Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

An Overview on Device to Device Communication (D2D) and Security Issues

Dogra Anutusha [1*], Singh Randhir [2]

[1*]Department of ECE, SSCET, Badhani, Pathankot, India-145001
[2]Department of ECE, SSCET, Badhani, Pathankot, India-145001
Email: [1*]antusha001@gmail.com, [2]errandhirsend@gmail.com
Phone no.: [1*]+917889860843, [2] +918288870823

ABSTRACT

Device to Device communication is the sprouting technology of 5G network. It has many significant advantages over the traditional systems. It enhances the coverage area of the systems and provide it with the indefinitely low latency. No doubt, Device to Device communication is going to boon the new generation systems but there are many aspects of this variety of communication is still under threat. Device to Device communication. These communications is also a type of machine to machine communication. Devices communicate on direct basis to reduce the load on system. Security and privacy of device of device communication is an unopened area by the researchers. Device to Device constitute the direct link between the users without any assistantship of the base station. These type of communication are more prone to privacy attack. This paper provides an overview on Device to Device and various types of Device to Device communication with Security issues related to the Device to Device communication. After that various techniques required to solve the security issues has been discussed. At last the paper is concluded in the conclusion section.

KEYWORDS: D2D communication, Cases of D2D, Security attack, Inband D2D, Outband D2D.

***Corresponding Author**

Anutusha Dogra

Department of ECE,

Sri Sai College of Engineering and Technology

Badhani, Pathankot, India-145001

Email address: antusha001@gmail.com Mob. No. +917889860843

1. INTRODUCTION:

5G network is the combination of a number of technologies performing on the same platform. Number of technologies like Massive MIMO, Ultra-Dense network, Small Cell, Cognitive radio etc. are the fundamental technologies that are being used in 5G network[1]. Each technology may provide some feature to the system. Like Massive MIMO have the feature of increasing the spectral efficiency and making the system robust. Ultra-Dense network helps in increasing the capacity of the system and enable the system to handle a large number of users effectively. Small cells does the same job of handling large number of users effectively. These competent technologies make the system reliable and more efficient[2]. D2D communication is one of these technology. It ensures the systems with low latency and higher capacity. It is simply defined as the direct connection between two users without any interference from the controller[3,4]. This technology along with its features also have some areas which need to be explored such as Security. Security of D2D communication is the area of threat to the users where the attention is required[5,6].

2. D2D COMMUNICATION:

D2D is most promising technology of next generation systems[7]. It permits communication on direct basis between two nearby devices. It is suspected to have a significant role in future wireless systems .These communication systems enables the cellular networks on optimum performance[8,9]. These systems have been classified on the basis of its operation into following categories.

2.1. Types of Device to Device Communication:

D2D communication has two types. Inband and Outband.

2.1.1 . Inband D2D communication

Inband makes use of cellular frequencies for the communication between the devices. These setups do not require decoding of the data between the two users. Inband communication has two further types, Underlay and Overlay. Underlay donot requires dedicated paths for communication and interference management is easy in this case where as in Overlay, the interference management is difficult to attain and dedicated paths are provided for carrying out communication between the devices.

2.1.2 . Outband D2D communication

Outband makes use of frequencies other than the cellular frequencies. These communications requires coding of data between the two users. Outband is further of two types, Controlled and Autonomous. In Controlled interference management is easy to establish and in Autonomous Interference management is not under the control of system. Quality of service is very low and dedicated paths are not required.

D2D is also studied in terms of cases. There are about four cases of D2D communication. These four cases are given as:

a. Devices relaying with base assisted link development.

In this case base station takes part in communication and set up the connection between two devices by using relays. The communication is the Inband communication.

b. D2D communication with base assisted link development.

In this case direct connection is made between two devices with the help of base station. The communication is performed with in the in band communication.

c. Devices relaying with device assisted link development.

In this case the base station do not make any connection. Connection is made by device and terminated by device itself. The relay is used when the two devices are not near to each other.

d. Direct D2D communication with device assisted link development.

In this case the base station do not involve and connection is developed by device and direct communication is formed. It is same like outband autonomous communication.

These cases depends on how the device connects to other device. Whether it is communicating through the help of base station or communicating directly[10]. Devices when communicates with the help of Base station it is called as base assisted. And when the devices communicates with the help of devices itself, it is called as device assisted communication.

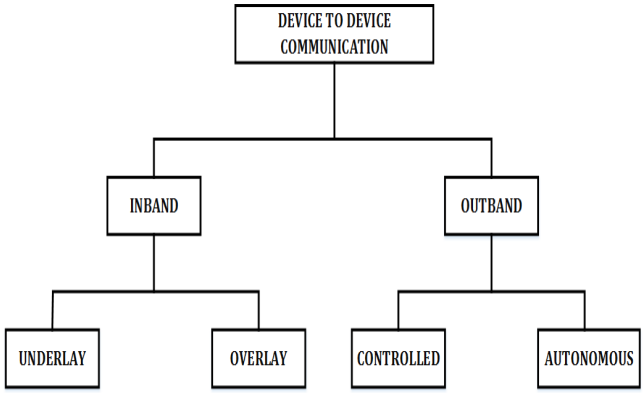

Figure 1: Classification of D2D communication.

Devices connected with the help of base station are rarely threaten by the security attack where as the devices which are under the device control and not in the base station control and prone to common attacks and security in this case is very important[11] . D2D communication need to be protected from security attacks and privacy of the system must be maintained[12]. Classification of device to device communication is shown in figure 1. The two main categories inband and outband with its further classification is shown.

3. SECURITY AND PRIVACY IN D2D COMMUNICATION

D2D communication is prone to many types of security attacks. A survey over various security threats are discussed[13]. These attacks affect the reliability of the system and reduces the efficiency of the system. It also reduces the performance of the system. Wireless Networks are susceptible to various types of attacks. A lot of security algorithms are being deployed for securing the systems. Integrity, confidentiality, authentication etc[14].are the common solutions that is provided to make the system secure[15]. A security attack may be considered an attempt to gain unauthorised access to information to cause damage to the system. It is a malicious activity that can harm the security and privacy of the system[16] .Various common attacks of Wireless system that may influence its efficiency are stated below:

3.1. Spoofing Attack:

Spoofing attack deals with the capturing of path information and identity of the user by spoofing the path information. Spoofing can be Bandwidth spoofing attack, IP spoofing attack etc.

3.2. Denial of Service attack:

This type of attack is very common in wireless system. The system is flooded with useless packet of data in order to consume the bandwidth of the network. The Main aim of the attacker is to make the channel busy and not accessible[17].

3.3. Sybil Attack:

In Sybil attack, the malicious node shares its secret key with other malicious node and thereby increases the number of malicious nodes[18]. Increased number of malicious nodes increases the probability of the attack.

3.4. Modification attack:

This type of attack generally occurs when the attacker modifies the routing route and the sender chooses a long route to send the packets. This results in delaying of the packets between the sender and the attacker.

3.5. Monitoring Attack:

This type of attack include the assessment of channel by the attacker. The Attacker read the confidential data and harms the privacy of the system.

3.6. Rushing attack:

The attacker in this case captures the packet from the sender and alters the information and sends it to the receiver. After that the attacker starts sending its duplicate packet to the receiver and receiver remains busy continuously.

3.7. Eavesdropping:

The main aim of the attacker is to find out the confidential information of the system. The attacker continuously sense the information of the system. And specifically attack on the secret information. Eavesdropping attack can be passive attack or Active attack.\

3.8. Traffic Analysis :

In this type of attack the attacker sense the information path continuously and also found the amount of data that is being transferred over the channel. The data is not modified by the attacker.

3.9. Password attack:

In this attack the password of the user is attacked and attacker used to guess the password of the intended user to capture its personal information. Password is guessed by Brute-Force method.

3.10. Malware attack:

In this type of attack the malicious software is installed in the system without any knowledge of the user and the system start working inefficiently.

3.11. Drive –by attack:

This type of attack is very common type of attack in which a malware is spread by the hackers by introducing malicious data into the Http or PHP codes. Due to this data the malware is directly introduced in the system directly.

3.12. Man-in-the-middle attack:

Man in middle type of attacks are like someone id watching the communication between the devices. The whole data transfer is watched by some middle person[19]. It is an attack to privacy of the system. Man in middle attack is very similar to the eavesdropping attack[20].

3.13. Phishing:

In this attack an attacker may send an email that the user may think that it is from its trusted user. It seem to be safe and legitimate but it is not. When any user tries to open it or click on the given link in in. the malware is installed in system.

3.14. Browser attack:

This attack basically affect the end user that are browsing the internet. The attacker tries to encourage the user to install the malware in the system. The best way to avoid these types of attack is to update web browsers regularly.

3.15. Botnet Attack:

Botnet is the group of hijacked computers that are already under attack and are controlled by some malicious attacker or node. The botnet group tries to hijack another systems also. Millions of

the system can be attacked by this type of attack. Attackers make use of this type of attack to jam the system fully and capture all the information of the intended user[21].

There are many other security attacks that can attack the system and hampers the performance of the system[22].

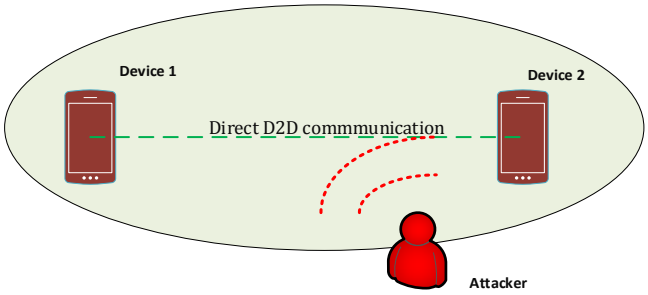

Figure 2: Direct D2D communication under attack.

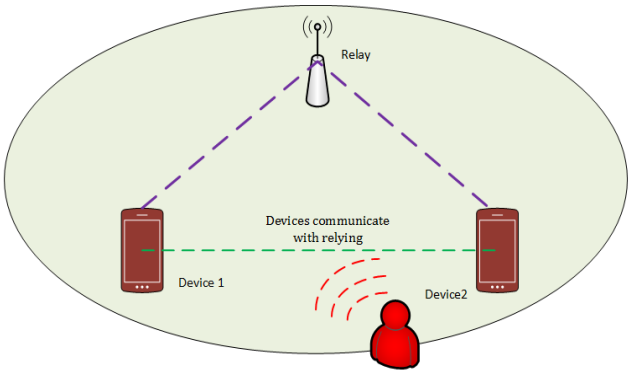

Figure 3: Devices communicating with the help of relay under attack.

4. METHODS TO PREVENT AGAINST ATTACKS

Various security solutions are being presented to minimize the effect of attack on wireless systems[23,24]. These security algorithms ensures the privacy of the system. Some of the security algorithms are discussed below:

4.1. Authentication:

Authentication ensures the identification of Sender and receiver and regular checking of the devices[25]. By authenticating devices the system can be secured from any interferences from the unintended users[26,27].

4.2. Privacy:

Privacy of information is assured such as identity, geographical position, SIM card number etc. Privacy can assured by using cryptographic keys. The data which is private is not accessible to the outer devices[28].

4.3. Data confidentiality:

Confidentiality of data involve the secrecy of the data by encryption. Data is transferred with encryption that maintains the confidentiality of data and thereby secure the system.

4.4. Data integrity:

It involves transfer of data within authorised devices that is verified and not altered. The integrity of data assures the security of the system. The data reached to the receiver unaltered.

4.5. Cryptographic key:

It involve the protection of data with the help of key[29]. The key can be private key or public key. The key helps in maintaining the confidentiality of data.

4.6. Triple DES:

It is the Data encryption algorithm in which the key length is about 168 bits. It is the Symmetric algorithms which is most widely used now a days.

4.7. Blowfish:

It is same like DES but it has extremely high speed and very effective in its working. It is the most flexible encryption algorithms which is available till now. It is available freely on public domain.

4.8. AES:

Advanced Encryption standard is the standard algorithm that is being used by many companies now a days. It uses the key of about 192 and 256 bits for better encryption[30]. This is one of the efficient algorithm to prevent data from attacks.

4.9. Twofish:

This algorithm is the successor of Blowfish Cipher algorithm, which is more flexible than the previous algorithms and can be used on the small computers also. This algorithm is free and present in public domain.

4.10. RSA:

Rivest-Shamir-Adelman is the most common Public key algorithm. It is the traditional method of encrypting data and provides protection to the data.

5. CONCLUSION:

D2D communication is the innovative technology and its deployment in 5G systems will makes its superior over the previous systems. D2D communication makes the system reliable and improves the performance of the system but its security is still an issue of discussion. Attacks like eavesdropping, Traffic sensing, Denial of services attack are very common in D2D communication and can be prevented by providing privacy to the network and maintaining the integrity of data.

REFERENCES

1. M. Agiwal, A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey", IEEE Communications Surveys & Tutorials, 2016.; 18(3): 1617-1655,
2. Gandotra P., Jha R.K., and Jain S., "A survey on device-to-device (d2d) communication: Architecture and security issues," Journal of Network and Computer Applications, 2017; 78: 9 – 29,
3. D. Ma and G. Tsudik, "Security and Privacy in Emerging Wireless Networks [Invited Paper]," IEEE Wireless Communications, 2010; 17(5): 12–21,.
4. Koskela, T., Hakola, S., Chen, T., Lehtomaki, J., "Clustering concept using device to-device communication in cellular system" In: Proceedings of the IEEE Wireless Communications and Networking Conference, 2016.
5. R. Alkurd, R. M. Shubair, and I. Abualhaol, "Survey on Device to-Device Communications: Challenges and Design Issues," in Proceedings of the IEEE 12th International New Circuits and Systems Conference (NEWCAS), 2014; 361–364,.
6. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," in Proceedings of the 7th International Workshop on Security Protocols, 1999; 172–182,.
7. D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, S. Li, and G. Feng, "Device-to Device Communications in Cellular Networks," IEEE Communications Magazine, 2014; 52(4): 49–55,.
8. Arash Asadi, Qing Wang and Vincenzo Mancuso, "A Survey on Device-to-Device Communication in Cellular Network", IEEE Communications Surveys & Tutorials, 2014; 16(4): 1801 - 1819.
9. Militano, L., "Device-to-Device Communications for 5G Internet of Things.", IOT, EAI, 2015
10. Wang, Mingjun, Zheng Yan, 2015 "Security in D2D Communications: A Review" Trustcom/BigDataSE/ISPA, IEEE, 2015; 1.

11. Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, Sasu Tarkoma, and Jörg Ott, "Security and Privacy in Device-to-Device (D2D) Communication: A Review" IEEE Communications Surveys & Tutorials, 2017; 19(2): 1054 – 1079,.
12. S. A. M. Ghanem and M. Ara, "Secure Communications with D2D Cooperation," in Proceedings of the International Conference on Communications, Signal Processing, and their Applications (ICCSPA), 2015; 1–6,.
13. Othmane Nait Hamoud, Tayeb Kenaza, Yacine Challal, "Security in device-to-device communications: a survey", IET Journal, 2018; 7(1): 14 – 22,.
14. M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software- defined mobile networks security", Mobile Networks and Applications, 2016; 21(5): 729-743,.
15. Yulong Zou, Jia Zhu, Xianbin Wang and Lajos Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends" proceedings of the IEEE, 2016; 104(9): 1727 – 1765,.
16. Dongfeng Fang, Yi Qian, and Rose Qingyang Hu, "Security for 5G Mobile Wireless Networks" IEEE Access, 2017; 6: 4850 – 4874,.
17. H. Huang, N. Ahmed, and P. Karthik, "On a New Type of Denial of Service Attack in Wireless Networks: The Distributed Jammer Network," IEEE Transactions on Wireless Communications, 2011; 10(7): 2316–2324,.
18. Ni, Yiyang, "Beam forming and interference cancellation for D2D communication underlaying cellular networks" ,IEEE Trans. Common. 2016; 64(2):832–846,.
19. U. Meyer and S. Wetzel, "A man-in-the middle attack on UMTS," in Proc. 3rd ACM Workshop Wireless Security, Philadelphia, PA, USA, 2004; 90–97.
20. M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks", IEEE Communications Surveys & Tutorials, 2016;18(3): 2027-2051,.
21. Mocktoolah and K. K. Khedo, "Privacy Challenges in Proximity based Social Networking: Techniques & Solutions," in Proceedings of the International Conference on Computing, Communication and Security (ICCCS), 2015;1–8,
22. N. Kayastha, D. Niyato, P. Wang, and E. Hossain, "Applications, Architectures, and Protocol Design Issues for Mobile Social Networks: A Survey," Proceedings of the IEEE, vol. 99, no. 12, pp. 2130–2158, 2011.
23. M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," IEEE Communications Surveys & Tutorials, 2013; 15(1): 446–471,.
24. Tata, C.H.A.F.I.K.A., Kadoch, M.I.C.H.E.L., " Secure network coding based data splitting for public safety D2D communications over LTE heterogeneous networks", Proceedings of

the 14th IEEE International Conference on Computer and Information Technology (CIT'14), 2014.

25. G. Raju and R. Akbani, "Authentication in wirelessnetworks,"inProc.40th Annu. Hawaii Int. Conf. Syst. Sci., Waikoloa, HI, USA, Jan.2007,doi:10.1109/HICSS.2007.93.
26. J. Wang and T. Lin, "Authentication system for device-to-device communication and authentication method therefore," EP2663051A1, 2013.
27. H. Yang and V. A. Oleshchuk, "An Improvement of the Batch Authentication and Key Agreement Framework for P2P-based Online Social Networks," in Proceedings of the International Conference on Privacy and Security in Mobile Systems (PRISMS), 2014; 1–4.
28. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," IEEE Communications Surveys Tutorials, 2015; 17(4): 2317–2346.
29. W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, and Y. Cheng, "Secure Key Establishment for Device-to-Device Communications," in Proceedings of the IEEE Global Communications Conference (GLOBECOM), 2014; 336–340.
30. Aiqing Zhang ; Jianxin Chen ; Rose Qingyang Hu ; Yi Qian, "Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks" IEEE Transactions on Vehicular Technology , 2016; 65(4): 2659 – 2672.