Design and Analysis for Privacy Protection user Authentication and Key Agreement Scheme

B. Neelima[1], N. Pravallika[2], S. Gayathri[3], T. Lavanya[4], T. Bhargavi[5]

[1]Assistant professor, Dept Of CSE, QIS Institute of Technology, Ongole, Prakasam (Dt)
[2, 3, 4, 5] Students, Dept Of CSE, QIS Institute of Technology, Ongole, Prakasam (Dt)

Abstract: With the rapid growth of smart phone and tablet users, Device-to-Device (D2D) communications have become an attractive solution for enhancing the performance of traditional cellular networks. However, relevant security issues involved in D2D communications have not been addressed yet. In this paper, we investigate the security requirements and challenges for D2D communications, and present a secure and efficient key agreement protocol, which enables two mobile devices to establish a shared secret key for D2D communications without prior knowledge. Our approach is based on the Diffie-Hellman key agreement protocol and commitment schemes. Compared to previous work, our proposed protocol introduces less communication and computation overhead. We present the design details and security analysis of the proposed protocol.

Keywords: D2D communications, Diffie-Hellman, Wi-Fi Direct, key agreement protocol.

I. INTRODUCTION

The emergence and popularity of personal mobile devices, such as smart phones and tablets, generates large amount of data traffic by accessing the Internet and downloading applications, which imposes a huge burden for the cellular infrastructure and spectrum. Device-to-Device (D2D) communications have been introduced to offload the traffic burden from cellular infrastructure to personal devices [1]. The D2D technology enables mobile device users directly establish wireless links between each other, without passing through the public cellular infrastructure or access points.

Many literatures have studied the application scenarios and possible technical solutions for D2D communications. In [1], the authors propose D2D communications as an underlay to the cellular network, and present a mechanism for integrating D2D communications into LTE-Advanced network. Yu et al. [2], [3] discuss the power control issue for D2D communications, and derive an optimum power allocation for D2D links under cellular network control. The work in [4] proposes to use Wi-Fi based D2D links among cellular users to improve the overall network performance in uplink transmission.

Wi-Fi Direct, initially called Wi-Fi P2P, is a Wi-Fi standard that enables devices to easily establish D2D connections using the Wi-Fi frequency band. [5] Gives a wide overview and experimental evaluation of the Wi-Fi Direct protocol. [6] Considers the practical implementation challenges of Wi-Fi Direct and shows that the Wi-Fi Direct features allow deploying the D2D paradigm on top of the LTE cellular infrastructure.

Though D2D communication has been a hot research topic in recent years, there is not much study focusing on the security aspect of D2D communications. [10] and [11] discuss the physical layer solutions for secure D2D communications, but their techniques are difficult to be implemented using devices on the market.

In fact, due to the broadcast nature of wireless communication, wireless channels are considered vulnerable to a variety of attacks, and security is one of the major concerns for D2D communications. To secure the communication between two end users of a D2D link, establishing a shared secret key is the first and most significant step. However, lack of trusted third party and infrastructure under D2D connection environment makes this step a non-trivial task. The well-known Diffie- Hellman key agreement protocol enables two parties jointly establish a shared secret key without any prior knowledge. However, this protocol is vulnerable to the man-in-the-middle attack (MITMA) [12]: an active adversary makes independent connections with the victims, making them believe that they are talking directly to each other. To address this issue, researchers have come up with various Diffie-Hellman based cryptographic protocols, which can prevent the MITMA by conducting mutual authentication.

One simple protocol was suggested in [7], in which devices A and B exchange the hashes of their public keys over a secure channel, thus performing the mutual authentication. However, this protocol requires a large number of bits to be mutually authenticated. The MANA protocol in [8] reduces the size of the authentication message to k bits, but requires a stronger notation of authentication channel. [9] presents a protocol based on commitment schemes and requires 4-round communication over the wireless channel.

II RELATED WORK

Guo et al. proposed an attribute-based authentication protocol with user privacy preservation for electronic healthcare (e-Health) systems [12]. Although attribute based encryption can provide fine-grained access control to resources, it also incurs high energy consumption [13]. Bilinear pairings are commonly used in identity-based authentication protocols. However, bilinear pairing operation is time-consuming and computationally expensive for a mobile device. Hence, a number of mobile user authentication protocols without bilinear pairings have been presented in the literature. Similar to the history of key establishment and agreement protocols, several protocols were found to be insecure after they have been published (e.g. the protocol in [10] was found to be vulnerable to impersonate attack mentioned in [3]).

In the existing system, existing protocols generally do not consider the security of private keys stored on mobile devices. To protect the private keys, researchers have explored the use of threshold secret sharing. For example, Chandra mowliswaran et al. proposed an authenticated key distributed protocol based on Chinese reminder theory to protect the key information broadcast from a center to shareholders in a group [12]. Jarecki et al. proposed a high-efficient password-based secret sharing protocol, for protecting the private key of the bit coin account.

Hu et al. presented a cloud storage system where the key is split into three pieces held by users, cloud storage providers and an alternative third trusted party respectively [13]. Although these protocols are secure against external attackers in terms of key protection, it still suffers the potential security issues for the compromise of the complete key during key reconstruction, not to mention that the secret sharing is not efficient for mobile devices.

III METHODOLOGY

In this paper, we propose a 3-round key agreement protocol based on commitment scheme. Our proposed protocol is similar to the protocol in [9], but with less communication and computation overhead, meantime achieving the same level of security. Major contributions of this paper are summarized as follows:

1) We analyze the secure threats and challenges for D2D communications;
2) We design a secure and efficient Diffie-Hellman based key agreement protocol, and provide the security analysis;

We integrate our proposed key agreement protocol into the existing Wi-Fi Direct protocol, and implement it on Android smart phones.

We consider the following scenario. Two mobile device users want to establish a shared secret key for their D2D communications. Both of them are equipped with a smart- phone or tablet which is capable of communicating over a wireless channel. Both devices have the computation capacity to perform Diffie-Hellman key agreement protocol, and are capable of displaying sequence of digits. The two users do not have any pre-shared cryptographic information, and there is no trusted third party or infrastructure available. They can visually or verbally recognize each other for the purpose of mutually authenticate a short message.

We assume devices A and B agree on a finite cyclic group G, its generating element *g*, and a large prime number *p*. We assume G to be a subgroup of Z^*_p of prime order q, where, Z^*_p is the multiplicative group consists of nonzero integers modulo *p*.

We consider the Dolev-Yao adversary model [12]: The attacker has fully control over the wireless channel. It can overhear, intercept, and modify any message. The attacker can also initiate a conversation with any other user. We further assume that legitimate users will follow the protocol and are not compromised.

Commitment Scheme:

A commitment scheme allows one user to commit to a chosen value or statement while keep it hidden to others, with the ability to reveal the commitment value latter. A commitment scheme has the following two main properties:

1. A user cannot modify the value or statement after they have committed to it;

that is, the commitment scheme is binding and

2. The receiver can only know the committed value after the sender "opens" it; that is, the commitment scheme is hiding. A commitment scheme is defined by two algorithms **Commit** and **Open**:

Commit(c,d) m transforms a value m into a commitment/open pair (c, d). The commit value c reveals no information of m, but with decommit value d together (c, d) will reveal m.

Open m (c, d) output original value m if (c, d) is the commitment/open pare generated by **Commit**(m).

IV ARCHITECTURE

Our Proposed protocol is as shown in the following figure.

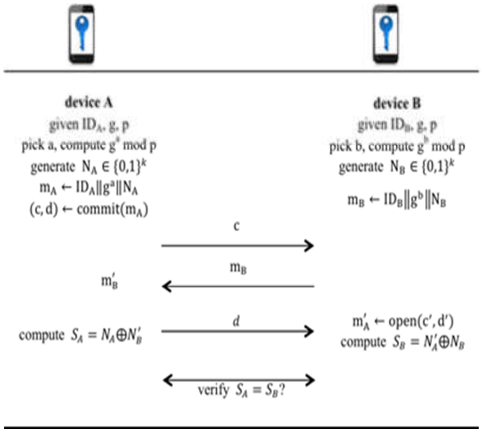
device A
given ID_A, g, p
pick a, compute g^a mod p
generate $N_A \in \{0,1\}^k$
$m_A \leftarrow ID_A \| g^a \| N_A$
$(c, d) \leftarrow commit(m_A)$
device B
given ID_B, g, p
pick b, compute g^b mod p
generate $N_B \in \{0,1\}^k$
$m_B \leftarrow ID_B \| g^b \| N_B$
c
m_B
m'_B
d
compute $S_A = N_A \oplus N'_B$
$m'_A \leftarrow open(c', d')$
compute $S_B = N'_A \oplus N_B$
verify $S_A = S_B$?

Fig 1: Secure Key Exchange Protocol

IMPLEMENTATION

Protocol Design

Here we present our design of the key agreement protocol, which is based on the traditional Diffie-Hellman key agreement protocol and a commitment scheme. In out protocol, two mobile users A and B respectively generate k-bit random strings N_A and N_B, and N_A N_B as the short authentication string for mutual authentication.

Fig. 1 shows the message flow of our proposed proto- col. At the initial stage, user A and B select their Diffie-Hellman parameter a and b, then compute g^a and g^b. A and B randomly generate their k-bit strings NA *and* N_B. $m_A = ID_A\ g^a\ N_A$ and $m_B = ID_B\ g^b\ N_B$ are formed by concatenation, in which ID_A and ID_B are human readable identifiers for user A and B, such as names or e-mail addresses. A also ~~ne~~eds to calculates the commitment/opening (c, d) for

$$m_A = ID_A \| g^a \| N_A.$$

After the initial stage, user A and user B perform the following message exchange over their D2D communications channel. User A sends the c, the commitment value of m_A to user B; after receiving c, user B sends m_B to user A. In return, user A sends the decommit value d to user B. User B opens the commitment and

$$\text{gets } m_A = ID_A \| g^a \| N_A.$$

In the final stage, user A and B generate the k bits authentication string by $S_A = N_A \oplus N^jB$ and $S_B = N^jA \oplus N_B$, in which N^jB and N^jA are derived from messages received by A and B. Then user A and B verify if $S_A = S_B$ via trusted channel (visual or verbal comparison). If the authentication strings match, A and B accept each other's Diffie-Hellman parameters and calculate the shared secret key $K = g^{ab}$ mod p. The reason for comparing authentication string before generating Diffie-Hellman secret key is that if the strings do not match, both users can save the computation for secret key generation.

V. CONCLUSION

In this paper, we analyzed the secure requirements and challenges for secret key establishment between two mobile devices. The proposed key agreement protocol enables two mobile users to securely set up a secret key with a small computation cost and low mutual authentication overhead. The security analysis of the proposed protocol in a real world environment in order to be fully assured of its real-world utility. Therefore, one future research agenda is to collaborate with a mobile device developer to implement the proposed protocol for real-world evaluation.

VI REFERENCES

[1] K. Doppler, M. Rinne, C. Wijting, C.B. Ribeiro, and K. Hugl, "Device- to-device communication as an underlay to LTE-advanced networks," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 42-49, 2009.

[2] C. Yu, O. Tirkkonen, K. Doppler, and C. Ribeiro, "Power optimization of device-to-device communication underlaying cellular communication," in Proc. IEEE ICC, pp. 1-5, 2009.

[3] C. Yu, K. Doppler, C.B. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks," IEEE Trans. Wireless Commun., vol. 10, no. 8, pp. 2752- 2763, 2011.

[4] A. Asadi and V. Mancuso, "Energy efficient opportunistic uplink packet forwarding in hybrid wireless networks," in Proceedings of the fourth international conference on future energy systems, ACM pp. 261-262, 2013

[[5] A.G. Saavedra and P. Serrano, "Device-to-device communications with WiFi Direct: overview and experimentation," IEEE Wireless Communications, vol. 20, no. 3, 2013.

[6] D. Balfanz, D.K. Smetters, P. Stewart, and H.C. Wong, "Talking to strangers: authentication in Ad-Hoc wireless networks," in Proc. Net- work and Distributed System Security Symposium Conference, 2002.

[7] C. Gehrmann, C.J. Mitchell, and K. Nyberg, "Manual authentication for wireless devices," RSA Cryptobytes, vol. 7, No. 1, pp. 29-37, 2004.

[8] M. Cagalj, S. Capkun, and J.P. Hubaux, "Key agreement in peer-to-peer wireless networks," in Proc. IEEE (Special Issue on Cryptography and Security), 2006.

[9] J. Wang, Ch. Li, and J. Wu, "Physical layer security of D2D communications underlying cellular networks," Applied Mechanics and Materials, vol. 441, pp. 951-954, 2014.

[10] D. Zhu, A.L. Swindlehurst, S.A. Fakoorian, W. Xu, and Ch. Zhao, "Device-to-device communications: the physical layer security advantage." in IEEE ICASSP, 2014.

[11] W. Mao, Modern Cryptography: Theory and Practice, Prentice Hall PTR, New Jersey, USA, 2004

[12] Wi-Fi Direct Demo, available on line: http://www.androidside.com

[13] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklos, and Z. Turanyi.

Authors Profile

B Neelima, M.Tech., is working as an Asst. Professor in the department of Computer Science & Engineering in QIS Institute of Technology, Ongole.

N Pravallika, pursuing B.Tech., in the department of Computer Science & Engineering in QIS Institute of Technology, Ongole.

S Gayathri, pursuing B.Tech., in the department of Computer Science & Engineering in QIS Institute of Technology, Ongole.

T Lavanya, pursuing B.Tech., in the department of Computer Science & Engineering in QIS Institute of Technology, Ongole.

T Bhargavi, pursuing B.Tech., in the department of Computer Science & Engineering in QIS Institute of Technology, Ongole.