Researches about Security User Authentication System of Internet of Things: Comparison Recent Schemes

Jiwei Leng

Chengdu University of Technology, Chengdu 610059, China.

***Abstract*:** Internet of Things(IoT) is a new kind of high technology which has significant meaning in many ares such as industry and military. The popularity of the technology bring a lot of convenience for people. However, network attacks are huge threats of IoT. Since the features of IoT, traditional cyber security schemes are not suitable for modern IoT applying occasions. Throughout this article, the author review IoT basic knowledge and IoT security protocols in recently years. Particularly, choosing two papers which focus on user authentication of sensors to compare and analyse their core indexes. This paper provide useful information for IoT security beginner and point out future changes.

Keywords: Internet of Things(IoT); Radio Frequency Identification(RFID); Intelligent Device; Wireless Sensor Networks(WSNs); Security; Gateway (GWN); Sensor; Encryption; Authentication; Server; Encryption; Decryption; Authentication; Server; Node; Hash Algorithm; Secret Key; Public Key; Layer; Attack

Introduction

Internet of Things (IoT) is an emerging technology which has significant effects in many domains such as industries, military and infrastructures. Nowadays, IoT has deeply fitted in the daily lives of residents in a large amount of occasions. For instance, everyone could use intelligent facilities to study and work. Similarly, manufactures could also utilize IoT devices to gain higher producing efficiency or less management cost. Some researches mentioned that it was estimated by Cisco that the IoT would expand to approximately 25 billion units installed by 2020[2].

However, ascending number of IoT devices is a huge challenge to the security system. Because this also means more people could visit the whole network, including some criminal Organizations[8]. Besides, almost these devices working without someone to protect them every time. When the device is used frequently, it will be more vulnerable to attack. Definitely, IoT security system is the focus of network security in recent years. According to the some major academic journals, the figure of articles about IoT security has increased sharply in recent years[1].

This paper choose scheme of Foroozan Ghosairi Darbandeh et al[6] and Anup Kumar Maurya et al[7] in IoT nodes user authentication to do comparison analysis. This article will systematically explain their algorithms, principles, and benefits when they applying on different occasions. In addition, comparing their efficient through core indexes such as computation cost and security. Lastly, giving some comments about their contributions and mentioning few future trends about this domain.

1. Related works

In fact, many researchers had provide hundreds of security authentication schemes. A survey[5] pointed out the reasons of IoT security issues are the heterogeneity, volume, inner-connectivity and dynamism. In addition, that essay also emphasized the difficulties of maintaining IoT security are much harder than traditional cybersecurity. Exactly speaking, related researches in authentication in IoT-WSNs can be categorized into 2 parts. The first item is the authentication of the gateway to the sensor nodes. The second item is the authentication of the user to sensor nodes.[6] This article focus on the security authentication of user.

To help the industry 4.0, author of one paper[4] introduced one robust, lightweight, and secure authentication protocol specifically for IoT nodes. But it can not against active attacks efficiently.

Further more, sometimes IoT security solutions also can be integrated by technology from other area. For example, the author in article[3] suggest a digital signature way applied in hardware to improve security. But also requires better hardware. Another article[8] present a methodology called BCmECC which combined blockchain technology into IoT nodes to allow the authentication message be verifiable, immutable, and undeniable. However, this method demand more time to communicate. Different from these researches, this paper focuses on efficient, secure and widely applicable user authentication schemes for different hardware bases.

2. Preliminaries

Understanding the basic 4 layers architecture is vital. The IoT has a logical framework with 4 layers: Sensing, Accessing, Network and Application.[1] Firstly, The task of sensing layer be responsible for collecting information and recognizing objects. Then, the accessing layer is accessing layer which could transport data to the network. Thirdly, network layer is the communication center of IoT. It is the container of existing communication networks (e.g. 4G, 5G). Lastly, the application layer mainly provides multiple devices that could interact with users such as smart phones.

Readers would better to know universal attacks at different layers or stages because schemes are designed to prevent these attacks.

In addition, symmetric encryption algorithm such as DES need to be understood. This is necessary to know xOR, hash functions and binary calculations, which is mathematical requirements.

3. Principles and algorithms

Since this paper discuss 2 article, so this chapter will interpret the principle and basic logic of their algorithm. Both of them focused on the authentication of the user to the sensor nodes. In fact, identity authentication is the first step of network security and also one of the most important parts of IoT security.

The first article[6] provided a new algorithm like this:

Registration phase

Firstly, sensors(SN) register the GW(gateway), the ID and list of keywords(cipher suites) of sensors will be send to GW. Then, the GW will generate a encrypted value of these two through hash function and encrypts the ID and cipher suites by public key. After that, sending this all to Users. User decrypt this package by decryption functions(PKj) with secret key(Xi). This time he get the ID and cipher suites, so this time applying the symmetric encryption(ENC()) on secret key and cipher suites. This value called Y, sending Y to GW and sensor. Finally, the SN decrypt Y by symmetric decryption(Dec()) to check the cipher suites, if cipher suites is right, finishing this phase.

Authentication phase

This phase will let user and the senor identify each other. Firstly, importing a random number N to calculate other temporary number z by XOR and Hash operation. Then, using z to do the similar thing after the user receive this z. Diving the 16-bits z into two parts to get z1 and z2.

Handling this procedure for 4 times to achieve a circle which come back to sensors. Eventually, checking the final temporary number P and R’. If they follow the conditions, the authentication finished. The four temporary variables are used to check the algorithm is safe in the transmitting. But only use one key to check is not good enough. So, applying Tx(timestamp) to help it. Timestamp can not easily be fake by others. Doing an additional calculations to get a temporary A by adding this T1(timestamp1) into former expressions. Then, sending it to next step and checking if this operation is not out time. Repeating this operation for 4 times until the package back to the sensor. So, this time enhance the previous algorithm to use 2 parameters when doing authentication. Besides,these 2 parameters are interlocking which means each of them can not be wrong, or it will return false.

4. Key establishment phase

After finish all steps above, the key will established to ensure their communicating security. $K1 = N \oplus L$ and $K2 = N \oplus P$ and then compute the value of key $K = F(ENC(K1||K2, Xi))$.

The another article [7] mentioned an authentication method based on Bloom filters. In fact, the basic stages resemble the former one.

Pre-deployment phase

The GWN assigns a vector Vsn of Bloom filter to each sensor node SNi of a cluster using k-coloring problem and collecting them all together to store.

Registration phase

The users(Ui) input biological information(Bi), then, applying Gen() function to extract it. Also, calculating parameter IPB through hash function depend on ID, password and biological information. The next step is sending this parameter to GWN and generating public key and secret key for Ui.

Finally, using a series of complex Hash and XOR algorithm to get the 3 core parameters. After sending them to users, users have access passwords based on biological information and parameters. Inserting this construct data into the smart card SC1.

User authenticated and session key establishment phase.

This time to dispose the session key. Firstly, calculate another biological parameter σ1 by Rep function. Getting the current timestamp Tu. Generating Ru and Bu through Hash and XOR. The m1 and m2 are also like this. Sending this construct message to GWN. Once the sensor get this message it will derive more variables. The first step is always check the timestamp to prevent t timeout. Then, verify whether the parameters in the construct is valid. If true, calculating the session key using EDCH algorithm. Besides, m3 derived by hash functions. Returning this construct message including all parameters to user.

Lastly, at user stage it will check the timestamp again and compute the session key. In addition, verifying m3' is equal to m3. When the above steps are right, the session key is established.

From the point of calculation difficulty, both of 2 algorithms is complex. Besides, they took DES algorithm as basic thought. But the former one may difficult to do passive attacks because its parameters are progressive and repeating 4 times in different nodes, so it's almost impossible to attack from an intermediate steps. The latter one take more complex calculations at each stage and call more hash functions. Besides, there are some defined functions which handle the biological information of users. It is more like an advanced human biological information verifying way which combined cryptography. But it also has multiple parameters in a list to transport. By contrast, former scheme take less parameters to communicate.

5. Comparative analysis

In general, both of them are effective and suitable for modern IoT occasions. But they still have advantages in different indicators. This chapter stands by various points to compare their features. Because many IoT sensors and devices have fixed size specifications, so they have limited room to put CPU and batteries. Thus, this article focus on computation cost and security.

Testing ends	Paper1[6]	Paper2[7]
Basic thought and technology	Lightweight authentication	Bloom filter
Computation cost(all sides)	18Th, the totally time of doing hash function(Th) ≈ 9ms 2.Complex calculation process and multiple parameters. 3. Calculating 3 sides (user, sensor, GWN)	1.Time on user stage is 8Th + TM+TFE≈106.8ms, on sensor side is ≈ 754.5 ms 2.Less steps and do not need to compute the GWN cost
Security	Against : User impersonation attack Gateway impersonation attack Traceability attack Secret disclosure attacks Replay attacks	Against: Replay attack Man-in-the-middle attack Stolen smart card attack Against exhausting energy attack User impersonation attack Password guessing attacks.

Because the latter paper test the algorithm on particular hardware(Intel (R) Core (TM) 2 Quad CPU Q8300, @2.50 Hz processor, Windows 7 OS, and 2GB RAM), so it contain specific data. In conclusion, the former is a lightweight protocol so it may occupy less memory and communication bits. By contrast, the latter used biological information into algorithm with corresponding functions, so it perhaps taking more memory. In general, from the author's perspective, the former protocol may adopt more situation because of the less time and lower hardware requirements. By contrast, the latter one is safer due to the benefits from biological information from user which is hard to fake. Also, it can prevent more type of attacks in formal tests.

6. Conclusion

IoT will offer the world a higher level of accessibility, integrity, availability, scalability, confidentiality, and interoperability. Meanwhile, cybersecurity issues is becoming one of biggest challenge of future IoT[1]. In the future, as hardware facilities such as CPU and batteries are optimized, the computing power and battery life of sensor nodes will increase. This will drive the upgrade of Internet of Things security solutions. Besides, future protocols will pay attention on combing strong keys such as fingerprints in the algorithm. In conclusion, the author summarizes some patterns in the area of IoT security and compares the two solutions in detail. I mainly analyzed the algorithm and effect of these two schemes to judge their security and other indicators. From the analysis results, both have their advantages. Also, their emphasis is also on light weight and high safety when equipment conditions allow, respectively. But because they took a different fundamental designing principles, they can be applied to different occasions which depend on hardware supports. Even they can be combined to make a better scheme prospectively.

References

[1] Yang L and Li DX, “Internet of Things (IoT) Cybersecurity Research:
A Review of Current Research Topics”, IEEE trans, IEEE internet of things journal, vol. 6, no. 2, pp. 2103-2115, 2019.

[2] Mojtaba A, Mohammad HT and Alireza J, “Secure ticket-based authentication method for IoT applications”, Elsevier, Digital Communications and Networks, 2021.

[3] Nishant S, Parveen SH, Rahul S, Shriniwas, “Secure Hash Authentication in IoT based Applications”, Elsevier, Global Transitions Proceedings, vol. 2, no. 2021, pp. 84-90, 2021.

[4] Sahil Garg, Member, Kuljeet Kaur, Georges Kaddoum and Kim-Kwang Raymond Choo, “Toward Secure and Provable Authentication for Internet of Things: Realizing Industry 4.0”, IEEE trans, IEEE internet of things journal, vol. 7,

no. 5, pp. 4598-4606, 2020.
[5] PatilIqbal H. Sarker, Asif Irshad Khan,   Yoosef B. Abushark, Fawaz Alsolami, “Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions” , Springer, Mobile Networks and Applications, 2022.
[6] Foroozan GD and Masoumeh S, “A New Lightweight User Authentication and Key Agreement Scheme for WSN”, Springer, Wireless Personal Communications, pp. 3247-3269, 2020.
[7] Anup KM, Ashok KD, Sajjad SJ, Debasis G, “Secure user authentication mechanism for IoT-enabled Wireless Sensor Networks based on multiple Bloom filters”, Elsevier, Journal of Systems Architecture, 2021.
[8] Jan L, Amir MR, Saqib Ali, et al, “BCmECC: A Lightweight Blockchain-Based Authentication and Key Agreement Protocol for Internet of Things”, MDPI, mathematics, 2021.