IJETST- Vol.||02||Issue||06||Pages 2710-2716||June||ISSN 2348-9480 2015

Open access Journal International Journal of Emerging Trends in Science and Technology

A Robust Low Power Security System for Multi-Node Communication

Authors
Lazeena V P[1], Prasanth M[2]
[1]M. Tech, Applied Electronics and Communication System, NCERC,Pampady
Email: *lazeenahussain@gmail.com*
[2]Assistant Professor, ECE Department, NCERC, Pampady
Email: *prasanthlmc@gmail.com*

Abstract
Wireless sensor network (WSN) is a collection of sensors organized into a cooperative network. The sensors are monitor the physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. Security and energy consumption are considered to be long-lasting technical challenges in WSNs. In order to avoid this security and energy consumption problem, channel aware encryption and decision fusion is to provide a secure transmission from sensors to the Ally Fusion Center (AFC) without using any traditional cryptographic techniques. Consider a passive eavesdropping where an Enemy Fusion Center (EFC) located in a vicinity of an AFC tries to eavesdrop on wireless communication between sensors and AFC. Two groups of sensors are activated and send their data in different ways by a random exploiting channel gain over parallel access channel to the AFC.AFC properly detect the target while the EFC is totally ignorant it. The performance evaluation show that detection performance at the AFC exponentially decays with growing the number of sensors. Clustering technique provides an effective way to overcome these problems. Clustering technique can partition the nodes into clusters and select the cluster head (CH) among the nodes and Non Cluster Head (NCH) nodes. The CH receive the data from other nodes then sent to a sink to accomplish a specific goal.CH remain closer to their follower sensor nodes compared to the sink. It take less energy to transmit data to the cluster head instead of the sink, which allows the sensor nodes to conserve more energy and live longer in WSN, also provide a secure communication from nodes to the main station.

Keywords— *Wireless sensor networks (WSN), decision fusion, perfect secrecy, sensor nodes, clustering.*

I. INTRODUCTION

A wireless sensor network (WSN) is a collection of nodes organized into a cooperative network and it become an important research area in the field of computers and electronics in the last decade.WSN is composed of a large number of spatially distributed sensor nodes which are cheap, low power, limited in memory, energy constrained due to their small size. These sensor node work together to monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. There are three main functions of a sensor node-sensing, processing and communication. They have wide-ranging applications such as military, environment monitoring agriculture, home automation, smart transportation, and health. Before wireless sensor networks became popular, the wired sensor networks were being used for the same purpose but due to high cost of installation, termination, maintenance, up gradation and infeasibility of wired sensor networks in hostile and remote locations, wireless sensor networks became a good alternative.

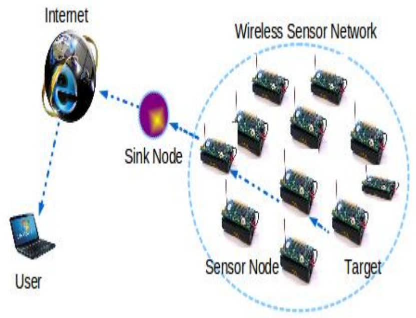

Fig 1.1: Schematics diagram of WSN

In wireless sensor networks (WSNs), security and energy consumption have been considered as long-lasting technical challenges as sensors usually suffer from complexity and energy constraints. The existing method provide a simple and efficient physical-layer security to provide data confidentiality in a distributed detection scenario without using any cryptographic techniques. To resolve the technical challenge of secure communications in WSNs, there have been several notable approaches, where the ability of the physical layer is explored as a solution to the data confidentiality for the distributed detection in WSNs. Assuming the presence of a passive eavesdropper called an enemy fusion center (EFC), sensors in a WSN individually or collaboratively transmit their local decisions on a target state to an ally fusion center (AFC), where final decision is made. But the performance evaluations show that detection performance at the AFC exponentially decays with growing the number of sensors so it take some time delay for the data transmission over the whole network. Energy consumption and relatively high niose level are the major drawbacks of this method. Clustering technique provides an effective way to overcome the problems related to existing method. Clustering in one of the widely accepted techniques, it is also used in wireless adhoc networks, mobile adhoc networks along with sensor networks. Clustering is a technique in which sensor nodes are grouped into some clusters. Only one sensor node is solely responsible to communicate to the base station in a cluster. This sensor node is called cluster head and the remaining sensor nodes in the cluster are called followers. The followers collect data and send it to their corresponding cluster heads. The cluster heads aggregate its own data with the data received from its followers. Aggregated data is then sent to a sink to accomplish a specific goal. Cluster heads remain closer to their follower sensor nodes compared to the sink. It takes less energy to transmit data to the cluster head instead of the sink, which allows the sensor nodes to conserve more energy and live longer in WSN. Security has been achieved by isolating the malicious nodes using sink based routing pattern analysis. Clustering method attempt to improve the network stability period, it can serve as a better platform for upper layer functionality such as broadcasting, aggregation etc.

II. EXISTING SYSTEM

Existing methods on using in WSNs can be grouped into two categories: 1) Perfect secrecy and 2) fusion rule. Distributed detection is a common process for decision making on physical phenomena in wireless sensor networks. A set of sensors is generally deployed for gathering information from a hostile area or placements where human intervention is impossible. Each sensor measures physical phenomena and makes a local decision based on its measurement that is transmitted to a fusion center (FC) where a final decision is made. The problem in the distributed detection is that eavesdropping on transmitting data can be easily accomplished by adversaries**.** In this paper, we explore a new integrated design for distributed detection that takes into account security issues at a physical layer, and thereby ensures confidentiality of transmitting data from sensors. The advantage of this integration is that security is achieved by using existing transmission techniques at the physical layer without any cryptographic algorithms..

1. PERFECT SECRECY

First the AFC broadcasts a pilot signal to initiate distributed detection, and each sensor measures the strength of the received pilot signal. If the pilot signal synchronization occur then each sensor autonomously joins one of three groups, dormant, flipping, and nonflipping groups, based on the AFC broadcasts the pilot signal. The sensors in the flipping and nonflipping groups are called activated sensors, and they report their local decisions over a PAC in the time-division duplexing (TDD) manner to the AFC. The main idea behind that the sensors in the flipping and nonflipping groups send their local decisions to the AFC in the completely opposite ways from each other to make the EFC confused. For example, when two activated sensors involved in the two different groups, i.e., flipping and nonflipping groups, make the same local decision on the target state, the transmitted data from the sensor in one group becomes a bit-flipping version of the other's. Meanwhile, at the AFC and EFC, the transmitting data from activated sensors in different groups should be fused in an appropriate way to make a final decision on the target state. AFC detect the target properly meanwhile the EFC totally confused and fail to detect the target properly.

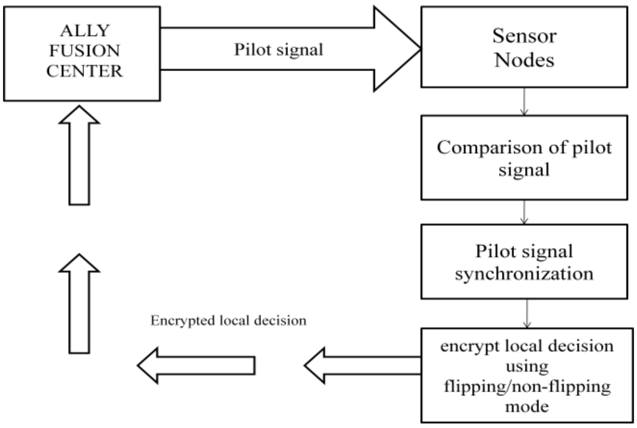
ALLY FUSION CENTER
Pilot signal
Sensor Nodes
Comparison of pilot signal
Pilot signal synchronization
Encrypted local decision
encrypt local decision using flipping/non-flipping mode

Fig 2.1: Flow diagram

2. FUSION RULE

The AFC and EFC, the transmitting data from activated sensors in different groups should be fused in an appropriate way to make a final decision on the target state. Since the activated sensors report their data in the TDD manner, the received signal strengths at the AFC provide estimates of the channel condition of each sensors, and thus the AFC can incorporate such estimates into the fusion. On the other hand, the EFC eavesdrops the signals from the sensors over a statistically independent PAC, and is totally ignorant of the channel condition. In this way AFC detect the target properly based on the Log Likelihood Ratio (LLR) fusion rule meanwhile the unauthorized fusion center EFC totally confused and fail to detect the target properly.Then, the LLR is denoted by

Li = log Ai

Each sensor transmits a quantized version of its local LLR, denoted by u_i, to the AFC over the channel. Consider a binary decision from Li as $u_{i.}$ If u_i = 1 then decision made otherwise the decision not considered.

III. PROBLEM FORMULATION

It provide a simple and efficient physical-layer security to provide data confidentiality in a distributed detection scenario without using any cryptographic techniques. To resolve the technical challenge of secure communications in WSNs, there have been several notable approaches, where the ability of the physical layer is explored as a solution to the data confidentiality for the distributed detection in WSNs. Assuming the presence of a passive eavesdropper called an enemy fusion center (EFC), sensors in a WSN individually or collaboratively transmit their local decisions on a target state to an ally fusion center (AFC), where final decision is made. But the performance evaluations show that detection performance at the AFC exponentially decays with growing the number of sensors so it take some time delay for the data transmission over the whole network. Energy consumption and relatively high niose level are the major drawbacks of this method.

IV. MODEL OF CLUSTERING MECHANISM

Clustering in one of the widely accepted technique to improve network lifetime in WSN and also used in wireless ad hoc network, mobile ad hoc network along with sensor networks Clustering is a technique in which the sensor nodes are grouped in to some clusters. In a cluster, only one sensor node is communicate to the base station and this node is called cluster head and remaining sensor node is called followers. The followers collect data and send it to their corresponding cluster heads. The cluster heads combines its own data with the data accepted from its followers. These combined data is directly sent to the base station. Cluster head is closer to the base station compared with followers so it take less energy for data transmission , which allows the sensor nodes to conserve more energy and live longer in WSN.

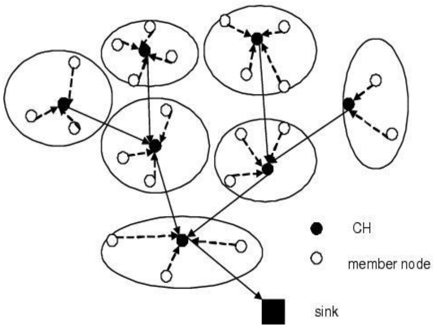

Fig 4.1 : Clustering technique

Initially, the base station send a request message to every nodes in the network. When the nodes have received the request message, based on the number of nodes and its sensing range they form different clusters. Every cluster group can select its own cluster head which located near to the base stations and other nodes act as followers. Followers send their data to its cluster head then cluster head combine all the data to a single data which send to the base station directly. In some cases, some nodes in a cluster located at the edge of the network or beyond the radio range which leads to the tradeoff among the connectivity, energy storage, and communication latency. In this case we select a node which excluded from the cluster is called Non Cluster Head (NCH). Then the sensor node and CH communicate by using this NCH. If any of the node is attacked by an attacker, the base station analyze the routing pattern then the attacked node is isolated from the network or BS change the data transmission path. In this way this method provide a secure data transmission from nodes to BS without using any cryptographic techniques.

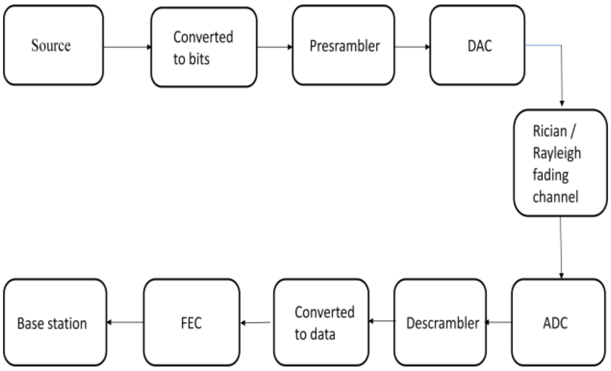

Fig 4.2: The block diagram of the system

The input source generate the input bits, the prescrambler generate the bits into frames which include data, pilot signals and checksum bits. Each frames converted in to analog form then send to the channel. In this system all performance parameters are evaluated both Rician and Rayleigh channel. At the receiver side, the descrambler extract the original data from the frames and converted bits are directly send to the base station.

V. SIMULATION RESULTS

The proposed system approach is implemented in WSN with a particular dimension. The performance evaluations are based on the simulation of 500 wireless sensor nodes that form a WSN over a1000x1000m area. In this proposed system we fix the distance between source to sink to be 350m and other 498 nodes are distributed over these area. In this part we compare the performance of clustering technique over the existing system with the help of some simulation results and evaluate several performance metrics, including the power, SNR, BER and packet delivery ratio (PDR) over both Rayleigh fading channel and Ricean fading channel. The performance setting parameters are given in the table 5.1

Table 5.1 Simulation parameters

Area of sensing field	1000*1000 m
Number of sensor nodes	500
Simulation time	600 s
Frequency	2.4 GHz
Bit rate	Variable bit rate
Sensor node transmission range	30 m
Number of loads	200 packets
Number of clusters	20
Channel bandwidth	20 Kbs

A. POWER REDUCTION

According to our simulations results with typical parameter setting, 67 % power reduction observed in clustering compared over Rician fading channel and 61.32 % over Rayleigh fading channel with existing system. In clustering, the CH closer to the BS than the follower nodes and CH directly communicate to the BS. So it take less energy for the data transmission in the network. The power consumption over both Rician and Rayleigh fading channel shows in the fig 5.1&5.2.

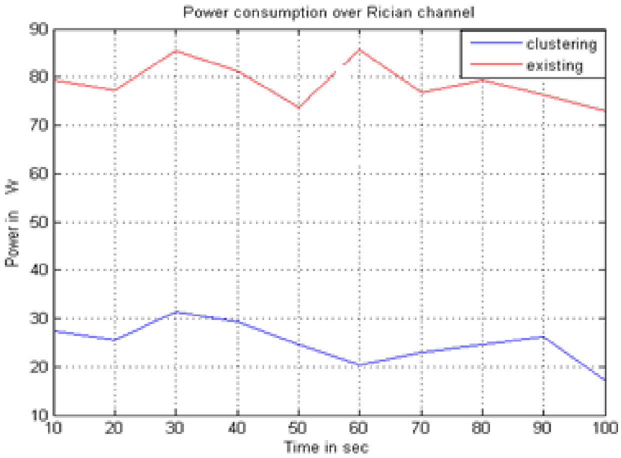

Fig 5.1 Power consumption over Rician fading channel

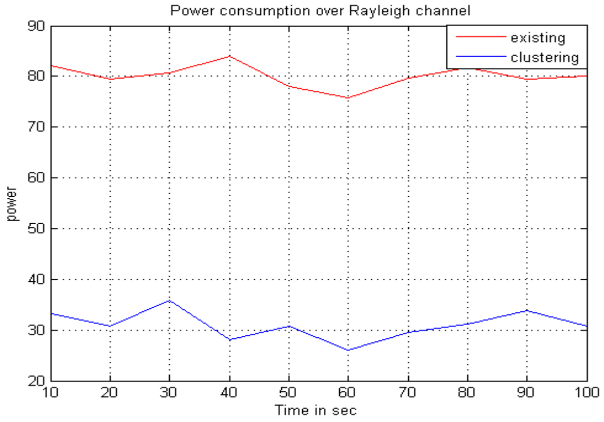

Fig 5.2 Power consumption Over Rayleigh fading channel

B. SNR

In proposed system 64% SNR value improved compared with existing system over Rician fading channel and 61.1 % SNR value improved over Rayleigh fading channel are shown in fig 5.3&5.4.

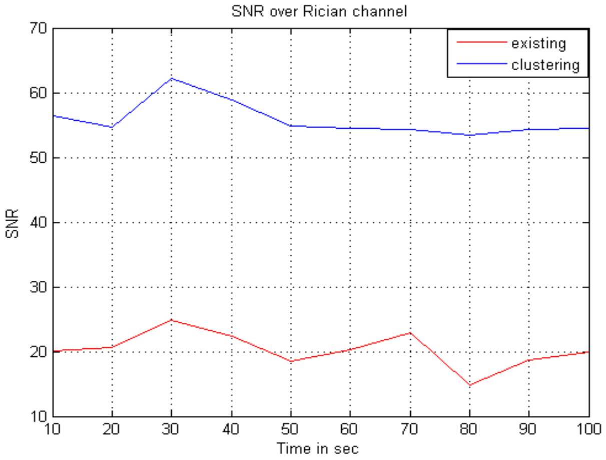

Fig 5.3: SNR over Rician fading channel

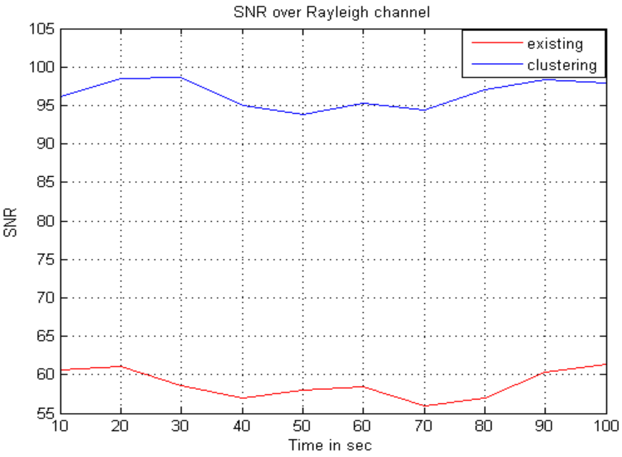

Fig 5.4 : SNR over Rayleigh fading channel

C. Packet delivery Ratio (PDR)

PDR is the ratio of the successfully delivered data to the total number of data packets transmitted. PDR over both Rician and Rayleigh fading channel shown in fig 5.5&5.6.

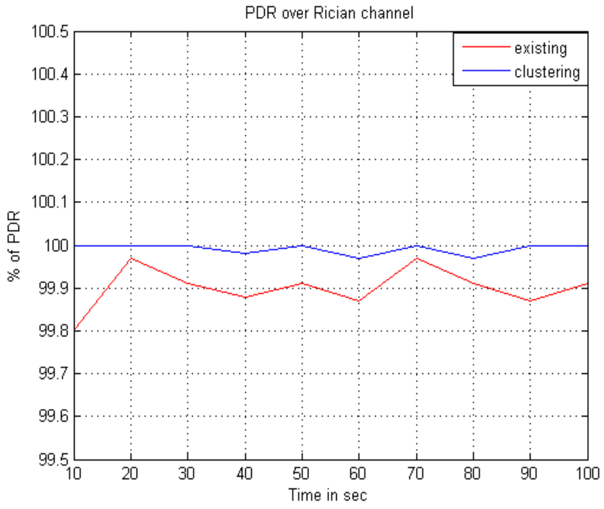

Fig 5.5: PDR over Rician fading channel

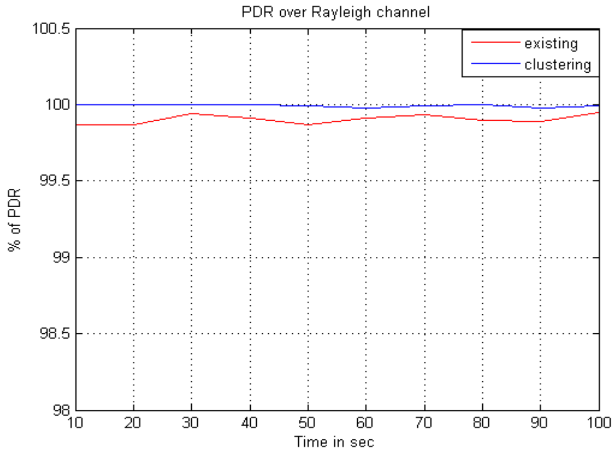

Fig 5.6 : PDR over Rayleigh fading channel

D. BER

In the clustering technique the bit error rate can be reduced from 3.2 to 1.5. The proposed system gives better performance compared with existing system.

VI. EXPERIMENTAL SETUP

The Wireless Sensor Network (WSN) can be used to gather the data from source to sink in a given area and also measure different parameters such as sound, vibration, pressure, etc. This paper presents the design of low cost low power security system. During the design process, ARM processor, LCD Display, transceiver modules, MAX232 and sensors as the main hardware components is used as hardware components while C compiler, Proteus, visual Basic and Keil were used for software elements. The data from the source was measured by the sensor then the data will be displayed on the LCD screen on the receiver and also displayed on the PC which support up to 100 m range. By using this system, it provide a low power low cost security system without using any cryptographic system.

VII. ACKNOWLEDGMENTS

We would like to thank Nehru College Of Engineering And Research Center, Pampady for providing the technical support.

VIII. CONCLUSION

Wireless sensor networks are being deployed for a wide variety of applications. It is an important challenge to find out practical secure schemes for wireless sensor networks due to limitation of power, computation and storage resources. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. In this existing method, we considered data confidentiality in distributed detection. Our adversary model was that the EFC passively eavesdrops on communications between the sensors and the AFC. The main idea behind the secure transmission is that two groups of activated sensors encrypt their quantized measurements in different ways based on instantaneous CSI of the main channel. Thus the EFC who receives sensors' reports over the eavesdropping channel cannot perform data decryption since the eavesdropping channel is independent of the main channel and the AFC appropriately decrypts received data by using the channel statistics of the main channel and LLR based fusion rule. Our performance evaluations show that detection performance at the AFC exponentially decays with growing the number of sensors so it take some time delay for the data transmission over the whole network. Power consumption, SNR, BER and packet delivery ratio are the major drawbacks of this method. The proposed scheme clustering technique provides an effective way to overcome the problems related to existing method. The nodes are grouped in to CH and followers. The CH only communicate to main station. It takes less energy to transmit data to the cluster head instead of the sink, which allows the sensor nodes to conserve more energy and live longer in WSN. Security has been achieved by isolating the malicious nodes using sink based routing pattern analysis. Clustering method attempt to improve the network stability period, it can serve as a better platform for upper layer functionality such as broadcasting, aggregation etc.

REFERENCES

1. M. Bloch and J. Barros, "Physical-Layer Security: From Information Theory to Security Engineering" Cambridge, U.K.: Cambridge Univ.Press, 2011.
2. J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," IEEE Commun. Lett.,vol. 14, no. 10, pp. 885–887, Oct. 2010.
3. S Ali A. Fakoorian and A.Lee Swindlehurst,Fellow,IEEE"MIMO Interference Channel With Confidential Messages: Achievable Secrecy Rates and Precoder Design "IEEE transactions on information forensics and security, vol. 6, no. 3, september 2011.
4. S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise,"IEEE Trans Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
5. Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
6. H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," IEEE Commun. Lett., vol. 4, no. 2, pp.52–55, Feb. 2000.
7. K.Kant and N.Gupta, Application based Study on Wireless Sensor Network**",** International Journal of Computer Applications, Vol. 21, March 2011
8. Y. Sangho, H. Junyoung, C. Yookun and H.Jiman, "PEACH: Power-Efficient and adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," Computer Communications,Vol.30, No.14-15, pp. 2842-2852, April 2007.
9. M. Diwakar and S .Kumar , An Energy Efficient Levelbased Clustering routing protocol for WSN International Journal of Advanced Smart Sensor Network Systems, Vol.2, issue 2, pp 55- 65, April 2012 .
10. S .Ganesh and R.Amutha Efficient and Secure Routing Protocol for Wireless Sensor Networks through Two level intrusion detection mechanism Wulfenia Journal, Vol.19, pp.388– 406, December 2012.
11. R.V.Kulkarni and A.Forester Computational intelligence in wireless sensor networks: A survey, IEEE Communications Surveys & Tutorials, Vol.13, issue1, pp. 68–96, April 2011.
12. S.Mohammadi,R.A.Ebrahimi,H.Jadidoleslamy, "A Comparison of Routing Attacks on Wireless Sensor Networks," International Journal of Information Assurance and Security, Vol. 6, No.3, pp. 195-215, July 2011.
13. C.Li, Shiwenhe, L.Yang and W.P Zhu, Joint power allocation for multicast systems with physical-layer network coding,‖ EURASIP Journal on Wireless Communications and Networking, pp.1-9, July 2010.