A Review On Security Issues In D2D IoT Networks

Prince Kumar Patel[1], Prof. Vijay Bisen[2]
[1, 2] Dept of Electronics and Communication Engineering
[1, 2] VITM, Indore, India

Abstract- *Device to Device Networks are being developed for reducing the load on existing wireless networks. The main idea is to distribute the load so as to avoid network congestion. Device-to-device (D2D) communication is expected to play a significant role in upcoming networks as it will reduce the burden from the cellular systems. This may make big data applications easier. However the D2D networks don't use the security provided by cellular networks. Hence there is a chance of attacks. The major attack in D2D devices is the eavesdropping attack in which mobile hosts share the same wireless medium and broadcast signals over airwaves, which can be easily intercepted by receivers tuned to the proper frequency. Thus, the attacker can read exchanged messages and is able to inject fake messages to manipulate other users. This paper investigates the salient approaches of D2D networks in the context of security and access control.*

Keywords- Device-to-device (D2D) Networks, Cellular network, Resource management LTE direct, Probability of Interception, Secrecy of Outage.

I. INTRODUCTION

Cellular network is now four generations old. Need for fast multimedia-rich data exchange along with high quality voice calls has been the primary motivation in this forward journey. As newer and more demanding applications arise and subscriber base increases exponentially, there is an urgent requirement for more novel techniques to boost data rates and reduce latency. D2D communication is a new paradigm in cellular networks. It allows user equipments (UEs) in close proximity to communicate using a direct link rather than having their radio signal travel all the way through the base station (BS) or the core network. One of its main benefits is the ultra-low latency in communication due to a shorter signal traversal path. Various short-range wireless technologies like Bluetooth, WiFi Direct and LTE Direct (defined by the Third Generation Partnership Project (3GPP) can be used to enable D2D communication. They differ mostly in the data rates, distance between -hop devices, device discovery mechanisms and typical applications.

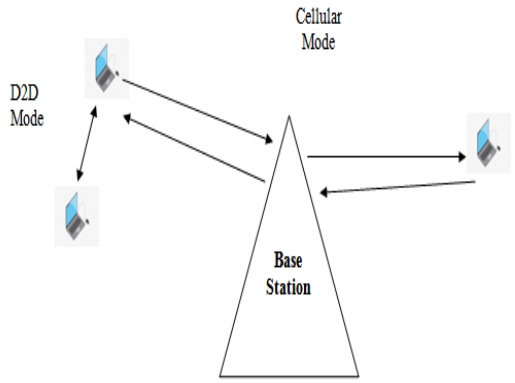

Fig.1 Model for D2D Networks

For example, Bluetooth supports a maximum data rate of Mbps and a range close to m, WiFi Direct allows up to Mbps rate and m range while LTE Direct provides rates up to 13.5 Mbps and a range of m. D2D connectivity will make operators more flexible in terms of offloading traffic from the core network, increase spectral efficiency and reduce the energy and the cost per bit. Figure.1 illustrates how cellular communication and D2D communication function. Till recently D2D communication did not appear financially viable to cellular network providers. But the current boom in context-aware and location discovery services is bringing a rapid change to this situation. Readers will find a list of authoritative surveys and original research on D2D communication. We do not attempt another survey here but only provide a high-level tutorial-style overview of the field.Further, reduced interference levels in system lead to higher system capacity and spectrum efficiency. Furthermore, D2D communications can improve the throughput, power efficiency and cell coverage. D2D users can either reuse the cellular network resources in the licensed spectrum (i.e., in band D2D) or use the resources from the unlicensed spectrum (i.e., out band D2D).

II. PREVIOUS WORK

Khalid et al. in [1] investigated the physical layer security and data transmission for the underlay device-to-device (D2D) networks, and considers a combination of the reconfigurable intelligent surface (RIS) and full-duplex (FD) jamming

receiver for the robustness and security enhancements of the system. In the demonstrated spectrum sharing setup, the total power of the D2D networks is conceived to the transmitter and receiver to transmit a private message and emit the artificial noise (AN) signals. To prevent information leakage, a beamforming design is presented for a multi-antenna FD D2D receiver in order to suppress and inject the AN signals in the direction of legitimate users and eavesdropper, respectively. The statistical characterization of end-to-end RIS-assisted wireless channels is presented, and the achievable ergodic secrecy rate of the system is derived in novel approximate expressions. The numerical and simulation results confirm the accuracy and effectiveness of the proposed analytical framework. The results demonstrate an optimal selection of the D2D power allocations for different number of reflecting elements in terms of achievable ergodic secrecy rates of the system.

Long Kongy et al. in [2] proposed a Secrecy Analysis for D2D Networks over α-μ Fading Channels with Randomly Distributed Eavesdroppers. Performance evaluated for fading conditions under eaves dropping attacks. They also calculated the secrecy orcep.tutage, and probability of int. The paper concludes the following results, when and how to optimally exploit D2D mode to enhance Cellular capacity. The paper concludes that with the increase in both Cellular and D2D load, link capacity of both modes falls, but the switching distance for D2D mode recedes away from BS with cellular load whereas it tends towards BS with increase in D2D load. The paper also concludes that bandwidth required for D2D mode is almost flat with the exception of locations near the BS and for higher cell load where the bandwidth required for D2D mode becomes very large.

Yajun Chen et al. in [3] evaluated the power access control. This paper the key parameters which have been analyzed are ratio of signal power to noise plus interference power, outage probability, effect of variation of transmitter power, capacity, mode selection, and D2D mode switching distance. The main aim of this paper is to find optimum distance for switching to D2D mode from cellular mode for loads with different power ratio. In this paper they considered downlink mixed D2D and cellular scenario, where D2D are underlying cellular network. In this paper they calculate number of UEs in the transmitter coverage area. Power access control (PAC) protocol and generation of random frequencies were evaluate in terms of the D2D network parameters such as BER, outage and throughput.

M.Haus et al. in [4] proposed a method for establishing security and privacy parameters in D2D Networks. Authors showed that it is always a challenge to mitigate the effects of partially overlapping channels in the D2D model of data transfer in the presence of attacks. In such a case, it becomes mandatory to design a mechanism to circumvent the possibilities of overlapping of user data for different D2D pairs and revert the effects of BER and Outage of the system. In such a case, the concept of game theory is useful to evaluate the chance of overlap among user data for different pairs. This is to be employed in both in-band and out-band systems to improve the performance of the system.

H.Wang et al. in [5] proposed a mechanism for energy harvesting for the efficiency enhancement of D2D networks. In this case, the system designed also used the UAV assisted technique. The energy harvesting concept is basically a technique to leverage the available energy resources of the network so as to enhance the signal strength and thereby increase the signal to noise ratio. It is shown that such a mechanism is effective to enhance the performance of the conventional D2D based network.

C. Chen et al. in [6] showed that it is necessary to devise a mechanism for D2D switching distance. The switching distance is necessary to ascertain the distance at which the strength of a particular mode of data transmission is higher in the underlay network. The two modes are the conventional cellular mode and the D2D mode. It is necessary to compare the strengths of the signal modes prior to choosing a certain one at a particular distance ‘d’. It is however not only dependent on the distance alone and also depends on other parameters such as shadowing effects and signal fading. Hence it is necessary to compute the optimum distance so as to gauge the coverage of the D2D network.

S.Sobhi Givi et al. in [7] proposed a technique for mode selection in n D2D networks. It was shown that the Bit Error Rate (BER) is a serious errant in the performance in D2D networks. The bit error rate is closely related to the signal strength of the D2D network. Since the Base station is unavailable for boosting the signal strength and routing the network traffic, therefore the BER is a serious challenge to be reduced within acceptable limits. The major blow is the decrease in the signal strength of the signal which gets weakened due to the fading effects. Hence the bit error rate takes a surge due to decreasing signal to noise ratio. To circumvent this issue, corrective measures need to be taken based on the mode selection which would lead to least BER for a particular transmission mode.

H Ghavami et al. in [8] proposed a mechanism for the evaluation of the outage in D2D networks undergoing Suzuki

Fading. The outage means the chance of unacceptable quality of service. The outage primarily depends on the signal to noise ratio and the bit error rate of the system. The system outage often is represented in terms of the complementary cumulative distribution function or the CCDF. The need for using a probabilistic model for the description of the outage of the system is due to the fact that neither the BER no the SNR of the system can be used to ascertain the outage since both are subjective performance metrics. In general, it is shown that the outage is a function of the signal to noise plus interference ratio, the D2D distance and the channel fading effects

CM Stefanovic in [9] proposed a mechanism for the evaluation of the level crossing rate (LCR) for a general alpha and mu fading channel model. The level crossing rate (LCR) is the measure of the number of time the signal strength plummets below a fading dip threshold. The significance of the fading dip based analysis is the fact that it helps to gauge the number of times the system needs to switch from the D2D mode to the cellular mode of data transmission, The threshold for the fading dip of the LCR is generally considered to switch from cellular to D2D and D2D to cellular mode of data transmission. Another important aspect tis the variation of the level crossing rate with the signal to noise ratio. Often a chance of false alarm is obtained due to the noise effects in alpha-Mu fading environment. This often results in the increasing BER of the system.

D Tetreault et al. in [10] explained the concept of multi-path propagation and synchronization in D2D networks. The effect of multi-path propagation is the fact that the channel response is not a single impulse response. In this case, the multi-path propagating waves traverse different distances and hence have different run lengths. This results in the different times of travel and different time of arrival at the receiving D2D device. This is also results in the fading and interference effects. The wave clusters arriving at slightly different times often create in interference pattern which causes the strength to wax and wean and hence makes the strength variable. This may lead to the occurrence of inter symbol interference.

III. FUNCTIONAL DESCRIPTION

The major attack in D2D devices is the eavesdropping attack in which mobile hosts share the same wireless medium and broadcast signals over airwaves, which can be easily intercepted by receivers tuned to the proper frequency. Thus, the attacker can read exchanged messages and is able to inject fake messages to manipulate other users.

Artificial noise (AN) addition algorithm is to be used in the guard bands of the multiplexed user signal. The artificial noise is added in the guard band to:

1) Decrease the chances of intercept of the actual signal
2) Decrease the system secrecy outage. Secrecy outage means the chances of non acceptable secrecy. This is computed as:

$$y = \mathbf{Pr}\,(X_A \geq X_{AN}) \qquad \textbf{(1)}$$

Here,
Pr stands for probability
X_A represents actual signal
X_{AN} represents artificial noise

To minimize the bandwidth use, frequency re-use is to be used. The frequency re-use factor is defined as:

$$\theta = \frac{d}{r} \qquad \textbf{(2)}$$

θ represents frequency re-use factor
d represents frequency re-use distance
r is radius of cell.

Device to device communication is one the effective ways to improve network efficiency and suggested technique (LTE-Direct) to offload base station traffic in LTE advanced and future networks. D2D communications are significant in applications like self driving cars, machine to machine communications and other internet of things applications. 5G technology will make use of D2D communication for wide range of applications. Internet of Things will connect billions smart things (devices and sensors) to internet. D2D communication can be implemented in IoT applications for low power mesh networking and smart sensor clouds. Mission critical application is one of the most significant applications of D2D communication. During an emergency situation, network availability might be limited or unavailable.

IV. CONCLUSION

It can be concluded that the concept of device to device communication is briskly catching up as the conventional cellular system mechanism is facing extreme loading due to increase in number of users and need for enhanced bandwidth. D2D networks don't use the security provided by cellular networks. Hence there is a chance of attacks. The major attack in D2D devices is the eavesdropping attack in which mobile hosts share the same wireless medium

and broadcast signals over airwaves, which can be easily intercepted by receivers tuned to the proper frequency. Thus, the attacker can read exchanged messages and is able to inject fake messages to manipulate other users. The paper presents a various approaches used for security and access control for D2D networks.

REFERENCES

[1] W. Khalid, H. Yu, D. -T. Do, Z. Kaleem and S. Noh, "RIS-Aided Physical Layer Security With Full-Duplex Jamming in Underlay D2D Networks," in IEEE Access, vol. 9, pp. 99667-99679, 2021

[2] Long Kongy, Georges Kaddoumy, Satyanarayana Vuppala, Secrecy Analysis for D2D Networks over α-μ Fading Channels with Randomly Distributed Eavesdroppers, IEEE 2019

[3] Yajun Chen, Xinsheng J, Kaizhi Huang, Bin Li & Xiaolei Kang, "Opportunistic access control for enhancing security in D2D-enabled cellular networks", Springer 2018

[4] M Haus, M Waqas, AY Ding, Y Li, "Security and privacy in device-to-device (D2D) communication: A review", IEEE 2017

[5] H Wang, J Wang, G Ding, L Wang., "Resource allocation for energy harvesting-powered D2D communication underlaying UAV-assisted networks", IEEE 2018

[6] G Chen, J Tang, JP Coon., "Optimal routing for multihop social-based D2D communications in the Internet of Things", IEEE Internet of Things Journal 2018

[7] S Sobhi-Givi, A Khazali, H Kalbkhani.,"Joint mode selection and resource allocation in D2D communication based underlaying cellular networks", Springer 2018

[8] H Ghavami, SS Moghaddam, "Outage probability of device to device communications underlaying cellular network in Suzuki fading channel", IEEE 2017.

[9] CM Stefanovic, "LCR of amplify and forward wireless relay systems in general alpha-Mu fading environment", IEEE 2017.

[10] D Tetreault-La Roche, B Champagne, "On the use of distributed synchronization in 5G device-to-device networks", IEEE 2017

[11] X Li, Z Wang, Y Sun, Y Gu, J Hu, "Mathematical characteristics of uplink and downlink interference regions in D2D communications underlaying cellular networks", Springer 2017

[12] M Afshang, HS Dhillon, "Modeling and performance analysis of clustered device-to-device networks", IEEE 2016.

[13] HS Nguyen, AH Bui, DT Do, Vincent W. S. Wong, "Imperfect channel state information of AF and DF energy harvesting cooperative networks", IEEE 2016

[14] T Li, P Fan, KB Letaief, "Outage probability of energy harvesting relay-aided cooperative networks over Rayleigh fading channel", IEEE 2015

[15] R Martinek, J Vanus, P Bilik, "The implementation of equalization algorithms for real transmission channels", IEEE 2015