iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Communication in Physical Layer through Cooperative Relay Networks

Ponselvi S [1], Dr. V. Seethalakshmi [2]

[1]PG Scholar, [2] Assistant Professor (SG), Department of ECE
Dr. Mahalingam College of Engineering and Technology

Abstract: ***Nowadays, increasing number of wireless users because of the mobility and comfort in the wireless communication leads to security issues. For security of wireless systems, cryptography techniques, which are higher layer security techniques, are preferred in many systems. But with the invention of ad-hoc networks and decentralized networks, the higher layer security techniques are difficult to implement. In order to reduce the burden of the higher layers of the network, the security by exploiting the characteristics of the physical layer has been implemented. Cooperative relay networks improve the reliability of the network. Amplify and Forward (AF) is the scheme of cooperative relay networks, which is simulated and the performance of this system is improved when compared to the systems which are not employing the cooperative communication. AF protocol is preferred since it is the one which does not involves any decoding operations at the relay, makes the transmission characteristics to be simple.***
Keywords: Physical Layer Security, Cryptographic Algorithms, Cooperative Relay Networks, Amplify and Forward Scheme, SNR

I. INTRODUCTION

Wireless Communications and its inventions play a vital role in the day to day life of human beings [1]. By having the benefits like ease of installation & maintenance, flexibility and mobility, it is preferable by everyone. Beyond these advantages, because of the broadcast nature of the wireless medium, it has the disadvantages in terms of security. Security is a main concern in wireless systems. Confidentiality and Authentication are the basic security requirements of the wireless systems [2]. The techniques to ensure the secure transmission in the communication becomes the greatest issue [3].

The problem of secure transmission in the presence of eavesdropper was first studied by Wyner in [5] is the first stone in the physical layer security. He implemented memory less wiretap channel and showed that secure transmission is possible without the secret key, if eavesdropper's channel is the degraded version of the legitimate channel.

On the other hand the mostly implemented security schemes rely on the upper layers. The cryptographic security was considered to be the most efficient security technique because of the larger key size. Longer the key size, Larger the security is. But it is identified that [6] emerging of the computationally efficient computer systems leads to the greater issue. In order to overcome from this issue, the security method based on information – theoretic perspective, which doesn't assume anything on the system parameter, Physical Layer Security is implemented. Cooperative relaying is an effective method of increasing the reliability and range in the wireless networks. In [1], cooperative communication is proposed for the method to be used in the Physical layer Security techniques. The [7] investigates the physical layer security for the cooperative broadcast networks.

Cooperative Communication enables single-antenna systems to share their antennas in order to create a virtual multiple antenna transmitter to achieve transmit diversity in a Multi-user environment [8]. It is a technique where three or more active users in a common wireless network, share their resources to jointly transmit messages while showing the improvement in the performance of the system through their inherent spatial diversity. In simple, it creates a virtual MIMO system [9].

The cooperative communication has many forwarding schemes which include Amplify and Forward (AF), Decode and Forward (DF), Quantize and Forward (QF) [10]. These schemes will be implemented at the relays. This paper investigates the cooperative techniques such as relay, multi cell coordination, Group cell and CoMP.

In [11] it is shown that with the emerging technologies in the computers, Brute-force attack leads to the questionable situation in terms of security. [12] Discusses the Symbol Error Rate performance analysis of uncoded cooperative communication networks.

II. COOPERATIVE COMMUNICATION

A cooperative system with three nodes which include Source, Destination and an intermediate node which is called as Relay has

been implemented. It applies the concept of space diversity and time diversity. The strategies in the relay transmission can be of many types which includes the following:
Amplify and Forward (AF)
Decode and Forward (DF)
Quantize and Forward (QF)

A. AF Relay Transmission

It just amplifies the incoming signal with an amplification factor. It will not decode or demodulate the received signal at the relay. It also amplifies the noise with the amplification of the signal. It is the simplest scheme since it does not require any additional circuitries for decoding and quantization. This scheme is most preferable since it reduces the work load of the relays.

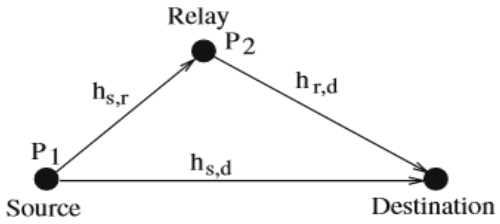


Fig 1: Simple Cooperative Relay Communication

B. DF Relay Transmission

Decode and Forward (DF) relay is quite accurate technique since it involves the decoding and re encoding process at the relay. But in terms of complexity and implementation it has a disadvantage.
Where the accuracy is of concern without considering the complexity, DF relay scheme is preferable.

C. QF Relay Transmission

Quantize and Forward (QF) relay has the moderate performance when compared to AF and DF Cooperative schemes. It can also be called as Compress and Forward (CF) relay.
In this scheme, the relay has only a little work since it will not fully decode the signal, but it just compress the signal using some quantization levels. Its performance also moderate between AF and DF relays.

III. PHYSICAL LAYER SECURITY

Wireless security is of a major concern nowadays because of the increasing users and demands of the wireless communication. As of today the security depends on higher layer security techniques called Cryptography Mechanism.
But now an emerging technique which uses only the physical layer properties to provide the security is identified. It is called Physical Layer Security.

A. Traditional Security Technique

In general, the wireless networks will be having seven layers approach. From the emergence of wireless systems, the security was depending on the higher layer. It is called as Cryptography. In cryptography the major process is Encryption and Decryption. It is of two major types
Asymmetric Key Cryptography
Symmetric Key Cryptography
In the former method, different keys will be used for encryption and decryption. In the latter, same key will be used for both the processes. Here, the security level depends on the size of the key used. Larger key size will give the greater security. It has a trade off with the complexity. But nowadays with the emergence of higher performance computers, the hackers can crack the security of the system by employing the Brute-Force attack.

B. Physical Layer Security Technique

To overcome this shortcoming of the higher layer security and to reduce the burden of the higher layer by employing the security measures at the bottom most layers called physical layer.
This will be achieved by utilizing the physical layer properties including channel, noise, fading. Physical layer security can be implemented by using the techniques like Cooperative Communication, Diversity, Artificial Noise, Beam forming, Polar codes,

Game Theory and few more techniques are available.

IV. RELATED WORK

L.J. Rodriguez [1] states the linkage of the physical layer security with the cooperative communication. It states that the cooperative relaying is the efficient method to achieve the reliability and longer coverage. Relay forwarding techniques has been discussed for both trusted and untrusted relays. In assistance to Relaying both Jamming and hybrid Jamming / Relaying strategies can be employed in this cooperative relay networks.

Yiliang Liu [2] describes the physical layer security which satisfies the two basic factors of the secret communication. With this, the extra security will not be needed in the upper layers. In this various types of attacks available in the wireless networks and the remedy techniques which are available already also discussed. Challenges associated with the wiretap coding design and technologies have been explained. As a summary, the existing and future challenges and techniques have been presented.

Yi S. Shiu [6] gives the effect of the primary attacks like Eavesdropping and Jamming. And also the security techniques to improve the performance of the system even with the environment of eavesdroppers or jammers. The security requirements and also the physical layer security approaches to meet those security requirements. The approaches like theoretical channel capacity, channel, code, power and signal design approaches and the techniques available with them were discussed.

H Mahdavifar [13] depicted the secrecy capacity of the wiretap channels using Polar codes. Polar codes which are invented by Arkan, provides strong security with low encoding and decoding complexity. The channel considered here is Binary – Input Symmetric Memory less (BSM) discrete channel. Here the assumption made is, the wiretap channel is degraded when compared to the main channel.

Zhiguo Ding [14] examined the wireless security for the bidirectional communication resources. With that of the Relaying, the cooperative Jamming can also be preferred for the improvement of Secrecy Capacity. The outage probability and the achievable rates are depicted against the number of single and multiple antenna relays. The outage probability decreases to zero with the increase in the number of relays.

Wanyang Xiao [15] presented the study on physical layer security with the Game Theory. This paper analyzes the already available security problems and also the methods to overcome those problems. It also shows the tradeoff of the complex techniques with the performance and complexity of the system. The methods like Artificial Noise and Beam forming are giving the higher secrecy rate but with the very complex system. Whereas, the Game theory assumes the scenario as a Game and proceeds toward the performance compared to the complex techniques.

Liang Chen [7] analyzed two cooperative schemes named Decode and Forward (DF) and Compress and Forward (CF) for Broadcast networks. The former one is preferred when both the channels are good, but the latter will be preferable though one of its channels is of lower secrecy clearance.

Song Wenbo [3] presented the performance of amplify and forward (AF) and Cooperative Jamming (CJ). The Three – Node wiretap and Collaborative communication wiretap channels had been established and analyzed. It results that secrecy capacity of the AF is superior to the CJ in terms of various simulation parameters.

The authors in [9],[10] reviewed the cooperative routing for Mesh, Adhoc and Wireless sensor networks. They proved that the cooperative communication yields better performance than the non – cooperative one. In addition to the relay techniques, Distributed Antennas System (DAS), Multi cell Coordination, Group Cell and CoMP are also the techniques in the cooperative communication.

V. SYSTEM MODEL

A three node relay network comprises of Source, Destination and a Relay has been designed. The transmitter power is divided and given to the source and the relay. The AWGN channel is modeled for the transmission of the information.

Since it is the AWGN channel, the channel coefficients and the channel gains can be calculated in a random manner. Initially the system with only direct communication has been designed and then it is compared with the other Cooperative relay techniques.

The signal received at the relay from the source is given as

$$R_{s,r} = X_s \, . \, h_{s,r} + n_{s,r}$$

Where,

X_s - the information signal

$h_{s,r}$ - Channel between source and relay

$n_{s,r}$ - Noise added in the above channel

The signal received at the destination from the relay and the source is formulated as

$$D_{r,d} = \beta . R_{s,r} . h_{r,d} + n_{r,d}$$

$$D_{s,d} = X_s . h_{s,d} + n_{s,d}$$

Where the former is the data received from the relay and the latter is the data received directly from the source. β is the amplification factor which will be designed from the transmitter power, channel and the noise associated with it. It will be given by

$$\beta = \sqrt{\frac{P_R}{h_{SR^2} \; E_S + 1}}$$

This is the amplification factor of the system which will be multiplied with the signal received at the relay. Then at the destination the signals from the relay and directly from the source are combined together using maximal ratio combining.
Then the Signal to Noise Ratio (SNR) and the Symbol Error Rate (SER) are depicted for the systems with and without cooperative relay forwarding techniques.

VI. RESULTS AND DISCUSSION

A wireless network with the following simulation parameters is designed and simulated using MATLAB.

TABLE I
SIMULATION PARAMETERS

Parameters	Specification
Channel used	AWGN
No. of nodes	3
Transmitter Power	Pt = 1/2
Relay Power	Pr = 1/2
Signal to Noise Ratio	0 - 40
No. of symbols to be transmitted	10^3
Modulation Used	QPSK

The symbols to be transmitted are initially modulated using Quadrature Phase Shift Keying (QPSK) modulation. The respective channels between source and destination, source and relay, relay and destination has been established.

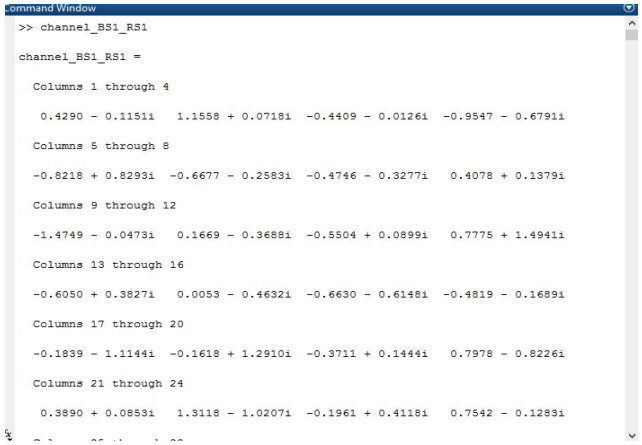


Fig 2 : Channel coefficients for the Channel1

The channel coefficients shown in the above figure are generated using the 'randn' function in MATLAB for all the symbols that are transmitted.

The below figure gives the channel gains for all three channels. And the AWGN noise can also be added with all the symbols that are transmitted. The amplification factor is generated using the expression given before. It involves the channel gain a11 and also the transmitter power. It is about 1.1304. Then it is multiplied with the data that is received at the relay from the source. At the receiver, the signals are combined using the Maximal Ratio Combining (MRC).

```
>> a11
a11 =
    0.8845
>> b11
b11 =
    0.8757
>> c11
c11 =
    0.8713
>>
```

Fig 3: Channel gains

The below figure shows the comparison of SNR performance against the BER (Bit Error Rate) of the Amplify and Forward (AF) system and the system without employing the AF forwarding technique. It shows that the AF relay outperforms the No-Relay network. It has better immunity to noise than the No-Relay network.

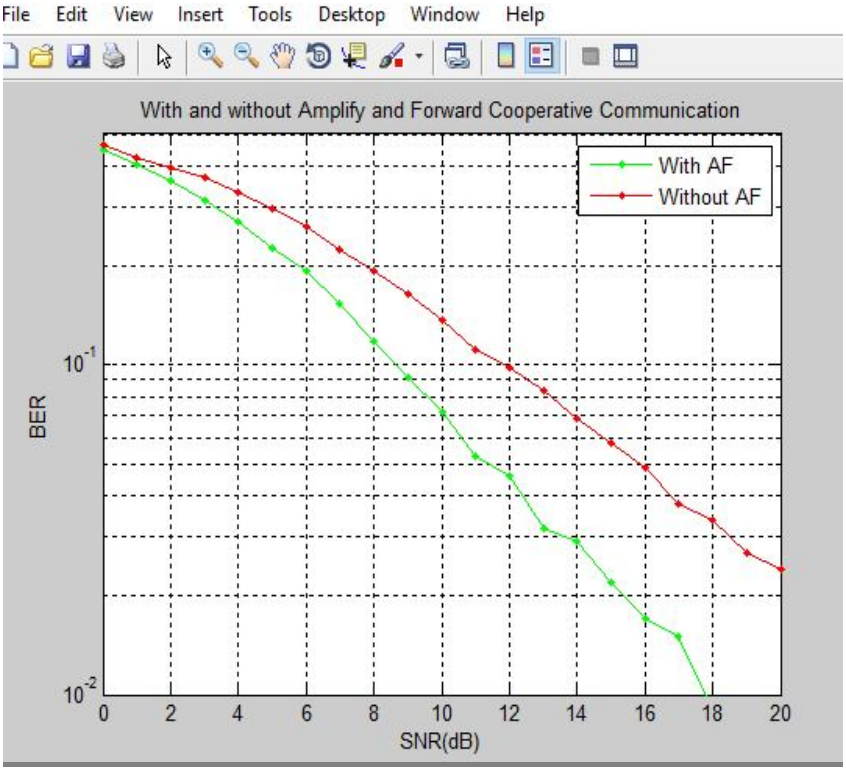


Fig 4: BER Vs SNR for a System with AF and without AF

The SNR performance of the system is directly proportional to the system power and inversely proportional to the noise power in the signal. It degrades with respect to the increase in the Noise power. The figure below depicts the relation between the noise power and the SNR.

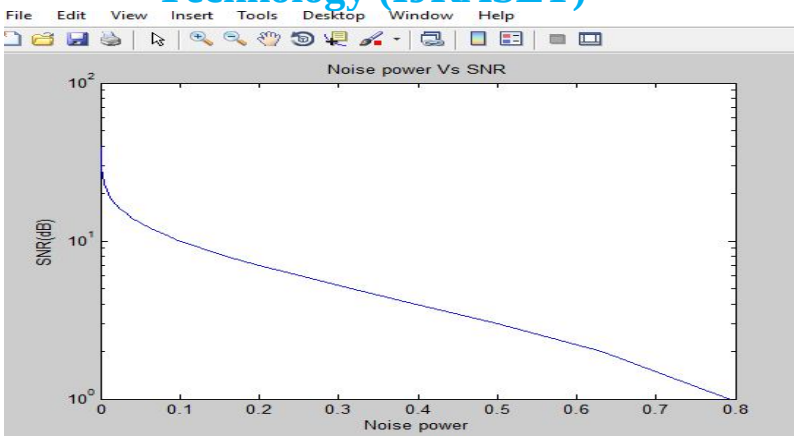


Fig 5: SNR performance under various noise powers

It shows that when the noise power is at 0.1, the SNR is high, whereas the SNR is of low value at high noise power 0.8.

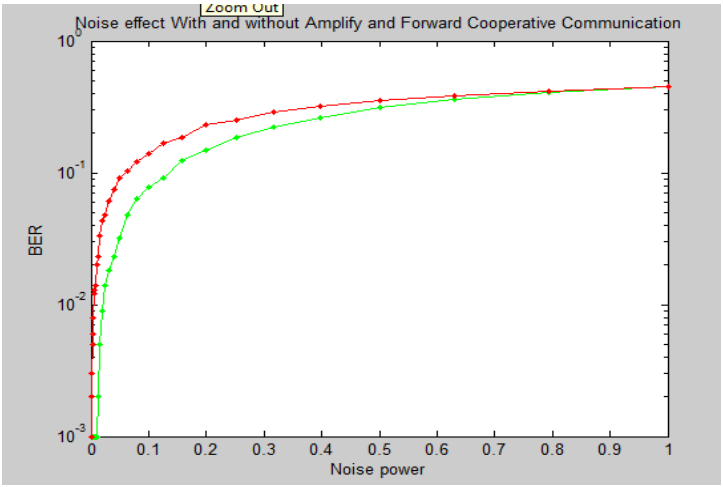


Fig 6: BER performance curve with Noise Power

The above graph depicts the comparison of the systems with and without employing the AF relay forwarding technique with the parameter BER against the noise power. Here it shows that the AF relay technique outperforms the system which is not having the AF relay forwarding technique.

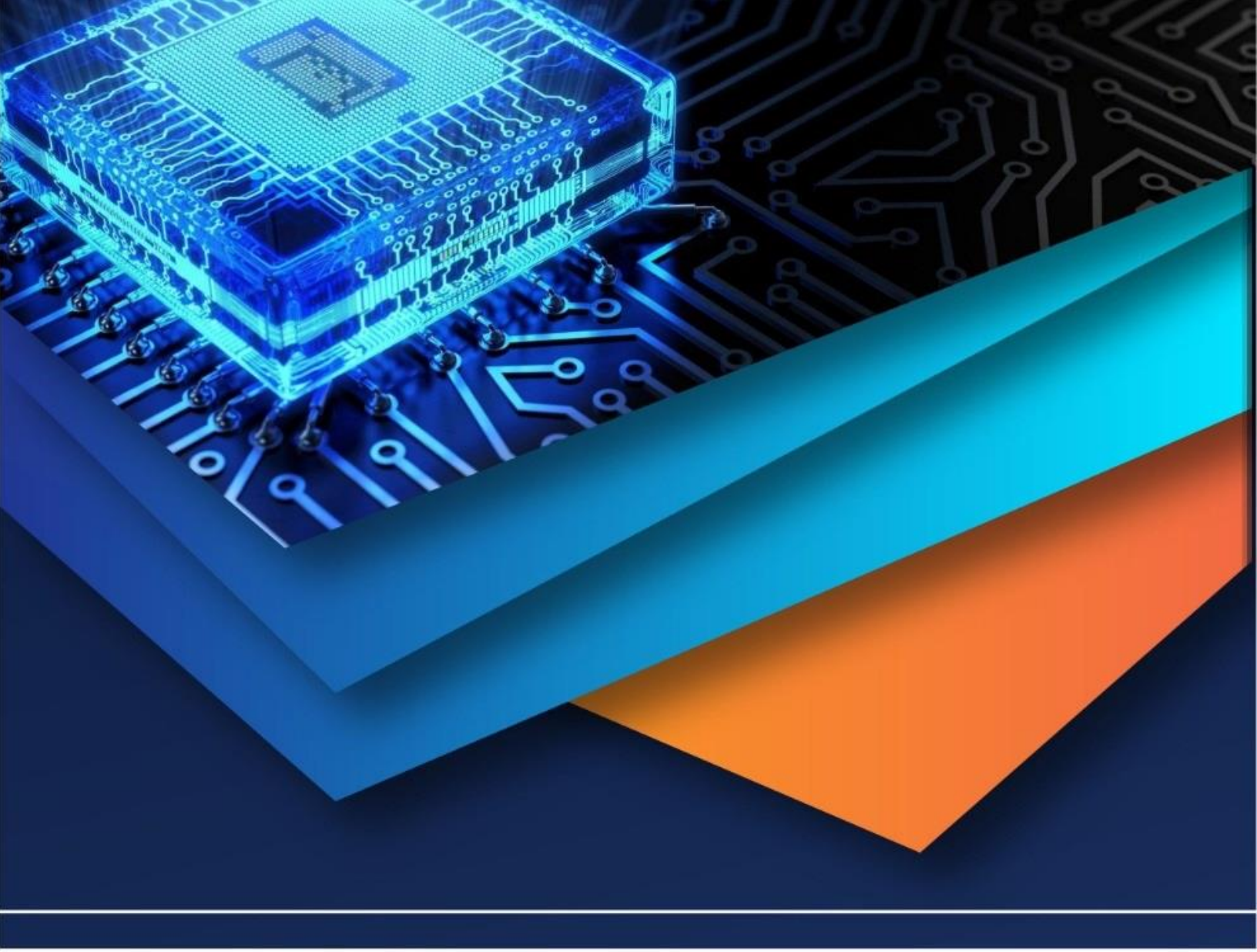
VII. CONCLUSION

From the above discussions it is evident that the relay network improves the total performance of the system. Even in the noisy environment, the Amplify and Forward relay (AF) outperforms the system which is not having the relay network with it. This scenario is simulated for various amplification factors. Increase in the amplification factor leads to better performance. But while the signal amplification takes place, noise is also getting amplified. It is the simplest method of cooperative relay forwarding technique, since it didn't involve in the relay processing. The performance of the AF Relay system can be compared with that of the other forwarding techniques. And it can be employed with many existence techniques to improve their performance.

REFERENCES

[1] L.J. Rodriguez, N. H. Tran, T.Q. Duong, Tho Le-Ngoc, M. Elkashlan, Sachin Shetty, "Physical Layer Security in Wireless Cooperative Relay Networks: State of the Art and Beyond," IEEE Communications Magazine, Vol 15, pp. 0163-6804, December 2015
[2] Yiliang Liu, Hsiao-Hwa Chen and Liangmin Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," IEEE Communications Surveys & Tutorials, 2016
[3] Song Wenbo, "Research on Physical Layer Security Schemes based on Cooperative Wireless Communication," Seventh International Conference on Measuring Technology and Mechatronics Automation © 2015 IEEE

[4] Mukherjee, S. Ali A. Fakoorian, Jing Huang and A. Lee Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," IEEE Conference, January 2014.
[5] Wyner "The wire-tap channel," Bell. Syst Tech. J, vol.54, no.8, pp.1355-1387, Jan 1975
[6] Yi S. Shiu, S. U. Chang, H. C. Wu, Scott C.-H. Huang, H. H. Chen, "Physical Layer Security in wireless Networks : A Tutorial", IEEE Wireless Communications, Vol 11, pp. 1536 – 1284, April 2011
[7] Liang Chen, "Physical Layer Security for Cooperative Relaying in Broadcast Networks," The Military Communications Conference - Track 1 - Waveforms and Signal Processing, 2011
[8] Aria Nosratinia, Todd E. Hunter, Ahmadreza Hedayat, "Cooperative Communication in Wireless Networks," IEEE Communications Magazine, Oct 2004
[9] F. M. Shahen Shah, Md. Shariful Islam, "A Survey on Cooperative Communication in Wireless Networks," vol 07, pp 66-78, I.J. Intelligent Systems and Applications, 2014
[10] Xiaofeng Tao, Xiaodong Xu, Qimei Cui, "An Overview of Cooperative Communications," IEEE Communications Magazine, June 2012
[11] Yulong Zou, Jia Zhu, Xianbin Wang, Victor C.M. Leung, "Improving Physical-Layer Security in Wireless Communications Using Diversity Techniques," IEEE Network, February 2015
[12] Weifeng Su, Ahmed K. Sadek, K. J. Ray Liu, "Cooperative Communication Protocols in Wireless Networks: Performance Analysis and Optimum Power Allocation," Wireless Personal Communication, © Springer Science + Business Media LLC 2007
[13] H Mahdavifar, Alexander Vardy "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes," arXiv:1007. 3568v2, September 25, 2011
[14] Zhiguo Ding, Member, Mai Xu, Jianhua Lu, and Fei Liu, "Improving Wireless Security for Bidirectional Communication Scenarios," IEEE Transactions on Vehicular Technology, Vol. 61, No. 6, July2012
[15] Wanyang Xiao, Kaizhi Huang, Xingguo Luo, and Ying Hong, "Study on Physical Layer Security with Game Theory," IEEE Transactions, pp – 697- 700, Vol 13, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY