MAC address based Sensor Network Authentication: Survey

Sunghyuck Hong¹, Kyungil Ko²
¹ Div. of Information and Communication, Baekseok University, Cheonan, Republic of Korea
² Div. of Business and Commerce, Baekseok University, Cheonan, Republic of Korea

Abstract - As the interest in the Internet has increased, various security technologies suitable for the Internet have been researched. Especially, in the device sensor network area, the use of low-end devices has been increased and diversified due to the nature of things Internet. However, it is difficult to apply security technologies such as current authentication technology to low-power and low-power devices, and security threats have also increased. Therefore, the internal authentication protocol on the sensor network communication of the Internet of things is being studied. In this paper, we propose an improved authentication protocol for sensor networks in object internet environment by analyzing the vulnerability of authentication protocol based on secure and lightweight protocol.

Keywords: IoT protocol, Secure Networks, IoT Networking, Device authentication

1 Introduction

Nowadays, because information about IoT is overflowing, what exactly is IoT. The dictionary definition of IoT Human beings, objects, and services. Intelligent relationships such as sensing, networking, and information processing, without intervention The object space network that forms the object space. The main technologies for realizing this kind of internet are as follows.

2 SENSOR TECHNOLOGIES

2.1 Sensing Technology

Sensor technology is a tool that collects information instead of human senses. The sensor technology has developed so that the human senses can not recognize it. Typically, sensors that are frequently used determine the presence or absence of objects. There are different optical digital sensors and analog sensors that discriminate temperature, humidity, distance, etc. Nowadays, sensors that determine speed can be used in advanced devices such as smartphones, and it is expanding its possibilities [1-3].

2.2 Network Infrastructure

There are WiFi, 3G / 4G / LTE, Bluetooth, Ethernet, serial communication, Zigbee, WPAN, BCN, which are well-known communication methods as a communication device constituting the network of Internet [4-6].

2.3 IoT Interface skill

Service interface technology is the role of storing, processing, and converting information. This includes big data technologies that store, analyze and process vast amounts of information obtained using various sensors. In addition to analyzing and processing information obtained from the present time, data mining technology extracts valuable information from past accumulated data. Also, the area of personal privacy and security of information are also included in the service interface technology [7].

3 FUTURE OF IOT

Cisco, a global communications company in the United States, estimated the value of enterprises on the Internet over the next decade at $ 14.4 trillion. Also, Gartner will connect to the Internet in 2015.

The number of devices is estimated at 4.9 billion, which will increase to 25 billion by 2020. Countries are investing at the national level to prepare for the Internet of Things. In 2009, China announced the Sensor Network Information Center, the 2010 Intelligence Communication Center [8].

The European Union announced an action plan for the specific implementation plan of IoT in 2009. In particular, the UK announced its plan to increase the Internet development fund of about 45 million pounds and to expand the technology investment to £ 100 billion in IoT by 2025 Announced plans to do.

In 2008, the United States had selected IoT as one of the six major destructive innovation technologies that could affect national competitiveness by 2025 and is focusing on establishing a super-connection infrastructure that will expand existing communications infrastructure to IoT. Japan is promoting IOT-related policies from the early 2000s. In 2013, the Ministry of Internal Affairs and Communications launched the ICT Growth Strategy Meeting and established a development strategy using ICT that includes Smart Town, Smart Grid, and Remote Monitoring [9].
In this section, the vulnerability that can occur in the call. A spoofing attack is an attack which is spoof address or identity. When you are done with the protocol, it is an attack to illegally obtain an authentication key. In the sensor network, After storing the elements used in the procedure, it is an attack that is reused and authenticated in the authentication procedure. The authentication key guessing attack is the attacker 's User-to-sensor and sensor-to-sensor authentication procedures. Stores elements transmitted and received by the user, To find the same key as the final agreed upon authentication key [10].

A denial of service attack is an attack that involves an attacker. This is an attack in which the authentication service which is denied by intercepting the response even when the sensor or the user requests the authentication. Privacy infringement is the authentication procedure on the sensor network. The entity participating in the communication from the element transmitted. It is exposed and infringes privacy.

5 Proposed work

To prevent hacking attacks from the malicious sensor network, each sensor must have its authentication. Authentication is the first step of security procedures. This research work proposed MAC address based authentication in sensor networks. Fig. 1 shows how to spoof legitimate users on network networks.

Fig. 1 is a defense for Sybil attack using different radio channel. There are legitimate users and one attacker node among them. Registration - To prevent the Sybil attack, any node could check the list of “known-good” identities to validate another node as legitimate. Position Verification - the network verifies the physical position of each node. Sybil nodes can be detected using this approach because they will appear to be at the same position as the malicious node that generates them. This is an example of anti-hacking skill for Sybil attack.

To prevent Sybil Attack, each sensor must have its own authentication scheme. MAC address is a unique address which assigned from IEEE network card manufacturers. A Media Access Control (MAC) address-based authentication has been proposed to compensate for the weakness of a self-signed certificate-based authentication [11]. An MAC-based address is matched with an IP address. The IP address is for routing over outside networks, and the MAC address is an internal address to broadcast network packets to the final destination in a local area. Both IP and MAC addresses can be traced. If an attacker impersonates a MAC address, then they must have their new MAC address to the router of the LAN to communicate with other network users. Finally, their MAC address is automatically exposed to other networks. Thus, using a MAC address-based authentication can prevent impersonation in sensor network environments.

Furthermore, an adversary who is trying to impersonate someone must expose their network location and can be traced by the MAC-based address tracking method. The MAC-based address can identify a machine, but it does not identify a member. Thus, there is a prerequisite to accomplishing a secure and efficient MAC address identification, in which each member must use their machine to communicate with others. More secure features always lead to more constraints. To establish a secure and efficient group communication, the prerequisite must be satisfied [12][13] with various conditions. An extension on an X.509 Certificate ver. 4 is needed to permanently implement a MAC address-based authentication scheme into a conventional certificate-based authentication. Group members can define their extensions and include them in the certificates they issue. These extensions are called proprietary, custom or private extensions, and they carry information unique to their business or institution. In this paper, a member’s MAC address will be able to put into the extension of the X.509 certificate version 4 for the additional confirm of group member’s authentication [15][16]. Secure authentication in a self-signed certificate-based authentication system can be achieved by implementing a member’s MAC address on the extension of a conventional certificate. A MAC address is an additional security feature on an X.509 version 4 certificate to track down a member’s physical location. This research is based upon the physical characteristics of a member’s system, which has been proposed by other researchers [17]. However, it is not well used. This approach supports group member authentication by focusing on where a
member is in addition to who a member is. Therefore, the proposed authentication enhancements have the potential to reduce the risks in participating in group communication, protect members’ privacy, and ultimately improve secure member authentication.

The authentication process proposed is depicted in Figure 2. Suppose two members, Node 1 and Node 2, agree to communicate with each other. When Node 1’s system initiates contact with Node 2’s system, its X.509 digital certificate, which includes its MAC address in the “extensions” portion of the certificate, is transmitted to Node 2. In this scenario, the MAC address in Node 1’s certificate is used as a security deposit and Node 1 must initially offer something of value to initiate interaction. Node 2’s system validates Node 1’s certificate by using the tracert function to contact Node 1’s NIC(Network Interface Card) card and verify that the MAC address on his certificate matches the one on its NIC. Once this process is proceeded, communication between the two members can begin.

As depicted in Figure 2 and described above, the new scheme for verifying a member’s MAC address relies upon the tracert function and can be implemented by any operating systems such as Windows, MAC, and Linux. This method will be able to used so that each party on a network can verify the other’s MAC address. The Java code for getting a MAC address on a certificate is shown in Figure 3. The inclusion of a MAC address information in digital certificates, when paired with verification using the tracert function, will offer a significant additional assurance in verification of each member identity.

Thus, Certificate Authority (CA) can begin to add MAC address information to the digital certificates they issue and mitigate security risks currently endemic in group communication. In this figure, members Node1 and Node2 request a certificate which is a public key to a CA. The CA then issues the public key that each member requests. Thus, each member can possess a certified public key, containing the member’s name, the date of issue, the MAC address, and the CA’s signature.

- Certificate
  - Version Number
  - Serial Number
  - Signature Algorithm ID
  - Issuer Name
  - Validity period
    - Not Before
    - Not After
  - Subject name
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)
  - Extensions (optional)
  - Certificate Signature Algorithm
  - Certificate Signature

![Fig. 2: Verification of MAC Address Diagram](image)

![Fig. 3: MAC address on X509 version 4 Certificate](image)

Also, by using the tracert above function, each member in Figure 4 can verify the other’s identity and trace the other’s physical location in the network using the MAC address on the certificate. Thus, one party shows its certificate to another party as proof of its identity. Another party can verify and
match the MAC address on the certificate and the MAC address that was traced.

6 Conclusion and future work

Sensor networks are growing fast due to IoT development. However, security is a major issue on sensor networks. Therefore, each node must have its authentication with their unique identifier to develop and improve a secure sensor network communication on IoT environment.

7 Acknowledgment

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2017003394).

8 References


