ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 4, April 2017

Light weight Secured Protocol for Internet of Things (IOT) Data

[1] Ms. Divya T, [2] Dr. Vidya Raj C
Department of Computer Science and Engineering
[1] [2] National Institute of Engineering (NIE), Mysuru, Karnataka, India

***Abstract*— The Internet of Things (IOT) is an ecosystem of connected physical objects that are accessible through the internet based on interoperable information and communication technology. In the secure communication areas, key exchange protocol is an important cryptographic technique. When two users would like to exchange a message, the transmitted message is encrypted by a session key. This session key is exchanged between two ends of the corresponding connection with the help of trusted third party protocol. This type of protocol protects message delivered between two authorized users. Even this inefficiency, unreliability, inflexibility problems of the existing protocols. Therefore, in this paper, secure multi key exchange protocol based on trusted third party is to provide users with a efficiency and secure protocol which employs Elliptic Curve Cryptography (ECC) and two dimensional operation. These protocols achieve fully mutual authentication between user and trusted server.**

***Keyword*: Multiple key exchange, trusted third party, Elliptic curve cryptograpy.**

I. INTRODUCTION

Wireless communications is, by any measures, the fastest growing segment of the communication industry. Wireless communication is a broad term that corporates all procedures and forms of connecting and communicating between two or more devices using a wireless signal through wireless communication technologies and devices. However, many security issues in the wireless communications such as personal privacy, data leakage etc. In the privacy viewpoint, wireless security is a decisive work since messages are delivered to their destinations through the medium so hackers can maliciously intercept the messages and decrypt the messages.

In wireless communication network, cryptography is used to protect user's guarantee integrity of data and secret data. RSA encryption algorithm is one of the Asymmetric cryptographic methods to encrypt and decrypt the data. The computational cost of these algorithms is relatively high due to employing long keys and complex encryption/decryption processes. However, these data often consumes lot of energy and a long time. To overcome this problem another key exchange protocol is introduced i.e. Diffie-Hellmen key exchange protocol. This protocol helps users to establish a shared secret key over an insecure channel, with which to encrypt subsequent communication using a symmetric key cipher. Unfortunately, each of them has its own weakness in security and performance. Li et al. [11] proposed three-party password-authenticated multiple key exchange protocol for wireless mobile networks. Li's protocol establishes multiple session keys in its key exchanging process and reduces the user's and server's computation costs and claimed that it had reliability, high efficiency, scalability and flexibility. However, it is still insecure and inefficient.
Therefore, this paper propose a secure multi-key exchange protocol based on trusted third party which provides a high-efficiency, reliability, scalable key exchange method for data communication. In contrast, trusted third party is used to authenticate the users and their messages, the certificate authority (CA) issues digital certificates to the users. So that two users can safely exchange important keys. To achieve this, the trusted third party system's clock derives dynamic keys to encrypt exchanged keys and random numbers to prevent eavesdropping and replay attacks. Besides, proposed protocol mainly utilizes the logical XOR operation rather than ECC
multiplications to encrypt and decrypt security parameters, since generally an XOR operation consumes less time than an ECC multiplication. This protocol also prevents against replay attacks, eavesdropping attacks, forgery attacks, known key and impersonation.

The rest of the paper is organized as follows. Section II introduces the related studies. Section III describes the problem definition. Section IV describes the proposed protocol. Section V concludes the paper.

II. RELATED WORKS

In 1992, Bellovin et al. [1] proposed an encrypted key exchange (EKE) protocol which used a combination of a public key and a secret key created to prevent delivered data from dictionary attacks. To simply the EKE protocol,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 4, April 2017

Abdalla et al. [2] presented a two-password-based EKE protocol which only needs a random oracle instance and is more efficient than the EKE protocol [1]. However, the adversary may enumerate user passwords. When two users are communicating, the password shared between them is drawn from a small set of values, and thus dictionary attacks may be viable. Several password-based authenticated key exchange (PAKE) protocols to enhance the security of 2PAKE. These protocols have been developed to guarantee the effectiveness of the protocol proposed by [3]. Lu et al [4] proposed a simple three-party password based authenticated key exchange protocol(S-3PAKE), which eliminates the need of a server's public key and is able to resist against various attacks. Chung et al.[5] found that the S-3PAKE is still vulnerable to impersonation-of-initiator attack and used counter measure against such attacks. Chang et al. [6] proposed an efficient three-party authenticated key exchange using ECC. The proposed protocol has less computation costs and lower computation. In order to design a low-computation and high- efficient 3PAKE protocol for mobile applications, Li et al. [7] proposed a three-party password- authenticated multiple key exchange(3MPAKE) protocols for wireless mobile networks to improved computation costs. The 3MPAKE protocol allows two communication parties to establish session keys and authenticate each other with the help of server.

III. PROBLEM DEFINITION

For secure communication in network environment, TTP based key exchange protocol is used to protect messages delivered between two authorized users. But this, unreliability, inflexibility, and inefficiency problems still exists. In this paper we have tried to avoid these types of problems and provide users with reliable, high- efficient and scalable key exchange method for data communication using secure multi-key exchange protocol.

IV. PROPOSED SYSTEM

To design a multi-key exchange key, named the secure multi-key exchange protocol based on trusted third party, to provide reliable, scalable and high-efficient protocol.

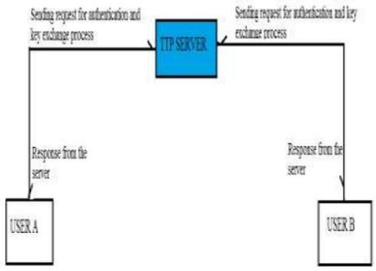

Fig. 1 System architecture

In this paper, mainly concentrated on secure multi-key exchange protocol based on trusted third party. This protocol also comprises two phases, namely initialization phase and authentication and key exchange phase.

1) Initialization phase

In this phase, system parameters are generated by Trusted Third Party(TTP) server. Firstly, TTP server chooses two prime numbers q and n and a finite field over q> . Then TTP server

1. Specifies an elliptic curve equation E: ≡ + ax + b(mod q) with the order n over F_q where a,b ε F_q and $4a^3+27b^3 \neq 0$ (mod q);
2. Chooses a public point P and create a cyclic additive G by using P, where both P and G are of the same order of n over E;
3. Determine a secure hash function $H_5: U^7 * G^2 \rightarrow Z_n^*$;
4. Determine a secure pseudo-random function F;
5. Declare the system parameters{ G, P, H_4, F}

Assume that user A and user B would like to join the system

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 4, April 2017

1. User A(B) determines its own password $pw_A(pw_B)$ from the password space D;
2. TTP server then produce the password keys k_{pwA} and k_{pwB} for users A and user B.

2) Authentication and key exchange phase

As shown in the Fig.1, with the help of TTP server, user A and user B are able to individually produce the same session keys for future communication by the following procedures.

Round 1:

TTP server,

a) Select two random numbers $s_A, s_B \in Z_n^*$;
b) Fetches its system time $t_{nonce,s}$ and produce k_{CT} from $t_{nonce,s}$;
c) Calculates $S_A \equiv s_A P$, $S_B \equiv s_B P$, $s'_A = [s_A \oplus (k_{CT} \oplus k_{pwA})] +_2 (k_{CT} +_2 k_{pwA})$ $s'_B = [s_B \oplus (k_{CT} \oplus k_{pwB})] +_2 (k_{CT} +_2 k_{pwB})$;
d) Delivers $\{ID_S, t_{nonce,s}, s'_A, S_A\}$ to user A and $\{ID_S, t_{nonce,s}, s'_B, S_B\}$ to user B.

Round 2:

a. Upon receiving the message , user A
b. Fetches its system time $t_{nonce,A}$;
c. To verifies whether or not $t_{nonce,s}$ satisfying $|t_{nonce,A} - t_{nonce,s}| \leq \Delta t$, where Δt is a predefined time threshold for the allowable maximum transmission delay from TTP server to user A.
d. Produce k_{CT} from $t_{nonce,s}$;
e. Computes $s_{A,C} = (s'_A -_2 (k_{CT} +_2 k_{pwA})) \oplus (k_{CT} \oplus k_{pwA})$ and $S_{A,C} \equiv s_{A,C}.P$
f. Checks to see whether $S_{A,C} \equiv S_A$; If not, it discards this message. Otherwise, go to next step.
g. User A generate a random number x_A;
h. Calculates $X_A \equiv x_A P$ and $x'_A = [(x_A \oplus s_A) \oplus k_{CT}] +_2 (k_{CT} \oplus k_{pwA})$;
i. Sends $\{ID_A, x'_A, X_A\}$ to server TTP server.

The same steps have been done by user B with the subscript A substituted by B.

Round 3:

Upon receiving message $\{ID_A, x'_A, X_A\}$ from user A, TTP server S

a. Computes $x_{A,c} = \{[x'_A -_2 (k_{CT} \oplus k_{pwA})] \oplus k_{CT}\} \oplus s_A$ and $X_{A,C} \equiv x_{A,C}.P$;
b. Checks to see whether $X_{A,C} \equiv X_A$;
c. If not, S discards this message. Otherwise, go to next step a.
d. Similarly, S computes $x_{B,C}, X_{B,C}$ and undergoes the check for B, aa mentioned in step a.
e. TTP server S computes $\eta_A = H_5(ID_A, ID_S, ID_B, x_A, s_A, X_B, S_B, k_{pwA}, k_{CT})$, and $\eta_B = H_5(ID_B, ID_S, ID_A, x_B, s_B, X_A, S_A, k_{pwB}, k_{CT})$;
f. Sends $\{ID_S, ID_B, X_B, S_B, \eta_A\}$ to user A and $\{ID_S, ID_A, X_A, S_A, \eta_B\}$ to user B.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 4, April 2017

Key computation:

User A,

a. Computes $\eta_{A,C}=H_5(ID_A, ID_S, ID_B, x_A, s_A, X_B, S_B, k_{pwA}, k_{CT})$;
b. Checks to see whether $\eta_{A,C}= \eta_A$;
c. If not, it discards this message. Otherwise, it computes
d. $K_{A1} \equiv x_A X_B, K_{A2} \equiv x_A S_B, K_{A3} \equiv s_A X_B, K_{A4} \equiv s_A S_B$ and
e. $SK_{Aj}= F_{KAj}(ID_s, ID_A, ID_B)$, where j={1,2,3,4}.
f. Analogously, user B Computes and verifies $\eta_{B,C}$ with the process similar to that mentioned in step a;

g. Calculates $K_{B1} = x_B X_A, K_{B2} = x_B S_A, K_{B3} = s_B X_A, K_{B4} = s_B S_A$ and $SK_{Bj}= F_{KBj}(ID_s, ID_A, ID_B)$, where j={1,2,3,4}.

V. CONCLUSION

To improve the performance and security of the key exchange process in mobile communication, in this paper, propose a secure multi key exchange protocol based on the trusted third party server. This protocol has lower computation and communication costs and impersonation attacks. Besides, this protocol can resist eavesdropping, replay, impersonation, known key attacks and achieve efficiency, reliability and scalability at the same time.

REFERENCES

[1] S. M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure against Dictionary Attacks," in Proceedings of the Symposium on Security and Privacy,pp. 72-84, may 1992.

[2] M. Abdalla and D. Pointcheval, "Simple Password-based Encrypted Key Exchange Protocols", Topics in cryptology-CT-RSA 2005, LNCS Springer-Verla,pp, 191-208,2005.

[3] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-Based Authentication Key Exchange in the Three-Party Setting," in Proceedings of the International Workshop on Theory and Practice in Public Key Cryptography, pp. 65-84, January 2005.

[4] R.X. Lu and Z.F. Cao, "Simple Three-Party Key Exchange Protocol," computers and security, vol. 26, no. 1,pp. 94-97, February 2007

[5] H.R. Chung and W.C Ku, "Three weaknesses in a Simple Three-party Key Exchange Protocol," Information Sciences. vol. 178, no. 1, pp. 220-229, January 2008.

[6] J.H. Yang and C.C. Chang," An Efficient Three-Party Authenticated Key Exchange Protocol Using Elliptic Curve Cryptography for Mobile Commerce Environment," Journal of Systems and Software, vol. 82, no. 9, pp. 1497-1502, September 2009.

[7] W. M. Li, Q. Y. Wen, Q. Su, H. Zhang, and Z. P. Jin, "Password-Authenticated Multiple Key Exchange Protocol for Mobile Application", China Communications, vol. 9, no. 1, pp. 64-72, January 2012.