Term Project Topic:

MAJOR SECURITY ISSUES AND THEIR PROPOSED SOLUTIONS BY VARIOUS PEOPLE AND ENTITIES IN DEVICE TO DEVICE (D2D) COMMUNICATIONS

For Course:

Computer and Network Security (CS549)

By

Vanja Vivek Vardhan
190101097, B.Tech, 3rd Year, C.S.E.
vanjavivek@iitg.ac.in

Abstract

Device-to-device (D2D) communication often refers to the technology that allows user equipment (UE) to communicate with each other with or without the involvement of network infrastructures such as an access point or base stations. D2D is promising as it is used to make ultra-low latency communication possible. D2D potentially improves the spectral utilization, enhancing the overall throughput and increasing energy efficiency. A very often low range D2D technique we use in our daily life involves Bluetooth and WiFi. D2D can support local data services very efficiently through uni-cast, group-cast and broadcast transmissions. The use cases involves : Local data Services, Information Sharing, Data and Computation Offloading, Coverage Extension, Machine to Machine communications. Without base stations/network infrastructure involvement in the communication, there would be a lot of security concerns, like, basic security checking at the routers, protocols verification, etc. In the network core, there would be strict following of protocols and error checking. But when it comes to D2D, we would be sharing our data to others but there is no guarantee of security. Also, wireless channels are broadcast in nature. So, because of weak security, there are various threats that are possible. The possible security threats involved are Man in the Middle, Masquerading, DOS (Denial Of Service), and sorts of Passive attacks are also possible, like, Eavesdropping, etc. So, in this paper, I am going to explore the major security problems in the D2D and provide the solutions which are proposed by various people and entities(entities like IEEE, etc.). I will be giving the standard security solutions which are proposed over the years. By providing the best solutions up to date, and by using them, the entire D2D communication can have a good security standard. With good security, most of the security threats can be dealt effectively. And as D2D already had some good advantages, with added security, many users can be able to use D2D securely. There may be a lot of security problems, but when we deal with the main security problems (their number is few compared to all), then we could have an assurance of minimum security. The goal of this paper is to give solutions to those main problems and assure minimum security for a D2D communication. So, I would be focusing on identifying and giving solutions to those problems. I would be reading the various research papers & solutions published by various authors & professors and I will identify the best solutions and add those security solutions here. A well written documentation would help engineers to easily add the security solutions to D2D communication.

INTRODUCTION

Due to the rapid growth of wireless technology in the past decade, it gave to birth to new and some promising services. One of it, is the Device to Device communication, which is popularly refereed as D2D. D2D is expected to be one of the main technology components of the evolving 5G architecture. The D2D allows devices to interconnect with each other without the involvement of the network core or access points. D2D can be able to use high spectral efficiency thereby increasing the throughput, and decreasing the delay. [1] The main difference between the expected 5G and the first four generations is that 5G is heading towards a device-centric network architecture contrary to the previous generations which have been network centric. The main advantage of the D2D is the energy efficiency. An essential part of the use of D2D in the mentioned application areas is energy efficiency, which is heavily dependent on the used radio interfaces. [2]

RELATED WORKS

All the previous works on concerned on one specific attack and focused on it's prevention. Like, *RL assisted impersonation attack detection proposed by Shanshan Tu, Muhammad Waqas, Sadaqat Ur Rehman* focuses only on detecting impersonation attack. And in the case of ECDH proposed schemes [29], they fully support session keys protection, but they can't prevent man in the middle attack. So, if we want to prevent man in the middle, we have to search for another relevant research paper. So, in order to save time, this paper has

put all the solutions together, so that one can find solutions for all the relevant attacks in one paper. The rest of the paper is divided as follows: Scenarios of use cases followed by all attacks and their solutions.

SCENARIOS OF USE CASES

The application scenarios has been majorly classified into 3 types based on the involvement of network entities and the type of spectrum utilization.[3]

In-Coverage: In-coverage is a situation in which the communicating D2D devices are in the range of a base-station(BS). In this case, the network operator/administrator has full control over user identify authentication, access control and security management [4]. The direct Communication link between devices is established by network operator [6].

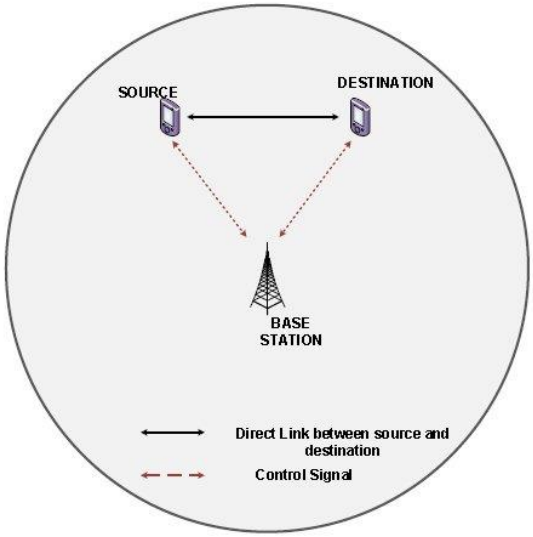

Figure 1: : Source :Titus Turinawe, Isaac Mukonyezi, "DEVICE TO DEVICE COMMUNICATION IN 5G TECHNOLOGY". Found at https://www.researchgate.net/publication/319393025_DEVICE_TO_DEVICE_COMMUNICATION_IN_5G_TECHNOLOGY.

The main use cases of In-coverage are [5] :

1.Local Traffic offloading
2.Content Sharing
3. Gaming
4. Machine to Machine

This type of D2D communication involves sharing of the cellular licensed spectrum with normal cellular connections [7]

Relay-Coverage: Relay-Coverage is a situation in which the device is not in the range of BS (or) at the very edge of network. In this case, the device will connect to a device which is already connected to BS and thereby eventually connecting to the BS. After the connection is made, the device will be counted as in range of BS even-though physically it isn't. Now, once it is connected, this situation will be considered as In-Coverage scenario. All the things happening in In-Coverage will happen in Relay-Coverage as well.

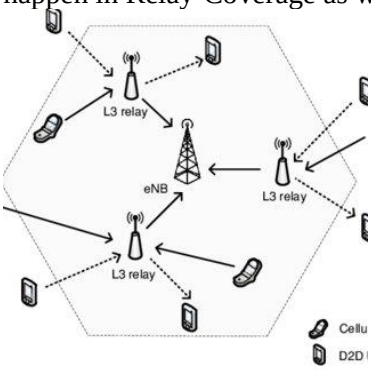

Figure 2 Source : Monowar Hasan and Ekram Hossain, "Distributed Resource Allocation for Relay-AidedDevice-to-Device Communication: A MessagePassing Approach". Found at : https://www.researchgate.net/publication/2630 91579

The main use cases of Relay-Coverage[8]:

1. Network Range Extension

2. Improve quality of service at the edge of network[9].

In addition to in charge of D2D connection, operator is in charge of BS to device connection[10] as well. This type of D2D communication also uses the shared cellular licensed spectrum just like In-Coverage scenario.

Out-of-Coverage: Out-of-Coverage is a situation in which the communicating devices are out of range of Base Station(BS) or any access point. Here, there will be no operator to control the security maintenance or users authentication. In Out-of-Coverage scenario, there is no involvement of core network infrastructure[11].

The main uses cases of Out-of-Coverage are:

1. During natural disasters

2. In Emergency situations

It has no involvement of network core, but this type of D2D link can use reserved cellular licensed spectrum[12] and can use unlicensed spectrum[13] as well.

WHY D2D HAS SECURITY ISSUES?

The main reason for the security threats in D2D is the wireless communication nature of them. Generally, to establish a communication with other device in D2D, the host device must broadcast messages over wireless network[14]. Now, if there is no proper security, then, anyone can receive this messages. An attacker might use this channels to launch an attack on your system. We can also say that, D2D communication is of broadcast nature[16].

TYPES OF SECURITY THREATS IN D2D

1. Impersonation Attack: An attacker will pretend as a legitimate user and tries to steal the users information/service.

In which situation this attack could happen?

In a general D2D situation, there is a transmitter and a receiver. Now, a channel will establish between them while there are communicating. This channel will undergo so many variations while communication because of constantly changing throughput of data. And other parameter known as CHANNEL GAIN. It says about the attenuation of the signal and phase shift of the signal at a given moment of time. As it changes continuously, we can't predict it. So, an attacker uses this chance. As channel gain is difficult to predict, nobody can say whether a given channel gain is genuine / not. So, the attacker will establish a channel with the transmitter/receiver. And he creates his own channel gains and will make the communication. Even-though he created his own channel gains, nobody can say it's a false connection, because we can't predict the channel gain.

Solution:

Given the situation and the constraints, there is a solution. It's [15] *Reinforcement Learning(RL) Assisted Impersonation Attack Detection proposed by Shanshan Tu, Muhammad Waqas, Sadaqat Ur Rehman*. It says that, due to the constant changing of the channel gain and variation, we can use a RL based approach to predict the possible channel gains between 2 authentic D2D users.

While communicating, the transmitter sends a training symbol(signal) to all the receivers. And the receivers will receive it and they will calculate the channel gain of the corresponding transmitter using that training symbol. And this process continues for every signal sent by the corresponding transmitter. Every system will store the log of the channel gains they got from the signals from corresponding transmitters.

We implement the hypothesis tests to examine the validity of the channel gain from the training symbols. And every time they got a channel gain, they run 2 hypothesis tests. If the estimated value and original value are same, then the transmitter that sent the signal is confirmed as a genuine user, if not, it's an intruder.

2. Eavesdropping: An attacker will try to overhear the information between authentic D2D users by means wiretapping or some mechanism.

In which situation this attack could happen?

This attack could happen in a situation where there is no proper security protection of transmitting data. Because of the broadcasting nature of D2D, an attacker could easily intercept the information between authentic users.

Solution:

Given this situation, and considering the fact that, D2D's broadcast nature, we can't stop attacker from intercepting the information. So, we are going to implement a protocol from the transmitters end so that even though the attacker gained the information, he can't decrypt it. So, the protocol we are going to use

is [17*]"Secure Data Sharing(SeDS) Protocol" proposed by Aiqing Zhang, Jianxin Chen , Rose Qingyang Hu , Yi Qian .*

This SeDS protocol [18] uses symmetric encryption and public key-based signature. In contrast to traditional symmetrical key exchange, here the receiver will not send the key directly to sender. The secret key is transmitted by the eNB.

To send the remaining key, receiver must request the key to the eNB. When a key request comes, the system will check for the admissible time window of that user. Once the checking is done, the key will be shared to the receiver.

Even though the eavesdropper knows the key hints, he cannot decrypt the information because he didn't have the shared key between sender and receiver. Thus, even though attacker has encrypted information, it is unreadable.

3. Malware Attack: An attacker will insert a malicious program in the network. As it is unknown to user, he'll run that malware and it'll spread to other devices and eventually the whole network will get affected.

In which situation this attack could happen?

In D2D communication, while data offloading, the malware could come along with the data easily. It can able to compromise the devices easily and will spread throughout the network.

Solution:

Given this situation, the solution is proposed by *Letian Zhang, Linqi Song, Jie Xu in their* research paper *Preventing Malware Propagation in D2D Offloading Networks with Strategic Mobile Users*[19].

In this, the operator has control over device participation. If operator knows malware exists in the network, then, he can stop the participation of devices beforehand.

In the other case, the interaction between attacker and defender(system) is modelled as a zero-sum game(only one could win). The authors proved there exists a saddle point(minimax) equilibrium. Saddle point consists game value. And with Pontryagon's Maximum principle, an optimal defending strategy is defined.

4. Free-riding Attack: An attacker will gain the information or services or resources from an ongoing D2D communication which he is a part of, but he doesn't contribute his part/services.

In which situation this attack could happen?

It's an In-Coverage scenario. And we also assume that, D2D users are authenticated to the same eNB. This situation could happen when a D2D communication has resource constraints and when free riding happens, the work load of attacker will be placed on the remaining devices. If the work load is more, then the devices may crash.

Solution:

Given the situation (resource constraint), we can use the solution proposed by [22] *Man Chun Chow, Maode Ma in their paper "A Lightweight D2D Authentication Scheme against Free-riding Attacks in 5G Cellular Network"*. They proposed a ECC based D2D authentication and key agreement protocol.

[23] In this proposal, the UE_a and Cellular/Core Network (CN) must mutually authenticate it's connection with each other. If UE_a wants a D2D connection, it'll broadcast a request message. If UE_b wants to connect with UE_a, it'll have to request AMF. After that, if UE_a gets connected to UE_b, then UE_a have to send a successful D2D connection message to 5GC.

Now, the CN also keeps the log of users. If we get repeated success indication message from a certain user, this means that, he must be a free rider who didn't want to share the resources, so he disconnects frequently. So, he will be marked as Free-rider and will be disconnected.

5. Man in the Middle Attack: The attacker will hijack the conversation between 2 authentic D2D users and tries to alter the messages, which the communicating parties are sending each other. So, the attacker would act as receiver for sender and sender for receiver. The sender-receiver parties think that, they are communicating directly.

In which situation this attack could happen?

When the channel is insecure, and the contents of the message are not encrypted, then this attack can take place easily.

Solution:

Given the situation, a solution is proposed by [24]*Baskaran and Raja in their paper "A Lightweight Incognito Key Exchange Mechanism for LTE-A Assisted D2D Communication* ".

It's a In-Coverage scenario. It says that, any UE, who wants to connect, must authenticate with the eNB. When 2 devices(D1,D2) wants to connect each other in D2D, they first need to authenticate with the eNB. In contrast to the general authentication process, in this [25]LIKE protocol, the main role of authentication is played by eNB. This authentication process of UE is done with the help of "incognito device identifiers", "shared secret keys" and "signatures".

It's like encryption but it has a unique advantage. Generally, in normal encryption, even though the attacker doesn't know the session key, he can change the unencrypted contents. But here in the LIKE protocol, because of the authentication [26], it'll prevent Man in the middle attack.

6. Forge Attack: An attacker tries to modify the message content that an authentic source is transmitting.

In which situation this attack could happen?

It's different from the man-in-the-middle attack (MITM). In MITM, the attacker acts as sender &receiver. But here, the attackers just tries to change the contents of the message. By changing the contents of the message, it may lead to, for example, in an organization, it may be the changing the privileges which are not meant for them.

Solution:

Given the situation, the situation could be handled by checking the integrity of the data which can be done using "*Secure Data Sharing(SeDS)" protocol proposed by Zhang[27]*.

According to the SeDS, every message or information sent by a user is signed by the data provider. And while transmitting the message, the sender will sign it again. Furthermore, the contents of the message are encrypted. To decrypt it, a key request message must be sent to Enb by receiver. Attacker can't request the key, because if he does, he first needs to authenticate himself.

So, without the secret key, the attacker can't modify the messages.

7.Replay Attack: The attacker, to gain the services of a D2D communication, tries to re-transmit a service request that is made by an authentic D2D user.

In which situation this attack could happen?

In an In-Coverage scenario, in which a sensitive information/service is shared between 2 authentic D2D users, an attacker might just play a reply attack quickly to obtain the related information/service.

Solution:

A solution is proposed by Baskaran and Raja, in their research paper, "*A Lightweight Incognito Key Exchange Mechanism for LTE-A Assisted D2D Communication*".

This protocol is discussed detail in the *Man-in-the-middle attack* part. According to them, every service request sent by the UE (user equipment) to the eNB, consists of a timestamp[28].

Now, if an attacker tries to replay the attack, i.e, the previous timestamp would present on that service message. If he tries to replay it, it'll be discarded because of the difference of time.

CONCLUSION

This paper tried to put all the possible main attacks and their corresponding solutions in a D2D network in one place.

REFERENCES

[1] A. Asadi, Q. Wang, and V. Mancuso, “A survey on device-to-device communication in cellular networks,” IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 1801–1819, 4th Quart., 2014.

[2]Marko Höyhtyä, Olli Apilo and Mika Lasanen, “Review of Latest Advances in 3GPP Standardization: D2D Communication in 5G Systems and Its Energy Consumption Models” Available at : Future Internet | Free Full-Text | Review of Latest Advances in 3GPP Standardization: D2D Communication in 5G Systems and Its Energy Consumption Models | HTML (mdpi.com)

[3],[9],[10]Mingjun Wang, Zheng Yan, “Security in D2D communications,” IEEE Commum.

[4],[5],[7],[8],[12]Mingjun Wang & Zheng Yan, “A Survey on Security in D2D Communications ”, found at : A Survey on Security in D2D Communications (springer.com)

Figure1 : Source :Titus Turinawe, Isaac Mukonyezi, “DEVICE TO DEVICE COMMUNICATION IN 5G TECHNOLOGY”. Available at : https://www.researchgate.net/publication/319393025_DEVICE_TO_DEVICE_COMMUNICATION_IN_5G_TECHNOLOGY

[6]Titus Turinawe, Isaac Mukonyezi, “DEVICE TO DEVICE COMMUNICATION IN 5G TECHNOLOGY”. Available at : https://www.researchgate.net/publication/319393025_DEVICE_TO_DEVICE_COMMUNICATION_IN_5G_TECHNOLOGY

Figure 2: Source : Monowar Hasan and Ekram Hossain, "Distributed Resource Allocation for Relay-AidedDevice-to-Device Communication: A MessagePassing Approach". Found at : https://www.researchgate.net/publication/263091579

[11] Jian Wang, Richard A. Rouil, and Fernando J. Cintron, “Distributed Resource Allocation Schemes for Out-of-Coverage D2D Communications” found at: Distributed Resource Allocation Schemes for Out-of-Coverage D2D Communications | IEEE Conference Publication | IEEE Xplore

[13], [14] Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, Senior Member, IEEE, Sasu Tarkoma, Senior Member, IEEE, and Jörg Ott, Member, IEEE, “Security and Privacy in Device-to-Device (D2D) Communication: A Review”

[15] Shanshan Tu, Muhammad Waqas, Sadaqat Ur Rehman, “Reinforcement Learning (RL) Assisted Impersonation Attack Detection”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 70, NO. 2, FEBRUARY 2021.

[16]Yingdong Hu, Ye Li, Ruifeng Gao, Xiaodong Ji, Shibing Zhang, Zhihua Bao, Jun Zhu, “Proactive Eavesdropping in Underlaid D2D Communication Networks”, IEEE Xplore, 2-4 Dec. 2019.

[17], [18], [27]Aiqing Zhang, Jianxin Chen , Rose Qingyang Hu , Yi Qian, “Secure Data Sharing(SeDS) Protocol”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 65, NO. 4, APRIL 2016.

[19],[20],[21] Letian Zhang, Linqi Song, Jie Xu, “Preventing Malware Propagation in D2D Offloading Networks with Strategic Mobile Users”, IEEE, 2019.

[22], [23] Man Chun Chow, Maode Ma, “A Lightweight D2D Authentication Scheme against Free-riding Attacks in 5G Cellular Network”, found at: A Lightweight D2D Authentication Scheme against Free-riding Attacks in 5G Cellular Network | Proceedings of the 2020 2nd International Electronics Communication Conference (acm.org)

[24], [25], [26], [28] Baskaran and Raja, “A Lightweight Incognito Key Exchange Mechanism for LTE-A Assisted D2D Communication”,9th International Conference on Advanced Computing (IcoAC), 2017