Delay-Tolerant Network Based Secure Transmission System Design

Gang Ming[1] and Zhenxiang Chen[1,2(✉)]

[1] School of Information Science and Engineering, University of Jinan, Jinan, China
czx@ujn.edu.cn

[2] Shandong Provincial Key Laboratory of Network Based Intelligent Computing, Jinan, China

Abstract. The Internet has been a great success but its architecture need relatively complete infrastructure construction to implement and operate. Especially, the situation worsens on resource-limited devices, so delay-tolerant network was proposed to overcome these disadvantages. The development of delay-tolerant network provides a new approach to transmit data but its confidentiality and integrity cannot be guaranteed well. The public-key cryptography provides a feasible mechanism to protect data. However, the maintenance cost of certificate authorities is large. Identity-based cryptography allows users to encrypt message with their identity information. Based on the above-mentioned technologies, we proposed a secure transmission system based on delay-tolerant network and identity-based cryptography, which does not rely on traditional key distribution mechanism and simplifies identity verification.

Keywords: Delay-tolerant network · Identity-based cryptography · Identity-based encryption · Secure transmission system

1 Introduction

The Internet has been a highly successful architecture and protocol at interconnecting communication while operating poorly environments characterized by long delay path and distributed network location. In addition, the resource usage for end nodes is unfriendly. Delay-tolerant network (DTN) is an overlay on top of special-purpose networks including the Internet which can accommodate long distributions and delays among those networks so that it is fit for embedded devices communication. Since communications are supposed to store and transmit data among lots of nodes, malicious nodes constructed intentionally may catch and modify data packets that are not belong to them.

Public-key cryptography (PKC) is a cryptographic system using pairs of keys which public key may be disseminated widely and private key is only known to the owner. Certification authority (CA) is introduced for issuing public and private keys. However, it is almost infeasible to establish such CAs at DTN due to frequent network partitions and high latency so that the confidentiality

J. Wan et al. (Eds.): CloudComp 2016, SPNCE 2016, LNICST 197, pp. 227–231, 2018.
https://doi.org/10.1007/978-3-319-69605-8_21

and integrity of data cannot be guaranteed. To handle this problem, we choose identity-based cryptography (IBC) which allows a sender to encrypt a message to an identity without access to a public key certificate.

We designed a secure transmission system by applying DTN and IBC which can deploy on embedded devices to communicate in Internet of Things, Internet of Cars, etc.

2 Related Work

DTN was proposed by Fall [1]. Internet Research Task Force (IRTF) founded Delay Tolerant Networking Research Group (DTNRG)[2] that formulated DTN architecture [3] and bundle protocol specification [4].

In 1984, Shamir proposed a concept of identity-based cryptography [5]. In this theory, users' email or IP address can be used as public key for encryption and signature scheme without managing public key infrastructure. Certificateless public key cryptography (CL-PKC) was proposed by Al-Riyami and Paterson [6] to overcome the disadvantages associated with public key infrastructure (PKI) and identity-based public key cryptography (ID-PKC) which does not require the use of certificates and built-in key escrow of ID-PKC.

Current identity-based encryption schemes are based on bilinear group, but its computational efficiency limits real-world applications. Guo and others [7] proposed Online/Offline IBE (OO-IBE) to reduce encryption time. The application of identity-based cryptography in wireless networks is comprehensive. Shim et al. [8] proposed EIBAS: An efficient identity-based broadcast authentication scheme. A fuzzy identity-based encryption (FIBE) scheme [9] is used for resolving data transmission security problem in Internet of Things (IoT).

3 System Architecture

Our work is based on DTN and IBC. Due to the latency and unstable connection status of point-to-point communication in delay-tolerant network, public key infrastructure is almost unavailable so that we use identity-based cryptography to implement identification of endpoints.

3.1 The Implementation of Delay-Tolerant Network

We implement a simple delay-tolerant network model with libevent, a library that provides asynchronous communication. How to figure the path from source node to destination node aka routing in delay-tolerant network is a critical problem. Traditional routing algorithms cannot accommodate, so modified Dijkstra algorithm using time-varying edge costs [10] is recommended.

Algorithm 1 shows the logic. s is the source node. T is the start time. L is the array returning the cost of the shortest path for all nodes. $G(V, E)$ is the map of DTN. $w(e, t)$ is the cost function. e is an edge from node u to node v.

Algorithm 1. Dijkstra's Algorithm modified to use time-varying edge costs.

Require: G=(V, E), s: source node; t: start time; W(e, t)
Ensure: L;
1: $Q \leftarrow \{V\}$
2: L[s] $\leftarrow$ *0*, L[v] $\leftarrow \infty \; \forall \; v \in V \; s.t \; v \neq s$
3: **while** $Q \neq \{\}$ **do**
4: Let $u \in Q$ be the node s.t L[u] = $min_{x \in Q}$ L[x]
5: $Q = Q \leftarrow \{u\}$
6: **for** each edge $e \in E$, s.t. $e = (u, v)$ **do**
7: **if** L[v] > (L[u] + $w(e,$ L[u] + $T)$) **then**
8: L[v] $\in$ L[u] + $w(e$,L[u] + $T)$
9: **end if**
10: **end for**
11: **end while**

The DTN architecture implements store-and-forward message by overlaying a new transmission protocol called the bundle protocol. When a node receive information, it should judge whether it is receiver or it shall transmit it.

3.2 Key Distribution

We deploy key generation center (KGC) and key privacy authority (KPA) to maintain user register information and issue key (Fig. 1 shows the system). KGC records secret parameter B. KPA provides key distribution and query user information form KGC according to user requests. Calculate key encrypted with secret parameter s and public parameter $P, P_{pub}, H_1, H_2, H_3$ to send to users if identity confirmed as following. The encryption of key and signature is based on type A of pair of curves from PBC library.

$$K = H_3(A \cdot B \cdot P) \tag{1}$$

$$D_{ID} = s \cdot H_1(ID) \tag{2}$$

$$D = DES_k(D_{ID}) \tag{3}$$

Users can get private key D_{ID} as following after receiving encrypted key from KPA.

$$K = H_3(B \cdot A \cdot P) \tag{4}$$

$$D_{ID} = DES_k(D) \tag{5}$$

3.3 Signature Scheme

User generates a random number $K \in Z_q$ and calculates signature R of message M.

$$R = K^{-1}(H_2(M) \cdot P + H_3 \cdot (R) \cdot D_{ID}) \tag{6}$$

Receiver should calculate *ê(U, V)* and compare with to verify signature. If (R, S) is a available signature on message M, we will get

$$\hat{e}(R, S) = \hat{e}(P, P)^{H_2(M)} \cdot \hat{e}(P_{pub}, Q_{ID})^{H3(R)} \tag{7}$$

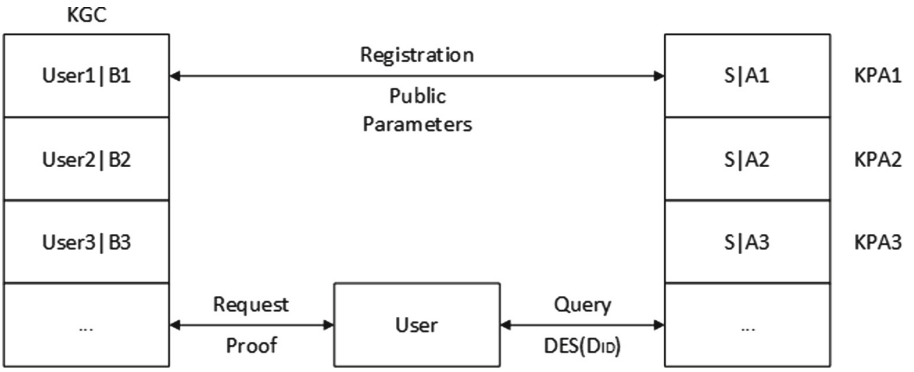

Fig. 1. Key distribution system

3.4 Identity-Based Encryption

An Identity-Based Encryption system (IBE) consists of four algorithms: Setup, Extract, Encrypt and Decrypt. The Setup algorithm generates system parameters and a master key by PKG one time for initializing IBE environment. The Extract algorithm uses the master key to extract a private key when PKG respond a request form users. The encryption algorithm encrypts messages with given identity and system parameters outputting cipher texts. In the end, the decryption algorithm decrypts encoded data using the private key.

4 Evaluation

With the development of IoT, there need a new and secure approach to transmit data. TCP/IP protocol suite, ZigBee and Bluetooth are alternative but their disadvantages are also obvious. ZigBee and Bluetooth are used for short-distance wireless data exchange while TCP/IP performs well at traditional scenes. Our work accommodate distance-varying and frequent network partitions without additional channel resource requirement. We use IBC to ensure the security of data and identities of nodes without construction of PKI reducing the requirement of networks and devices, which keeps DTN light and effective. Therefore, the security of data is also guaranteed.

The system can be applied to anonymity networks like Tor and temporary communication at disaster-affected area. Our system allows users to improve privacy and security with a new architecture avoiding existing monitoring measures. The communication at earthquake zone will break off and the top priority is to recover communication to coordinate rescue efforts. Rescuers can use mobile devices like cellphone to set up simple and secure communication network with our system.

5 Conclusion

DTN is a new type wireless network accommodating asynchronous network to provide interoperable communications between a wide range of networks which may have exceptionally poor and disparate performance characteristics. Our work provides an effective and secure approach to transmit information. However, DTN cannot afford large traffic transmission so it can be only used at discrete and small data exchange. Due to the unstable connection path and status, data delivery speed may be low.

Acknowledgments. This work was supported by the National Natural Science Foundation of China under Grants Nos. 61672262 and 61472164, the Natural Science Foundation of Shandong Province under Grants Nos. ZR2014JL042 and ZR2012FM010, the Shandong Provincial Key R&D Program under Grants No. 2016GGX101001 and the Program for youth science and technology star fund of Jinan No. TNK1108.

References

1. Fall, K.: A delay-tolerant network architecture for challenged internets. In: Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp. 27–34. ACM (2003)
2. Delay tolerant networking research group. http://www.dtnrg.org
3. Delay-tolerant networking architecture. https://www.rfc-editor.org/rfc/pdfrfc/rfc4838.txt.pdf
4. Bundle protocol specification. https://www.rfc-editor.org/rfc/pdfrfc/rfc5050.txt.pdf
5. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
6. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40061-5_29
7. Guo, F., Mu, Y., Chen, Z.: Identity-based online/offline encryption. In: Tsudik, G. (ed.) FC 2008. LNCS, vol. 5143, pp. 247–261. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85230-8_22
8. Shim, K., Lee, Y., Park, C.: EIBAS: an efficient identity-based broadcast authentication scheme in wireless sensor networks. Ad Hoc Netw. **11**(1), 182–189 (2013)
9. Mao, Y., Li, J., Chen, M., Liu, J., Xie, C., Zhan, Y.: Fully secure fuzzy identity-based encryption for secure IoT communications. In: Computer Standards and Interfaces, vol. 44, pp. 117–121. Elsevier (2016)
10. Jain, S., Fall, K., Patra, R.: Routing in a Delay Tolerant Network, vol. 34. ACM, New York (2004)