

# Physical Layer Security in Wireless Sensor Networks (WSNs) with Reduced Outage

Shubham Kumawat<sup>1</sup>; Ravi Khatri<sup>2</sup>

M.Tech Scholar (Cyber Security)<sup>1</sup>, Professor and Head (Computer Science)<sup>2</sup>, VITM Indore<sup>1,2</sup>

s.kumawat9907@gmail.com<sup>1</sup>; k.ravi@vitmindore.com<sup>2</sup>

## ABSTRACT

Wireless sensor networks (WSNs) are widely used for military applications such as navigation and surveillance as well as for industrial automation. Link security is a critical aspect of successful WSN operation. Traditional cryptographic techniques are not suitable for securing WSNs, because they require hardware complexity and consume large amounts of energy that are not affordable in a WSN. 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. Since PLS techniques such as artificial noise generation do not suit WSNs due to their limited energy resources, sensor scheduling has been proposed as a less energy-intensive scheme for WSN security. The issues of privacy and security in wireless communication networks have taken on an increasingly important role as these networks continue to flourish worldwide. Traditionally, security is viewed as an independent feature with little or no relation to the remaining data communication tasks and, therefore, state-of-the-art encryption algorithms are insensitive to the physical nature of the wireless medium. The proposed system uses a PN sequence-based technique to reduce secrecy outage.

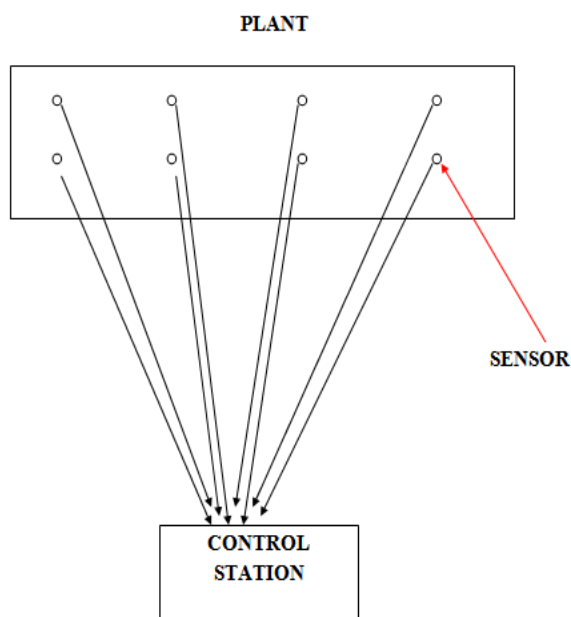
**Keywords:** Wireless Sensor Network, Clustering, Pseudo Random Sequence, Secrecy Outage.

## 1. INTRODUCTION

Several Automation industries rely heavily on wireless sensor networks (WSN) for their functioning. Wireless sensor networks (WSNs) are widely used for military applications such as navigation and surveillance [1] as well as for industrial automation [2]. Link security is a critical aspect of successful WSN operation.

Traditional cryptographic techniques are not suitable for securing WSNs, because they require hardware complexity and consume large amounts of energy that are not affordable in a WSN [1]. 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 [3]. Since PLS techniques such as artificial noise generation do not suit WSNs due to their limited energy resources [3], sensor scheduling has been proposed as a less energy-intensive scheme for WSN security [2]. In recent years, the Weibull distribution has been successfully used to model small-scale fading (SSF) measured in indoor and outdoor scenarios of practical significance, see for example [4], [5] and references therein. In [4], the authors refer to Vehicle to Vehicle channel measurements in the 5 and 10-GHz band; they propose to model the SSF with the Weibull distribution with its shape parameter  $\alpha$  between 1.77 and 3.9 for the 5-GHz band, and in the range 2.02-3.95 for the 10-GHz band. In [5], the authors reported on mobile-to-mobile channel measurements at 1.85 GHz in a dense scattering suburban scenario. They observed that the SSF is accurately modeled by the Weibull with its  $\alpha$  taking values between 1.16 and 1.5; note that decreasing  $\alpha$  values model increasing fading severity. Despite this practical significance of the Weibull fading model, PLS under Weibull fading has not been sufficiently investigated in the literature. Recently in [6], an expression for the average value of the secrecy capacity (SC) under Weibull fading was derived but no practical scheme was proposed to improve the secrecy performance. Moreover, most PLS investigations consider the ideal case that perfect channel state information (CSI) is available for the eavesdropper channel [2], [6]. The submitted work addresses these

limitations by providing a complete characterization of the secrecy outage performance with outdated eavesdropper CSI.



**Fig 1: A typical wireless sensor network configuration**

The figure above depicts the basic configuration for a wireless sensor network where data from the plant is collected by the sensors of the sensor network and transmitted wirelessly to the control station also termed as the sink node.

## 2. RELATED WORK

There have been several approaches in enhancing the security of wireless sensor networks. The following section presents a summary for the same.

In Springer 2019, Jon R. Ward et al. in [1] presented applications the sensor nodes forward their measurements to a central base station (BS). The unique role of the BS makes it a natural target for an adversary's attack. Even if a WSN employs conventional security mechanisms such as encryption and authentication, an adversary may apply traffic analysis techniques to locate the BS. This motivates a significant need for improved BS anonymity to protect the identity, role, and location of the BS. Previous work presented distributed beamforming as a very effective anonymity-boosting technique. However, such work assumed that the adversary is unaware of the countermeasure, and thus the anonymity performance could be unattainable.

In IEEE 2019, Prosanta Gope et al. in [2] showed that security and privacy is one of the major challenges in IWSN as the nodes are connected to Internet and usually located in an unattended environment with minimum human interventions. In IWSN, there is a fundamental requirement for a user to access the real-time information directly from the designated sensor nodes. This task demands to have a user authentication protocol. To satisfy this requirement, this article proposes a lightweight and privacy-preserving mutual user authentication protocol in which only the user with a trusted device has the right to access the IWSN. Therefore, in the proposed scheme, the authors considered the physical layer security of the sensor nodes. The work showed that the proposed scheme ensures security even if a sensor node is captured by an adversary. The proposed protocol uses the lightweight cryptographic primitives, such as one way cryptographic hash function, Physically Unclonable Function (PUF) and bitwise exclusive (XOR) operations. Security and performance analysis shows that the proposed scheme is secure, and is efficient for the resource-constrained sensing devices in IWSN.

In Springer 2019, Tanmoy Maitra et al. in [3] presented an inexpensive resolution of real-world problems such as weather forecasting, measurement of underground water level, traffic monitoring, activity of enemies, animals counting in forest, and so on, wireless sensor networks (WSNs) are widely used. Energy-efficient routing protocol is needed to provide the longevity of network lifetime by reducing power consumption of sensor nodes as well as whole networks. Besides, authenticity of sensor nodes and privacy of sensed data are needed in routing protocol for WSNs to provide secure communications, i.e., sensor-to-sensor as well as sensors-to-base station. The authors showed that clustering technique provides an energy-efficient topology control approach. A minimum connected dominating set (MCDS) can be discovered by applying clustering technique which reduces power consumption in inter-cluster network routing. Cluster head and route selection can be used to provide an energy-efficient outer-cluster routing in WSNs.

In Elsevier 2018, Xiong Li et al. in [4] proposed that the Internet of Things (IoT) is an emerging technology, which makes the remote sensing and control across heterogeneous network a reality, and has good prospects in industrial applications. As an important infrastructure, Wireless Sensor Networks

(WSNs) play a crucial role in industrial IoT. Due to the resource constrained feature of sensor nodes, the design of security and efficiency balanced authentication scheme for WSNs becomes a big challenge in IoT applications. First, a two-factor authentication scheme for WSNs proposed by Jiang et al. is reviewed, and the functional and security flaws of their scheme are analyzed. Then, we proposed a three-factor anonymous authentication scheme for WSNs in Internet of Things environments, where fuzzy commitment scheme is adopted to handle the user's biometric information. Analysis and comparison results show that the proposed scheme keeps computational efficiency, and also achieves more security and functional features. Compared with other related work, the proposed scheme is more suitable for Internet of Things environments.

In IEEE 2017, Xuanxuan Tang et al in [7] presented Secrecy Outage Analysis of Buffer-Aided Cooperative MIMO Relaying Systems. It investigated the secrecy outage performance of buffer-aided multi-relay multiple-input multiple-output (MIMO) cooperative systems in the presence of a passive eavesdropper. Due to the unavailability of the channel state information (CSI) of eavesdropper's channel, a buffer-aided joint transmit antenna and relay selection (JTARS) scheme based on the main channel is proposed to enhance the secrecy performance. Specifically, we model the evolution of the relay buffers as a Markov chain and derive new exact and asymptotic closed-form expressions for the secrecy outage probability, which provides an efficient way to assess the effect of system parameters on the secrecy outage probability

### 3. System Model

Here, we consider a WSN consisting of N sensor nodes transmitting over orthogonal channels to a sink in the presence of an eavesdropper. The main-links experience statistically independent identically distributed flat Weibull fading, whereas the Weibull fading on wire-tap links, between sensors and the eavesdropper, is not necessarily identically distributed. The sink as the supervisory node facilitates communication among different nodes through feedback; hence it is assumed to have CSI for the N sensor channels as well as the eavesdropper channels [7]. To be more specific, each sensor estimates its own CSI and transmits this information to the sink [2] under the assumption of reciprocal channels. The eavesdropper itself is assumed to be a legitimate receiver in the network for some signals and acts as an

eavesdropper for others as in a multicast and unicast scenario, respectively [8], [9]. Under these conditions the eavesdropper's CSI estimated during its legitimate reception may become outdated during its eavesdropping activity.

Consider, the wireless sensor nodes measure a quantity designated by 'x' which is a function of time. Let x be mathematically represented by:

$$x = f(t) \quad (1)$$

Let the optimal value of the parameter to be measured be designated by  $x_{opt}$

If n time steps are needed to reach the optimal value, then there lies a possibility that out of  $t_n$  transmissions,  $t_{n-m}$  transmissions do not reach a value near enough of the optimal value  $x_{opt}$ . Hence it is better to start transmissions only after  $t_{n-m}$  transmissions are over. In such a case the transmissions reduce. The probability of occurrence of an event and the associated information is given by;

$$I_i = \log_2 \frac{1}{P_i} \quad (2)$$

Here,

I represents the information content on the event 'I'  
 $P_i$  represents the probability of occurrence if the event

It can be inferred from equation (2) that as the probability of a parameter value 'x' is near  $x_{opt}$ , the information content in it is less. Hence it is obvious that re-transmission is effective only if the parameter value deviates from the optimal value by at least a magnitude of  $\delta$ .

Thus re-transmission takes place only if the parameter reaches a value:

$$x_{thresh2} = x_{opt} - \delta \quad (3)$$

However, if for some malfunctioning of the network, no re-transmissions take place for a long interval, it is better to have a delay period  $t_{delay}$  which if exceeded, must result in re-transmission of parameter value even if  $x_{thresh2}$  is not exceeded. This adds a sense of reliability to the proposed system.

Devising the frequency shifting mechanism for a signal needs its spectral attributes which need to be changed in case of applying jamming as a protective tool.

Consider a time domain signal  $x(t)$ .

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:

$$x(t) = a_0 + \sum_{n=1}^{\infty} a_n \cos(n\omega_0 t) + b_n \sin(n\omega_0 t) \quad (4)$$

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:

$$a_0 = \frac{1}{T_0} \int_t^{t+T_0} x(t) dt \quad (5)$$

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

$$a_n = \frac{2}{T_0} \int_t^{t+T_0} x(t) \cos(n\omega_0 t) dt \quad (6)$$

$$b_n = \frac{2}{T_0} \int_t^{t+T_0} x(t) \sin(n\omega_0 t) dt \quad (7)$$

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

$$x(t) = C_0 + \sum_{n=1}^{\infty} C_n \cos(n\omega_0 t + \phi_n) \quad (8)$$

Where,

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

And

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

And

$$C_0 = \text{Average value of } x(t) = a_0 \quad (9)$$

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

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

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

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

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

Here,

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

While considering the value of  $x(t)$  extending from

$$t = \frac{-T_0}{2} \text{ to } t = \frac{T_0}{2}$$

Value of  $C_n$

Let  $x(t) = A$  for  $t = -\tau/2$  to  $\tau/2$ .

Hence,

$$C_n = \frac{1}{T_0} \int_{-\tau/2}^{\tau/2} A e^{-j2\pi n t / T_0} dt \quad (14)$$

#### 4. PROPOSED METHODOLOGY

Considering the signal to be any random series of bits (1s and 0s),

the spectrum now becomes continuous in place of the discrete version. Such a continuous version of the signal spectrum is can be given by the frequency spectrum of the Fourier Transform:

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

Equation (15) yields the magnitude spectrum of the signal and we obtain the spectrum of the signal.

If it so happens that the spectrum of the signal hops or jumps apparently randomly, over a frequency range of ( $f_1, f_2, \dots, f_n$ ),

then such a process is called frequency hopping. Frequency hopping: In this case the symbol period is less than the hop period.

$$T_{sym} > T_{hop}$$

Here,

$T_{sym}$  is the symbol period

$T_{hop}$  is the hopping period

The probability of finding error bits in the spreading factor ( $L$ ) with frequency hopping is given by:

$$P_{hop} = \{(L - 1)/L\} e^{-\frac{E_b}{L}} + 1/2L \quad (16)$$

Here,

$P_{hop}$  is the probability of error with hopping

$L$  is the spreading factor

$E_b$  is the energy per bit

A typical illustration of the mechanism to be used is given in the following figure.

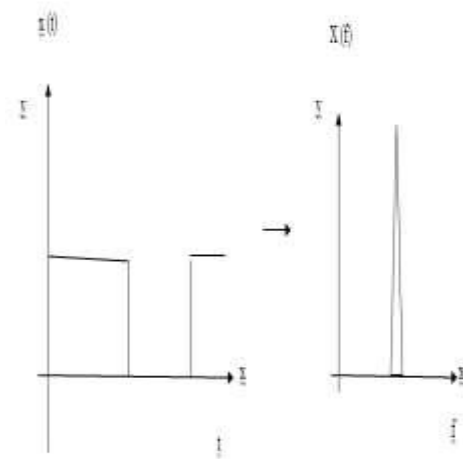
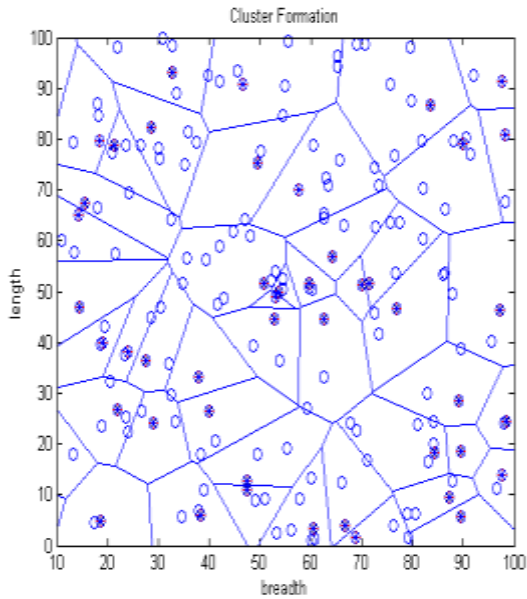


Figure 2 Spectrum Assessment

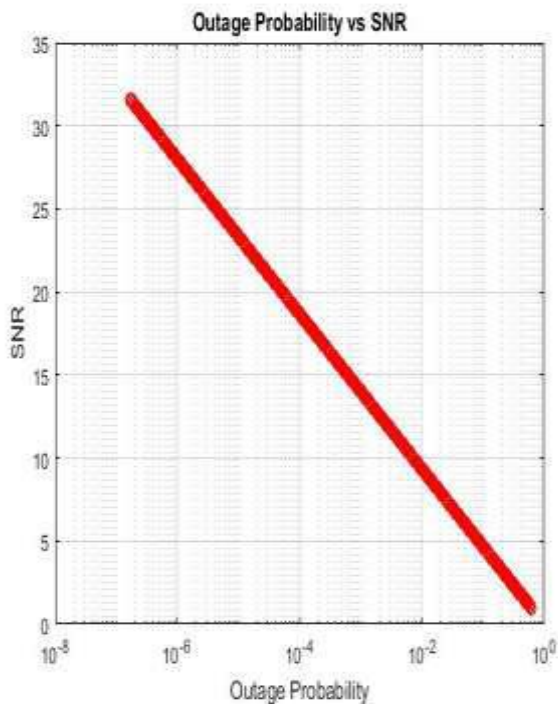
#### 5. RESULTS

The results obtained are for the simulations for the designed system which render insight into the performance of the proposed system in terms of the outage probability, the signal to noise ratio and the simulation of the wireless sensor network in terms of the clustering.



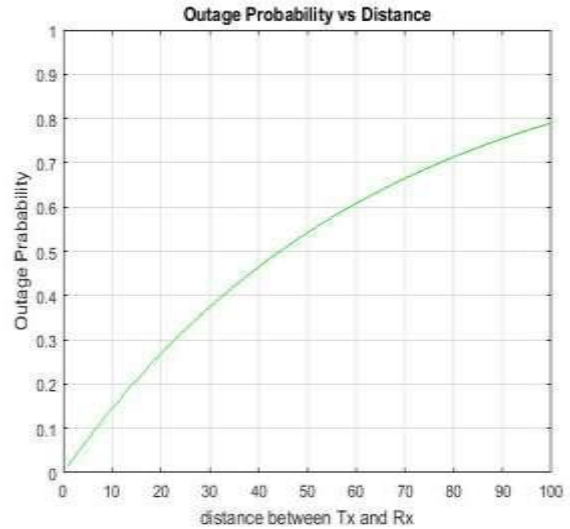
**Figure 3. Formation of Clusters and cluster heads**

The above figure depicts the formation of clusters and cluster heads in the network. The dimensions of the network have been chosen as 100mx100m.



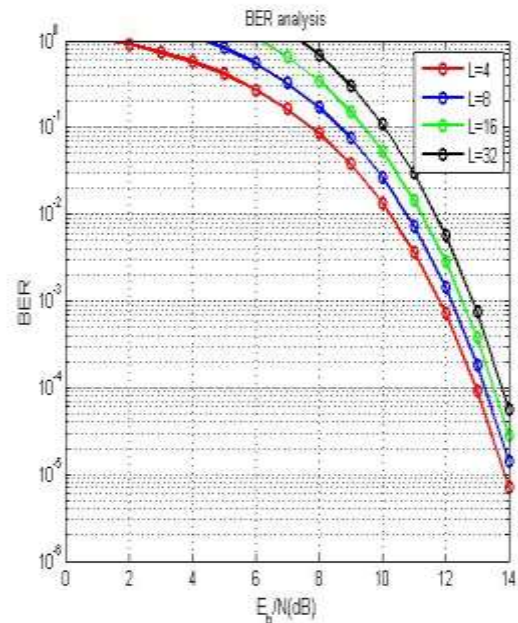
**Fig. 4 Decrease in Outage with Increase in SNR**

The above graph depicts the variation of the signal outage probability with respect to the signal to noise ratio. It can be inferred from the graph, as the SNR of the system increases, the outage decreases.



**Fig. 5. Increase in Outage with Increase in Distance between Tx and Rx**

It can be seen from the above graph that the outage probability also depends on the distance between the transmitting end and the receiving end. The simulation has been run for a distance of 100m which it has been observed that the outage increases with the increase in the distance.



**Fig. 6. BER performance of system**

The figure above represents the variation in the BER of the system as a function of (a) SNR designated by  $E_b/N_0$ . It can be seen that as the SNR increases, the BER decreases. Also as the number of frequencies changed (L) increase, the BER decreases due to the

fact that it becomes difficult for the receiver to recover the data.

## 6. 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 WSN operation. Traditional cryptographic techniques are not suitable for securing WSNs, because they require hardware complexity and consume large amounts of energy that are not affordable in a WSN. 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. Since PLS techniques such as artificial noise generation do not suit WSNs due to their limited energy resources, sensor scheduling has been proposed as a less energy-intensive scheme for WSN security. The performance metrics are outage probability and BER of the system.

## 7. REFERENCES

- [1] Cross-layer traffic analysis countermeasures against adaptive attackers of wireless sensor networks, Jon R. Ward ; Mohamed Younis, Springer 2019
- [2] Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks, Prosanta Gope ; Ashok Kumar Das ; Neeraj Kumar ; Yongqiang Cheng, IEEE 2019
- [3] Cluster-Based Energy-Efficient Secure Routing in Wireless Sensor Networks, Tanmoy Maitra ; Subhabrata Barman ; Debasis Giri ,Springer 2019
- [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.
- [15] "Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach", Yansha Deng ; Lifeng Wang ; Maged ElKashlan ; Arumugam Nallanathan ; Ranjan K. Mallik, Volume 11; Issue 6 ; IEEE 2016
- [16] Secrecy Outage of a Simultaneous Wireless Information and Power Transfer Cognitive Radio System, Ajay Singh ; Manav R. Bhatnagar ; Ranjan K. Mallik, IEEE 2016
- [17] Wireless Network Intrinsic Secrecy Alberto Rabbachin ; Andrea Conti ; Moe Z. IEEE 2015
- [18] Secrecy Performance Analysis for SIMO Simultaneous Wireless Information and Power Transfer Systems, by Gaofeng Pan ; Chaoqing Tang ; Tingting Li ; Yunfei Chen, IEEE 2015
- [19] Secrecy outage analysis of cognitive wireless sensor networks, Satyanarayana Vuppala ; Weigang Liu ; Tharmalingam Ratnarajah IEEE 2014
- [20] Physical Layer Security in Downlink Multi-Antenna Cellular Networks, Giovanni Geraci ; Harpreet S. Dhillon ; Jeffrey G. Andrews ; Jinhong Yuan ; Iain B. Collings, IEEE 2014
- [21] Challenges and research opportunities in wireless communication networks for smart grid Quang-Dung Ho ; Yue Gao ; Tho Le-Ngoc, IEEE 2013
- [22] Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks, Yulong Zou ; Xianbin Wang ; Weiming Shen, IEEE 2013

[23] Wireless sensor network: Security challenges, Asmae Blilat ; Anas Bouayad ; Nour El Houda Chaoui ; Mohammed El Ghazi IEEE 2012

[24] Secret Key Cryptography based Security Approach for Wireless Sensor Networks, V. Thirupathy Kesavan ; S. Radhakrishnan IEEE 2012

[25] A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks ,S Ehsan, B Hamdaoui, , Volume-14, Issue-2, IEEE 2012

[26] An energy-efficient routing protocol for UWSNs using physical distance and residual energy,A Wahid, S Lee, D Kim., OCEANS, IEEE 2011.

[27] Hierarchical adaptive balanced energy efficient routing protocol (HABRP) for heterogeneous wireless sensor networks, Said Ben Alla, Abdellah Ezzati , Abderrahim Beni Hssane, Moulay Lahcen Hasnaoui, , IEEE 2011.

[28] Energy efficient and QoS based routing protocol for wireless sensor networks ,J Ben-Othman, B Yahya, Elsevier 2010.

[29] Data security and privacy in wireless body area networks,Ming Li ; Wenjing Lou ; Kui Ren, , Volume 17; Issue 1, IEEE 2010.

[30] , “Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey”David Martins ; Herve Guyennet, IEEE 2010.

**ijournals**