I J C T A, 9(39) 2016, pp. 327-333

A Survey on Device to Device Authentication Schemes

Charanpreet Kaur[1], Gurjot Singh Gaba[2], Rajan Miglani[3] and Sandeep Kumar Arora[4*]

ABSTRACT

The exciting and innovative feature of D2D network enables direct communication between nearby mobiles. But it may be risky if the surrounding device is malicious. The security of any network depends upon the strength of the encryption and authenticity procedures. In this paper, working, applications, vulnerability, and drawbacks of recently introduced Authentication techniques are discussed to analyze the performance of the techniques on various aspects.

Keywords: Authentication, D2D, threats, security, protocols.

I. INTRODUCTION

The popular mobiles of new generation are smart phone, and tablets which generate the maximum amount of traffic due to use of smart applications. The D2D communication is introduced to conserve the bandwidth and to reduce the amount of traffic flow which in turn will increase the QOS. In this technology, the user can built the wireless link between each other without interfacing with the AP. The principle of this technique is to limit the power consumption which was being consumed earlier due to uplink and downlink transmission to far located mobile towers. D2D uses the similar frequency band used by Wi-Fi [1]. An entity may be required for authorizing a person to access the network.

This entity principle is based on the key exchange protocol. The entity in the smart grid is a research issue for the Ecosystem and EV (Electric Vehicle). The electric field in the vehicle system helps to find the vehicle location and in identifying the owner of the vehicle. But it works only when the power is allocated to them. To ensure the identity of the vehicle, we use standards ISO/IEC15118. This standard dictates the reliable method for identification. There is smarter grid authentication method also which gives more salient features for authentication [3]. In the peer to peer network, the authentication to the devices can be carried out through IBC protocol also.

IBC [2] entity is applicable in E-mail. The author has explained the way to eliminate the public key sharing requirements. As we know, authentication plays the important role in cryptography. With the help of authentication, we can analyse the authenticity of the user. The user deals with the two types of authentication (i) mutual authentication (ii) unilateral authentication. In mutual authentication, the user is being authenticated in two ways at the same time. In the unilateral authentication, the user is authenticated only once. The mutual authentication is used for the higher-level security [4]. D2D communication is the best technology of the communication which has improved the bandwidth efficiency [6]. The 3GPP (Third generation of partnership project) is the D2D service of the communication in LTE-A which is also known as Prose (proximity services). LTE is providing the physical layer for the higher communication capacity to allocate resources with the help of E-UTRAN (Evolved Universal Terrestrial Radio Access Network).

[1,2,3,4] Discipline of Electronics and Communication Engineering, Lovely Professional University, Phagwara, Punjab, India - 144411, *E-mails: [1]charanpreet0146@gmail.com, [2]er.gurjotgaba@gmail.com, [3]rajan.16957@lpu.co.in*

[*]Corresponding Author: [4]sandeep.16930@lpu.co.in

The E-UTRAN is used for the high density cellular system but it may not be worth enough if the network is having fewer resources [6]. The D2D communication is the trustworthy communication as it improves the utilization of the resources, increases throughput and increases the battery lifetime [7]. If we talk about the cyber devices, smart grid and vehicle ecosystem are the sub types of the D2D security system.

Identity based cryptography is the technique which aims to solve the authentication problem in the email application. IBC is providing authentication and administration to the network users. IBC has enormous advantages over the conventional authentication strategies. Authentication deals with the pre-shared key, public key and Kerberos. The IBC advises use of symmetric protocol applied to multi domain and peer to peer authentication device.

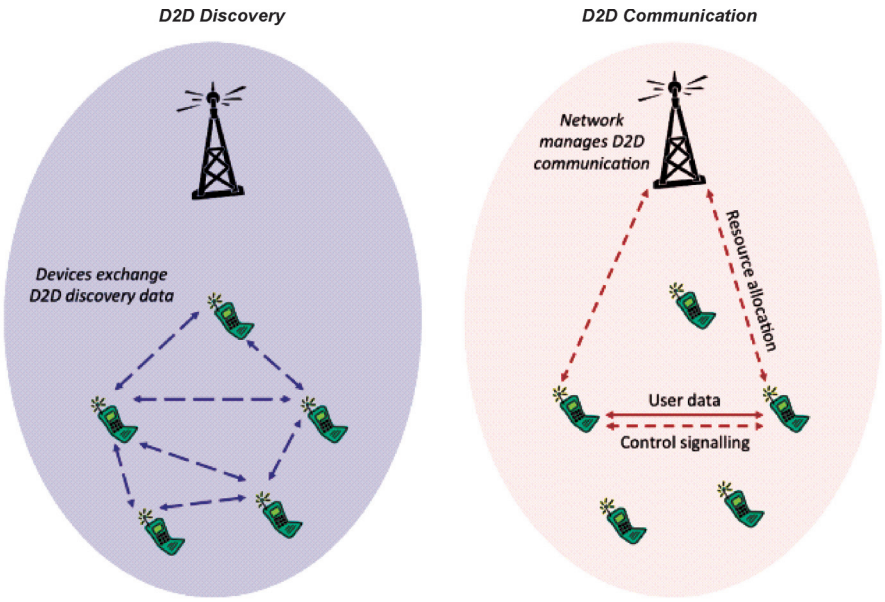

Figure 1: D2D Communication Scenario

Fig. 1 portrays the two phases of communication in D2D. The initial phase is discovery phase where the devices in the surroundings are found and their addresses are stored and later by using two different channels, communication is carried out. Those two channels differ by the data they carry. One channel carries the User data while the others carry the Control signalling which helps the nodes to prevent collisions.

II. D2D: AUTHENTICATION PROTOCOLS

Diffie Hellman based cryptography protocol which can prevent the MITMA by processing mutual authentication. It is a simple protocol which is suggested where devices exchange the hash key in the public network so as to make the channel secure. It requires large number of bits to conduct mutual authentication [1].

The shared key is shared ahead of time prior to start of communication using the key agreement protocol. There are plenty of similar methods which use the phenomenon of shared key, such as ‘challenges and response’ and another one is ‘key derivation function’.

MANA protocol (Manual Authentication) is used to reduce the size of the authentication message to Kbits but it requires the stronger authentication channel. MANA is purposed with 4 round key commitment schemes over the wireless channel [2].

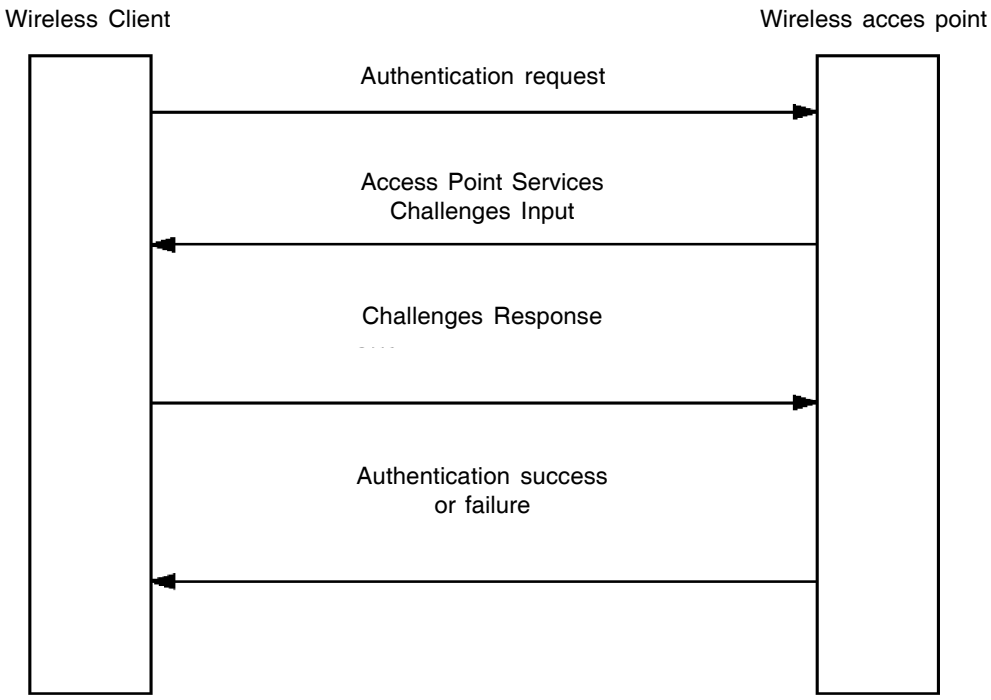

Figure 2: Authentication Procedure

OCM (Organization Change Management) deals with organization and helps to manage the security tools. MANA is less susceptible to attacks because it exchanges the short code and never deals with the extra channels operated on another MAC address.

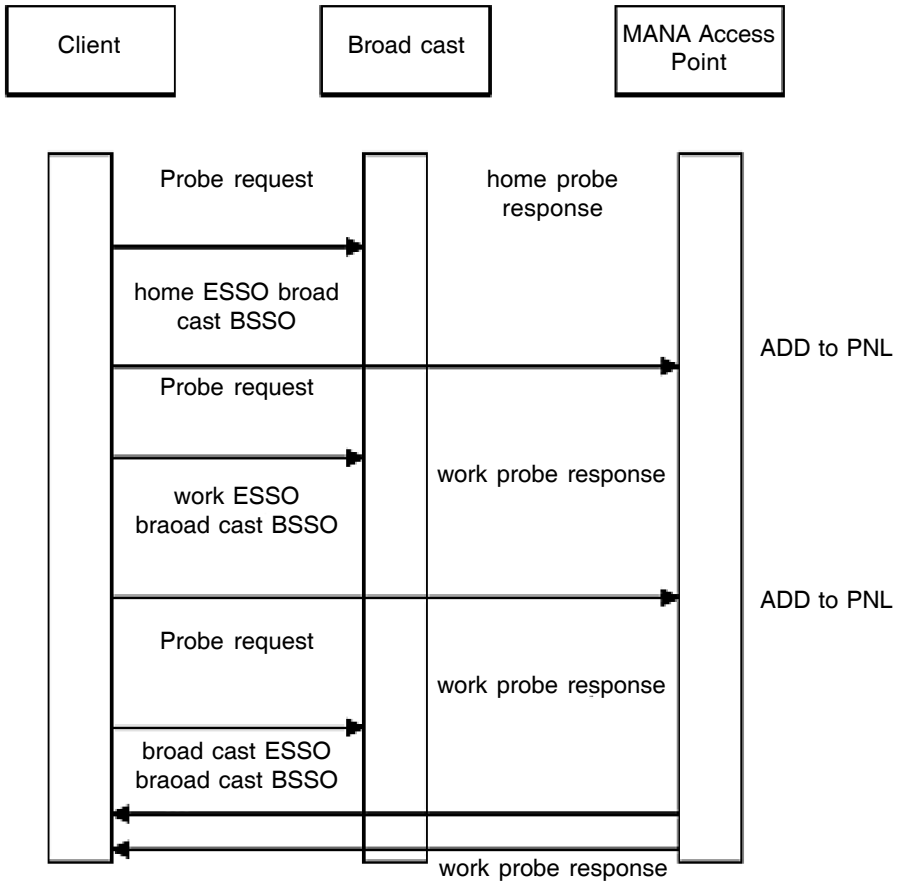

Figure 3: MANA Protocol

MANA works on three stages i.e. Client, Broadcast and Access point. The client broadcasts the request of authentication followed by data transfer to the successful authenticated receivers. Figure 3 clearly describes the operation.

Dolev-Yao Model: The hacker can attack easily on the wireless or WLAN channels. The hacker may impersonate. So, attacker can easily communicate with another user from your system. Identity based cryptography (IBC): IBC is used for the security as well as administrative perspective. IBC uses pre-shared and public shared key algorithms [5]. IBC is motivated from RSA which used public key algorithm. Identity based cryptography (figure 4) find its applications in Email etc.

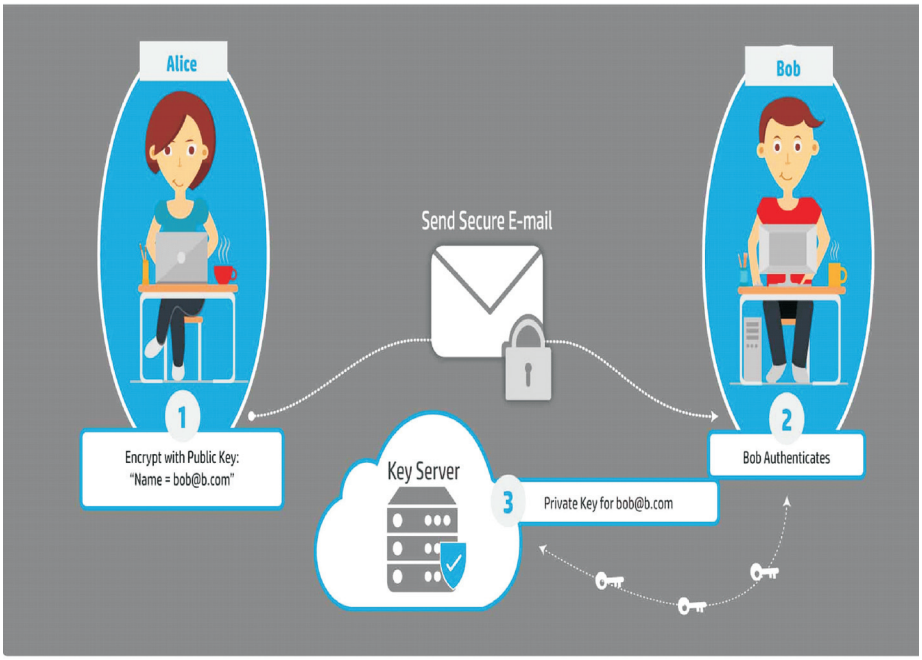

Figure 4: IBC Cryptography

Paved and Martine: Their technique work on hardware security architecture to provide a trusted computing platform for device authentication, but doesn't consider co-ordinate cyber physical attacks into consideration [2].

Mutual and Unilateral Authentication: The mutual authentication is the two-way authentication whereas the unilateral is one-way. In mutual authentication, both the participants are authenticated at the same time whereas in unilateral, one participant is authenticated first which later on authenticates the other one and so on. [4]

It is observed that the Wi-Fi based D2D communication is more reliable than cellular networks. Wi-Fi is also represented as Wi-Fi P2P for the D2D Wi-Fi Frequency band. Few challenges are identified which needs to be taken care of for provisioning of Security i.e. Confidentiality, Integrity and Availability. The challenges identified are portrayed in figure 5.

When we transmit the signal through wireless channels we need to secure the message. To enhance the security, authentication is must. Authentication needs key sharing. It can be shared in the form of public key and shared secret key which helps to connect with the large number of mobile users. If the two mobiles are in distance to each other and they want to make the call, then one channel is established to share the shared secret key between the both devices [2]. But there might be risk; the key established through the human communication is too weak in many of the cases. So, the third person can attack easily through brute force method.

Figure 5: Challenges in D2D security

The Quantization and the error correction techniques for authentication operate on same secret key but it has not been implemented widely because the transmission and generation rate is low to share the secret key. For the longer bit digits like 128 bits to 32 Hex decimals HASH function is suggested [2]. Dolev-Yoo has advised a method to protect the hackers on the wireless media [1].

III. ATTACKS ON D2D NETWORKS

When third person steal our information is called as Attack. The attacks may be inside attack or the outside attack. The inside attack happens within the premises. For example, the system is authorized to use the services but it is not approved the guarantee of authentication. The outside attacker deals with the unauthorized system. They are usually outsiders with the intentions to harm the network through disruption, modification etc.

(A) Types of Attack

- Attack based on communication
- Attack based on vulnerabilities in software application
- Attack based on hardware vulnerabilities
- Password cracking

There are various categories of attacks which are discussed in this section:

- *Attack based on communication*: Some attacks are based on communication which is carried out through the SMS and MMS. There are some mobile phones which are having the problem to manage the SMS. If the user is using the Siemens S55 mobile, it receives the text message in the form of Chinese character which is later denied to provide service to the user [6].
- *Attack based on vulnerabilities in software application*: Phone breaking is a firmware which is totally based on the web browser. Smart phones are susceptible to these phishing and malicious attacks which occurs while browsing the website.

- *Hardware vulnerability*: In these types of attacks, the attacker finds the bugs or drawbacks in the hardware and tries to exploit the characteristics of the hardware.
- *Password attack*: The password attack is based on the keystroke, gesture of the mobile systems etc.

The attacker main intentions are to attack the weaker systems. Though there are plenty of methods to attack a system but in this paper the discussion is restricted to few significant attacks only.

Table 1
Types of Attacks on Heterogeneous Devices

Categories	*Medium*	*Vulnerable Devices*
Based on communication	SMS, MMS,Wi-Fi, Bluetooth, GSM network	Siemens S55,WEP & WAP, Smart phone devices.
Vulnerabilities in software application	WEB browser	I phone, Android phones.
Vulnerabilities in hardware applications	Electromagnetic waveform, juice jacking	Audio interface with the help of headphone, USB charge port.
Password attacks	Malicious software	Mobile virus

Table 1 highlights the important attacks which can be detected and prevented. It is observed that smart phone does not run strong anti-virus tools as they consume more power. Attacks may be based on hardware or software but the basic intentions are to disrupt the services offered [7]. Password based attacks are usually carried out by the misfeasors as they know the victim well. They use password guessing method to attack the system.

IV. COMPARISON OF EXISTING PROTOCOLS

Table 2 discusses the various approaches adopted in different research methodologies and its applications.

Table 2
Approach and Applications of Traditional Protocols

Ref.	*Approach Adopted*	*Applications*
[1]	Diffie Hellman protocol, MANA protocol.	Newest android OS 4.4 Kit Kat
[2]	Handshake Authentication protocol	Machine to Machine communication, VANET.
[3]	Multiple pre-shared key authentication	Mobile to Mobile Communication
[4]	SHOR algorithm	Finance transactions and electronic communications
[5]	IND-CPA encryption and CN-GD2C	Supply chain WEB services JAVA2 platform
[6]	DNP3	Smart meter reading, market price information, 5G security
[7]	Data sharing protocol	Bluetooth, Wi-Fi and WLAN

Table 3 points out to the weaknesses of the traditional techniques. The strength of any technique can be found only after finding their resistance against attacks but if they fail to provide that then new research is required.

V. CONCLUSION

D2D communication has capabilities which can enhance the Bandwidth efficiency and can reduce the traffic to a great extent thereby improving QOS. But to retain the QOS, the network must be made resistant

Table 3
Threats and Drawbacks

Reference	*Attacks*
[1]	Man-In-The-Middle- Attack
[2]	Reply attack
[3]	Brute force key space search attack
[4]	Lattice Attack
[5]	Plain text attack
[6]	Attack on SCADA
[7]	Trap door Attack

against attacks such as disclosure. It is observed from the discussion that the system can be prevented from attacks if the access is denied to the non legitimate users. It is possible with the help of authentication techniques.

REFERENCES

[1] W. Shen, W. Hong and X. Cao, "Secure key establishment for device-to device communication," IEEE Global Communications Conference, pp.336-340, 2014.

[2] A.C-F Chan, J .Zhou, "Cyber-Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem," IEEE Journal on Selected Areas in Communication, vol. 32, no. 7, pp.1509-1517, 2014.

[3] K. V. Nguyen, "Simplify Peer to Peer Device Authentication Using Identify-Based Cryptography," Proceedings of the IEEE, International Conference on Network and Services, pp.43-47, 2006.

[4] N. Saxena, V. Jun Choi, R. Lu, "Authentication and Authorization Scheme for various user Roles and Device in Smart Grid," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp.907-921, 2016.

[5] V. Clupek, V. Zeman, "Unilateral authentication on low-cost device," 38th International Conference on Telecommunications and Signal Processing, pp. 88-92, 2015.

[6] R. Hau Hsu and J. Lee, "Group anonymous D2D communication with end-to-end security in LTE-A," Proceedings of the IEEE, Conference on Communications and Network Security, pp. 451-459, 2015.

[7] A. Zhang, J. Chen and R. Qingyang Hu, "SeDs: Secure Data Sharing Strategy for D2D Communication in LTE-Advance Network," IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp.2659-2672, 2016.