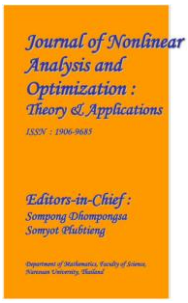
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 12, No. 1, (2021),
ISSN : **1906-9685**



AN EFFICIENT AUTHENTICATION METHOD FOR MOBILE DEVICES BASED ON PROTECTED KEY AGREEMENTS

[1]Bodla Shivakumar, [2]Srujana Gaunani, [3]Bharathi Durgam, [4]Nellore Vishnu Priya
[1,2,3]Assistant Professor, [4]UG Student, [1,2,3,4]Department of Computer science and Engineering, Rishi MS Institute of Engineering and Technlogy for Women, Kukatpally, Hyderabad.

ABSTRACT
Device-to-Device (D2D) trades have gained popularity as a viable alternative to the launch of conventional mobile frameworks due to the rapid growth of cutting-edge cell and tablet users. However, material security concerns about D2D trades have not yet been addressed. In this study, we examine the security requirements and difficulties for D2D communications, and we propose a safe and practical key obtaining demonstration that enables two cells to establish a shared secret key for D2D communications without the need for prior knowledge. The Diffie-Hellman key obtaining show and obligation schemes are the foundation of our theory. Our suggested presentation seems differently from previous work in that it features less upward computation and correspondence. We discuss the planned show's design details and security analysis.
Keywords: D2D interchanges, Diffie-Hellman, Wi-Fi Direct, key understanding convention.

INTRODUCTION
By connecting to the Internet and downloading programmers, individual mobile phones, like PDAs and tablets, are becoming more and more common, which places a significant burden on the cell network's infrastructure. Device-to-Device (D2D) interchanges are known for shifting the burden of traffic from the cellular infrastructure to individual devices [1]. Without using the public cell network or corridors, D2D technology enables cell phone users to easily establish remote connections with one another.

Numerous written works have focused on the possible specialized solutions and application scenarios for D2D exchanges. The authors of [1] introduce a component for coordinating D2D exchanges into LTE-Advanced organization and suggest D2D correspondences as an underlay to the cell organization. Yu et al. [2], [3] examine the power control issue for D2D interchanges, and infer an ideal power portion for D2D joins under cell network control. The work in [4] proposes to utilize Wi-Fi based D2D joins among cell clients to further develop the general organization execution in uplink transmission.

Wi-Fi Direct, at first called Wi-Fi P2P, is a Wi-Fi standard that empowers gadgets to handily set up D2D associations utilizing the Wi-Fi recurrence band. [5] Gives a wide outline and trial assessment of the Wi-Fi Direct convention. [6] Considers the viable execution difficulties of Wi-Fi Direct and shows that the Wi-Fi Direct highlights permit conveying the D2D worldview on top of the LTE cell foundation.

http://doi.org/10.36893/JNAO.2021.V12I1.157-161

However D2D correspondence has been a hot examination point lately, there isn't a lot of study zeroing in on the security part of D2D interchanges. and [11] talk about the actual layer answers for secure D2D correspondences, yet their procedures are hard to be carried out utilizing gadgets available.

Indeed, because of the transmission idea of remote correspondence, remote channels are viewed as defenseless against an assortment of assaults, and security is one of the central issues for D2D interchanges. To get the correspondence between two end clients of a D2D connect, setting up a common mystery key is the first and most critical stage. Nonetheless, absence of believed outsider and foundation under D2D association climate makes this stage a non-paltry assignment. The notable Diffie-Hellman key understanding convention empowers two gatherings mutually set up a common mystery key with no earlier information. In any case, this convention is helpless against the man-in-the-center assault (MITMA) [12]: a functioning foe makes autonomous associations with the people in question, causing them to accept that they are talking straightforwardly to one another. To resolve this issue, scientists have concocted different Diffie-Hellman based cryptographic conventions, which can forestall the MITMA by leading common validation.
One basic convention was proposed in [7], in which gadgets An and B trade the hashes of their public keys over a protected channel, in this way playing out the shared verification. Notwithstanding, this convention requires countless pieces to be verified together. The MANA convention in [8] diminishes the size of the validation message to k pieces, however requires a more grounded documentation of verification channel. [9] presents a convention in light of responsibility plots and requires 4-round correspondence over the remote channel.

RELATED WORK

Guo et al. proposed a characteristic based verification convention with client protection conservation for electronic medical care (e-Health) frameworks [12]. Despite the fact that property based encryption can give fine-grained admittance control to assets, it additionally brings about high energy utilization [13]. Bilinear pairings are generally utilized in personality based validation conventions. Notwithstanding, bilinear matching activity is tedious and computationallyexpensive for a cell phone. Subsequently, various versatile client validation conventions without bilinear pairings have been introduced in the writing. Like the historical backdrop of key foundation and arrangement conventions, a few conventions were viewed as uncertain after they have been distributed (for example the convention in [10] was viewed as defenseless against imitate assault referenced in [3]).

EXISTING SYSTEM

In the current framework, existing conventions for the most part don't consider the security of private keys put away on cell phones. To ensure the private keys, analysts have investigated the utilization of limit secret sharing. For instance, Chandra mowliswaran et al. proposed a confirmed key circulated convention in view of Chinese update hypothesis to shield the key data broadcast from a middle to investors in a gathering. Jarecki et al. proposed a high-effective secret word based mystery sharing convention, for ensuring the private key of the piece coin account. Hu et al. introduced a distributed storage framework where the key is parted into three pieces held by clients, distributed storage suppliers and an elective third confided in party separately.
Drawbacks:
Albeit these conventions are secure against outside aggressors as far as key
assurance, it actually languishes the potential security issues over the trade off of the total key during key recreation, also that the mystery sharing isn't proficient for cell phones.

4. PROPOSED SYSTEM

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

We analyze the secure threats and challenges for D2Dcommunications;

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 shortmessage.

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 : 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:

A user cannot modify the value or statement after they have committed to it; that is, the commitment scheme is binding and

The receiver can only know the committed value after the sender “opens” it; that is, the commitment scheme is hiding.

Algorithm Used:

A commitment scheme is defined by two algorithms

Commit andOpen:

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. random strings NA and NB, and NANB 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 NB. mA = IDA g^a NA and mB = IDB g^b NB are formed by concatenation, in which IDA and IDB are human readable identifiers for user A and B, such as names or e-mail addresses.

Open m (c, d) output original value m if also needs to calculates the ←

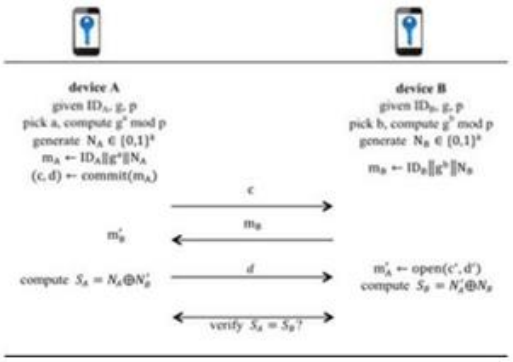
(c, d) is the commitment/open pare generated by Commit(m).

ARCHITECTURE

Our Proposed protocol is as shown in the following figure.

Fig 1: Secure Key Exchange Protocol V.IMPLEMENTATION

http://doi.org/10.36893/JNAO.2021.V12I1.157-161



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 commitment/opening (c, d) for
mA = IDA‖g[a]‖NA.

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 mA to user B; after receiving c, user B sends mB to user A. In return, user A sends the decommit value d to user B. User B opens the commitment and
gets mA = IDA‖g[a]‖NA.

In the final stage, user A and B generate the k bits authentication string by SA = NA ⨁NjB and SB = NjA ⨁NB, in which NjB and NjA are derived from messages received by A and B. Then user A and B verify if SA = SB 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 = gab 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.

CONCLUSION

In this research, we examined the security conditions and difficulties of establishing a secret key between two mobile devices. The suggested key agreement protocol enables secure establishment of a secret key between two mobile users with low mutual authentication overhead and cheap computation cost. To be sure that the suggested protocol will be useful in practice, it must undergo a security analysis in a real-world setting. As a result, one item on the future research agenda is to work together with a developer of mobile devices to put the suggested technique into practice for actual evaluation.

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 B. 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 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 G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklos, and Z. Turanyi.

http://doi.org/10.36893/JNAO.2021.V12I1.157-161