Literature Review on Internet of Things (IOT) Authentication Schemes

Minjie Shen
PID: Minjiesh
Virginia Tech

Nikhita Sattiraju
PID: nagasainikhita
Virginia Tech

ABSTRACT

The emergence of Internet of Things (IOT) gives rise to unparalleled convenience, but at the same time, IOT devices and networks suffer from much more vulnerabilities compared with traditional networks. The nature of IOT (scalability, distributed system, cost/energy constraints) makes ensuring its security extremely challenging, and the consequences resulted from security compromise of IOT networks will be even severe. IOT architecture stack usually contains three layers: perception layer (physical layer and MAC layer), network layer, application layer. CIAAAA (confidentiality, integrity, availability, anonymity, authenticity) are key principles in cybersecurity. In this study, we explored and analyzed authentication protocols for IOT systems.

1 INTRODUCTION

Internet of Things (IOT) devices are becoming increasingly ubiquitous and are utilized in more and more vital areas which expands the attacking surface for the adversaries and exposes the users to greater security threats [5].

IOT devices are resource-constrained, they are restricted with limited energy consumption, limited memory space, and low computation power due its low cost. In addition, IOT devices may move from one place to another, and may increase dramatically in scale. These unique characteristics of IOT devices make existing security protocols for human-to-human networks no longer feasible, as a result, numerous new security protocols specially designed for IOT networks are developed and studied.

A three-layer protocol stack for IOT is widely adopted in the academia, which consists of perception layer, network layer, and application layer [2]. The perception layer perceives the physical world via sensors (edge nodes) as its name implies, which is equivalent to the physical layer and data link layer in the well-known OSI model [4]. The network layer transmits the data. The application layer serves as an user interface and provides services to the users (i.e. end nodes). According Gartner report, it is predicted that "by 2020 more than 25% of identified attacks in healthcare delivery organization will involve the IoT" and with this current pandemic crippling the world to solely depend on technology, it is never a better time to review IoT's security protocols.

The security protocols in IoT network therefore have to ensure confidentiality, integrity and authentication to its end users, so that they are protected from the now programmable physical world as well as ensure privacy using the resource constrained devices. According to [1], authentication in IoT network is identified to be the first step in ensuring security, because if even a single node gets compromised it could lead to the collapse of entire network o worse create disasters for human kind.

1.1 Authentication

Authenticity is one of the key principles (i.e. confidentiality, integrity, availability, anonymity, authenticity etc.) in cybersecurity, it requires identification and verification of the legitimacy of entities in the networks. In Internet of Things (IOT) networks, authentication is the core requirement indispensable for all layers in the architecture. Enormous authentication protocols are developed to guarantee the authenticity of IOT networks.

There are a variety of taxonomies of authentication protocols, they can be categorized into one-way, two-way, or three-way protocols by the way that the objects are authenticated (i.e. unidirectional authentication, mutual authentication, authentication by a third party authority); they can also be categorized with respect to the layers where they located (i.e. perception layer, network layer, application layer, or cross multiple layers), or which type of system they target at (i.e. centralized system, decentralized system, distributed system) [2].

Due to the unique nature of IOT networks, authentication protocols are required to be light-weight in order to support resource-constrained devices which have limited memory storage, computation power, and energy. Authentication protocols are also required to support mobility and scalability of nodes. In addition, there is no international standard for IOT devices, that is, devices from different manufacturers will follow different standard, so that the protocols have to also address the heterogeneity of end devices.

For the rest of paper: in section 2, we analyzes authentication protocols for IOT networks on different layers, where each subsection emphasizes on a specific layer in the sequence of application layer, network layer, and perception layer, respectively. Section 3 states the contribution of each of the authors. Section 4 concludes this paper with a comprehensive table containing all of the protocols discussed in this paper.

2 SURVEY ON AUTHENTICATION PROTOCOLS ON DIFFERENT LAYERS OF THE IOT NETWORK ARCHITECTURE

2.1 Application layer

Application layer is directly associated with the end users, so the authentication protocols designed for the application layer support authentication between edge nodes (i.e. sensors, actuators) and end users which is called end-to-end authentication. Application layer authentication is necessary because the data are decrypted at every intermediate node and thus the security of end-to-end communication can be easily compromised [6]. One of the advantages of applying authentication at application layer is that it is superior when the IOT devices scale because the cryptographic overhead only appears in the end nodes while network layer authentication protocols have more cryptographic overhead as they would occur at every hop [6].

Constrained Application Protocol (CoAP) is an application layer communication protocol especially designed for resource-constrained networks (e.g. IOT networks). It only support User Datagram Protocol (UDP) links at present, which is unreliable, but pervasive in IOT networks [4]. CoAP defines bindings to Datagram Transport Layer Security (DTLS), which is a communication protocol derived from Transport Layer Security (TLS) [4, 11]. DTLS supports authentication at the transport layer [4].

[6] first proposed a fully implemented mutual authentication protocol based on DTLS, which utilizes fully authenticated DTLS handshake and X.509 certificates containing RSA keys [12], which is a popular public key cryptography algorithm. This protocol supports high interoperability, but the overhead introduced by the RSA is relatively heavy[11].

Since a 160-bit Elliptic Curve Cryptography (ECC) has equivalent security level with a 1024-bit RSA [6], ECC based security countermeasures have fewer overhead and outperform RSA, so that an increasingly number of ECC-based authentication protocols have been developed recently [11]. [12] proposed a two-phase application layer authentication protocol for distributed IOT systems. The first phase is registration in which nodes are able to obtain cryptographic credentials from Certificate Authority (CA) which is a third-party authority; the second phase is authentication which provides mutual end-to-end authentication utilizing Elliptic Curve Cryptography (ECC) based implicit certificates. It allows authentication both inside and outside the IOT network. This protocol is lightweight due to the ECC based implicit certificates [6]. In addition, since the certificates are issued by a CA, which is independent of the device location, and the newly-added nodes can self-authenticated during the registration phase, so this protocol supports mobility and scalability of nodes.

Due to the memory constraint of IOT devices, which is one of the major challenges in IOT security, Cloud is introduced with the benefit of unlimited storage. [8] propose a client-based authentication protocol supporting the cloud computing technology. This protocol is also a two-phase protocol, which first assigns a unique identifier to the users during the registration phase, then provides authentication as well as access control. An authentication agent (UA) on the side of users supports user registration and self-authentication, that's why it is called client-based. In addition, there's also another agent based on Diffie-Hellman to make the authentication of unregistered nodes feasible [8]. In this scheme, the authentication server and the cryptography server are independent of the cloud server. As mentioned previously, client-based authentication can achieve desirable performance when the IOT system scales. It is also robust in terms of the various of attacks such as man-in-the-middle attacks, brute-force attacks, timing attacks and so on [8].

2.2 Network layer

Network layer authentication protocols support authentication between intermediate nodes (e.g. gateway, router) and edge node devices (i.e. sensors, actuators).

In current IOT networks, the communication relies on IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) technology. While host authentication as well as key management are not supported in 6LoWPAN, protocol suite IPsec is able to support authentication for 6LoWPAN via Authentication Header (AH) [13].

[15] proposes a privacy preserving authentication protocol for vehicular ad-hoc networks. This paper proposes a distributed aggregate privacy preserving authentication (DAPPA) protocol enabling the vehicle to parse many simultaneous messages securely at the same time. This is achieved by having the vehicle share the private keys for the RSU for a authorised amount of time thus making it more robust to key leakage. Once the authorised time elapses, all the shared keys are deleted, and if the authenticated message is found to be counterfeit, This protocol can reveal the real identity of the vehicle providing unlinkability.

Besides those specially deigned authentication protocols, communication protocols reside in the network layer also implement security mechanisms to support authentication as well as other security requirements. Routing Protocol for Low power and Lossy Networks (RPL) is a network layer protocol especially developed for secure routing in IOT networks. It supports data/device authentication by implementing digital signatures using RSA with cryptographic algorithm SHA-256 and it also implements a number of security modes such as preinstalled mode and authenticated mode [4]. The RPL protocol requires IOT devices to pre-install a symmetric key and then acquire a cryptographic key from the authority before actual routing [4].

2.3 Perception layer

Perception layer authentication protocols are related to the hardware design of IoT devices. These protocols mainly target to keep the node hidden or keep the communication between nodes to the server a secret, because if adversary identifies the node participating in the IoT system then the whole system can be compromised and IoTs are made up of numerous low power physical devices, which calls for security at the physical level too.

[9] is based on one of the popular authentication technique which could be implemented at the hardware level of the IoT devices. Physically unclonable authentication function based authentication protocol claims to provide provide session keying with all of its challenge response pairs enabling smart devices to have secure communication. This protocol is resistant to replay attacks .

RFIDs are the primary targets for such physical attacks, because on the basis of appearance its just a thin chip enclosed in plastic but rising to supremacy in the field of power level and cost of installation RFID system arose to be one of the most indispensable role in identifying the internet of things devices in a cost effective manner. RFID system have time and again proven themselves to be the strength of IoT applications which enable physical objects to be smart. RFIDs, being very portable and light, are widely used to track, record, and locate objects or bulk goods and sometimes also used as implants, where if proper security is not enforced can lead to loss of life. Since RFIDs do not require a battery of its own, they are considered more usable than other typical IoT sensors which hugely depend on their power to communicate with the server. Typical RFID system has three components: RFID tag, RFID reader and a back-end server. Being highly involved with IoT also comes with huge trade off, RFIDs are highly vulnerable to security and privacy issues.

Therefore some of the most common authentication protocols used for RFID technology use symmetric key systems or hash functions. This [3] protocol handles eavesdropping, forward secrecy, Desynchronization or DoS attacks, Impersonation attacks,physical attacks. This [3]authentication protocol is used for RFID systems with the assumption of the presence of PUF. Physically Unclonable Functions(PUF) ensures security against physical tampering of the tag, which if committed results in PUF to change the behaviour of the tag .This protocol provides authentication from both tag and the read-server unit. The following is a short description of how this protocol takes place.

Proposed scheme setup: Server initiates the communication by sending a set of random challenges C_i, to which the tag uses its unique physically unclonable function, to respond to the i^{th} round of communication along with a set of emergency responses. After receiving a response from the tag, the server generates a temporary id and sends this information to the tag, thereby establishing a secure communication channel between the server(server+reader) and the tag.

Authentication phase: Tag responds to the above message from the server with a nonce,COUNT and selects ith round temporary identity and sends a message consisting of the temporary identity issued by the server earlier.Server searches for this TID from its memory and generates a random number computes its response with this randomly generated number and sends this message back to the tag.

If the search for the temporary identity fails during the authentication, the request is rejected. Server again asks tag to resend the request.

After successful verification server unit, server stores further computed values consisting of temporary ID, challenge it sent initially, and the response received in its memory for next round communication.

Enhanced authentication protocol with noisy PUF uses mostly similar methods up till verification at the server unit where it begins its search with the challenge rather than the temporary id it previously sent. It uses the challenge to gather helper data, which again calculates key, with count, and temporary id for the next round of communication. During this verification process if hampered, this phase of enhanced scheme will be terminated proving to be beneficial in the face of DoD attacks but the major drawback of this scheme is that it does not consider the possibility where the existing challenge response pool could become empty with repetitive feeding into the network.

This [10], authentication protocol is used to secure authentication on network and physical layer of IoT devices. In this protocol authors propose a mutual authentication scheme for smart grids (SGMA) and a key management protocol (SGKM) using secure remote protocol (SRP) [14] which stores verifiers instead of passwords. This strategy helps in providing robust security even if password,server or even session key gets compromised, making it the ideal protocol to be used in an authentication protocol. In order to secure communications or data exchanges, this protocol utilizes the power of PKI enhanced for encryption and decryption in key management. However the only downside of this protocol is that it does not consider the storage cost involved.

3 CONTRIBUTIONS

3.1 Minjie shen

Minjie was very proactive in gathering all the literature materials required for the project. She was an active proponent towards this topic though out. She extensively studied about authentication protocols in the application and network layers of the IoT architecture.

3.2 Nikhita Sattiraju

Nikhita was hands-on on this project, she helped to bring attention to different aspects and structure of the project. Nikhita approached authentication protocols on network and perception layers of the IoT architecture.

4 CONCLUSION

The following table consists of surmised version of all the protocols studied and reviewed for this project.

Ref	Layer	Advantages	Limitations
[12]	Application	mutual authentication, lightweight, support heterogeneity, mobility, scalability, distributed system	vulnerable to node capturing attacks
[8]	Application	support cloud computing, scalability, high efficiency, two seperate servers, resistance to various attacks	NA
[6]	Application + Network	first implemented mutual authentication, high interoperability	significant overhead
[13]	Application	not an authentication protocol, but implement multiple security mechanisms (e.g. AH)	NA
[4]	Network	support for secure routing, not an authentication protocol but security modes available	NA
[7]	Network + Perception	improve the original RFID protocols using XOR	Does not keep the location information in secret.
[3]	Perception	Resistant to DoS attacks, forward secrecy, physical attacks. computationally and economically efficient	Does not consider unavailability of the challenge-response pairs in the pool.
[10]	Networks + Perception	Protection against to Impersonation, Brute force, DoS, MITM, and Replay attacks	Storage cost is not considered
[9]	Perception	Protects against Replay attacks, computing and communication efficient	vulnerable to machine- learning attacks
[15]	Networks + Perception	Resistance to DoS, Replay,Sybil, and Falsemessage attacks.preserves privacy.	Non-repudiation attack is not considered.

REFERENCES

[1] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The Internet of Things: A survey. *Computer Networks* 54, 15 (2010), 2787 – 2805. https://doi.org/10.1016/j.comnet.2010.05.010

[2] Mohammed El-hajj, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni. 2019. A survey of internet of things (IoT) Authentication schemes. *Sensors* 19, 5 (2019), 1141.

[3] P. Gope, J. Lee, and T. Q. S. Quek. 2018. Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions. *IEEE Transactions on Information Forensics and Security* 13, 11 (2018), 2831–2843.

[4] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. 2015. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials* 17, 3 (2015), 1294–1312.

[5] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and other botnets. *Computer* 50, 7 (2017), 80–84.

[6] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brünig, and Georg Carle. 2013. DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks* 11, 8 (2013), 2710–2723.

[7] Jun-Ya Lee, Wei-Cheng Lin, and Yu-Hung Huang. 2014. A lightweight authentication protocol for internet of things. In *2014 International Symposium on Next-Generation Electronics (ISNE)*. IEEE, 1–2.

[8] Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi, and Shirin Dabbaghi Varnosfaderani. 2014. A scalable and efficient user authentication scheme for cloud computing environments. In *2014 IEEE Region 10 Symposium*. IEEE, 508–513.

[9] Muhammad Arif Muhal, Xiong Luo, Zahid Mahmood, and Ata Ullah. 2018. Physical unclonable function based authentication scheme for smart devices in Internet of Things. In *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*. IEEE, 160–165.

[10] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung. 2014. Efficient Authentication and Key Management Mechanisms for Smart Grid Communications. *IEEE Systems Journal* 8, 2 (2014), 629–640.

[11] Pawani Porambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Mika Ylianttila. 2014. PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications. *International Journal of Distributed Sensor Networks* 10, 7 (2014), 357430.

[12] Pawani Porambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Mika Ylianttila. 2014. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*. Ieee, 2728–2733.

[13] Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, and Utz Roedig. 2011. Securing communication in 6LoWPAN with compressed IPsec. In *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*. IEEE, 1–8.

[14] Thomas D Wu et al. 1998. The Secure Remote Password Protocol.. In *NDSS*, Vol. 98. Citeseer, 97–111.

[15] Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, and Chuanyan Hu. 2016. Distributed aggregate privacy-preserving authentication in VANETs. *IEEE Transactions on Intelligent Transportation Systems* 18, 3 (2016), 516–526.