A Physical Layer Security Mechanism For D2D Networks Against Eavesdropping Attacks

Mayur Jagdale[1], Prof. Megha Jat[2]
[1, 2] PCST, Indore, India

Abstract- *Conventional networks with the mediation of base station are being explored to be replaced at shorter distances by D2D Networks. To avoid network congestion, the fundamental goal is to distribute the load. Device-to-device (D2D) communication is anticipated to be crucial in future networks since it would lighten the load on cellular systems. Big data applications may become simpler as a result. The D2D networks, however, do not make use of the security offered by cellular networks. Thus, there is a possibility of attacks. However, a listener with unlimited computational power might still use a brute-force attack to crack these methods. In this situation, Physical Layer Security (PLS), which takes advantage of the features of the wireless channel, has become a viable option for safeguarding wireless transmissions. Along with other technologies, the power access control protocol has been. The performance metrics are outage probability and BER of the system.*

Keywords- Wireless Sensor Network, Clustering, Pseudo Random Sequence, Secrecy Outage.

I. INTRODUCTION

Information exchange between people has been fundamentally changed by new technologies, such as mobile computing and wireless communication. In spite of rapid advancements, mobile techniques like cellular networks are infrastructure-dependent. The connectivity of mobile users is confined to the coverage of base stations and direct communication between mobile devices is not permitted [1]. The traffic is routed via a core network, even if source and destination are in close proximity to one another. This inflexibility limits the potential of data exchange between mobile users. Especially, when considering the shift in personal computing from stationary PCs and heavier laptops to mobile devices.

The present scenario of cellular systems in challenging due to the increasing user number and data magnitude. The base station which routes the data from devices is becoming more and more loaded with data. This has led to the concerns on the upcoming years when the number of users would increase manifold and so would be the data rate. With emerging technologies on the forefront, a new technical solution to the aforesaid problem is inevitable. One of the major contenders for the same is the Device to Device Network (D2D) model. In this model, the base station is completely bypassed and the data is communicated among the devices directly. In this scenario, the load is hence not subjected to the base station of the cellular system although it exists [1]. The device to device geometry is depicted in the figure below.

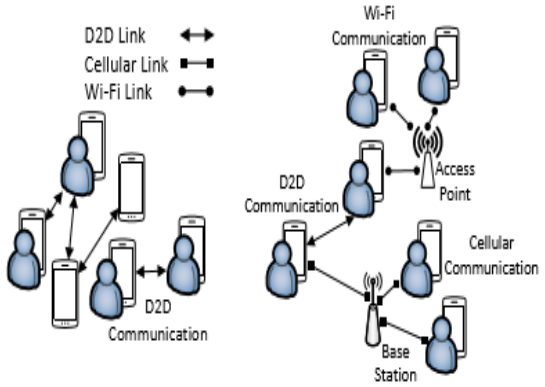


Fig.1 TheD2D Model

This above figure describes a simple D2D communication system architecture. However, there are serious challenges in the IoT framework due to the following constraints:

1) Increasing number of users leading to more data traffic.
2) Excessive load on the cellular system for involvement in data routing through the base station subsystem (BSS).

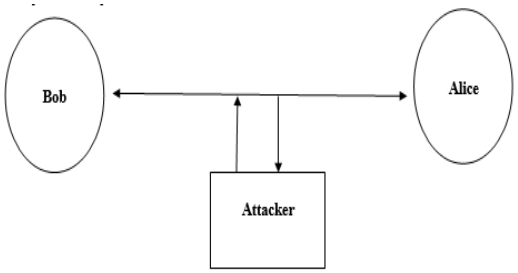


Fig.1 Man in the middle attack in D2D model

The IoT framework can be categorized as

1) Cellular based IoT
2) Non Cellular based IoT

With increasing load on the BSS, the focus has shifted on non-cellular based IoT so that devices can communicate with each other by completely bypassing the BSS. The following diagram renders the visualization:
Here the process starts with the D2D mode where the Base station communicates with the devices. This device to device communication provides the benefit of directly communicating network. The major challenge in D2D based IoT networks is security.

II. METHODOLOGY

Random Frequency Generation is changing the frequency continuous in a random manner.

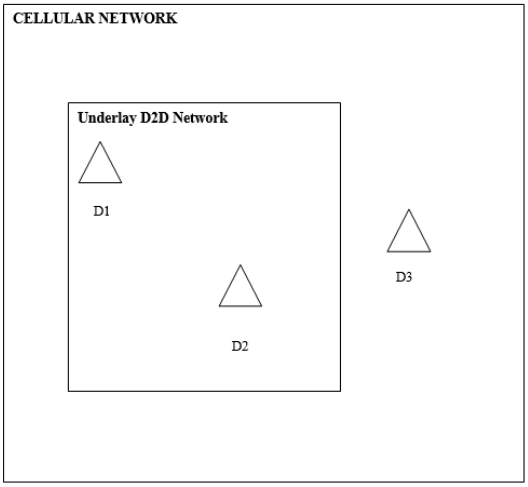


Fig.3Underlay D2D Model

The proposed algorithm is presented as:

To obtain the spectral attributes, we need to seek the help of Fourier Methods for deciding the spectral range which needs to be spread. The step wise description of the proposed approach is given below:

The channel is to be sensed based on the jamming activity and can be done using energy sensing.

The proposed technique can be explained using the following algorithm:

Step1. Generate a random serial data set that is to be transmitted in the form of 0s and 1s.

Let it be given by:

x(n)=random (n); where n is the number of bits are completely random

Segregate the power levels for **Data and Artificial Noise.** Apply Power Access Control (PAC) Protocol.

Step2. Design a typical channel response of an ideal cognitive system.

Let the channel response in time domain be h(t)

in the frequency domain, let the channel response be H(f)

H(f)=F.T. {h(n)}

F.T. denotes the Fourier Transform

Step3. Design frequency dependent jamming mechanism.

Let the jamming power be:

Pjam=f(frequency or subcarrier)

here,

different frequencies are used for different users in the network, which are also called sub-carriers

Step4. Design and add spectral noise

Design a time domain noise signal n(t)

Add it to the signal in the channel to get

X=S+N

Step5. Detect low, moderate and high jamming action

The decision is to be based on:

Low Jamming Activity: if sub-carrier gain<1.5*Ideal Subcarrier Gain

Moderate Jamming Activity: if sub-carrier gain>1.5*Ideal Subcarrier Gain>2*Ideal Subcarrier

High Jamming Activity: if sub-carrier gain>2*Ideal Subcarrier Gain

Step6. Generate signaling points for the system and obtain the scatter plot for:

No Jamming Action
Low Jamming Action
Moderate Jamming Action

High Jamming Action

The scatter plots can be plotted for

Re{x(n)}

Img{x(n)}

Step8. Compute Throughput for 3 cases:

1) Low Jamming activity
2) Moderate Jamming Activity
3) High Jamming activity

Also compute the allied parameters
The performance metrics to be evaluated are:

1) $Throughput = \frac{Transmitted\ Data}{Time}$

2) $$BER = \frac{Number\ of\ Bit\ Errors}{Total\ Bits\ Transmitted}$$

3) $$ccdf(outage) = 1 - cdf(outage)$$

The throughput is critically affected by the strength of the jamming/eavesdropping attack. High values of throughput are targeted.

The BER of the system is a measure of the reliability of the data transfer. Low values of BER are targeted.

The number of frequencies changed is given by the **generation length (L).** However increasing L also increases BER of the system. Power Access Control means sending the data at low power level in between artificial noise. The time duration of artificial noise and actual signal is know only to Tx and Rx. Thus, only receiver can access the transmitted signal.

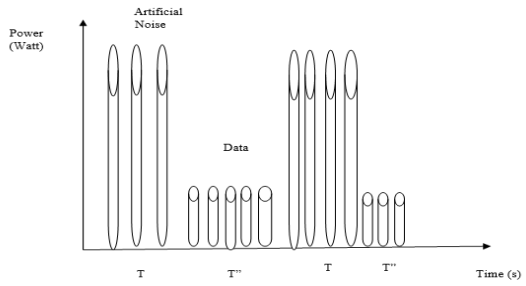


Fig.4Noise Injection

Here,
T is the time duration of Artificial Noise
T" is the duration of data

SIMULATION RESULTS

The results obtained are for the simulations run for the following specifications:

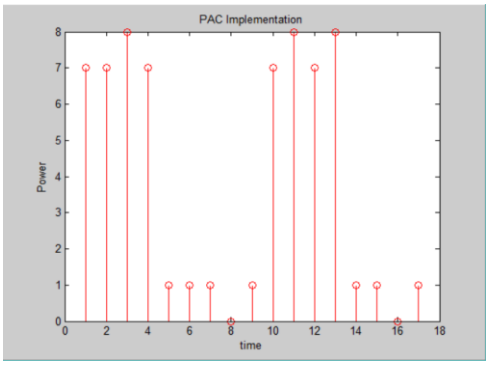


Fig.5 Injecting artificial noise at frequency slots

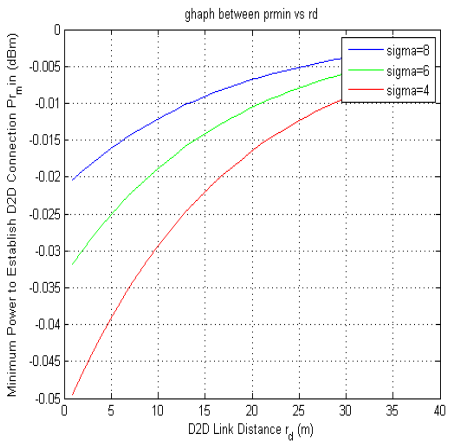
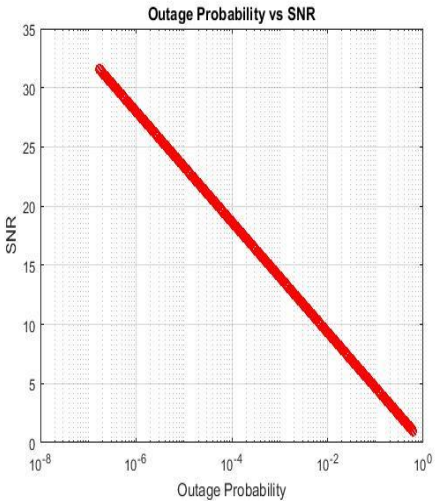


Fig. 6 Minimum Power Required to establish D2D link as a function of distance and fading (sigma)



Fig, 7 Decrease in Outage with Increase in SNR

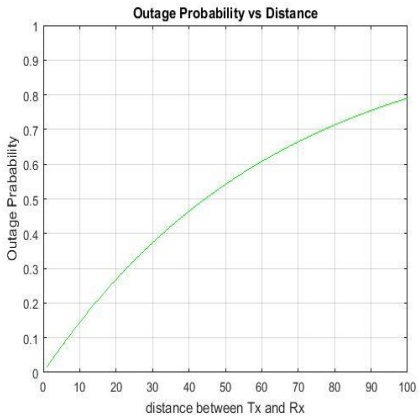


Fig. 8. Increase in Outage with Increase in Distance between Tx and Rx

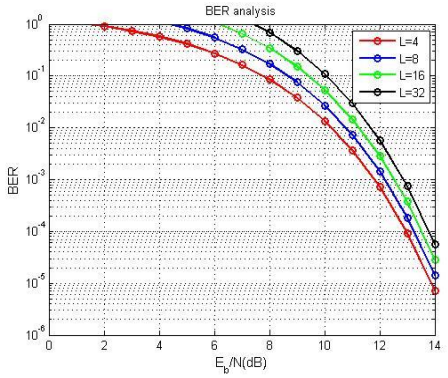


Fig. 9. BER performance of system

CONCLUSION

The proposed work presents a power access protocol for securing device to device networks. It has been discussed that with the increase in the data transfer capacity of stationary and predominantly handheld mobile devices, the data traffic of networks has increased manifold. The problem is more aggravating since the allocated bandwidth to networks is limited yet the bandwidth requirement of users is increasing by the day due to multimedia applications. The ease of cloud and bog data platforms is adding more data traffic to the already loaded network conditions. This has resulted in the inevitable surge of device to device (D2D) networks. The device to device networks aim at bypassing the cellular network for transfer of data and create an ad-hoc network which is mobile in nature. These ad-hoc networks however can be categorized as:

1) Standalone networks
2) Cellular assisted networks

In both cases though, the security of the data to be transferred is a serious concern since the network security layer is bypassed and the device level security is to be utilized. Hence, eavesdropping, impersonation, man in the middle and jamming attacks are predominant in D2D based networks. In this work, a power access control based strategy is developed for securing and authenticating D2D network data sharing. Here, the adversary is misled by generating artificial noise and it is injected into the actual data or bit stream. Due to the high signal strength of the artificial noise, it is difficult to detect the actual data stream with accuracy.

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