International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Physical Layer Security Requirements and Solutions for Device to Device Communication

Anagha Kulkarni, A. Ramakrishna

Abstract: ***Device-to-Device (D2D) communication is used for cellular networks. D2d communication is the direct communication from one mobile station to other mobile station, without the involvement of the base station. By using the device to device communication lesser delay is possible. By using d2d communication along with 5G network improves the bit rate. 5G network provides the communication with more data rate and lesser delay. Security and privacy are very important for communication. In this paper security and privacy requirements of device to device communication and physical layer privacy solutions are discussed.***

Keywords: D2D communication, security, 5G

I. INTRODUCTION

The mobile device is used by every user and now a days it is becoming essential device for one and all. For this high demand of mobile devices, device to device communication and 5G network is used. With this, data can be accessed anytime, anywhere from any device to any device. It is found that in upcoming years, there will be a 500 times increase in wireless cellular data traffic. 5g networks support the high data rate and minimum delay of just 4ms. These features have motivated researchers to research towards 5G cellular network. Device to device (d2d) communication is direct connection between two devices without the involvement of base station. It has the advantage of reduced communication delay and high spectral efficiency[1]. D2d communication may be in-band d2d communication that is communication is done within cellular spectrum and out-band D2D communication that is d2d uses another band of frequency for communication other than cellular frequency. In In-band communication both cellular and d2d uses the same cellular spectrum. Two types in In-band communication are Underlay in-band communication and overlay in-band communication.

- Underlay in-band communication: Here d2d and cellular shares the same band of spectrum. And d2d, access the resources occupied by cellular users when it wants to communicate. It provides high spectral efficiency, but causes interference because of sharing of same band of spectrum.
- Overlay in-band communication: Separate band of frequency is used for device to device communication. Interference can be reduced by using this technique.
- Out-band D2D communication: In in-band communication, d2d uses the licensed band of cellular spectrum. Out-band d2d communication uses unlicensed band of cellular spectrum for communication. It completely reduces the interference[2] because separate band of frequency. Figure1 shows the in-band and out-band d2d communications.

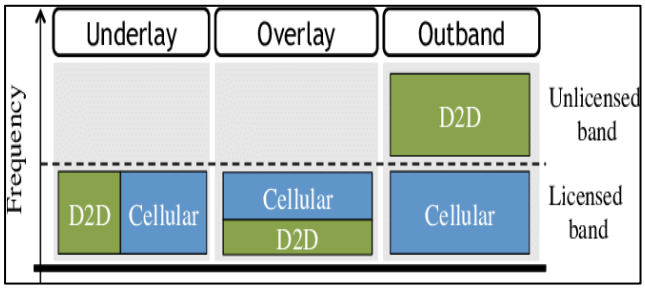

Fig1: device to device communication

My work focuses on the security and privacy difficulties in device to device communication. Security is required because of the distributed nature of d2d communications. Therefore end user should take care of the functionalities like login information, authentication etc. And secondly, device to device communication broadcast the message to find the receiver. This allows the attacker to track the location of sender, thus it breaks the location privacy.

II. SECURITY AND PRIVACY NECESSARIES FOR D2D

Security is required to provide the protection against the hackers. Security requirements are

1. Authentication: It helps only the device to device communication user should able to take the d2d services.
2. Availability and Dependability: Authorized d2d user should able to take the d2d services anytime and anywhere even under the attacks.
3. Non Repudiation: Receiver should have the information about the transmitter so that receiver can verify the transmitter and message from the transmitter.
4. Secure Routing and Transmission: It ensure that only authenticated D2D users are able to read the messages.
5. Confidentiality: D2D service controls the data information to all other users, and the communication is possible only with authenticated users.

Revised Manuscript Received on February 05, 2020.
* Correspondence Author
Anagha Kulkarni*, Asstistant professor, VJIT, Telangana, India. E-mail:jan31.anu@gmail.com
Dr. A. Ramakrishna, Associate professor, KLU, Guntur, Andhra Pradesh, India. E-mail: ramakrishna.a@kluniversity.in

6. Integrity: Information exchanged between d2d user should correct without any modification. It is possible through interity.

Privacy issues: if the privacy is guaranteed user will exchange data to some extent. Otherwise exchange of the information will be limited. Privacy issues are

1. Anonymity / Indistinguishability: It hides the information about the sender. And this is done for security purpose.
2. Un-linkability: D2d same users are not linkable to each other like they are having different identification number. So it is difficult to hackers for predict the information of d2d users.
3. Context privacy: Here the user information is hidden like talk time, identification number etc.
4. Confidentiality and integrity: Using confidentiality hacker are not able to read the messages transmitted between two D2D users. Message modification can be avoided using integrity.

Using non-repudiation, receiver should have the information about the transmitter so the unknown transmitter can be recognized. Context privacy hides the information during the D2D communication, such as location of user, identification number, and talk time. The security requirement means only the D2D user can able to access the data. Context privacy also protect against hackers. Otherwise, only the content is secured but attackers can able to find the communicating parties by noting the amount and how many times message has been exchanged.

III. PHYSICAL LAYER SECURITY SOLUTIONS FOR D2D

Here, authors introduce different types of cryptographic methods and gives the corresponding solutions in D2D communications. Device to device communication is the direct communication between two users without involvement of base stations. So this communication is going to perform in limited area. And the service provider has the details of of the device to device communication location, name and more information. Because of this information, there is a chance for hackers to hack the user location and other information. So it is very important to protect user information by hackers. Some techniques for location privacy are: k-anonymity, dummy locations, and location encryption.

Cryptographic techniques is applied for security in D2D communication. Cryptographic is used for the security and privacy approaches in D2D. The cryptographic used for privacy those are anonymity, un-linkability, content privacy, confidentiality, and integrity for exchanging messages between d2d users. Public Key Infrastructure (PKI) is used for the security purpose. In PKI users have two keys, those are private and public keys for message authentication. But, the PKI has to be changed for the better security and privacy. In PKI keys are changed each time for more security purpose. Key management and distribution is a major problem in D2D. To solve this problem many algorithms are used. By using these algorithms, D2D users can distribute the message without mutual trust. In Identity Based Cryptography, public key is based on the information given by user. So public key can be exchanged easily. But for the security and privacy centralized trusted authority is not necessary. Each sender has a private key and has separate signs in the messages. Other members use a shared group key to verify signed messages without the knowledge of signed party.

Homomorphic encryption (HE) is another technique for encryption. And homomorphic encryption can be used in D2D communication. In this type of encryption authors used the different technique. Here users can request the data from any other users in the network. And that requesting user will send the data in encrypted form. And receiving the data from the requested user, he performs the encryption operation to get the original text using homomorphic encryption. Finally plain text is generated. This is important for product sellers who don't know each other.

One more technique is the power assignment technique. Here signal to interference plus noise ratio can also be calculated. Here total power required for the individual user and the all users are calculated. Authors are doing all these things to provide maximum quantity of service. Here authors analyze and calculates the power used for each users and D2D link and find the power requirement for individual usres. The difference between the of the D2D data rate with respect to the individual users power budgets are calculated and based on this result, users can use the best method to achieve minimum power budget with good security levels. For multi-channel D2D communication, signal-to-interference-plus-noise ratios (SINRs) are calculated and they found out the power requirement and how the channels are allocated. Then, effective methods are used to find out the power allocation, channel assignment, and D2D SINR levels with convergence and performance guarantees. By using this power assignment technique, number of users and security can also be improved.

In this paper [4] authors uses the secure beamforming to prevent hackers on multiple-input multiple-output (MIMO) device-to-device (D2D) communication. The main aim of this method is to minimise mean square error by using the signal to interference plus noise ratio threshold value. To calculate the errors, Gaussian Markov uncertainty model is used. And the beamforming design minimizes the mean square error of the D2D communication while applying signal-to-interference-plus-noise ratio (SINR) threshold constraints to avoid the possible hackers.

In paper [5] PNC based D2D communication, XOR operation is used. User, who wants to communicate with the other user, will send th information with XOR operation. So this provides the more security for the intended users. Along with the XOR encryption of the message can also be done with public and private keys. So this operation will add extra security from hackers.

Another method to protect data from hackers is by using deffie hellman algorithm. In this algorithm public key and private key are used. Public Key is used for encryption and private key is used for decryption. And public key is shared by both users but the private key is not shared. User1, who wants to send the information will encrypt the information using public key.

While encrypting the information user uses the prime number and primitive root and also log function. So it is very strong and can not be easily decode by hackers. After receiving the information by user2, he will decrypt the message by using private key. This algorithm is more secure. Among all algorithm I have discussed so far, I found that diffie hellman algorithm is the most efficient algorithm for encryption.

IV. RESULTS

Diffie-hellman algorithm require 3072 bit key length hence provides more security.

Above graph shows the security level for diffie-hellman algorithm. As we observe from the graph, delay increases with more number of bits. But security level increases with the key length. For more security highest key length is used. It protects from attacks.

Table1:Comparison table of algorithms

	Diffie-hellman algorithm	**Other algorithms**
Security	More	Moderate
Delay	More delay as the number of bits increased	Moderate

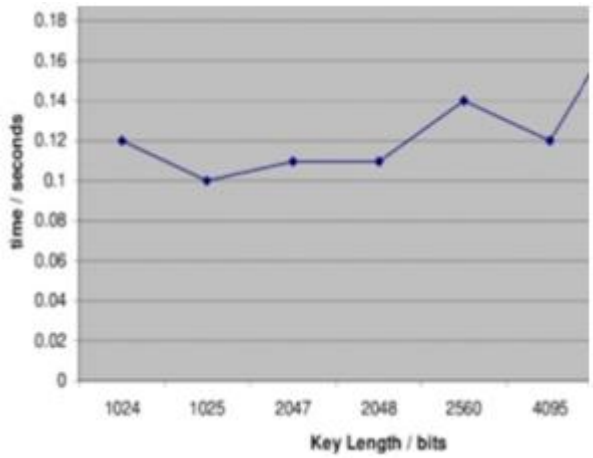

Figure2: diffie-hellman delay graph

Diffie-hellman algorithm provides more securit as the number of bits increased but provides more delay for higher numbe of bits.

V. CONCLUSION

D2D communication provides many benefits compare to existing cellular networks. D2D communication provides the communication with lesser delay. In this survey, a detailed overview of D2D physical layer security and privacy requirements along with various algorithms has been discussed. Among all algorithms diffie hellman algorithm is the more secure algorithm. This survey will help future readers better understand the D2D concepts.

REFERENCES

1. Authors Furqan Jameel, Zara Hamid, Farhana Jabeen, Sherali Zeadally and Muhammad Awais Javed, published a paper on 'A Survey of Device-to-Device Communications: Research Issues and Challenges' in IEEE, DOI 10.1109
2. Authors Arash Asadi, Qing Wang, published a paper on 'A Survey on Device-to-Device Communication in Cellular Networks', IEEE,DOI 10.1109
3. Authors Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, Senior Member, Sasu Tarkoma, and Jörg Ott, published a paper on 'Security and Privacy in Device-to-Device (D2D) Communication: A Review', IEEE, DOI 10.1109
4. Authors Jayasinghe, Praneeth Jayasinghe, Nandana Rajatheva, and Matti Latva-aho, published a paper on 'Physical Layer Security for Relay Assisted MIMO D2D Communication', IEEE ICC 2015.
5. Authors Aiqing Zhang and Xiaodong Lin, published paper on 'Security-Aware and Privacy-Preserving D2D Communications in 5G', IEEE, 0890-8044/17/2017