A Security Mechanism For Device To Device Networks Using Artificial Noise Injection

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. However, an eavesdropper with unlimited computing power may still decipher these techniques using brute-force attack. In this context, Physical Layer Security (PLS) has emerged as an attractive solution for securing wireless transmissions by exploiting the wireless channel characteristics. The power access control protocol has been implemented along with random frequency hoping to enhance the security of D2D networks. The performance metrics are outage probability and BER of the system.*

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

I. INTRODUCTION

Cellular

A Internet of things (IoT) and industrial IoT has become one of the most important areas of current research for several applications. The diagram below explains the concept of IoT. Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. Some applications of IoT are:

- Smart Cities.
- Healthcare
- Transportation
- Traffic Control
- Manufacturing
- Large Scale Automation
- Big Data Applications etc.

The functional structure of internet of things is shown in the figure below:

Fig. 1 The IoT Ecosystem

In the IoT ecosystem, the different devices are termed as things. The connectivity of the devices (things) is made over the internet. With increasing users and things, the IoT architecture is gaining more popularity due to its wide range of applications.

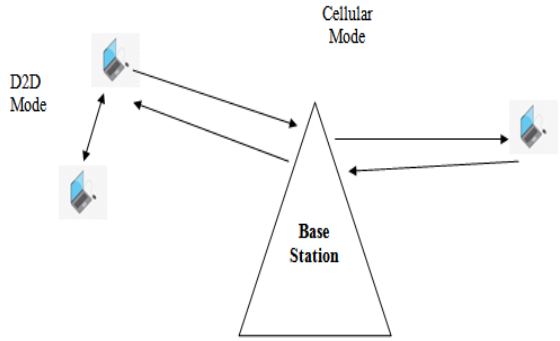


Fig. 2 Conceptual model of D2D Network

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)

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.

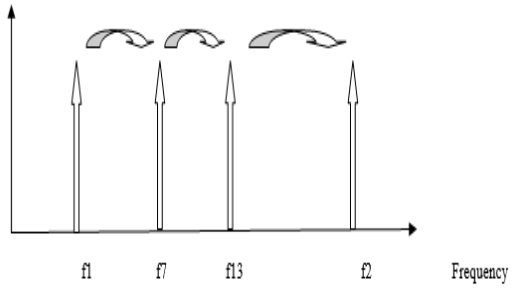


Fig.3 Random Frequency Generation

To obtain the spectral attributes, we need to seek the help of Fourier Methods for deciding the spectral range which needs to be spread.

Consider the signal to be composed of harmonics of single frequencies with dependencies of sine and cosine function given as:

$$x(t) = a_0 + \sum_{n=1}^{\infty} a_n \cos(n\omega_0 t) + b_n \sin(n\omega_0 t) \quad (1)$$

Here, a_0, a_n and b_n are known as the Fourier coefficients and $\omega_0 = 2\pi f_0 = 2\pi/T_0$

The evaluation of the co-efficients can be done using the following relations:

$$a_0 = \frac{1}{T_0}\int_t^{t+T_0} x(t)dt \quad (2)$$

This shows that the a_0 is the average value of x(t). It is also called as the dc component of x(t).

$$a_n = \frac{2}{T_0}\int_t^{t+T_0} x(t)\cos(n\omega 0t)dt \quad (3)$$

$$b_n = \frac{2}{T_0}\int_t^{t+T_0} x(t)\sin(n\omega 0t)dt \quad (4)$$

The trigonometric form of the series can be converted to the polar form which is given as under:

$$x(t) = C_0 + \sum_{n=1}^{\infty} C_n \cos(n\omega_0 t + \phi_n) \quad (5)$$

Where,

$C_n = [a_n^2 + b_n^2]^{1/2}$

And

$\phi_n = \tan^{-1}\left[\frac{b_n}{a_n}\right]$

And

C_0 = Average value of x(t) = a_0 (6)

The sine and cosine harmonics can be represented as functions of complex exponential functions given by:

$$\cos\theta = \frac{e^{j\theta}+e^{-j\theta}}{2} \quad (7)$$

$$\sin\theta = \frac{e^{j\theta}-e^{-j\theta}}{2} \quad (8)$$

Thus the spectral properties of the signal to be jammed x(t) can be given by the following equation:

$$x(t) = \sum_{n=1}^{\infty} C_n e^{j2\pi nt/T_0} \quad (9)$$

Here,

$$C_n = \frac{1}{T_0}\int_t^{t+T_0} x(t)e^{-j2\pi nt/T_0}dt \quad (10)$$

While considering the value of x(t) extending from t = $\frac{-T_0}{2}$ to t = $\frac{-T_0}{2}$.

Value of C_n

Let x(t) = A for t = -τ/2 to τ/2.

Hence,

$$C_n = \frac{1}{T_0}\int_{-\tau/2}^{\tau/2} Ae^{-j2\pi nt/T_0}dt \quad (11)$$

X(f) is changed randomly to make detection difficult

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.

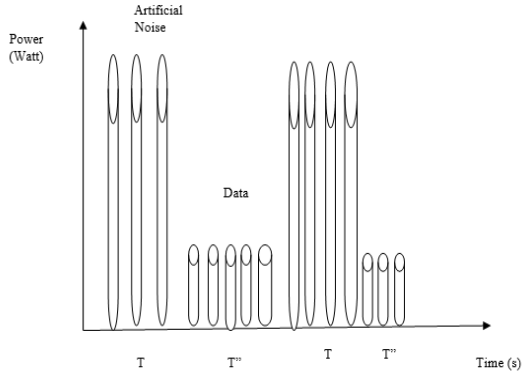


Fig.4Noise Injection

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

III. SIMULATION RESULTS

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

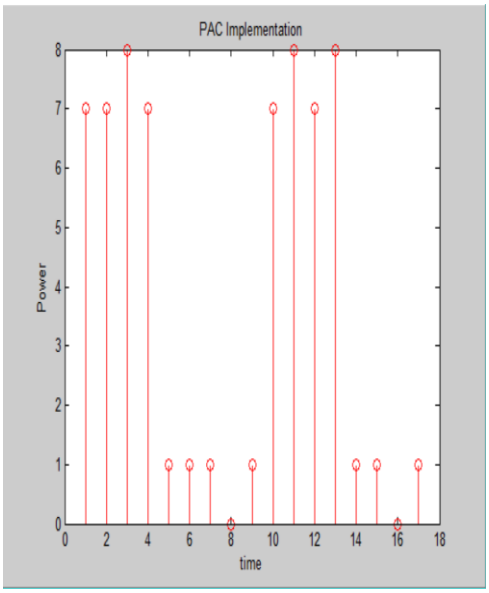


Fig.5 Injecting artificial noise at frequency slots

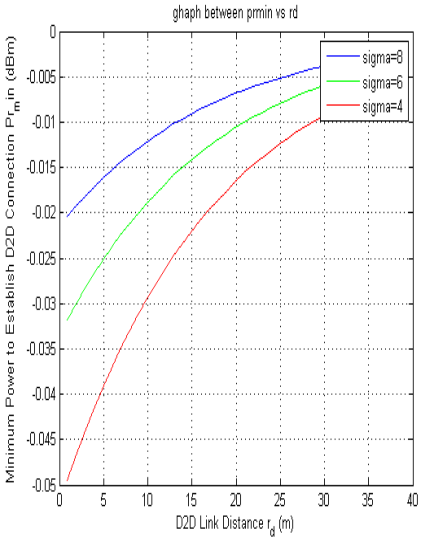
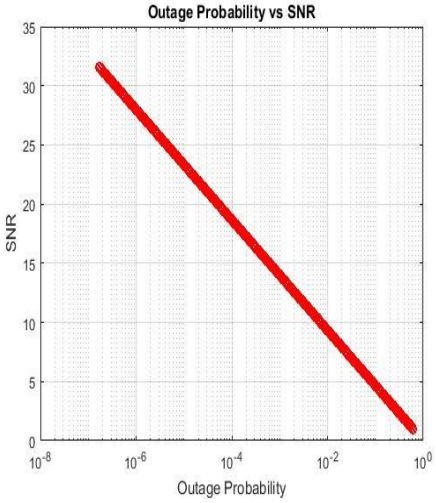


Fig. 6 Minimum Power Required to establish D2D link as a function of distance and fading (sigma)



Fig, 7 Decrease in Outage with Increase in SNR

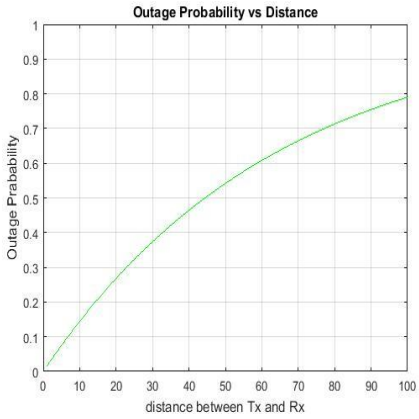


Fig. 8. Increase in Outage with Increase in Distance between Tx and Rx

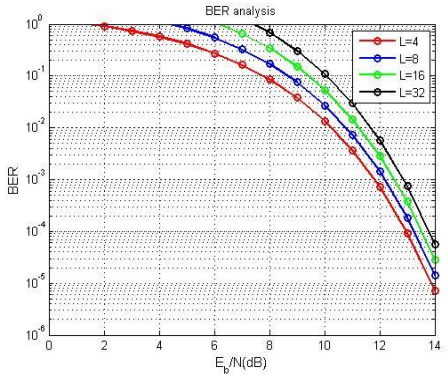


Fig. 9. BER performance of system

IV. CONCLUSION

It can be concluded from the previous discussions that the proposed system uses a PN sequence-based technique to reduce secrecy outage. The link security is a critical aspect of successful D2D operation. Traditional cryptographic techniques are not suitable for securing D2D Networks, because they require hardware complexity and consume large amounts of energy that are not affordable in a D2D Network. Moreover, an eavesdropper with unlimited computing power may still decipher these techniques using brute-force attack. In this context, Physical Layer Security (PLS) has emerged as an attractive solution for securing wireless transmissions by exploiting the wireless channel characteristics. The power access control protocol has been implemented along with random frequency hoping to enhance the security of D2D networks. The performance metrics are outage probability and BER of the system.

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