International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

A Survey on Security Mechanisms in D2D IoT Networks

Priyanka Thakre[1], Prof. Sonal Sharma[2]

Abstract: Due to the availability of handheld, mobile devices and the advent of cloud and bog data applications, the data traffic in the licensed bands has increased. This has led to the exploration of alternative avenues to de-load the conventional wireless networks. A new paradigm called device to device networks has evolved which is a category of mobile ad-hoc networks. 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 and existing research methods.

Keywords: Internet of Things (IoT), Network Security, D2D Security, Throughput, Error Rate.

I. INTRODUCTION

The cellular network has now undergone four generations. The main driving force behind this upward movement has been the need for quick, multimedia-rich data interchange and high-quality voice communications. More innovative methods to enhance data rates and decrease latency are urgently needed as new, more demanding applications emerge and subscriber bases grow quickly. A new paradigm in cellular networks is D2D communication. It enables close-by user equipments (UEs) to connect directly rather than having their radio signal pass through the base station (BS) or the core network to interact. Its ultra-low communication latency as a result of a shorter signal traversal path is one of its primary advantages. Bluetooth, WiFi Direct, and other short-range wireless technologies.

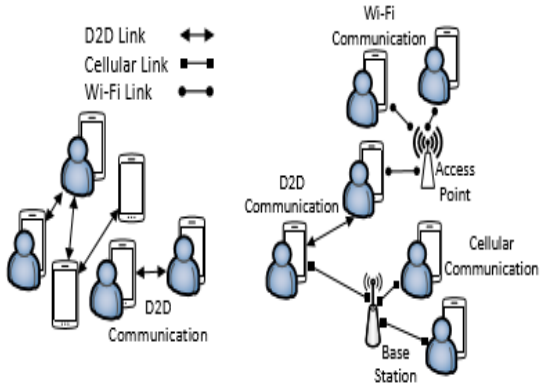

Fig.1 Architecture for D2D Networks

For instance, WiFi Direct permits up to Mbps rate and m range, while Bluetooth supports a maximum data rate of Mbps and a range close to m, LTE Direct offers speeds up to 13.5 Mbps and a range of m. Operators will have more flexibility when offloading traffic from the main network thanks to D2D connection, which will also improve spectral efficiency and lower energy and cost per bit. The operation of cellular and D2D communication is shown in Figure.1. D2D communication did not appear to be economically feasible to cellular network providers until recently. But this is quickly changing thanks to the current surge in context-aware and location discovery services. 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

Khaled et al proposed a 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

Kongy et al proposed 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.

Yujan et al evaluated the 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.

Henrique et al. have provided a Distance Based Study of D2D Communication for Improving Overall System Capacity. In this paper they investigate potential sum rate gain of D2D communication underlying cellular network and conventional cellular system without D2D communication, all investigation in this paper has been done in Uplink. In this paper two communication mode has been used, D2D mode and Cellular mode. For investigating systems overall performance improvement by using D2D communication they have made two different analyses: without and with restriction concerning the distance between D2D-Tx and D2D-Rx. The paper concluded that when user equipment (UE) is in the near base region the rates are higher than the UE is in the near cell region.

Xingqin Lin et al. have provided In this paper they addressed two fundamental issues in D2D communication underlying cellular networks, first one is how D2D user should access spectrum and second one is how D2D user should choose between communicating directly or via base station. To overcome these issues they proposed a tractable hybrid network model where the mobiles are positioned randomly following spatial Poisson point process. After that analytical rate expression has been applied to overcome the spectrum sharing issues. In this paper two spectrum sharing model has been described one of which

Haus et al. have provided a survey on D2D security. In this paper they presents a comprehensive and tractable analytical framework for D2D enabled uplink cellular networks with a flexible mode selection scheme along with truncated channel inversion power control. They proposed a mode selection scheme for a UE which accounts for both D2D and cellular communication, and also different from the existing one which accounts only for D2D

communication based on D2D link distance. In the paper with the help of numerical analysis they investigate the expected performance gain and provide guidelines for selecting the network parameters.

Zhang et al. analyzes the underlay and overlay mode selection of Device-to-Device (D2D) communication in the LTE-Advanced single-cell scenario. They mainly considered two cases, in one of which the cell contains the relay node and in the other the cell does not contains the relay node, and the study focuses on the location relationship between cellular UE and D2D UE. In the paper they proposed to preferred underlay mode when cellular user is closer to base station than the D2D user. In the paper they describe the different models of the network such as Infrastructural model in which network contains a circular cell of radius R, where a BS equipped with Omni-directional antennas is in the center of the cell and three relay nodes are uniformly distributed in the cell with the distance D to the BS.

In [6], Ramasubramanyam et al. proposed User model in which two kinds of users has been considered in the system. A cellular user (CU) communicates solely through the BS. On the other hand Device-to-Device users are those who do not communicate via the BS but communicate directly with each other over one hop. The paper describes about Overlay and Underlay mode selection under the condition of a single cell without a relay node and with a relay node. The paper concludes that the simulation results shows that the system parameter affect the condition of mode selection. By taking contradistinction between scenarios with and without relay nodes, it can conclude that the introduction of relay node will increase both chance and area of D2D pair using underlay mode.

Zengquin et al. proposed Overlay in-band D2D and another one is Underlay in-band D2D. In Overlay in-band D2D uplink spectrum is divided into two orthogonal portions, a fraction 'n' is assigned to D2D communication and a fraction '1-n' is assigned to cellular communication. While in Underlay D2D communication, each D2D transmitter uses frequency hopping to randomize its interference to other links. The paper concludes how to apply the derived result in underlay D2D to study spectrum sharing from coverage prospective. It also concludes that there is a tradeoff between spectrum sharing and mode selection in D2D communication.

Rawan et al. proposed s a biasing –based mode selection for D2D enabled cellular networks for security. The paper provides a bias value for which D2D communication is enabled in cellular network and the amount of traffic offloaded to the D2D communication mode. The paper also concludes an analytical prototype to evaluate outage and rate in the proposed D2D enabled cellular network, it also concludes that underlay D2D communication is capable of improving system performance in terms of spatial frequency reuse, link capacity, and total network capacity.

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:

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

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:

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

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.

Conclusion:

It can be concluded that the idea of device to device communication is quickly catching up as the traditional cellular system mechanism struggles under heavy usage from an increase in users and the demand for more bandwidth. Cellular network security is not used by D2D networks. Thus, there is a possibility of attacks. The primary threat to D2D devices is the eavesdropping assault, in which multiple mobile hosts use the same wireless network and broadcast signals that can be easily received by receivers tuned to the right frequency. As a result, the attacker has access to read messages that have been transmitted and can insert false messages to influence other users. The paper discusses a number of

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 Transactions on Vehicular Technology, 2022, vol. 9, pp. 99667-99679.
[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
[16] M Ji, G Caire, AF Molisch, "Fundamental limits of caching in wireless D2D networks", IEEE 2015.
[17] ZH Awan, A Sezgin "Fundamental limits of caching in D2D networks with secure delivery", IEEE 2015.

[18] AH Sakr, E Hossain, "Cognitive and energy harvesting-based D2D communication in cellular networks: Stochastic geometry modeling and analysis", IEEE 2015

[19] H Sun, M Wildemeersch, M Sheng, "D2D enhanced heterogeneous cellular networks with dynamic TDD", IEEE 2015

[20] H Chen, L Liu "Resource allocation for sensing-based device-to-device (D2D) networks". IEEE 2015.

[21] H Chen, L Liu, JD Matyjas, MJ Medley, "Optimal resource allocation for sensing-based spectrum sharing D2D networks", Elsevier 2014