles to require even more work by potential clients.

B.Desynchronization

An existing connection between two end points can be disrupted by *desynchronization*. In this attack, the adversary repeatedly forges messages to one or both end points. These messages carry sequence numbers or control flags that cause the end points to request re transmission of missed frames. If the adversary can maintain proper timing, it can prevent the end points from exchanging any useful information, causing them to waste energy in an endless synchronization-recovery protocol.

One counter to this attack *authenticates* all packets exchanged, including all control fields in the transport protocol header. Assuming that the adversary also cannot forge the authentication mechanism, the end points could then detect and ignore the malicious packets.

VI. OTHER ATTACKS

A. Clone attack

In a clone attack an adversary node is created that behaves exactly like the original node. They both are linked so that the attacker can retrieve the sensitive information to gain access to the higher level. Also this can update fake data to the remote data station.

The defense mechanisms that can be used are *Limiting the connection numbers* so that the damage can be minimized. The other defense mechanism is *Client puzzle.*

Acknowledgment

I would like to express my gratitude to Prof. Divya Lohani for giving us the opportunity to write a technical write up on the Internet of Thing for Security purposes. This task has broaden my understanding of IoT and I am able to understand IoT better.

REFERENCES

[1] http://www.infineon.com/cms/en/applications/smart-card-and-security/internet-of-things-security/

[2] https://blackboard.snu.edu.in/bbcswebdav/pid-20896-dt-content-rid-151695_1/courses/CSD-404-MO16/Kortuem.IEEEInternet2010.Camera.pdf

[3] https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things

[4] https://safenet.gemalto.com/data-protection/securing-internet-of-things-iot/

[5] http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

[6] https://www.google.co.in/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwjIoa_gp9jQAhXLqI8KHYSwB48QjRwIBw&url=http%3A%2F%2Fwww.keyword-suggestions.com%2Fc3liaWwgYXR0YWNr%2F&psig=AFQjCNFLsOvt_CyknQrmJSjYeQFigzn-Lw&ust=1480864350078989

[7] https://www.google.co.in/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwj-5-bjp9jQAhWKQo8KHSYJBw8QjRwIBw&url=https%3A%2F%2Fen.wikibooks.org%2Fwiki%2FCommunication_Networks%2FError_Control%2C_Flow_Control%2C_MAC&psig=AFQjCNEja-JrO6hcyu4xfnVoZjrAMOPkqg&ust=1480864355578738

[8] https://www.comsys.rwth-aachen.de/fileadmin/papers/2011/2011-heer-iot-challenges.pdf