Multimed Tools Appl
DOI 10.1007/s11042-015-3187-z

Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks

Hyunsoo Kwon[1] · **Daeyeong Kim**[1] · **Changhee Hahn**[1] · **Junbeom Hur**[1]

Received: 27 July 2015 / Revised: 28 October 2015 / Accepted: 18 December 2015

Abstract With the dramatic increase of the number of mobile devices such as smartphones and tablet PCs, mobile traffic has increased enormously. Especially, the multimedia data accounts for bulk of the traffic transmitted in mobile networks. To accommodate this growth, device-to-device connection (D2D), which provides infra-connection off-loading, is receiving significant attention. However, we have observed that the majority of the current D2D protocols including Bluetooth and Wi-Fi Direct are vulnerable to man-in-the-middle (MITM) and replay attacks in mobile multi-hop networks. To resolve this problem, in this paper, we propose a novel D2D authentication protocol with a secure initial key establishment using ciphertext-policy attribute-based encryption (CP-ABE). By leveraging CP-ABE, the proposed scheme allows the communicating parties to mutually authenticate and derive the link key in an expressive and secure manner in a multi-hop network environment. We also propose several variations of the proposed scheme for different scenarios in a multi-hop networks without network infrastructure. We prove that the proposed scheme is secure against MITM and replay attack in D2D mobile multi-hop networks. Experimental results indicate that the proposed scheme incurs reasonable computation cost in the real world.

Keywords D2D communication · Mobile multi-hop networks · CP-ABE · Authentication

✉ Junbeom Hur
jbhur@korea.ac.kr

Hyunsoo Kwon
hs_kwon@korea.ac.kr

Daeyeong Kim
rlaeod@korea.ac.kr

Changhee Hahn
manjungs@gmail.com

[1] Department of Computer Science and Engineering, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 136-701, Republic of Korea

Published online: 09 January 2016

1 Introduction

An enormous increase in usage of smart devices has resulted in a significant growth in mobile traffic. According to [6], mobile traffic will increase by a factor of 18 during the 5-year period beginning 2011 and expand three times faster than the growth of static IP traffic. Since the multimedia data traffic is in charge of mobile traffic and its size is relatively larger than other traffic size, the multimedia data traffic incurs a lot of overhead in communication networks. Because of this trend, the device-to-device (D2D) connection technique is receiving increased attention. This technique has the effect of reducing the concentrated infrastructure traffic because personal smart devices can communicate directly without using a network infrastructure. Furthermore, D2D standardization which supports location-based applications, has been developed by several IEEE communication working groups including IEEE 802 and 3GPP. The IEEE 802.15.8 working group is now developing PAC (Peer Aware Communication) specification [11] and 3GPP SA is developing ProSe (proximity Service) specification [1], which constructs a new mobile ecological system. For example, when a user enters a convenience store, the user can automatically obtain discount coupons and sale item information for the day in real time through a mobile device.

The D2D technique is currently available and widely used in current mobile environments such as Bluetooth and Wi-Fi Direct. Bluetooth supports authentication between different devices using a pre-shared PIN [18]. The Wi-Fi Direct protocol has been constructed based on Wi-Fi. It forms a group composed of a group manager and multiple clients. Each client can communicate directly to the manager [5]. However, in a multi-hop network environment where multiple relaying nodes exist between communicating parties, current D2D protocols cannot guarantee confidentiality or integrity of communications because malicious intermediate nodes can perform man-in-the-middle (MITM) and replay attacks during the transmission.

In this paper, we extend our previous work published in [16], which proposed an authentication protocol for D2D communications in a mobile multi-hop network environment. The proposed scheme enables end users to share initial secret keys in a scalable and secure manner by exploiting the ciphertext-policy attribute-based encryption (CP-ABE) scheme. Further, message integrity code generated by the PIN and sequence number is included in the messages to enhance security in the mobile multi-hop network. In this paper, we extend our previous work [16] by implementing our scheme, and analyzing its efficiency and security more rigorously.

The proposed scheme is based on the Bluetooth protocol. However, the initial secret key distribution process can be independently designed allowing the proposed scheme to be used in other D2D authentication protocols such as Wi-Fi Direct. Based on a security analysis, the proposed scheme has an acceptable cost and is secure against man-in-the-middle and replay attacks in the presence of malicious relaying nodes in a mobile multi-hop networks.

2 Related work

In this section, we introduce the mobile multi-hop network. Further, we present the authentication process and its security flaws in Bluetooth and Wi-Fi Direct pairing procedures for this network.

2.1 Mobile multi-hop network

An ad hoc network [22] features a mechanism that permits multiple nodes to compose a flexible and dynamic network without an infrastructure, such as a mesh network [4] or sensor network [9]. When it is composed of mobile nodes, it is called a Mobile Ad Hoc Network (MANET). Because each mobile node maintains a routing table for the networks and has the capability for routing information management, these mobile nodes establish networks for communication themselves, without infrastructure such as base stations or access points [8, 17]. Furthermore, the communication range of each mobile node can be extended by relaying it through multiple relaying nodes that are deployed in the middle of the communicating parties.

Compared to a direct communication environment, several novel security challenges must be considered in a mobile multi-hop network. The first challenge is the initial key establishment issue. Sharing initial secret keys with all of the different nodes in advance, especially in a large-scaled network, is impractical owing to the limited storage space of the mobile devices. Moreover, malicious relaying nodes can attempt man-in-the-middle attacks that can maliciously change the message or modify the authentication information that is being communicated between mobile nodes. The malicious relaying nodes are also able to capture previously sent messages en route and perform replay attacks that fraudulently repeat the stored messages in the mobile multi-hop network. Thus, scalable and secure key management and authentication protocols are necessary for secure D2D communications in mobile multi-hop networks. There have been several protocols proposed addressing this problem for the mobile multi-hop network, [10, 19, 20]. However, they only function in a static network structure. Moreover, existing authentication protocols [14, 27] in MANET exploit Public-Key Infrastructure (PKI) to prove identity of mobile nodes. This is not suitable for D2D infrastructureless environments.

2.2 Bluetooth pairing

Bluetooth is used for transferring data and short-range communication using low power [18]. Bluetooth devices authenticate with each other through a pairing process. Pairing verifies authenticity of each device. If authenticated, it allows the devices to generate a common link key.

Figure 1 illustrates the pairing process used to generate a link key using a shared PIN. To begin, Device A, which is a master device, acquires the PIN from the user and generates IN_RAND, which is a 128-bit random number. It then generates the initial key, K_{init}, using hash function E22 on the input address of slave device $ADDR_B$, the PIN, and IN_RAND. K_{init} is used to generate the link key, which is an encryption key for secure communications after the pairing process. After creating K_{init}, A transfers IN_RAND in plaintext to slave Device B. The slave device enters the PIN and obtains K_{init} in a manner similar to the master device. It then generates the link key for secure communications.

To secure the authentication process, the PIN must be shared between the devices in advance. In short distance communication, it is possible to share the secret information beforehand through direct communication between the devices. However, in a mobile multi-hop network environment, it is a challenge to share the PIN in advance making

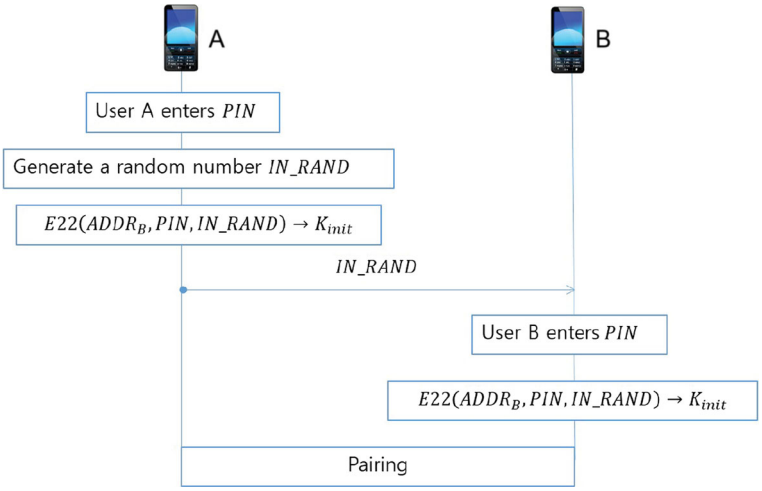


Fig. 1 Bluetooth pairing

the authentication process impossible and vulnerable to replay and MITM attacks [15]. Therefore, in a mobile multi-hop network environment, it is important to share the PIN safely for mutual authentication. When the PIN is sent as plaintext through a mobile multi-hop network, intermediate relaying nodes or outside adversaries can obtain the information illicitly. Further, using symmetric encryption for sharing the PIN incurs a scalability problem in key management because when the size of the network is N, the key size results in $O(N^2)$, rendering the keys difficult to manage in the network.

2.3 Wi-Fi direct pairing

Wi-Fi Direct [5] is based on the IEEE 802.11 standard [12]. It enables Wi-Fi devices to connect to each other directly. Wi-Fi Direct guarantees enhanced Quality of Service (QoS) [25] and security mechanisms [26], which are inherited properties from the Wi-Fi protocol. A device equipped with Wi-Fi Direct communication capability is called a P2P device. A P2P group consists of a P2P group owner (P2P GO) and clients.

Figure 2 illustrates the process of Wi-Fi Direct pairing. In the "Discovery" phase, a P2P device alternately switches between "listen" and "search" status to determine if there are other P2P devices. Once other P2P devices are found, they determine their roles between P2P GO and P2P client using a three-way handshake. This phase is called "GO Negotiation". In Fig. 2, Device A represents a P2P GO and B is a P2P client. In the subsequent WPS provisioning phase, P2P devices perform mutual authentication and share an encryption key. WPS provisioning is composed of Phase 1 and Phase 2. In Phase 1, P2P devices generate and share a master key. Then, using a 4-way handshake, they generate a link key from the shared master key in Phase 2.

In one-hop communications, the Wi-Fi Direct protocol provides secure authentication in the presence of outside adversaries. However, in a mobile multi-hop network, the authentication protocol cannot guarantee security owing to intermediate relaying nodes that can maliciously forge the messages or perform relay and MITM attacks en route.

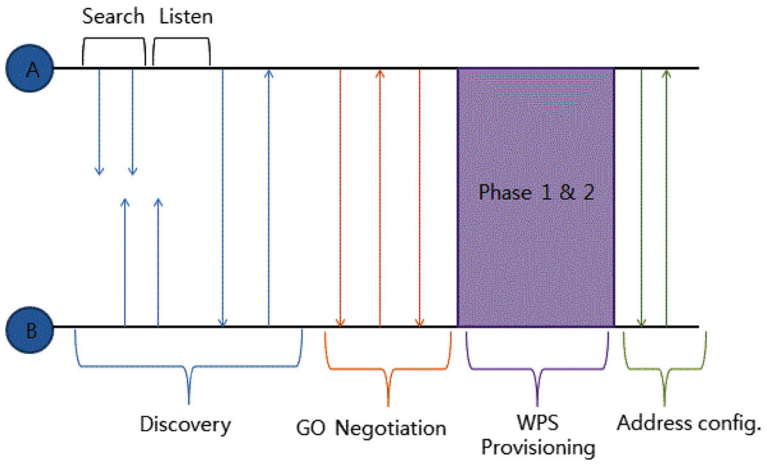


Fig. 2 Wi-Fi direct pairing

3 Secure D2D authentication protocol in mobile multi-hop networks

3.1 Attribute-based encryption

A public key cryptosystem is a promising solution to share initial secret keys between communicating parties in a mobile multi-hop network. However, public key encryption can only be implemented in PKI, which includes a trusted server for managing certificates. In an ad hoc network, public key encryption is difficult to implement because these networks are infrastructureless. Attribute-based encryption (ABE), however, is a possible solution for scalable and secure key distribution in such a multi-hop environment [24]. ABE has evolved from fuzzy identity-based encryption, which is based on identity-based encryption [3, 7, 23]. We assume that w and w' denote independent sets of attributes associated with a ciphertext and a user, respectively. Then, to decrypt a ciphertext encrypted with w, the overlapped value between user's attribute w' and w must be satisfied beyond a specific, predefined threshold. Accordingly, ABE can provide secure communication, without infrastructure, using only people's attributes. However, ABE could cause a problem in a specific individual communication because it uses a predefined threshold. Therefore, CP-ABE is proposed for fine-grained access control [2]. In CP-ABE, when generating ciphertext, the encryption key is generated directly by the sender's access policy. This allows refined management on the receiver as to its ability to decrypt the ciphertext without infrastructure. For example, an administrator of A school's grade evaluating program can use this to the access policy for encrypting the data. ((“workplace: A school” AND “party: B department”) OR “department number: 19253” AND (position > assistant professor)).

3.2 Proposed scheme

In this section, we propose a device-to-device authentication (D2DA) protocol that is secure in a mobile multi-hop network environment. The proposed scheme is constructed based on the Bluetooth authentication protocol by adding an additional initial-key sharing process. It enables scalable and secure initial key establishment in a mobile

multi-hop network environment. Further, the existing Bluetooth protocol is modified such that it is secure against replay and modification attack by malicious relaying nodes. Although the proposed scheme is developed based on the Bluetooth protocol, it is not limited to Bluetooth protocol and cloud be applicable to other direct communication protocols such as Wi-Fi Direct.

A mobile multi-hop network provides two possible scenarios. First, a device may wish to communicate with either an arbitrary mobile device or a specific group composed of multiple devices. Alternatively, a device may want to communicate with a specific device in a group. To address these two scenarios, we propose two authentication protocols Device-to-Device Authentication 1 (D2DA1) and Device-to-Device Authentication 2 (D2DA2), respectively. We assume that the attribute keys are distributed to each device during the initial setup phase before the proposed authentication protocol.

3.2.1 D2DA1

In this section, we present the D2DA1 protocol. This supports device-to-device and device-to-group authentication and communication. As mentioned previously, Bluetooth must share the PIN before pairing. However, in a mobile multi-hop network environment, it is difficult to guarantee the confidentiality and integrity of sharing secret information through D2D communication. Therefore, D2DA1 exploits CP-ABE, which enables a sender to define an access control policy and enforce it on the encrypted data. Thus, the sender can selectively distribute the PIN to a set of selected receivers in a scalable and secure manner. Additional random number and message integrity code (MIC) is adopted in the protocol to enhance integrity and confidentiality of authentication messages. Figure 3 illustrates the D2DA1 authentication procedure.

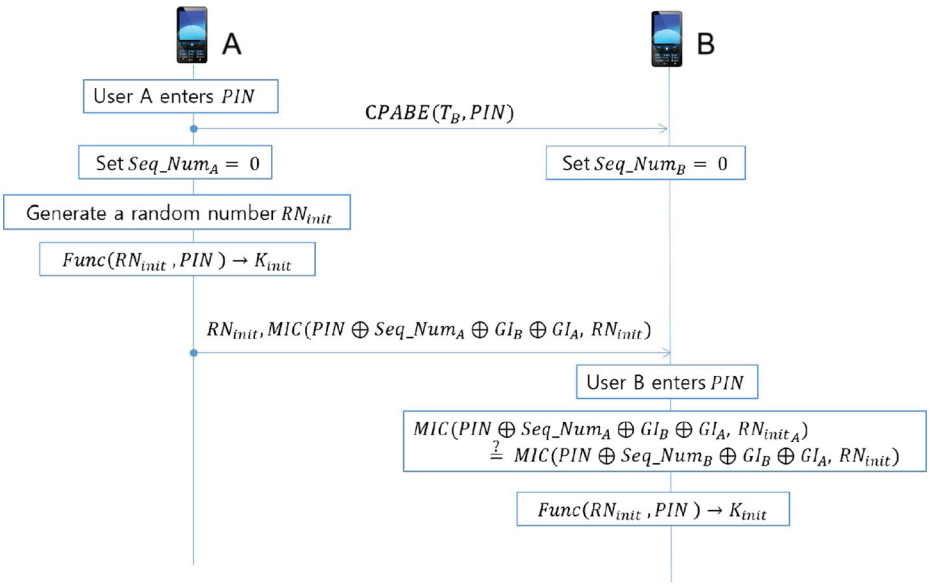


Fig. 3 D2DA1 authentication procedure

The D2DA1 protocol executes as follows:

1. User A enters the PIN to Device A
2. A → B: $CPABE(T_B, \text{PIN})$

Device A defines an access policy T_B with a set of attributes, encrypts the PIN using T_B, and sends it to Device B. Device A resets the Seq_Num to zero when transferred. Device B also resets the Seq_Num to zero when it receives the data from Device A. Device A generates a 128-bit random number. It then generates the initial key, K_{init}, using pseudo random function *Func* on inputs RN_{init} and PIN.

3. A → B: RN_{init}, $MIC(\text{PIN} \oplus \text{Seq\_Num} \oplus GI_B \oplus GI_A, RN_{init})$

Device A sends RN_{init} in plaintext and the MIC of the RN_{init} generated with a key that is the XOR of A's Seq_Num, B's device information GI_B, A's device information GI_A, and the PIN to Device B. Device B decrypts the PIN from the ciphertext if its set of attributes satisfies the access policy T_B. Then, user B enters the PIN and generates the MIC of the received RN_{init} with a key, PIN ⊕ Seq_Num ⊕ GI_B⊕ GI_A. If the MIC from B is equal to the MIC from A, B can generate an accurate initial key K_{init} using the pseudo random function *Func* on inputs RN_{init} and PIN.

Device-to-group authentication is similar to the above protocol except that GI_B is replaced by group information such as a group ID. After sharing the initial secret key, the other procedures for generating a link key are the same as the Bluetooth protocol.

3.2.2 D2DA2

In this section, we propose a D2DA2 protocol for device-to-device in a specific group. In the D2DA2 protocol, we assume that there is a group manager (GM). For example, the GO in Wi-Fi Direct fulfills the role of GM. In an environment where all group members know the PIN and can generate the initial key, it is impossible for an arbitrary device and a specific device in the group to communicate privately. Therefore, a GM is selected for the specific role of making this authentication and communication possible.

Figure 4 illustrates a sample scenario. Suppose that the PIN is shared between Device A and Group G by D2DA1 protocol. When Device A wishes to communicate with Device B3 in Group G, the GM is selected first, using the following strategy: it must be a device that knows the locations of each member of the group and does not belong to the group. If Device A sends a request message to the GM that A wants to communicate with B3, the GM sends encrypted secret information, ES, which can only be decrypted by A and B3. Because, only Device A and B3 possess both the PIN and ES, they can generate another initial key that others cannot generate. Figure 5 illustrates the D2DA2 protocol.

The D2DA2 protocol executes as follows:

1. User A enters the PIN to Device A
2. A → G: $CPABE(T_G, \text{PIN})$

Device A defines access policy T_G with a set of attributes, encrypts the PIN using T_G, and sends it to the Group G. Device A resets the Seq_Num to zero when transferred. Group G also

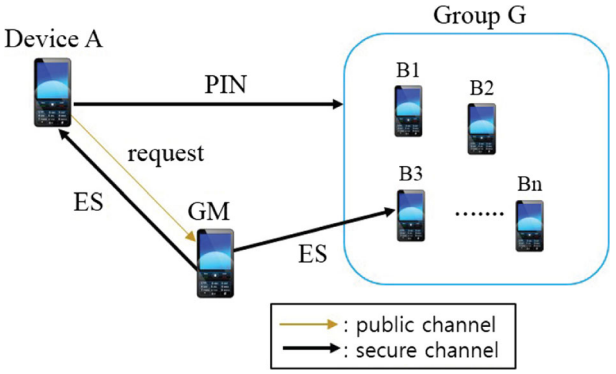


Fig. 4 Key sharing process in D2DA2

resets the Seq_Num to zero when it receives data from Device A. Device A generates a 128-bit random number. It then generates initial key, K_{init}, using pseudo random function *Func* on inputs RN_{init} and PIN.

3. A → G: RN_{init}, MIC(PIN ⊕ Seq_Num ⊕ GI_G ⊕ GI_A, RN_{init})

Device A sends RN_{init} in plaintext and the MIC of the RN_{init} generated with a key that is an XOR of A's Seq_Num, group information GI_G, A's device information GI_A, and the PIN to Group G. Any group member in G decrypts the PIN from the ciphertext if the set of their attributes satisfies access policy T_G. Then, Group G enters the PIN. Finally, G generates the MIC of the received RN_{init} with a key that is PIN ⊕ Seq_Num ⊕ GI_G ⊕ GI_A. If the MIC from G is equal to the MIC from A, G can generate an accurate initial key K_{init} using pseudo random function *Func* on inputs RN_{init} and PIN.

4. A → GM: Entity Request

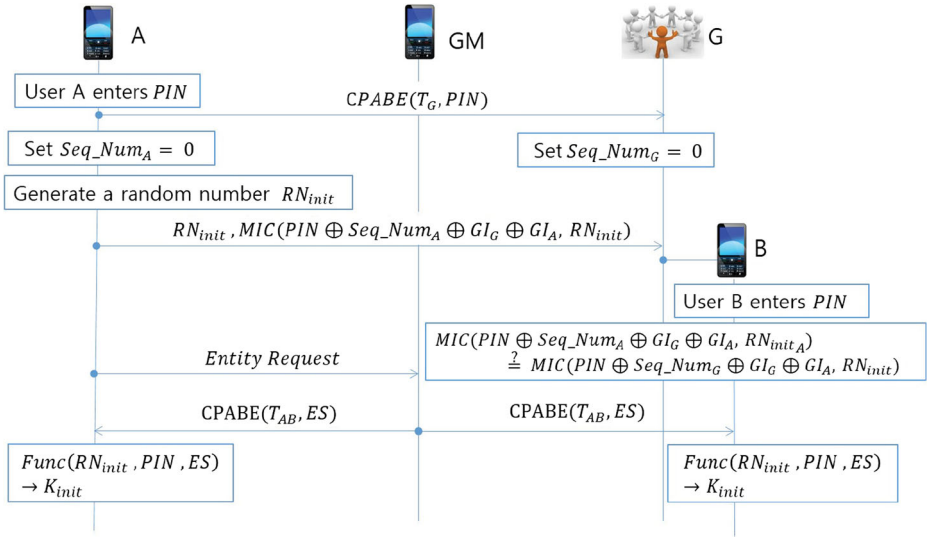


Fig. 5 D2DA2 authentication procedure

Device A sends the request message to the GM.

5. GM → A and B: $CPABE(T_{AB}, \text{ES})$

The GM encrypts the secret information ES using CP-ABE with access policy T_{AB} that is composed of the attributes of A and B. The GM sends the encrypted ES to A and B. Devices A and B obtain the ES by decrypting the message with their attributes. Then, they generate an initial key, $K_{init} = Func(RN_{init}, \text{PIN}, \text{ES})$.

4 Security and efficiency analysis

In this section, we examine the efficiency and security of the proposed scheme. We analyze the security against two common attacks: man-in-the-middle and replay. Furthermore, we address collision-resistance. Finally, we demonstrate how the scheme has been enhanced for computation, storage, and communication considerations and include experimental results.

4.1 Security anaylsis

4.1.1 Collusion-attack

One of the principal security challenges in ABE is collusion attack. This attack allows different users to combine their attributes to decrypt a ciphertext even if their attribute sets do not satisfy the embedded access policy of the ciphertext individually. In mobile multi-hop networks, if the malicious relaying node can collude with any of other devices and obtain the PIN through the collusion attack, the entire authentication process will fail.

In CP-ABE, users' private keys are associated with sets of attributes whereas the ciphertext is associated with access structures. The set of attributes of every user is randomized using some personalized random number such that the attributes from different users cannot be combined to satisfy the access policy embedded in the ciphertext [2]. Therefore, colluding attackers cannot decrypt the ciphertext unless their own attribute sets satisfy the access policy of the ciphertext. The proposed schemes guarantee collusion-resistance against colluding attackers in mobile multi-hop networks.

4.1.2 Man-in-the-middle attack

In the D2DA1 scheme, when a sender device transmits secret information such as PIN, it is sent after encryption using the CP-ABE algorithm. It ensures that even if malicious nodes relay the authentication exchanges en route, they cannot obtain the secret information as long as their attributes do not satisfy the access policy embedded in the ciphertext. End-to-end confidentiality is guaranteed against the individual attack of malicious nodes [2]. Therefore, sharing the PIN is secure from man-in-the-middle attack. Further, message integrity is preserved owing to the adoption of the MIC for a random number, which is generated with a securely shared PIN. Thus, the PIN sharing process is secure against both outside and inside adversaries such as relaying nodes in a multi-hop network.

In the D2DA2 scheme, the message exchange procedure between a device and a group for sharing the PIN is the same as in the D2DA1 scheme. However, it adopts additional secret

information, ES. The group manager encrypts ES using CP-ABE with an access policy that can be satisfied only by the communicating parties' attributes and sends it to the communicating devices. It is not possible for another device to decrypt the message and acquire the ES. Even though every device in the same group has a PIN, they cannot generate K_{init} without the ES. Therefore, the D2DA2 scheme is also secure against man-in-the-middle attack in the presence of an inside attacker.

4.1.3 Replay-attack

In a mobile multi-hop network, replay attack is performed by the relay node. To prevent a replay attack, we adopt sequential number Seq_Num. When the PIN is shared, Seq_Num is reset to zero. Every time a device performs the protocol, Seq_Num increases by one. When a receiver obtains sender's Seq_Num from the MIC for the RN_{init}, it can determine if the message is replayed by comparing its own Seq_Num and sender's Seq_Num. If they are not the same, it indicates that the received message should be replayed by a malicious relay node. Otherwise, it is considered a legitimate message. Thus, it is secure against replay attack.

4.2 Efficiency anaylsis

In this section, we compare the Bluetooth, D2DA1, and D2DA2 protocols in terms of computation, storage and communication. We also examine the experimental results.

4.2.1 Computation cost

Table 1 presents the comparison results of the computation cost. It is categorized into two different phases: communication cost for (1) protocols before PIN establishment (Phase 1 in the table) and (2) protocols after PIN establishment (Phase 2 in the table). In both of the proposed schemes, unlike the Bluetooth protocol, CP-ABE encryption and CP-ABE decryption are implemented to send the PIN securely in a mobile multi-hop network. In Phase 2, computation for the MIC generation is required to guarantee message integrity. Although it incurs computation cost, message integrity is guaranteed, which cannot be preserved in Bluetooth. In the D2DA2 scheme, the secret information ES must be delivered to the communicating parties by the GM, which requires one CP-ABE encryption in the GM and one CP-ABE decryption in each device.

Table 1 Computation cost

		Bluetooth	D2DA1	D2DA2	
				Device	GM
Computation	Phase 1		CAE + CAD	CAE + CAD	
	Phase 2	3P + 6H + 2SE + 2SD	3P + 7H + 2SE + 2SD	3P + 7H + 2SE + 2SD + 2CAD	CAE

P pseudo random generator, *SE*/*SD* symmetric encryption/decryption, *H* hash function, *CAE*/*CAD* ciphertext-policy attribute-based encryption/decryption

Table 2 Storage cost

	Bluetooth	D2DA1	D2DA2
Storage	IN_RAND, PIN, BD_ADDR(A, B)	PIN, RN_{init}, GI(A, B), Seq_Num	PIN, RN_{init}, ES, GI(A, B), Seq_Num

IN_RAND, RN_{init} random number, *PIN* personal identification number, *ES* entity secure information, *BD_ADDR*(*A*,*B*), *GI*(*A*,*B*) device identifier, *Seq_Num* sequence number

4.2.2 Storage cost

Table 2 presents the storage cost of each scheme. A random number, the PIN, and device identifier are commonly store in all protocols. In the D2DA1 and D2DA2 schemes, however, each device stores Seq_Num. Seq_Num is used to prevent replay attack. The D2DA2 scheme requires that only the communicating devices store the secret key, ES, which is used to guarantee more fine-grained access control.

4.2.3 Communication cost

Table 3 presents the analysis results in terms of communication. In the case of Phase 1, the proposed scheme requires additional communication cost for the secure PIN sharing. In Phase 2, the proposed scheme requires additional communication cost for sending the MIC. We note that it is an inevitable cost to ensure that the protocols are secure against any inside or outside adversaries in a mobile multi-hop network. In the case of D2DA2, additional communication cost, $2S_C$, is required for delivering ES to the communicating parties securely.

4.2.4 Implementation

To evaluate the performance of the proposed schemes, we implemented the initial key establishment protocol on an Android smartphone using Java and the CP-ABE open source library [21] based on the Java pairing-based cryptography (JPBC) library [13]. Open source CP-ABE uses Type A in JPBC as a curve parameter. Moreover, to indicate communication time, we selected the Android Bluetooth API. The smartphone employed for the measurement was an Android4.3 with a Samsung Exynos 4412 Quad Core (1.4 GHz × 4) and 2 GB RAM.

On the test machine, the communication time of the encrypted data through the Bluetooth was 0.03 s, the MIC using the javax.crypto library was 0.0015 s, and the pseudo-random number generator using the java.security library required 0.001 s. As anticipated, the limitation

Table 3 Communication cost

		Bluetooth	D2A1	D2DA2	
				Device	GM
Communication	Phase 1	·	·	S_C	·
	Phase 2	S_{RN}	$S_{RN} + S_{MIC}$	$S_{RN} + S_{MIC}$	$2\ S_C$

S_{RN} random number size, S_{MIC} MIC size, S_C ciphertext size

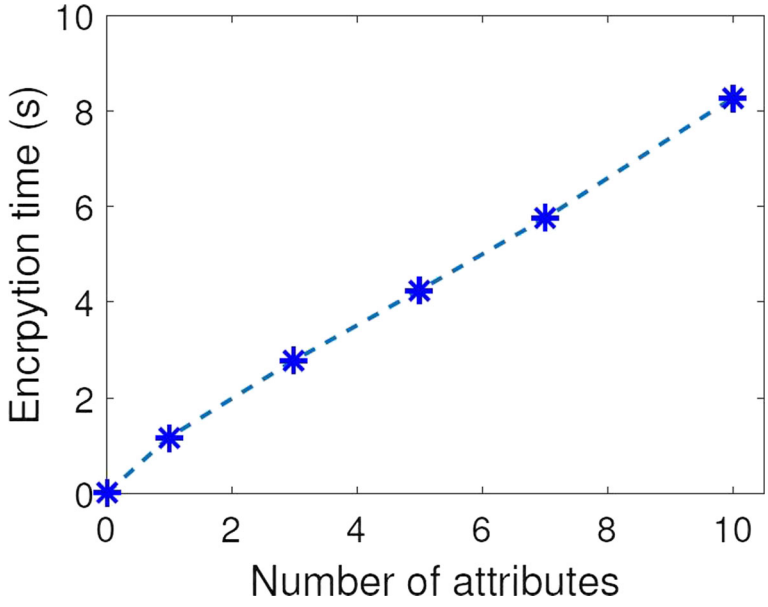


Fig. 6 Performance of the encryption time

of mobile computing power was the primary cause of the overhead in the encryption and decryption of CP-ABE.

Figure 6 indicates that the encryption time is proportional to the number of attributes in the access policy. The running time of the decryption is influenced by the complexity of the access policy rather than the number of attributes. If all the gates are OR gates in the access policy, the decryption cost would be constant as in Fig. 7a. Conversely, replacing those gates with AND gates, in Fig. 7b, renders the decryption time almost linear with respect to the number of attributes.

The performance demonstrates a reasonable result even though CP-ABE incurs relatively high cost. This is because it is done once and for a during the initial authentication procedure for the secure PIN delivery. When a device is authenticated again by devices with which it has previously authenticated, the CP-ABE computations need not to be performed afterwards.

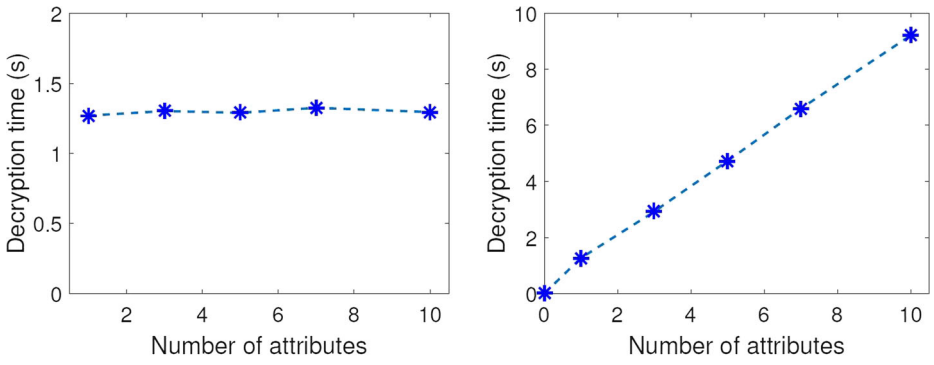


Fig. 7 Performance of the decryption time

5 Conclusion

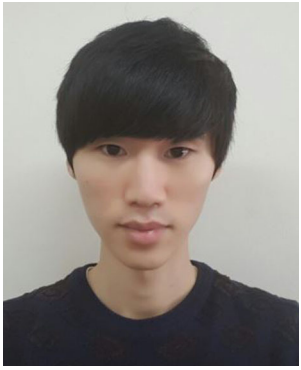
Device-to-device (D2D) communication is receiving significant attention owing to its applicability in infrastructureless network environments such as mobile multi-hop networks. However, current D2D authentication protocols cannot be used in multi-hop networks because they are vulnerable to inside attacks such as man-in-the-middle attack or replay attack by relaying nodes. In this paper, we proposed D2D authentication protocols using CP-ABE to resolve the issues regarding sharing the initial secret information securely under the attacks. Moreover, the proposed schemes guarantee the integrity of messages by implementing message integrity code. Although the proposed schemes are based on the Bluetooth protocol, the proposed schemes resolve the initial key establishment and integrity problems in the presence of inside adversaries in multi-hop networks. Therefore, the proposed schemes can be applicable to the other D2D protocols such as Wi-Fi Direct.

Acknowledgments This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2013R1A2A2A01005559). This work was also supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No. B0190-15-2028 and No. R0190-15-2011)

References

1. 3GPP (2012) Feasibility study on proximity-based services. Technical report, 3GPP
2. Bethencourt J, Sahai A, Waters B (2007) Ciphertext-policy attribute-based encryption. IEEE Symposium on Security and Privacy(SP'07):321–334
3. Boneh D, Matthew F (2001) Identity-based encryption from the Weil Pairing. CRYPTO, LNCS:213–229
4. Bruno R, Conti M, Gregori E (2005) Mesh networks: commodity multihop ad hoc networks. Commun Mag, IEEE 43(3):123–131
5. Camps-Mur D, Garcia-Saavedra A, Serrano P (2013) Device-to-device communications with Wi-Fi direct: overview and experimentation. Wirel Commun, IEEE 20(3):96–104
6. CISCO (2014) Cosco visual netowking index: global mobile data traffic forecast update, 2013–2018. White paper
7. Cocks C (2001) An identity based encryption scheme based on quadratic residues. Cryptography and Coding 2001, LNCS:360–363
8. Corson S, Macker J (1999) Mobile Ad hoc Networking(MANET): routing protocol performance issues and evaluation considerations. IETF RFC 2501
9. Estrin D, Girod L, Pottie G, Srivastava M (2001) Instrumenting the world with wireless sensor networks. International Conference on Acoustics, Speech and Signal Processing (ICASSP 2001), Salt Lake City, Utah 4:2033–2036
10. Huang J, Huang C (2011) Secure mutual authentication protocols for mobile multi-hop relay WIMAX networks against rogue base/relay stations. 2011 I.E. Int Conf Commun:1–5
11. IEEE 802.15 WPAN Task Group8 peer aware communications, http://www.ieee802.org/15/pub/TG8.html
12. IEEE Computer Society LAN MAN Standards Committee (1997) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Technical report, IEEE Computer Society LAN MAN Standards Committee
13. Java Pairing-Based Cryptography Library(JPBC), http://gas.dia.unisa.it/projects/jpbc
14. Khalil I, Bataineh S, Qubajah L, Khreishah A (2013) Distributed secure routing protocol for Mobile Ad-Hoc networks. Comput Sci Inform Technol 2013:106–110
15. Kugler D (2003) Man in the middle attacks on bluetooth. Financial cryptography. LNCS:149–161
16. Kwon H, Hahn C, Kim D, Kang K, Hur J (2014) Secure device-to-device authentication in mobile multi-hop networks. Wireless Algorithms. Syst Appl:267–278
17. Kwon H, Shin J, Lee B, Choi J, Nam S, Lim S (2003) Technical trends on mobile Ad Hoc networks. Electron Telecommun Trends 18:11–24
18. Lee C (2006) Bluetooth security protocol analysis and improvements. M.Sc. thesis at San Jose State University, http://www.cs.sjsu.edu/faculty/stamp/students/cs298ReportSteven.pdf

19. Lee Y, Lee H, Lee G, Kim H, Jeong C (2009) Design of hybrid authentication scheme and key distribution for mobile multi-hop relay in IEEE 802.16j. Euro American Conference on Telematics and Information Systems: New Opportunities to increase Digital Citizenship 12
20. Mahmoud ME, Shen XS (2009) Anonymous and authenticated routing in Multi- Hop cellular networks. IEEE Int Conf Commun:1–6
21. Open source project ciphertext-policy attribute based encryption(CP-ABE), https://github.com/junwei-wang/cpabe
22. Perkins CE (2008) Ad Hoc networking. Addison Wesley Professional, Indianapolis
23. Sahai A (1985) Identity-based crptosystems and signature schemes. Advances in Cryptology-CRYPTO, LNCS:47–53
24. Sahai A, Waters B (2005) Fuzzy identity-based encryption. Advances in cryptology-EUROCRYPT, LNCS:457–473
25. Wi-Fi Alliance (2005) Quality of Service (QoS) Task Group, Wi-Fi Multi-media(including WMM PowerSave) Specification v1.1
26. Wi-Fi Alliance (2007) Wi-Fi protected setup specification. Wi-Fi Alliance Document
27. Xingliang Z, Shilian X (2012) A new authentication scheme for wireless Ad Hoc Network. 2012 Information management. Innov Manag Ind Eng 2:312–315



Hyunsoo Kwon received the B.S. degree of computer science and engineering from Chung-Ang University, Seoul, Korea, in 2014. He is currently pursuing the M.S. degree in the Department of Computer Science and Engineering, Korea University, Korea. His research interests include information security, mobile computing security, cyber security, and applied cryptography.

Daeyeong Kim received the B.S. degree of computer science and engineering from Daejeon University, Daejeon, Korea, in 2014. He is currently pursuing the M.S. degree in the Department of Computer Science and Engineering, Korea University, Korea. His research interests include information security, mobile computing security, cyber security, and applied cryptography.

Changhee Hahn received the B.S. and M.S. degrees from Chung-Ang University, Seoul, Korea, in 2014 and 2016, respectively, all in Computer Science. He is currently pursuing the Ph.D. degree in the Department of Computer Science and Engineering, Korea University, Korea. His research interests include information security, mobile computing security, cyber security, and applied cryptography.

Junbeom Hur received the B.S. degree from Korea University, Seoul, South Korea, in 2001, and the M.S. and Ph.D. degrees from the Korea Advanced Institute of Science and Technology (KAIST) in 2005 and 2009, respectively, all in Computer Science. He was with the University of Illinois at Urbana-Champaign as a postdoctoral researcher from 2009 to 2011. He was an Assistant Professor with the School of Computer Science and Engineering at the Chung-Ang University, South Korea from 2011 to 2015. He is currently an Assistant Professor with the Department of Computer Science and Engineering at the Korea University, South Korea. His research interests include information security, cloud computing security, mobile security, and applied cryptography.