Implementing Physical Layer Security in Wireless Ad-hoc Networks and Wireless Sensor Networks with Reduced Outage and Bit Errors

Shubham Joshi
Research Scholar
Mewar University, Chittorgarh

Durgesh Mishra
Professor, SAIT & Research Supervisor
Mewar University Chittorgarh

ABSTRACT
Wireless ad-hoc networks (WANESTs) and Wireless Sensor Networks (WSNs) are typically de-centralized in nature with minimal pre-reliance on the network architecture. They are being extensively used for diverse applications such as military and defense, industrial automation, disaster management etc. Such networks generally are generally limited by their resources of data processing and memory due to large scale deployment and cost. One of the major challenges which WANETs and WSNs face is the possibility of data breach and security. Due to the limitations of memory and processing power, sophisticated encryption algorithms are often infeasible to be implemented for such networks in time critical applications. This poses a serious threat to the data transmission in the network. The way around the problem is the implementation of physical layer security (PLS) approaches, which can alleviate the issue. In this paper, an approach based on the generation of pseudo-noise sequences (PN Sequences) has been proposed so as to secure the data transfer. An adaptive clustering mechanism based on residual energy has also been proposed. The performance metrics of the proposed approach have been chosen as the bit error rate (BER) and the outage of the system. It has been shown that as the spreading factor increases, the BER of the system also increases thereby increasing the outage of the system which is a clear indication of the trade-off between the security and the reliability of the system.

General Terms
Wireless ad-hoc networks (WANESTs) and Wireless Sensor Networks (WSNs), Physical Layer Security.

Keywords
Wireless ad-hoc networks (WANESTs) and Wireless Sensor Networks (WSNs), Physical Layer Security, Bit Error Rate (BER), Outage, Frequency Hopping.

1. INTRODUCTION
Wireless ad-hoc networks (WANETs) and Wireless Sensor Networks (WSNs) are being used in diverse fields wherein human intervention is either infeasible or becomes a limiting factor. Typically they do not rely on a pre-conceived or rigid infrastructure and are also de-centralized [1]. They typically consist of nodes or sensors collecting data and then transferring the data to a central station called the base station or control station. They also share data among themselves. One of the most challenging aspects of such networks is the limitations of energy, computational prowess and memory. A typical representative illustration of wireless networks is shown below:

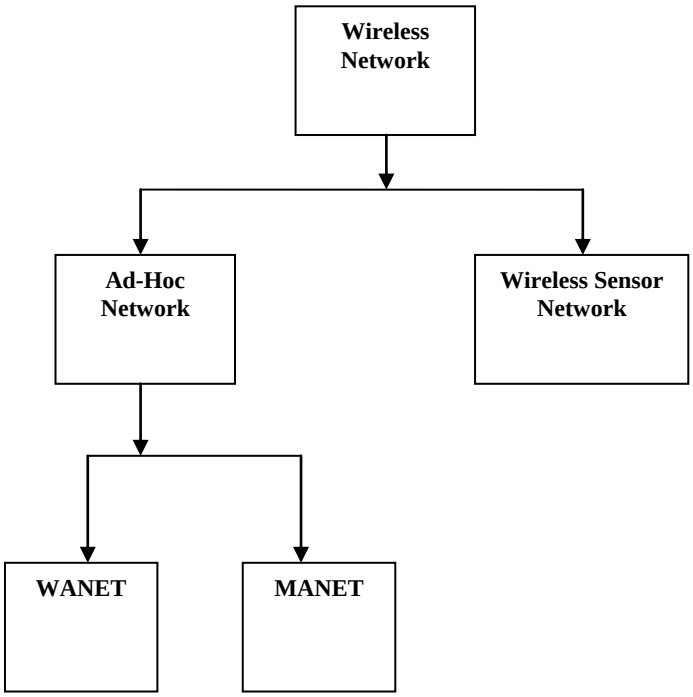

Fig 1: Categorization of Wireless Networks

The basic categorization of ad-hoc networks is Mobile ad-hoc networks and wireless ad hoc networks. Another category of wireless networks is wireless sensor networks[2]. Typically, the basic modules of the ad-hoc networks are:

1) Sensing node or module
2) Analog to Digital converter
3) Memory
4) Processor
5) Transceiver
6) Location detection sub-system
7) Mobilizer
8) Power Source

The mobilizer and the location detection system may be optional in the network and dependent on network requirements. The memory and the processing unit are typically constrained. Another limitation is the power source. The data needs to be sensed by the sensors and sent to remaining nodes or to the base station as represented by:

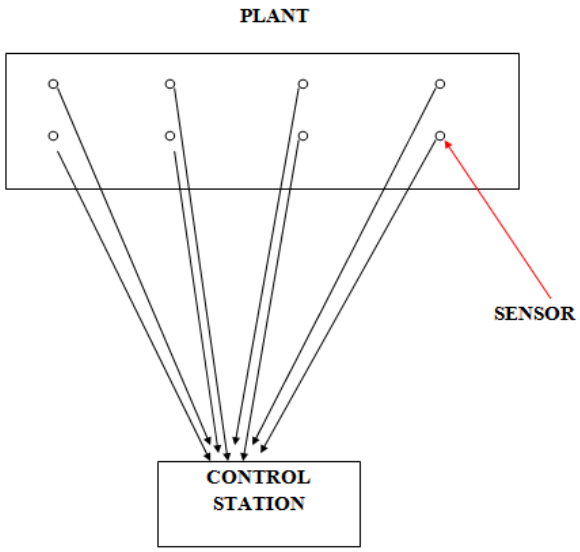

Fig 2: Typical data transfer in a WSN

The nodes gather the data and send them to the control station in the network. However the data needs to be sent in such a way that the energy consumption is minimized [3]. This is typically achieved by clustering of nodes and clustered data transfer.

2. CLUSTERING

Clustering is the technique typically used in wireless sensor networks to effectively manage the limited power resources in the network. This generally enhances the network lifetime of the network. In this process, some nodes are chosen as cluster heads and the other nodes are the regular nodes. The regular nodes send the data to the cluster heads and the cluster heads in turn send the aggregated received data to the control station[4]. Generally, the clustering is done based on several network parameters such as:

1) Energy left
2) Latency observed
3) Overall network delay
4) Clustering complexity etc.

The remaining energy for networks is generally estimated with respect to the initial energy of the network and it diminishes as the number of rounds of data transfer occur. Mathematically it is computed as:

$$E_{res,t} = E_{in} - \sum_{r=1}^{n} E_r N_r \quad (1)$$

Here

$E_{res,t}$ is the residual energy of the node at any instant 't'

E_{in} is the initial energy of the node

E_r is the energy expended in one transmission

N_r is the rounds of transmission completed prior to time 't'

Typically, it is envisaged that the value of E_r be as low as possible since the product of $E_r N_r$ is often constrained by power source. Moreover, the maximum energy utilization of the network is given by:

$$Max[E_U] = {Max[\int_{i=1}^{n} E_i]}/{\sum_{i=1}^{n} E_{int}^{i}} \quad (2)$$

Here,

E_U represents maximum energy utility

E_i represents the energy consumption of i[th] node

E_{int}^{i} is the initial energy of the i[th] node

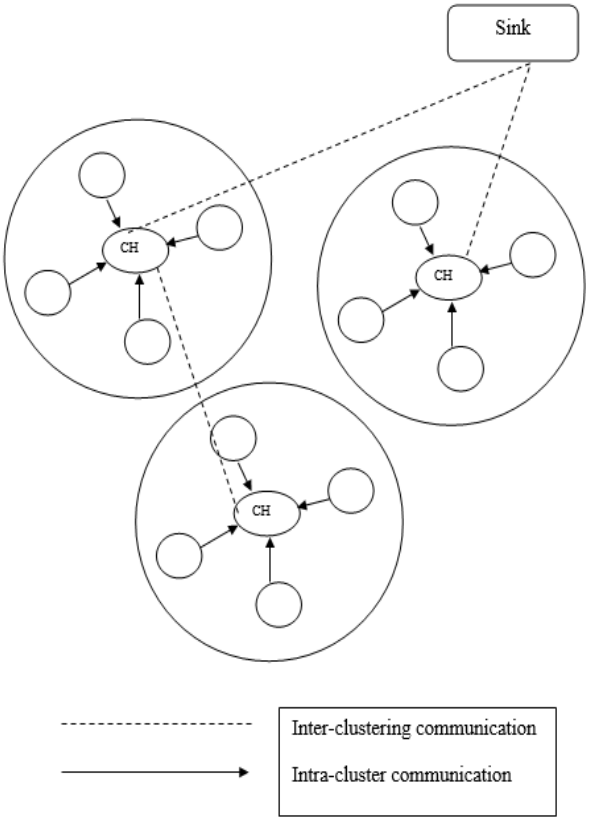

Fig 3: Data transfer in WSN

The design of the network should be such that the energy consumption is minimal for the network.

3. PHYSICAL LAYER SECURITY FOR WANETs AND WSNs: SYSTEM MODEL

Security for WANETs and WSNs are challenging due to the following attributes:

1) Limited processing power
2) Limited memory
3) De-centralized heterogeneous blocks

This doesn't allow a centralized security algorithm running to cater to the needs of system security requiring high computational cost or resulting in network latency. This calls for another mechanism of security which is the physical layer security[5]-[6]. The physical layer security is generally the security patch at the bit level architecture of the network. Since the data is transmitted in free space, it is possible to intercept the data by adversaries in the absence of any strong security mechanism[7]. The approach proposed here is based on the generation of pseudo-noise (PN) sequences, which would shroud the transmitted data for adversaries. The PN

sequence would typically control the transmission frequency of the data into free space and would be available only to the transmission and receiving ends[8]-[9]. The mathematical description of the proposed technique ensues. Let the time domain mathematical representation of the transmitted signal be given by:

$$x_{tran} = f(t) \quad (3)$$

Here,

x_{tran} is the time domain transmitted data

f represents a function of

t is the time metric

Without loss of generality, we can assume that the temporal transmission may be periodic, quasi-periodic or aperiodic. Considering the latter two cases, the transmission can be represented in the frequency domain using the Fourier Series Decomposition as:

$$x(t) = k_0 + \sum_{i=1}^{n} a_n cos(n\omega 0t) + \sum_{i=1}^{n} b_n sin(n\omega 0t) \quad (4)$$

Here,

k_0 is the constant independent of frequency of transmission

a_n and b_n are constants, dependent on frequency

$$\omega 0 = 2\pi f0 = \frac{2\pi}{T0} \quad (5)$$

Here,

$\omega 0$ is the angular frequency

$T0$ is the time period

f is the frequency of transmission

The co-efficient values can be evaluated as:

$$k_0 = \frac{1}{T_0}\int_t^{t+T_0} x(t)dt \quad (6)$$

The term k0 is the average or the dc component of the temporal data x(t). The other co-efficient values are given by:

$$a_n = \frac{2}{T_0}\int_t^{t+T_0} x(t)\cos(n\omega 0t)dt \quad (7)$$

$$b_n = \frac{2}{T_0}\int_t^{t+T_0} x(t)\sin(n\omega 0t)dt \quad (8)$$

The trigonometric to polar form representation of the temporal data stream x is given by:

$$x(t) = C_0 + \sum_{n=1}^{\infty} C_n \cos(n\omega_0 t + \phi_n) \quad (9)$$

Here,

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

And

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

And

C_0 represents dc component value of x(t) given by k_0

The complex form of the series yields the sine and cosine components of the frequencies given by the relations:

$$\cos\theta = \frac{e^{j\theta} + e^{-j\theta}}{2} \quad (10)$$

$$\sin\theta = \frac{e^{j\theta} - e^{-j\theta}}{2} \quad (11)$$

Now, the temporal signal x(t) can be represented as:

$$x(t) = \sum_{n=1}^{\infty} C_n e^{j2\pi nt/T_0} \quad (12)$$

Here,

C_n is the complex Fourier Series co-efficent given by:

$$C_n = \frac{1}{T_0}\int_t^{t+T_0} x(t)e^{-j2\pi nt/T_0}dt \quad (13)$$

If it is considered that x(t) extends from $t = \frac{-T_0}{2}$ to $t = \frac{-T_0}{2}$, then the complex Fourier co-efficient value reduces to:

$$C_n = \frac{1}{T_0}\int_{-\tau/2}^{\tau/2} Ae^{-j2\pi nt/T_0}dt \quad (14)$$

The transmission of the data is done in the form of sines or cosines and hence the signal may have a wide spectrum of bandwidth 'B'.

In case the signal is non-periodic, then the data to be transmitted can be represented in the frequency domain by dint of the Fourier Transform given by:

$$X(f) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft}\,dt \quad (15)$$

Here,

X(f) is the signal in the frequency domain

x(t) is a time domain representation of the aperiodic data

f is the frequency metric

t is the time metric

The equivalence in the f-domain is depicted in the figure below:

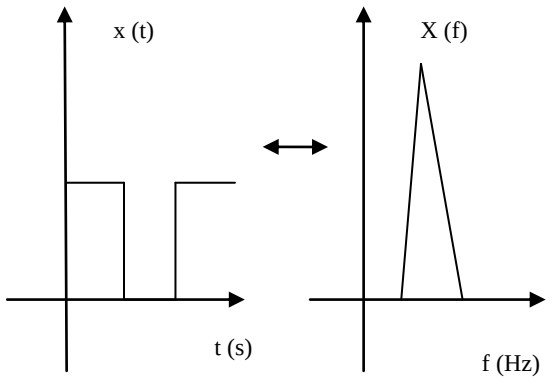

Fig 4: time and frequency domain equivalence of signals

The above figure depicts that the time dependent transmission of the data in the form of 1s and 0s can be mapped into the frequency domain equivalent of 'B' Hertz. If the frequency is varied in an interval given by:

$$B' \epsilon [f_1 \ldots\ldots\ldots\ldots\ldots\ldots f_n] \quad (16)$$

Here,

B' is the spread out frequency spectrum

The frequency spreading factor is given by:

$$L = B'/B \quad (17)$$

Here,

L is called the spreading factor

B is the original bandwidth occupied by the signal in the frequency domain.

The spreading out of the signal in the frequency domain is implemented by the generation of the PN sequence generator which generated 'n' random frequencies [10]. This is generally termed as frequency hopping and is categorized as fast frequency hopping (FFH) and slow frequency hopping (SFH), which are mathematically represented as:

Fast frequency hopping occurs when:

$$T_H < T_B \tag{18}$$

Slow frequency hopping occurs when:

$$T_H > T_B \tag{19}$$

Here,

T_H is called the hopping time

T_B is the bit period

Generally, the FFH is more secure compared to the SFH technique due to the faster transition of the frequencies [11]. However, the downside is the complexity of the decoding process as the receiving end. It is worth mentioning that the level of spreading is governed by 'L' and as the value of L increases, the security of the system also increases and vice versa. The flip side to this approach is the probability of increasing errors as the value of L increases [12]. Thus there is a tradeoff which correlated the level of security and the authenticity of data received the receiving end. This can be physically interpreted as:

$$P_e = p\left(\frac{0}{1}\right) + p(\frac{1}{0}) \tag{20}$$

Here,

P_e represents the probability of error often termed as the Bit Error Rate (BER)

$p\left(\frac{0}{1}\right)$ is the conditional probability of receiving a bit as 0 when 1 was transmitted.

$p\left(\frac{1}{0}\right)$ is the conditional probability of receiving a bit as 1 when 0 was transmitted.

The probability of error is critically dependent of the signal to noise ratio (SNR) of the system given by:

$$P_e = f(Q\left[\frac{S}{N}\right]) \tag{21}$$

Here,

f represents a function of

S represents the signal strength

N represents the noise strength

Q is the error function for non-exact definite integrals

By the virtue of the Q-function, it can be inferred that as the value of signal to noise ratio (SNR) increases, the value of $Q\left[\frac{S}{N}\right]$ decreases. However, as the value of the spreading factor increases, the same signal strength is smeared over a larger bandwidth which results in a decreased SNR value. Thus with the increase in the SNR, the BER or P_e decreases and vice versa. The probability of finding error bits in the spreading factor (L) with frequency hopping is given by:

$$P_{hop} = \{(L-1)/L\}e^{\frac{-E_b}{L}} + 1/2\text{L} \tag{22}$$

Here,

P_{hop} is the probability of error with hopping

L is the spreading factor

E_b is the energy per bit

Another important metric which is computed is the system outage which is necessary to access the possibility of acceptable quality of service. The outage is generally computed in terms of the complementary cumulative distribution function (ccdf) given by:

$$ccdf(x) = 1 - cdf(x) \tag{23}$$

The system outage should be as low as possible for acceptable transmission [13]. The outage is generally a function of signal to noise ratio and the distance between the transmitter and receiver.

To reduce the energy consumption of the system and the increase the lifetime of the network, redundancies in the transmitted data can be reduced by decreasing the number of transmissions by implementing the following protocol, which is based on the fundamental principle of information theory given by:

$$I_i = P_i log_2(\frac{1}{P_i}) \tag{24}$$

The above equation clearly states that the more the probability of occurrence of an event, the lesser is the information content in it[14]. Thus, the above relation can be used to minimize the number of re-transmissions as the sensed physical parameters do not change their values abruptly. Thus re-transmissions can occur after a certain threshold has been reached given mathematically by:

$if\ (i = k\ \&\&\ c \geq \Delta)$

{

Re-transmit data

}

Else

{

Do not transmit sensed data

}

This would mean, that for a quasi stationary process 'P', the re-transmission occurs only for variations which are significant on the sensed data. This approach has the benefit of reducing the average expenditure of the energy per transmission for the network given by equation (1). This clearly results in reducing the decay in the average energy of the nodes. Another aspect that can hinder the accurate reception of the data at the receiving end is the offset in the timing of the change of frequency hopping depicted by the figure below. Here

C1 is the transmitted frequency

C2 is the received frequency

ϕ is the offset between C1 and C2

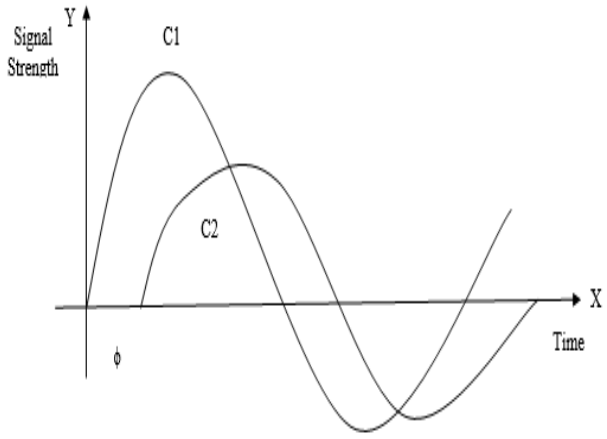

Fig 6: Offset of ϕ between frequencies at transmitting and receiving ends.

The figure above is indicative of the fact that as the offset between the transmitted and received frequency transitions increase, the chances of erroneous transmission also increase.

4. OBTAINED RESULTS

The simulations are run on Matlab 2018a. The results obtained are depicted in the following figures. The network size has been chosen as 100mx100m. The clustering has been shown in the figure below.

It can be seen that the plant area consists of both normal nodes and cluster heads which actually aggregate the data and send it to the cluster head.

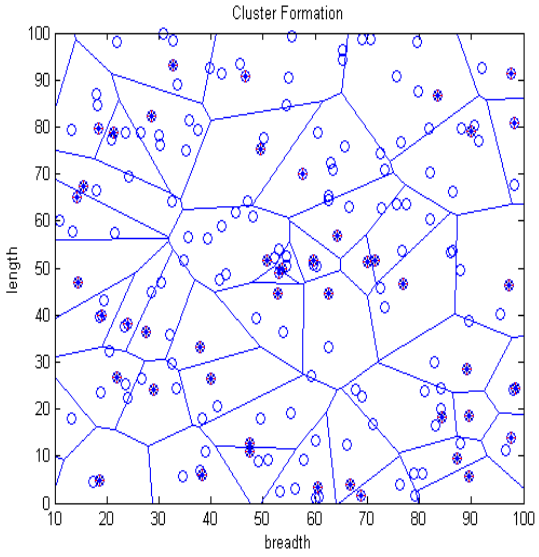

Fig 7: Clustering in the network

The figure below depicts the addition of random noise in the channel. The noise model used here is the Gaussian noise model in which the noise exists with the same power spectral density for all frequency ranges.

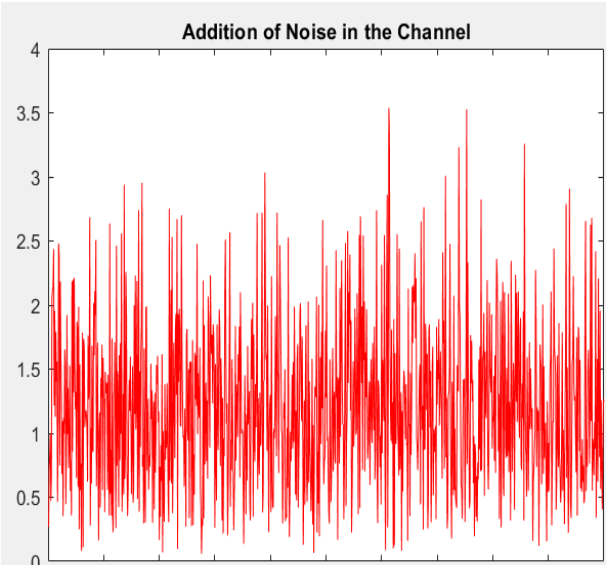

Fig 8: Random noise added in the channel

The figure below depicts the variation of the system outage with respect to the signal to noise ratio (SNR) customarily represented as energy per bit to noise ratio ($\frac{E_b}{N}$)

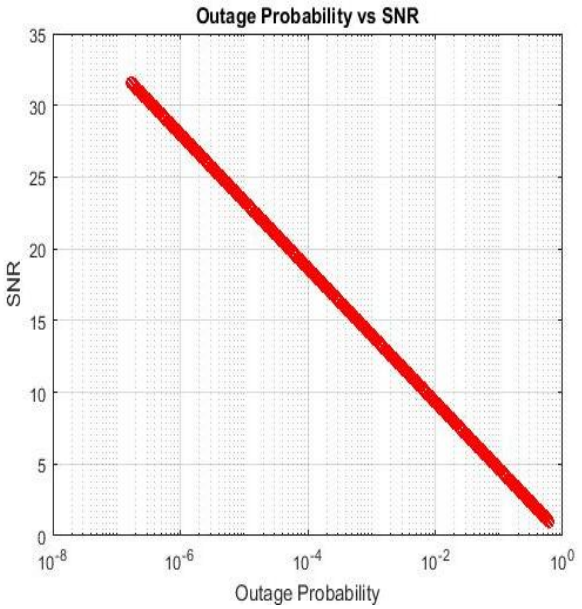

Fig 6: Variation of Outage w.r.t. SNR

The figure below depicts the variation of the system outage w.r.t. the separation between transmitter and receiver. It can be seen that as the distance between the transmitter and the receiver increases, the system outage also increase. This is indicative of the fact that the outage increases with the distance of data transfer. This happens due to the fact that with increasing separation among the transmitter and receiver, the signal strength plummets.

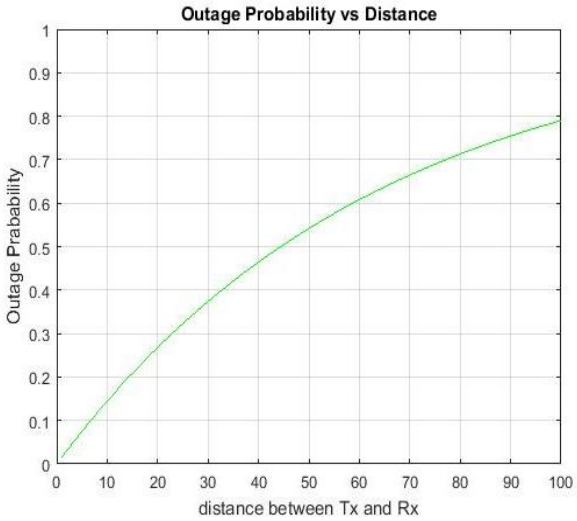

Fig 7: Variation of Outage w.r.t. distance between transmitter and receiver.

The figure below depicts the variation of the probability of error or BER of the system with the increasing values of the spreading factor 'L'. It can be seen that increasing values of L result in increase in the BER.

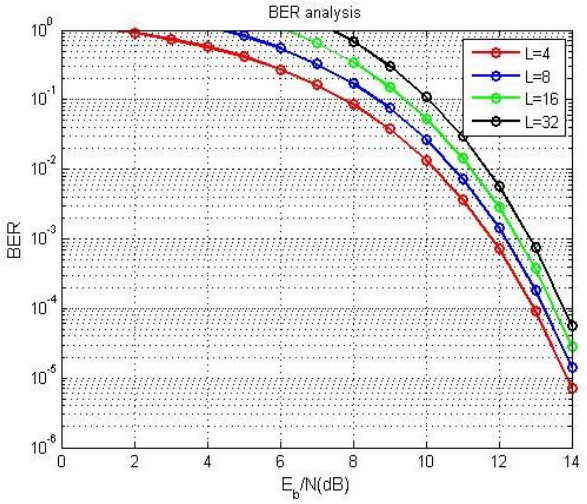

Fig 8: Variation of BER w.r.t. spreading factor L

It can be clearly seen that as the spreading length increase, the BER or P_e of the system also increases clearly indicating the tradeoff between the security and reliability of data transmission of the system.

5. CONCLUSION

The paper presents an approach for employing physical later security for wireless ad-hoc networks and wireless sensor networks using pseudo noise (PN) sequence generation. The technique employed is the fast frequency hopping technique. The mathematical modelling for the technique has been developed for periodic, quasi periodic as well as aperiodic data streams which may be transmitted in WANETs or WSNs. The channel model employed is the Gaussian channel model which considers the existence of noise with same psd smeared over all the frequency ranges of signal transmission. The evaluation parameters considered are the Bit Error Rate (BER) and the system outage. It has been shown that as the spreading factor increases, the security increase since the number of frequency transitions increase. However, the BER also increases as a result of decreasing signal strength and increased chances of frequency change offset. The same can be inferred from the system outage. The outage also increases with the increase in the separation of transmitting and receiving ends.

6. REFERENCES

[1] Mingfend Huan, Anfeng Liu , Neal N. Xiong, V. Tian Wang and Athanasios V. Vasilakos "A Low-Latency Communication Scheme for Mobile Wireless Sensor Control Systems", Vol:49, Issue-2,IEEE 2018.

[2] Y Xu, J Liu, O Takahashi, N Shiratori, "SOQR: Secure optimal QoS routing in wireless ad hoc networks", 2017 IEEE Wireless Communications and Networking Conference (WCNC),

[3] Y Xu, J Liu, Y Shen, X Jiang, "Security/QoS-aware route selection in multi-hop wireless ad hoc networks", 2016 IEEE International Conference on Communications (ICC)", IEEE 2016

[4] A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments, by Xiong Li ; Jianwei Niu Saru Kumari ; Fan Wu ; Arun Kumar Sangaiah ; Kim-Kwang Raymond Choo, Elsevier 2018

[5] Secure Routing Protocols for Wireless Sensor Networks, Reetu Singh ; Kajol Kathuria ; Anil Kumar Sagar , IEEE 2018

[6] WSN Security Mechanisms for CPS, Saqib Ali ; Taiseera Al Balushi ; Zia Nadir ; Omar Khadeer Hussain, Springer 2018

[7] ACO based key management routing mechanism for WSN security and data collection, Celestine Iwendi ; Zhiyong Zhang ; Xin Du, IEEE 2018

[8] Secrecy Outage on Transmit Antenna Selection/Maximal Ratio Combining in MIMO Cognitive Radio Networks, Hui Zhao ; Youyu Tan ; Gaofeng Pan ; Yunfei Chen ; Nan Yang, IEEE 2017

[9] A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols, Ivana Tomić ; Julie A. McCann, IEEE 2017

[10] An overview of Wireless Sensor Networks towards internet of things, Mustafa Kocakulak ; Ismail Butun, IEEE 2017

[11] Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring, Daojing He ; Sammy Chan ; Mohsen Guizani, IEEE 2017

[12] Security in software-defined wireless sensor networks: Threats, challenges and potential solutions ,Sean W. Pritchard ; Gerhard P. Hancke ; Adnan M. Abu-Mahfouz, "", IEEE 2017

[13] A survey of security in wireless sensor networks ;Aditi Rani ; Sanjeet Kumar, IEEE 2017.

[14] "Improving the security of wireless sensor networks in an IoT environmental monitoring system", Mauricio Tellez ; Samy El-Tawab ; Hossain M Heydari, , IEEE 2016.