DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4050

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

COMPARATIVE ANALYSIS OF INTERNET OF THINGS LIGHTWEIGHT AUTHENTICATION PROTOCOL DESIGN SCHEMES

Ahmed Mohammed Ibrahim Alkuhlani
School of Computational Sciences
SRTM University
Maharashtra-Nanded-India

Dr S.B. Thorat
Director of Institute of Technology & Management
ITM College
Maharashtra-Nanded-India

Abstract— Lightweight authentication is a branch of the modern authentication techniques, which intended to be used in constraints network such IoT and WSN which has devices with low or extremely low resources. There are several ways for designing a lightweight authentication protocol, researchers are competing to find the best ways that fit with the features of the Internet of Things. In this paper, we propose generalized approaches to design lightweight authentication protocols. Also, we highlight some principals and security requirements for the implementation of lightweight authentication. Finally, we provide a comparative study of using symmetric and asymmetric cryptography techniques for designing lightweight authentication protocols for IoT.

Keywords: IoT; IoT Security; lightweight Authentication; IoT authentication; authentication security attacks; constrained devices

I. INTRODUCTION

IoT and the expansion of smart technologies, embedded devices integrated with wireless technologies such as Bluetooth, Wi-Fi and identification technologies such as radio frequency identification (RFID). Besides usual personal computers, billions of small, tiny devices will be connected to what is called Future Internet (FI)[1]. These devices are resource constrained having small processing capability, limited memory and limited energy.

IoT device will be widely deployed and connected to the FI this deployment requires some solutions so that IoT constrained devices can work with the existing internet protocols .the main challenge that faces IoT is the security[2,3,4]. the existing traditional security techniques were designed to work on fully functional devices (FFD) but with constrained devices, we require lightweight solutions which these devices can handle.

Security appears to be one of the most challenging areas of designing IoT. While 'things' or objects forming the IoT can be extremely constrained (low-computational power, low-storage space, limited memory, lack of user interface), this is no excuse for them to have less security than any other devices on the internet. Sometimes, 'things' could lead critical roles, such as monitors in home security systems or controllers as a part of an intelligent transportation system. Compromise of such devices can be more catastrophic than that of a typical device on the internet (e.g. a personal computer (PC), or a mobile phone)[5].

Existing traditional authentication techniques consumes a significant amount of energy and memory as it requires extensive processing [6,7]also the size of messages and the number of handshakes hence, in IoT we need to design a robust and secure authentication protocol with lightweight cryptographic primitives with the same robustness and security strength of the existing systems.

In this paper we tried to analyze and generalize the main approaches to the design of lightweight authentication protocols to guide researchers how to design an authentication protocol for IoT by first explaining entities participating in the authentication protocol in section II. In section III different mutual authentication models. In section IV security requirements and security attacks which we have to be considered when designing an IoT authentication protocol. In section V we explore some lightweight security primitives and finally In section VI explaining symmetric and asymmetric authentication techniques that can be used in IoT environment as we concentrated on symmetric cryptography we provided a comparison of computational cost and time for symmetric authentication protocols

II. AUTHENTICATION COMPONENTS IN IOT NETWORK

Authentication in IoT network simply can be viewed as three components, the IoT device, user and a gateway in between to facilitate the communication between them. Gateway plays an important role in authentication as it is used to translate the IoT propriety protocols and the IP protocol which connect the user with the IoT network. The constrained devices in IoT and WSN use the gateway for extra processing and memory storage as in the figure[1] the gateway works as an authenticator for both the IoT node and users. Gateway verifies the identity of a (user, device) who wants to access data, resources, or applications. Validating that identity establishes a trust relationship for further interactions.

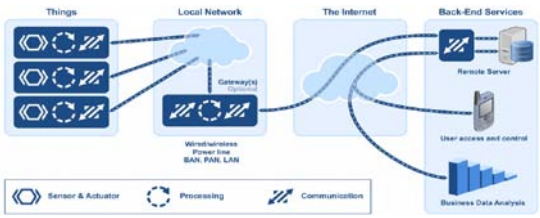

Figure 1:IoT Authentication Participants

gateway plays an important role in the network. In order to connect a specific sensor node, remote users have to reach the

gateway through the internet at first. Contrary, data sensed from the sensor nodes firstly gathered to the gateway, then further reaches the user end. If the data in the network is made available to the remote user on (demand), mutual authentication between (IoT device, user) must be ensured before allowing the remote user to access the device. With the help of the gateway, impenetrability of lightweight mutual authentication is going to be possible.

III. IOT MUTUAL LIGHTWEIGHT AUTHENTICATION MODELS

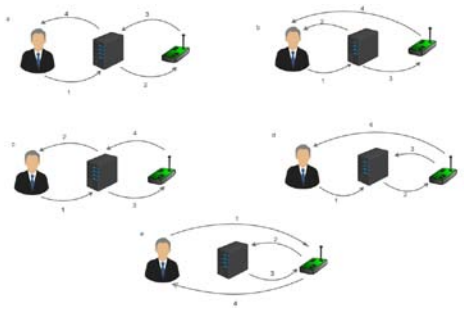

Figure 2:Constrined Network (four messages) Mutual Authentication Models

All the five models depicted in figure[2] was proposed in [8], mutual authentication is maintained between the user, gateway and constrain devices such as sensor .with the help of the gateway users and sensors get authenticated. Gateway is mainly used to assist the constrained devices in IoT and WSN to communicate with local and remote users in addition, to provide storage and processing as these devices may not have enough processing and memory capabilities to communicate directly with the users[9]. The first four models (a,b,c,d) is used when the user interact indirectly with the sensor it first communicates with gateway whereas the fifth model(e) is used with remote users in which users can communicate directly with the device which is the case with IoT network. All the five models mentioned above use four message handshakes which make the authentication lightweight. In authentication, we can use (something we know) like password-based authentication and (something we are) like Biometric- based authentication and (something we have) smartcards-based authentication. Combining these techniques to construct authentication schemes depend on the type, robustness and the target system capabilities.

There are certain principles should be considered when designing a lightweight authentication protocol

1) Protocol should be designed according to the common resource features of target constrained devices such as microprocessor or microcontroller, memory, and energy
2) Avoid highly computational mathematical operation as it requires much processing which consumes a lot of power and memory .low computational overheads makes memory and power requirement at minimal
3) Authentication Messages size should be small, as the bandwidth of wireless radio is small (IEEE 802.15.4 bandwidth is 256kbps)
4) Number of messages exchanged between authentication parties should be kept at minimum
5) Cryptographic primitives used while authentication should be lightweight such as symmetric cryptography, Message Authentication Code (MAC), HASHING, XOR and AND operations

IV. SECURITY FEATURES FOR A LIGHTWEIGHT AUTHENTICATION PROTOCOL

A. security requirements

when designing an authentication protocol certain security requirements must be considered, the design goal of a lightweight authentication scheme is finding a compromise between low resource requirements performance, and security strength which are discussed in this section.

1) *Lightweight security solution:* The nodes in the IoT networks are resource constrained in terms of processing power, battery backup, memory, speed, etc. Hence, a lightweight security primitives solution is required.
2) *Mutual authentication:* all parties involved in communication authenticate each other (user, gateway and IoT node). This is one of the most important requirements for IoT to have a secure communication.
3) *Anonymity***:** when data is transmitted the identity of communicating parties should be hidden so that the attacker can't distinguish between user/nodes and hence can't trace user/node by their identity.
4) *Scalability:* to keep the network scalable the addition of new nodes should be dynamic and the system should be able to cope with this increase.
5) *Confidentiality***:** in this requirement, the secret data transmitted between parties involved in authentication must be kept secret. only legitimate parties can get access to it.
6) *Availability:* In this requirement, the server/gateway or the nodes must be continuously available to the user to access information or send commands to the nodes, as and when required.
7) *Attack resistance:* To guarantee secure communication within the IoT network, the authentication process should be secure against several potential attacks, such as replay attacks, DoS attack, impersonate attack, user/node traceability attack, man-in-the- middle attacks, etc.

B. security attacks against authentication

There are some security attacks that an attacker can use to breach the security of the authentication protocol we explore some of them here

1) *Denial of Service attack:* The DoS attack hinders the avail- ability of a system offering services. During this attack the illegal entity consumes the resources exhaustively, thereby making the system unavailable to the legal entities. This at- tack is generally achieved by launching resource consuming activities. Such an attack becomes vital for constrained devices in IoT networks, where the resources are already limited.
2) *Impersonation attack***:** This attack occurs when an illegal user or node pretends to be a legal entity by replaying a genuine message intercepted from a previous successful communication.

3) *Man-in-the-middle attack:* This attack occurs when the adversary silently listens to the communication of two legal parties with the intent to delay, alter or delete messages exchanged during communication. Such attacks are mostly present within the context of Public-Key Cryptography (PKC). In case of PKC, the adversary does not try to break the keys of the communicating parties, rather it tries to become the falsely trusted man-in-the-middle. This is achieved by replacing the exchanged session key with its own. Thereby each of the parties establishes a secure channel with the adversary, who gains access to messages in plaintext.
4) *Smartcard stolen/breach attacks:* The user's smart card is a tamper-resistant device. If the smart card of a user is lost or stolen, an attacker can retrieve all the sensitive information stored in the stolen smart device's memory using the power analysis attack. Then, using this retrieved information, the attacker can retrieve other secret information of the communicating parties.
5) *Eavesdropping attack***:** It refers to the process of listening to an ongoing communication, which is an initial step for launching the other attacks. Such attacks are easier to perform on unprotected wireless channels, because the communication takes place in an open insecure wireless channel.
6) *Privileged insider and stolen-verifier attack:* In this attack an attacker or a privileged but malicious user could gather sensitive user information (i.e. verifiers), therefore he/she could not try and impersonate a user on any other network.
7) *Gateway node bypassing attack*: The illegitimate entity can bypass the legal gateway node and get connected to an IoT node without performing the authentication process.
8) *Offline guessing attack:* Any illegal entity can acquire passwords (offline guessing mode) using a "Brute-force" attack to guess the passwords.

V. LIGHTWEIGHT SECURITY CRYPTOGRAPHIC PRIMITIVES

A. *Hash Function*

A hash function maps a variable-length block of data into a smaller fixed-length block. This property is very important for constrained devices some keys require to be large for security purpose therefore, storing them in hash format save a lot of memory also message size becomes smaller when message exchanged between authentication parties. The purpose of a hash function is to produce a "fingerprint" of a file, message, or other block of data [10]. The interesting part about hashing is the output which is sensitive to even a tiny change hence if an attacker tries to modify the message digest(output) the output completely changes therefore, the integrity of the hash message is guaranteed in figure[3] there are some lightweight hash algorithms with their memory and energy consumption [11].

Table 1:lightweight Hash functions and its characteristics

Algorithm	Area (GE)	Mean Power (µW)	Technology (µm)
Spongent	738	1.57	0.13
Photon-80	865	1.59	0.18
Keccak	1,300	-	0.13
U-Quark	1,379	2.96	018
D-Quark	1,702	3.95	0.18
S-Quark	2,296	5.53	-
Armadillo2-A	2,923	44	-
Armadillo-A	3,972	69	-

B. *Message Authentication Code (MAC)*

A MAC is symmetric cryptography technique (sometimes called: keyed hash) takes two inputs, a message and a secret key which is shared between the authentication initiator and the authentication responder only. By using a secret key, a MAC allows the recipient of the message to not only verify the integrity of the message, but also authenticate that the sender of the message who has the shared secret key. If a sender doesn't know the secret key, the hash value would then be different, thus allowing the recipient to see the message was altered.

VI. CONSTRUCTING A LIGHTWEIGHT AUTHENTICATION SCHEME

The first step in designing a lightweight authentication scheme is to choose the right security primitives with respect to the target system how to use such primitives for building an efficient, secure and robust authentication and key management protocol with the IoT network constrained devices requirement.
There are two broad categories used for constructing a lightweight authentication .

A. *Using Symmetric-key Infrastructure (SKC)*

Symmetric cryptography approach is more preferable as it can easily implemented for constraint network such IoT, it is efficient in term of computational time and less complicated on mathematical operation, it takes only few milliseconds and can be run on memory restricted microcontroller with ram less than 1KB[12]. In symmetric-based authentication a single key is shared between authentication entities.
There are two types of symmetric-base authentication the first one is to use one of the well-known symmetric cryptography algorithms such as Advance Encryption Standard algorithm (AES) or Data Encryption Standard (DES).
The message exchanged during the authentication phase are encrypted using a key which is known in advance between the authentication entities.
MAC is implemented with a combination with these symmetric algorithm to provide authentication and integrity for the message exchanged between the sender and the receiver. Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.
The second method is using hash function and logical XOR operation. In this method no encryption/decryption algorithm is used, instead a cryptographic one- way hash function and XOR are used as in figure [4]. This method is secure and computationally lighter in term of memory and energy. In [13] an experiment was conducted the approximate running time used for computing hash function is $\approx$ 0.0004 ms where the time used for computing symmetric encryption/decryption is $\approx$ 0.312 ms. This experiment was performed using the AES symmetric encryption/decryption function, and the SHA-1

hash function. The result of comparison between different symmetric authentication protocols in Table(2) shows that the time of schemes using hash and XOR is more lightweight than other schemes using AES. The hash method works well with constraint network such IoT in which devices are battery powered and memory is limited.

Most of the recent work in IoT authentication schemes [2,3,4,14,15] Symmetric cryptography approach is used as its secure, fast and consume less energy the only problem is the key management and memory needed for storing these keys but this problem was solved by delegating key storing to the gateway node as it can be considered as powerful fully function device (FFD) which have constant energy and enough memory [4].

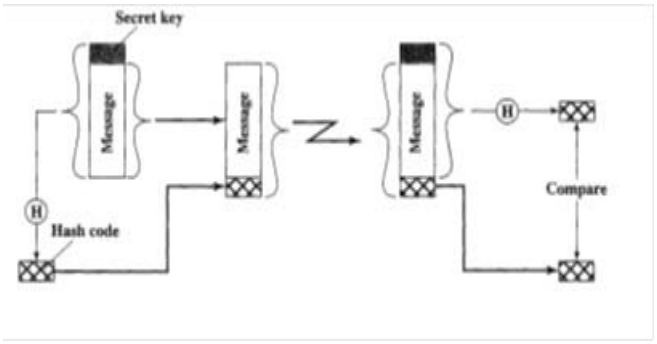

Figure 3:Message authentication using one-way hash function

B. Using Public Key-infrastructure (PKI)

Conventional PKI authentication techniques have a flexible key management but modular multiplication and squaring of large integers consumes a significant amount of microcontroller power and memory. The number of handshakes and size of the messages exchanged during authentication with constrained devices should be kept at the minimum. In particular, transmission of long messages containing conventional X.509 certificates yields a sizeable airtime consumption, a significant latency in the authentication protocol when running over a typical low-rate communication channel[16].

there are several methods used in literature to perform a secure authentication using PKI. RSA and ECC are two public key algorithms used for authentication. ECC offers smaller key size, faster computation as well as memory, energy and bandwidth saving and better suited to small devices than RSA

Using Digital Signature: Similar to MACs, digital signatures append an authentication tag to a message. The crucial difference between digital signatures and MACs is that digital signatures use a pair of keys public and private for both generating the authentication tag(signature) and verifying it. Most digital signature authentication schemes are implemented with the help of a hash function. Also, they are usually slower than MACs. Digital signature generation involves two steps. The first step is of hashing the authentication message and in the second step the hashed

Table 2:Comparison of computational cost between Symmetric protocols

Protocol	User	Sensor	Gateway	Total	Time
Turkanovic´et al. [4]	$7T_h$	$5\ T_h$	$7\ T_h$	$19\ T_h$	0.0076 ms
Farash et al. [14]	$11\ T_h$	$7\ T_h$	$14\ T_h$	$32\ T_h$	0.0128 ms
Das et al. [18]	$5\ T_h + 1\ T_{(d/e)}$	-	$5\ T_h + 4\ T_{(d/e)}$	$10\ T_h + 5\ T_{(d/e)}$	0.6555 ms
Khan and Alghathbar [19]	$4\ T_h$	$2\ T_h$	$6\ T_h$	$12\ T_h$	0.0048 ms
Turkanovic and Holbl [20]	$4\ T_h + 1\ T_{(d/e)}$	-	$7\ T_h + 5\ T_{(d/e)}$	$3\ T_h + 4\ T_{(d/e)}$	0.5224 ms
Huang et al.[21]	$4\ T_h$	$1\ T_h$	$6\ T_h$	$11\ T_h$	0.0044 ms
R.Amin et al.[3]	$12\ T_h$	$5\ T_h$	$15\ T_h$	$32\ T_h$	0.0128 ms

Th – time for a hash operation; TD/E – time for symmetric-key decryption/encryption

value(message digest) is signed using the sender private key .This second step produces a value (the 'signature') that is attached to the message.

using Digital Certificate: In [17] proposed PKI authentication and key agreement protocol for IoT which provides authentication without any explicit signature The author has used a combination of elliptic curve Diffie-Hellman (ECDH) for key agreement protocol and "implicit" certificate Elliptic Curve Qu-Vanstone (ECQV) .this combination found better than the traditional schemes relying on explicit X.509 certificates. 13 packets needed for the 725 bytes of the explicit X.509 certificate in the Privacy Enhanced (PEM) format, or the 9 packets required to send the 495 bytes of the explicit X.509 certificate in the Mail Distinguished Encoding Rules (DER) format

While relying on a standard and widely accepted ECDH scheme, it significantly improves airtime savings by employing implicit ECQV certificates.

usage of implicit certificates always ensures the maximal airtime saving, with performance gains over explicit X.509 PEM certificates ranging from 77,1% to 86,7%, and from 50,9% to 84,7% with respect to the explicit X.509 certificate in the (DER) format.

VII. CONCLUSION

IoT is an emerging technology, security and authentication is a center focused topic in IoT. we have analyzed the main approaches to the design of IoT lightweight authentication protocols and the constraints of their use. Symmetric-key infrastructure schemes are fast, secure and doesn't consumed much processing power but they require complicated key management, on the other hand, public-key infrastructure schemes have a flexible key management but consume much computational time and memory space. ECC prove its strength and reliability with constrained networks. IoT devices have small memory, restricted to certain power limits and computational capability hence PKI approach require to be improve to be adapted with IoT environment.

VIII. REFERENCES

[1] Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the internet of things (IoT). In: Recent trends in network security and applications. Springer Berlin, Heidelberg; 2010. p. 420–9. doi: 10. 1007/978-3- 642- 14478- 3 _ 42 .

[2] P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

[3] R. Amin et al., Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.006

[4] M. Turkanovic´ et al., A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Netw. (2014), http://dx.doi.org/10.1016/j.adhoc.2014.03.009

[5] JingLiu et al," Internet of things' authentication and access control", Int. J. Security and Networks, Vol. 7, No. 4, 2012

[6] Savio Sciancalepore et al,'Public Key Authentication and Key agreement in IoT devices with minimal airtime consumption', 2016 IEEE.

[7] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi.Key Management Protocol with Implicit Certificates for IoT systems. In ACM IoT-Sys Workshop, May 2015.

[8] K. Xue, C. Ma, P. Hong, R. Ding, A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, J. Netw. Comput. Appl. 36 (2012) 316–323.

[9] S. Ozdemir, Y. Xiao, Secure data aggregation in wireless sensor networks: a comprehensive overview, Comput. Netw. 53 (2009) 2022–2037.

[10] http://williamstallings.com/Cryptography/CRYPTOGRAPHY AND NETWORK SECURITY sixth edition

[11] Manjulata AK . Survey on lightweight primitives and protocols for RFID in wire- less sensor networks. International Journal of Communication Networks and Information Security (IJCNIS) Vol. 6, No. 1, April 2014

[12] Jorge Granjal et al,' Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues', DOI 10.1109/COMST.2015.2388550, IEEE Communications Surveys & Tutorials

[13] L. Xu , F. Wu , Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care, J. Med. Syst. 39 (2) (2015) 1–9 .

[14] M.S. Farash, M. Turkanović, S. Kumari, M. Hölbl, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment, Ad Hoc Networks (2015), doi: http://dx.doi.org/10.1016/j.adhoc.2015.05.014

[15] Sima Arasteh et al, "A New Lightweight Authentication and Key agreement Protocol For Internet of Things", 13th International ISC Conference on Information Security and Cryptology (ISCISC2016) September 7-8, 2016; Shahid Beheshti University – Tehran, Iran

[16] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk.'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, May 2008.

[17] Savio Sciancalepore et al' Public Key Authentication and Key agreement in IoT devices with minimal airtime consumption', 2016 IEEE.

[18] A. Das, Kumar, P. Sharma, S. Chatterjee, S.J. Sing, Kanta, A dynamic password-based user authentication scheme for hierarchical wireless sensor networks, J. Netw. Comput. Appl. 35 (2012) 1646– 1656.

[19] M.K. Khan, K. Alghathbar, Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks', Sensors 10 (2010) 2450–2459.

[20] M. Turkanovic´ , M. Hölbl, An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks, Electron. Electric. Eng. 19 (2013) 109–116.

[21] H.-F. Huang, Y.-F. Chang, C.-H. Liu, Enhancement of two-factor userauthentication in wireless sensor networks, in: IEEE Computer Society, 2010, pp. 27–30.

