A Study on Layer Wise Attacks on Service Oriented Architecture in Internet of Things and Their Defensive Mechanisms

A. Vinothini*, G. Padmavathi

Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India

DOI: 10.23956/ijarcsse/SV7I5/0118

Abstract—The Internet of Things (IoT) describes a worldwide network of intercommunicating devices. IoT is considered as part of Internet and the future will comprise billions of intelligent and communicating ‘things’. The future of the Internet will consist of heterogeneously connected devices that will further extend the borders of the world with physical entities and virtual components. Internet of Things (IoT) will empower the connected things with new capabilities. In this study, the applications, challenges, service oriented architecture (SoA) are detailed. Firstly, the various applications are discussed, secondly, the challenges of IoT are discussed, and thirdly, service oriented architecture concepts and the attacks on SoA are discussed. Finally, the defense mechanisms for SoA layer attacks are summarized and compared.

Keywords—IoT Applications and Challenges, Service oriented Architecture (SoA), Attacks in SoA layers, Defense Mechanisms for SoA layer attacks.

I. INTRODUCTION

"Internet of Things" IoT in short form deals with devices that use electronic sensors embedded in it and are connected to the Internet. The connection of physical things to the Internet makes it possible to access the remote sensor data and to control the remote systems. Internet of Things is the network of physical things, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and the network connectivity, which enable these objects to collect and exchange data[1]. Internet of Things allows objects to be sensed and controlled remotely across the existing network infrastructure, creating the opportunities for more-direct combination between the physical world and computer-based systems resulting in improved efficiency and accuracy. In order to understand their significance better, an attempt has been made to discuss about the applications and challenges of IoT. Out of many challenges observed, security of the service oriented architecture is considered important as SoA creates the platform over which the entire system is defined and operated. The specific attacks on SoA are identified and their countermeasures are listed and compared. The rest of the paper is organized as below:

Chapter 2 discusses about the Service oriented Architecture (SoA).
Chapter 3 discusses about the attacks on SoA layers.
Chapter 4 discuss about the Defense Mechanisms for SoA layer.
Finally Chapter 5 conclude the paper.

1.1 Applications and Challenges in IoT

There are several applications where IoT can be applied effectively. Some of them are Agriculture, Healthcare, Retail, Transport, Environment, Supply Chain Management, Infrastructure monitoring etc. Some of them are shown in fig.1.

![Fig.1.Applications of IoT](image-url)
The important challenges in IoT are security, privacy, interoperability, regulatory, legal, right issues, and general issues. Of the general challenges, interoperability issues are important for the adoption of IoT devices [5]. Today, the technology that offers promising situation to interoperability issues is Service oriented Architecture (SoA).

Fig.2. Challenges in IoT

The objective of the paper is to explore the attacks on service oriented architecture layers in IoT. Security attacks on SoA layers and the defense mechanisms for attacks in different layers of SoA are discussed.

II. SERVICE ORIENTED ARCHITECTURE (SOA)

A Service-Oriented Architecture (SoA) is imperative for the service providers and users in any authentication system [2]. The SoA challenges are discussed below. They are:

- Service identification
- Service location
- Service domain definition
- Service packaging
- Service orchestration
- Service routing
- Service governance
- Service messaging standards adoption
- Security

Security is considered as a very important challenge both at IoT level and its operations level especially SoA. Security in SoA is not a simple concept. It is defined under various layers. SoA ensures the interoperability between heterogeneous devices in multiple ways which consists of four layers with the distinguished functionalities as below:

- **Sensing Layer**: Sensing layer is integrated with available hardware objects to sense the position of things.
- **Network Layer**: Network Layer is the framework to support over wireless or wired connections among the things.
- **Service Layer**: Service Layer is to create and manage services required by users or applications.
- **Interfaces Layer**: Interfaces Layer consists of the interaction methods with users or applications [7].

Security is considered important as SoA is associated with various layers and each layer is exposed to different types of attacks. Specifically, it is imperative to study the attacks on SoA layers. The next section discusses the various attacks based on the true surveys of SoA shown in fig.3.

III. ATTACKS ON SOA LAYERS

Fig.3. Attacks on SoA layers

2.1 Sensing layer

First, anybody including adversaries can touch the sensors. Thus, the physical attacks including theft, loss, destroy, must be considered. Second, the confidentiality and integrity of data must be protected. That is, the data stored
or gathered in sensors (including tags), e.g., deposit balance or living blood pressure, are very sensitive, thus the reading and modifications to these data must be authorized even audited [2].

2.2 Network layer

The role of networking layer is to connect all things together and allow things to share the information with other connected things [2]. To design the networking layer in IoT, designers need to address issues such as network management technologies for heterogenous networks (such as fixed, wireless, mobile, etc.), energy efficiency in networks, security, and privacy. Some of the common network layer attacks are:

a) Wormhole Attack

In the wormhole attack, attacker records packets at one location in the network, channels them to another location, and retransmits them into the particular network.

b) Sybil Attack

In the Sybil attack, the adversary sensor node assumes the multiple identities to all other sensor nodes in the WSN. This has reduced the effectiveness of WSN. A fake node appears at several places at same time. Sybil attacks are prevented by changing the security keys and resetting the network devices.

c) Sinkhole Attack

Here an attacker makes a compromised node look more attractive to adjacent nodes by unfaithful routing information. Malevolent sensor nodes work as a black hole to attract the entire traffic of the network. Sinkhole attack is also called as Black hole attack.

d) Selective Forwarding

In the multi-hop networks, all nodes exactly forward the received data, but the attacker develops a malevolent sensor node which does selective forwarding of only certain data and drops the other data.

e) Hello Flood

Several routing protocols in WSN are required to broadcast HELLO packets to their neighbors. The sensor node has to accept the messages that are within the radio range of the sender. Sometimes a laptop-class-attacker can spread routing or other messages with appropriate broadcast power and encourage all other neighboring nodes in the network to receive packets.

f) Acknowledgement Spoofing

Acknowledgements are required to be sent when a routing algorithm is used in a sensor network. An adversary node can spoof the acknowledgments of an overheard packets meant for adjacent nodes to supply fake message to those adjacent nodes [3].

2.3 Service layer

Service layer relies on the middleware technology, which is a key enabling service for applications in IoT. The middleware technology provides a cost-effective platform, where the hardware and the software platform can be reused. Service APIs provide the interactions between services required by the users. The service layer attacks are dived into three types. They are listed below:

a) Web Services Description Language (WSDL) scanning

A Web service’s WSDL statement advertises its operations, parameters and network bindings. Some of these (internal) operations are to be used only by the service provider, for example, administrative operations. The rest of the operations (external operations) can be invoked by any service consumer. As the Web services end point is available in its WSDL statement, an attacker can try to guess its internal operation’s name and can invoke it via the endpoint. Such an attack is called WSDL scanning.

b) Cross-Site Scripting

Cross-Site Scripting attacks are the type of injection, in which malicious scripts are introduced into benign and trusted web sites. These attacks occur when an attacker uses a web application to send the malicious codes. It is generally in the form of a browser side script, to a different end user. Flaws that are allowed by these attacks to succeed are widespread and it occurs anywhere a web application uses the input from a user within the output it generates without validating or encoding it.

c) Injection

All favourite category of application attack is injection attack. Here the attackers modify a back-end statement of command through un-sanitized user input.
2.4 Interface Layer

IoT involves many types of devices. These devices are provided by different vendors and hence do not always comply with the same standards. This is shown in fig. 3. The interface layer attacks are further classified under two types namely, wired network and wireless network as shown in fig. 4.

![Interface layer Attacks](image)

**a) Wired network**

A wired network connects devices to the Internet or other networks using cables. The most common wired networks use the cables connected to Ethernet ports on the network router on one end and to a computer or other device on the cable’s other end.

- **Content Address Memory (CAM) table exhaustion attacks**
  The data link layer addresses data packets based on the destination of hardware’s physical Media Access Control (MAC) address. Switches within the network maintain the Content Address Tables (CATs) and map the switch’s ports to specific MAC addresses. A CAT Table Exhaustion Attack basically turns a switch into a hub. The attacker floods the CAT table with new MAC-to-port mappings until the table’s fixed memory allotment is full.

- **Address Routing Protocol (ARP) spoofing**
  At the data link layer, a logical IP address is assigned by the network layer and it is translated into a physical MAC address. In order to ensure the reliable data communications all switches in the network must maintain an up-to-date table for mapping logical address (IP) to physical (MAC) addresses. In an ARP spoofing attack, the adversary transmits the IP address of the machine which is to be attacked along with its own MAC address.

- **Dynamic Host Configuration Protocol (DHCP) starvation**
  In a DHCP starvation attack, once the adversary receives the IP address and lease period from the DHCP server, the adversary does not respond with the confirmation. Instead, the adversary floods the DHCP server with IP address requests until all addresses within the server’s address space have been reserved. At this point of period, any host wishing to join the network will be denied access, resulting in Denial of Service (DoS) attack, a very important attack which leads to series of attacks.

**b) Wireless networks**

Wireless networking is a method by which homes, telecommunication networks and enterprise (business) installations avoid the costly process of introducing the cables into a building, or as a connection between various equipment locations.

- **Hidden nodes**
  Here, Node A begins the transmission where Node B has to wait for the transmission. Although it cannot directly communicate with Node A, i.e. Node A is a hidden node, it knows to wait based on its communications with the access point. An attacker can exploit this functionality by flooding network with CTS (Clear to Send) messages.

- **Deauth (De-authentication)**
  Any client entering a wireless network first authenticates with an access point (AP) and is after associated with that access point. When the client leaves the network, it sends a de-authentication, or deauth, message to disassociate with the access point. An attacker can send deauth message to an access point tied to client IP addresses. Table 1 shows the classification of attacks in different layers of SoA [2].

<table>
<thead>
<tr>
<th>Layers</th>
<th>Attack Type</th>
<th>Mode of Attack</th>
<th>Result of Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensing Layer</td>
<td>Eaves dropping</td>
<td>By receiver tuning to proper frequency</td>
<td>Reading messages by unintended receiver</td>
</tr>
<tr>
<td></td>
<td>Jamming</td>
<td>By malicious node with known</td>
<td>Prevents reception of legitimate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>communication frequency</td>
<td>packets</td>
</tr>
<tr>
<td></td>
<td>Active interference</td>
<td>Blocks the communication channel</td>
<td>Change order of messages</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Black hole attack</td>
<td>Fake optimum route message</td>
<td>Loss of confidential information on</td>
</tr>
<tr>
<td></td>
<td>Rushing attack</td>
<td>Subvert route discovery process</td>
<td>packet</td>
</tr>
<tr>
<td>Service Layer</td>
<td>Malicious code attack</td>
<td>Viruses worms</td>
<td>Attack to OS</td>
</tr>
<tr>
<td></td>
<td>Repudiation attack</td>
<td>Denial of participation in parts of</td>
<td>Communication failure</td>
</tr>
</tbody>
</table>

Table 1: Classification of Attacks in SoA layer
Most of the attacks discussed above are malicious in nature. This chapter discusses about the various defense mechanisms for malicious attacks. The fig. 5. Shows the defense mechanism for SoA layers.

IV. DEFENSE MECHANISMS FOR SOA LAYER ATTACKS

The different defense mechanisms for SoA layer attacks are shown in fig.5.

4.1 Sensing layer
The security mechanisms are basically used to detect, prevent and recover from security attacks. A wide variety of security schemes can be invented to counter the malicious attacks. This is further categorized as high-level methods and low-level methods [3]. This is shown in fig.6.

4.2 Network layer
In network transport protocols, reliability deals with delivering each segment generated at the source successfully to the eventual destination. Reliability could be attained by detecting the dropped packets and retransmit the packets to significant sources. The network layer attacks are divided into five types. They are listed below:
a) Wormhole attack prevention

The mechanism to defend the wormhole attack is called DAWWSEN. It is a proactive routing protocol which is based on the structure of a hierarchical tree where the base station is the root node, and sensor nodes are internal nodes or the leaf nodes of the tree.

b) Sybil prevention

The mechanism to prevent against Sybil attacks is to utilize the identity certificates. The setup server assigns each sensor node to some unique information before the deployment. Identity certificates to bind the node’s identity and assigns unique information to it and then downloads this information of the node.

c) Sinkhole attacks prevention

Sinkhole attacks are very difficult to prevent against. One class of protocols resistant to these attacks is geographic routing protocols. These protocols construct a topology on demand using only localized interactions and information than without initiation from the base station.

d) Selective Forwarding attack prevention

Selective forwarding attacks can be used to counter these multipath routing. Messages routed over paths where the nodes are completely disjoint and are completely protected against the selective forwarding attacks. The compromised nodes have to dynamically choose a packet’s next hop probabilistically from a set of possible candidates to reduce the chances of an adversary gaining complete control of a data flow.

e) Hello flood attacks prevention

This attack can be avoided by checking the both the directions of a link, so that nodes ensure that they can reach their parent within one hop.

4.3 Service layer

This layer creates and manages services. It provides services to satisfy user needs [4]. The service layer attacks are divided into three types. They are listed below:

a) WSDL Scanning

➢ It is important to protect the WSDL file or provide limited access to it.
➢ Review the functions exposed by the WSDL interface (especially if you have to use a tool to generate it). Make sure that none of them are vulnerable to injection.

b) Cross site scripting

The following are general approaches to prevent cross-site scripting attacks:

• Encode output based on the input parameters.
• Filter input parameters used for special characters.
• Filter output based on input parameters for special characters.

c) Preventing SQL Injection Attacks

• Enterprise-class security against known and emerging attacks.
• Solutions for Hosting, Enterprise and Small or Medium-Sized Business.
• It supports multiple platforms and technologies - IIS, Apache, and Cloud.

4.4 Interface layer

The interface layer provides interaction methods to users and other applications and it includes wired and wireless networks. The interface layer attacks are divided into two types. They are listed below:

a) Wired network

The wired network security mechanisms are divided into two types. They are listed below:

• CAT table exhaustion detection
• ARP Spoofing

• CAT table exhaustion detection

Detecting a CAT Table Exhaustion Attack is a logical starting point. As it is mentioned, a CAT Table Attack attempts to overflow a switch’s table of MAC to IP translations by flooding it with excessive sources. Thus, it has to detect it, and needs at a logical point to observe it like a span port on the switch or a passive network tap en route to the switch. To detect this attack, one needs to simply or observe some threshold number of different MAC addresses during a specific period of time to consider excessive.
After sniffing each packet, Ethernet is stripped off the layer and MAC address is added to an array. Attack detection is executed by setting the middle for the number of addresses received in a minimum time frame secretly.

- **ARP Spoofing**
  The method of port security can prevent MAC flooding and cloning attacks. However, it does not prevent any ARP spoofing. Port security validates the MAC source address in the frame header, but ARP frames should contain an additional MAC source field in the data payload, and the host uses this field to populate their ARP cache. Some methods are used to prevent the ARP spoofing are listed below.
  - Static ARP
  - Intrusion Detection System
  - Dynamic ARP System
  - DHCP attack detection

- **Static ARP**: One of the recommended action is to employ the static ARP entries in the host ARP table. Static ARP entries are permanent entries in the ARP cache. However, this method is impractical. Also, it does not allow the use of some Dynamic Host Configuration Protocol (DHCP) as a static IP and its needs to be used for all hosts in the network.

- **Intrusion Detection System**: Intrusion Detection System (IDS) is a defense mechanism configured to detect the high amounts of ARP traffic. However, IDS is prone to reporting the false positives.

- **Dynamic ARP Inspection**: This is a method of preventing ARP spoofing and is similar to DHCP snooping. It uses the trusted and un-trusted ports. ARP replies are allowed into the switch interface and are available only on trusted ports. If an ARP reply comes to switch from an un-trusted port, the contents of the ARP reply packet is compared to DHCP binding table to verifying its accuracy. If the ARP reply is not valid, then ARP reply is dropped, and the port is disabled.

- **DHCP attack detection**
  For wired access, port security can currently prevent a DHCP starvation attack that is launched from a PC and connected to a switch that is using a tool called as Gobbler. The inability of the attack to succeed is due to the limitation of tool than the mitigation that can offer by port security.
  The only reason such as an attack fails is that Gobbler uses a different source of MAC address to generate a different DHCP request and can be mitigated by port protection. Though, if an attacker is able to use their MAC address in the Ethernet packet and simply changes the MAC address in the DHCP payload using a field called chaddr, port security would not stop the attack. In this case, DHCP snooping must be enabled and configured to verify a source of MAC address when the frame matches the client address field in DHCP packet payload.

**b) Wireless network**

The wireless network security mechanisms are discussed below [6].

- **Hidden nodes**
  The methods that can be employed to solve hidden node problem are:
  - Increase the Transmitting Power from the Nodes
  - Use omni-directional antennas
  - Remove obstacles
  - Move the nodes from their current position
  - Use protocol enhancement software
  - Use antenna diversity

- **Deauth flood detection**
  Deauth is used to detect wireless attacks. Again, one can specify a threshold of deauth frames that are considered flooding. Another option is to list hardware addresses of the machines and watch a deauth messages against them specifically. The detection of a significant deauth attack to disrupt service might suggest that one should consider and replace the wireless infrastructure with a RADIUS compliant solution that could be used as a management frame to prevent spoofing frames such as the deauth frame. Table 2 discusses the attacks in different layers and their defense mechanisms.

<table>
<thead>
<tr>
<th>Layers</th>
<th>Attacks</th>
<th>Techniques adopted</th>
<th>Defense Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensing Layer</td>
<td>Denial of Service</td>
<td>Priority Messages</td>
<td>At the time of intermittent jamming, it is sent by the node to the base station for reporting the attack occurrence.</td>
</tr>
<tr>
<td>Tampering</td>
<td>Tamper Proofing</td>
<td>Vaporize memory contents to prevent information leakage.</td>
<td></td>
</tr>
<tr>
<td>Radio Interference</td>
<td>Symmetric key Algorithm</td>
<td>If sensor nodes use wireless or infrared communication modes, they can change the mode of communication.</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Attacks in SoA layers and Defense Mechanisms
### Network Layer
- **Spoofed routing**
  - Information Selective forwarding
  - Egress filtering Monitoring
- **Ack. Flooding**
  - Bi-directional link verification
- **Byzantine Attack**
  - Secure network coding

**It is confirmed by this outbound filter that assigned and allocated IP address leaves the network. For proper routing behaviour detection, nodes also monitor their neighbours.**

**It confirms that a link is used equally for both directions.**

**It combines all-or-nothing transform with polynomial hash function.**

### Service Layer
- **Overwhelming sensors**
  - Sensor tuning
- **Jamming**
  - Collision
  - Error Correcting Codes
  - Receiver introduces some penalty to the next back-off value of the sender, if the sender’s misbehaviour is found for manipulation of back-off values.
  - Watchdog is used on every node to check whether neighbours of a node either forwarding all packets or not.
- **Traffic manipulation**
  - Misbehaviour detection techniques
  - Back-off value
  - watchdog
- **Exhaustion**
  - Rate limitation
- **Interrogation**
  - Anti-replay Protection
  - When packet arrives, sequence numbers are traced.

### Interface Layer

**IV. CONCLUSION AND FUTURE ENHANCEMENT**

In the past few years, IoT has developed rapidly and a large number of enabling technologies are proposed. Service oriented architecture (SoA) in IoT use loosely coupled software entities that implement a single software function. These software services are dynamically combined to form ad hoc applications. In regards to the Internet of Things, SoAs have two main limitations. This paper discusses about the attacks in SoA layers and defense mechanism for SoA layer attacks. In future we can identify the defense mechanism of any attacks practically.

**REFERENCES**


