Energy Efficient Authentication and Authorization for Multinode Cooperative Connectivity and Reliability

Rohokale, Vandana M.

Publication date:
2013

Document Version
Early version, also known as pre-print

Energy Efficient Authentication and Authorization for Multi-node Cooperative Connectivity and Reliability

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF
ELECTRONICS ENGINEERING

OF

AALBORG UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

VANDANA MILIND ROHOKALE
Sept 02, 2013

Supervisor:
Professor Ramjee Prasad, CTIF, Aalborg University, Denmark

Co-supervisors:
Professor Horia Cornean, AAU, Aalborg University, Denmark
Professor Debasis Saha, IIM Calcutta, India

The Assessment Committee:
Professor Ingrid Moerman, Ghent University, Belgium
Dr. Parag Pruthi, CEO of Niksun, USA
Assoc. Prof. Rasmus L. Olsen, (Chairman), Aalborg University, Denmark

Moderator:
Associate Professor Flemming Bjerge Frederiksen, Aalborg University, Denmark

Date of Defence: Sept 02, 2013

Report: 2013-2014
ISBN: 978-87-7152-018-7

Dedicated to.....

The dream of my beloved father Late Mr. Mhatarba Sakharam Baste
to make me Doctor

The great vision and extra-ordinary dream of Dr. Sandeep Inamdar

The prodigious support and pains of my friend, philosopher, guide - my life partner
Mr. Milind Rohokale

Abstract

Wireless communication is a great revolution but it still suffers from limited battery life, broken connections from multi-path fading and insufficient coverage. Simple cooperation can make a big difference in coverage range, energy and battery life. In CWC, the active nodes may increase their effective QoS via cooperation. The performance of wireless networks is greatly affected by some of the channel parameters such as bandwidth and power scarcity, multi-user interference, non-reliability due to signal fading, vulnerability to the attacks, etc. The cooperative diversity mechanism makes use of the benefits of wireless sensor network scalability in terms of cooperative resource sharing wherein multiple diversity channels are created that results into the higher transmission rates, increased throughput and coverage range, improvement in reliability and end-to-end performance and much more. Cooperative wireless communication (CWC) greatly improves the cross layer optimizations.

The cooperative wireless communication (CWC) concept is more applicable to wireless sensor networks and cognitive ad-hoc networks than that of cellular networks. In CWC, the active nodes may increase their effective QoS via cooperation. Cooperative diversity is a strong technique, which can provide the maximum throughput. Opportunistic Large Array (OLA) is nothing but a cluster of network nodes, which use active scattering mechanism in response to the signal of the source called leader. The intermediate nodes opportunistically relay the messages from the leader to the sink. Cooperative OLA algorithms can improve the reliability as well as the energy efficiency of the communication.

Security of private key cryptosystems depends on the secrecy of the secret key. In case of public key systems, it is infeasible to derive private key from the public key. Breaking of a public key is a complex and timely task. Wireless adhoc network nodes are inherently memory and energy constrained. Today's commonly utilized algorithms such as RSA, Diffie-Hellman, NTRU and Elliptic Curve Cryptography make use of large numbers for multiplication in their encryption and decryption mechanisms. Due to their huge demand of memory and energy, these cryptographic algorithms can't be employed to wireless sensor nodes. This research work proposes a novel secure lightweight protocol making use of cryptographic and Information Theoretic Security.

The original contributions of this research work include the following:

1) Performance evaluation of Cooperative opportunistic large array (COLA) with two different use cases as follows:
    - Spectrum sensing in cognitive radio networks
    - Malicious behaviour detection in the cooperative Internet of Things (CIoT)
2) QoS analysis of the Cooperative opportunistic large array (COLA) in terms of Energy Efficiency, Delay and throughput with the help of Network Simulator 2.
3) Proposal and performance evaluation of the Cooperative web of trust (CWoT) in which authentication and authorization is to be achieved based on trust levels of the network entities.
4) Construction of a total communication link with information theoretic source and channel coding techniques. The performance of the link is evaluated with the cooperative jamming and information theoretic physical layer security technique.

Dansk Resume

Trådløs kommunikation er en stor revolution, men den lider stadig under begrænset batterilevetid, brudte forbindelser fra multi-path fading og utilstrækkelig dækning. Simpelt samarbejde kan gøre en stor forskel i dækningsområde, energi og batterilevetid. I CWC kan de aktive noder øge deres effektive QoS via samarbejde. Ydeevnen af trådløse netværk er i høj grad påvirket af kanal parametre såsom båndbredde og energi knaphed, multi-bruger interferens, manglende pålidelighed på grund signal fading, sårbarhed over for angreb, osv. Den kooperative mangfoldigheds mekanisme gør brug af fordelene ved trådløse sensor netværks skalerbarhed i form af kooperativ ressourcedeling, hvor multiple mangfoldigheds-kanaler er dannet med det resultat at der opnåes højere transmissionshastigheder, øget kapacitet og dækning område, forbedrer pålidelighed og end-to-end ydelse og meget mere. Kooperativ trådløs kommunikation (CWC) vil i høj grad forbedre cross-layer optimeringer.

"Cooperative Wireless Communication" (CWC) konceptet er mere relevant for trådløse sensor netværk og kognitiv ad-hoc-netværk end mobilkommunikationsnetværk. I CWC kan de aktive knudepunkter øge deres effektive QoS via samarbejde. "Cooperative Diversity" er en stærk teknik, som kan levere den maksimale overførelseshastighed. "Opportunistic Large Array" (OLA) er ikke andet end en klynge af netværksknuder, som bruger en aktiv spredningsmekanisme som reaktion på signalet fra kilden kaldet "leader". De mellemliggende knudepunkter vil opportunistisk videregive beskeder fra "leader" til modtager. Cooperative OLA algoritmer kan forbedre pålideligheden samt energieffektiviteten for kommunikationen.

Sikkerhed for "private-keys" kryptosystemer afhænger af hemmeligholdelsen af "secret-key". I tilfælde af "public-key" systemer er det umuligt at udlede "private-key" fra "public-key". At bryde en "public-key" er en kompleks og tidskrævende opgave. Trådløse sensornoder er i sagens natur hukommelse og energi begrænset. I dag vil almindeligt anvendte algoritmer, såsom RSA, Diffie-Hellman, NTRU og "Elliptic Curve Cryptography" gøre brug af et stort antal multiplikationer ved kryptering og dekryptering. På grund af deres store ressourceforbrug kan disse kryptografi algoritmer ikke anvendes til trådløse sensornoder. Denne forskning præsenterer en ny sikker letvægts protokol, som gør brug af "Information Teoretisk Security".

Dette forskningsarbejde indeholder følgende bidrag:

1) Performance evaluering af Cooperative Opportunistic Large Array (COLA) med to forskellige use cases som følger:

- Spectrum sensing i kognitive radionetværk.
- Ondsindet adfærd detektering i den Cooperative Internet of Things (CIoT)

2) QoS analyse af Cooperative opportunistiske Large Array (COLA) i form af energieffektivitet, delay og kapacitet ved hjælp af Network Simulator 2.

3) Forslag og performance bedømmelse af Cooperative Web of Trust (CWoT), hvor godkendelse og autorisation er opnået baseret på tillidsniveauer af netværksnode enheder.

4) Konstruktion af en komplet kommunikationsforbindelse med informationteoretisk kilde og kanal kodningsteknikker. Performance af forbindelsen vurderes med kooperativ jamming og informationsteoretisk fysisk-lag sikkerhedsteknikker.

Acknowledgements

At first, I would like to thank whole heartedly Prof. Ramjee Prasad for his generous support and constant encouragement to complete my PhD from CTIF, Aalborg. I am indebted to Dr. Neeli prasad for her tireless and unconditional help and being a role model for me throughout the journey of research. I would like to thank GISFI and its members for always being inspiration.

I am very much thankful to my co-supervisors Prof. Horia Cornean and Prof. Debasis Saha for their backing. I must take this opportunity to thank Prof. M. N. Navale and Dr. Sunanda Navale for their great support in every aspect for this PhD program. I would like to extend my gratitude towards Dr. S. S. Inamdar for being instrumental for this PhD to happen.

I would like to thank Dr. Rasmus Hjorth Nielsen, Dr. Nicola Marchetti, Inga Hauge, Sussane Norrewang, Jens Erik Pederson and all CTIF staff members for their direct or indirect help. And a big thank to my sweet GISFI PhD batch team for their friendship and care without which it was not possible for me to accomplish this task. I would like to express my deep gratitude towards Prasad family for always being loving and supportive to make my stay at Aalborg very joyful and memorable.

Last but not the least; I would like to express huge thanks to my loving husband Mr. Milind for his great support and my little angels Madhura and Mugdha for making me forget all the pains with their innocent and playful smiles. I would like to extend my thanks to my in laws, my mother Radha, Sandeep, Dr.Nitin, Vaishu, Sujata, Manoj, Ram, Shital and Surekha for their loving support. I would like to thank Sudeep, Kishor, Chaitanya and Dipesh for their time to time cooperation.

Contents

List of Tables

List of Figures

List of Abbreviations

6LoWPAN	Integration of low power IEEE802.15.4 devices into Ipv6 networks
AES	Advanced Encryption Standard
AE-STFNC	ANTI-Eavesdropping Space Time Frequency Network Coding
AE-STNC	ANTI-Eavesdropping Space Time Network Coding
ANEC	European consumer voice in standardization
A-OLA-T	Alternating OLA with Threshold
AWGN	Additive White Gaussian Noise
BCH	Bose Chaudhury Hocquenghem
BER	Bit Error Rate
BEUC	The European Consumer's Organization
BPEL	Business Process Execution Language
BPSK	Binary Phase shift Keying
CASAGRAS	Coordination and support action for global RFID related activities and standardization
CEN	Committee of European Normalization
CENELEC	European Committee for Electro technical Standardization
CERP-IoT	Cluster of European Projects on the IoT
CIMIT	Center for Integration of Medicine and Innovative Technology
CJ	Cooperative Jamming
COLA	Cooperative Opportunistic Large Array
CPE	Consumer Premise Equipment
CPU	Central Processing Unit
CR	Cognitive Radio
CRN	Cognitive Radio Network
CSI	Channel State Information
CT	Cooperative Transmission
CWoT	Cooperative Web of Trust
CWC	Cooperative Wireless Communication
DES	Data Encryption Standard
DF	Decode and Forward
DoS	Denial of service attack
DSA	Dynamic Spectrum Access
DSDV	Destination Sequenced Distance Vector
DSL	Digital Subscriber Lines
DSSS	Direct Sequence Spread Spectrum
DT	Direct Transmission
EPC	Electronic Product Code
ETSI	European Telecommunication Standards Institute
FES	Fraction of Energy Savings

GCS	Global Coding System
GPS	Global Positioning System
GRIFS	Global RFID Forum
HESS	Hybrid Energy Storage System
HSDPA	High Speed Downlink Packet Access
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISO	International Organization for Standardization
ITS	Information Theoretic Security
ITU	International Telecommunication Union
LAN	Local Area Network
LAR	Location Aware Routing
LDPC	Low Density Parity Check Codes
LTE	Long Term Evolution
LZW	Lempel Ziv Welch
MAC	Media Access Control
MIMO	Multiple Input Multiple Output
NAT	Network Address Translation
NFC	Near Field Communication
OFDM	Orthogonal Frequency Division Multiplexing
OLA	Opportunistic Large Array
OLACRA	Opportunistic Large Array Concentric Routing Algorithm
OLA-VT	OLA with Variable Threshold
P2P	Point to point communication
PAN	Personal Area Network
PET	Privacy Enhancing Techniques
PHY	Physical Layer
PIR	Private Information Retrieval
PLS	Physical Layer Security
PN	Pseudo Random Noise
PU	Primary User
PUEA	Primary User Emulation Attack
QoS	Quality of Service
RACE	Raising Awareness and Competitiveness in Europe for Networked RFID
RF	Randomize and Forward
RFID	Radio Frequency Identification
RHC	Rural Healthcare Center
ROLL	Routing Protocols for heterogeneous low power and lossy networks
RS	Reed Solomon
RSA	Rivest Shamir Adleman algorithm
RSS	Received Signal Strength
RTS	Request to send
SLAM	Simultaneous Localization and Radio Environment Mapping Based Routing
S-MAC	Sensor-MAC
SNR	Signal to Noise Ratio
SOA	Service Oriented Architecture
SU	Secondary User
TLS	Transport Layer Security
TM-SCSS	Trust Methodology for Secrecy in Cooperative Spectrum Sensing

UMTS	Universal Mobile Telecommunication System
UNICEF	United Nations Children's Fund
USB	Universal Serial Bus
UWB	Ultra Wide Band
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WHO	World Health Organization
Wi-Fi	Wireless Fidelity
Wi-MAX	Worldwide Interoperability for Microwave Access
Wireless HART	Protocols for self-organizing, self-healing and mesh architectures over IEEE802.15.4 devices
WSDL	Web Services Definition Language
WSN	Wireless Sensor Network

1
Introduction

The goal of this chapter is to motivate the readers for cooperative communication because it is an important technique to address from both academic and industrial points of view. The key issues are explained in order to get an overview of the thesis. The contributions of this thesis are explained and the related publications provided. Finally, outline of the thesis is provided giving an overview of the individual chapters.

One day morning, we were waiting for our college bus to pick up us. Wipro industry's office bus was slowly passing by us looking for its employees. At the last moment, when the driver increased speed, we noticed one person hurriedly stepping down from an auto rickshaw and shouting 'stop the bus'. Voluntarily whoever was present there started shouting 'stop, stop the bus'. And the sound reached the bus driver and he stopped the bus and that person-an employee of Wipro could catch his bus in time. This is a classic example of cooperative communication being used effectively in our everyday life. We can think of many similar other scenarios that simply depict the spirit of cooperative wireless communication which utilizes the information overheard by neighbouring nodes to offer reliable communication between sender and receiver.

Currently, wireless communication and mobile computing are the buzz words for the telecom industry. For multimedia applications, the user needs higher data rates at which data transactions can take place efficiently. Gigabit wireless communication is the dream which is being chased by scientists and researchers. Different wireless networking technologies include cellular networks, Wi-Fi Networks, WiMAX Networks, Wireless sensor networks etc as shown in figure 1.1 below. Cooperation strategy can be effectively applied for these well- known networking techniques.

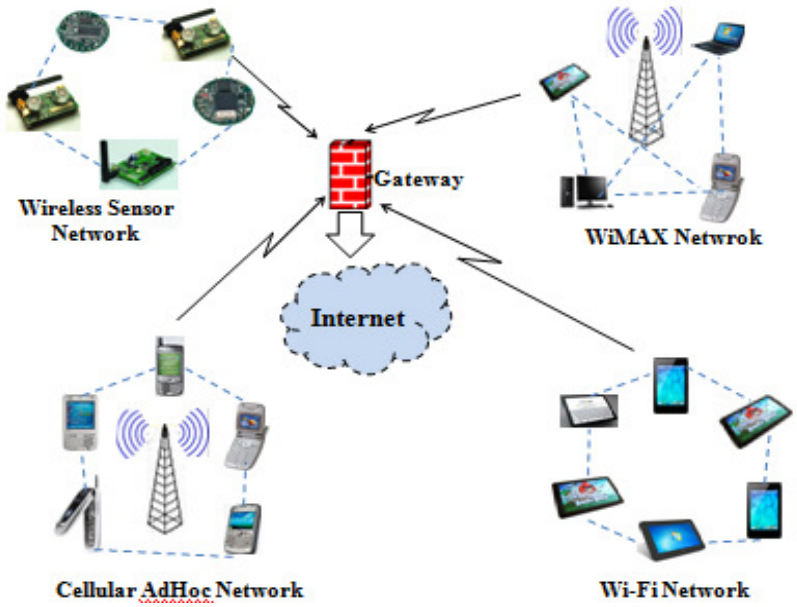

Figure 1.1 Wireless Networking Techniques

Capacity provided by single antenna systems is bounded by the Shannon's limit. Diversity gains like capacity and high data rates are possible with the MIMO systems [1]. Diversity is nothing but a mechanism for reliability improvement in the transmitted message signal which makes use of two or more

communication channels of different characteristics. But today's booming wireless techniques like adhoc networks, wireless sensor networks and cognitive radio networks are making use of resource constrained miniature devices. The hardware implementation of the MIMO system poses problem due to size, weight and cost [2]. MIMO is the only key solution to bring spectrally efficient Gigabyte wireless communication in reality. Cooperative communication creates the scenario of virtual MIMO by utilizing the group communicating nodes antennas. Multi-node cooperative communication is a relaying technique in which multiple, spatially separated radio nodes cooperate each other to transmit the same information so that the receiver can select the information with maximum diversity gain from the multiple transmissions. The cooperation from the wireless network nodes that otherwise do not directly contribute in the transmission is intelligently utilized in CWC.

The comparison in between Cooperative Transmission (CT) and Direct Transmission (DT) is mentioned in Table 1.1 and Figure 1.2 below. Figure 1.2 depicts the scenario of direct transmission, Cooperative transmission and selective relaying cooperative transmission. It also indicates coverage range extension due to cooperation.

Table 1.1 – Comparison of Cooperative and Direct Communication

	Cooperative Transmission	**Direct Transmission**
Components	Leader, Relay and Sink nodes	Source and destination
Communications	Cooperative	Single-hop or Multi-hop
Protocols	Cross layer (PHY+MAC)	Single layer
Mechanisms	Decode and forward, Amplify and forward, Coded Transmission	Simple transmission
Reliability	High reliability with less error probability	Less reliability due to increased error probabilities
Transmit Power	Less draining of power	More draining of power for long distance communication
Coverage Area	Increased	Fixed
Shadowing	Resistant to large scale shadowing	Less resistance to shadowing

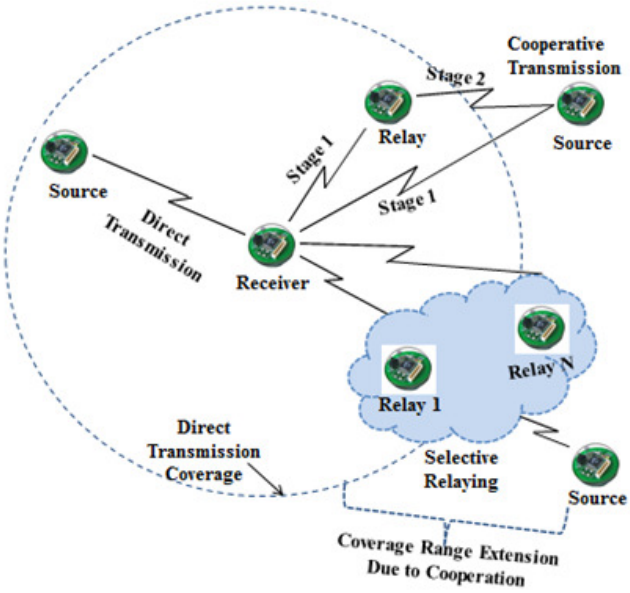

Figure 1.2 - Illustration of direct transmission, cooperative relaying and selective relaying

The traditional multi-hop wireless networks tend to generate contention while the cooperative transmission regulates the traffic by making use of cooperation levels as shown in Figure 1.3. Collisions are avoided due to regular and scheduled tasks in cooperative transmission. The levels of cooperation are decided depending on the particular node SNR figures and their values more than or equal to the threshold values. In multihop case, there is no such regulation of traffic with beamforming and that is why there are more chances of congestion and network flooding

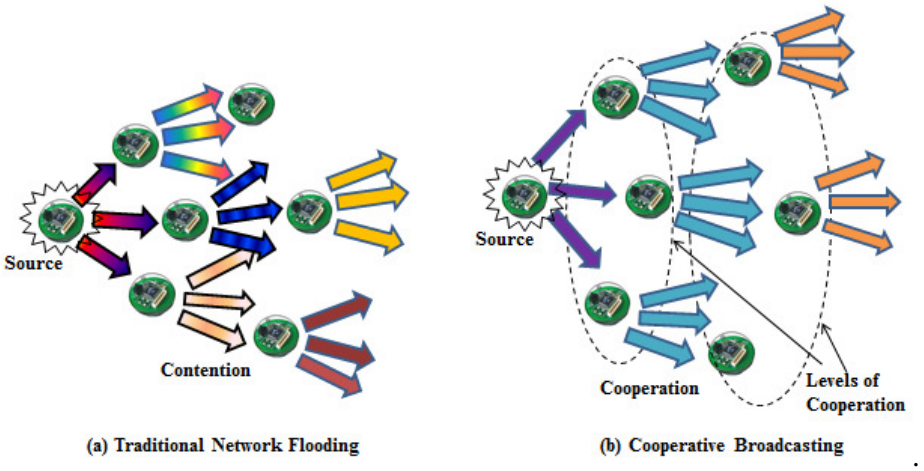

Figure 1.3 - Traditional Network Flooding and Cooperative Broadcasting

The conceptual view of cooperative wireless communication (CWC) is depicted in Figure 1.4. It covers collaborating entities, cooperating horizons, operational scenarios and benefits of cooperative behaviour of the system.

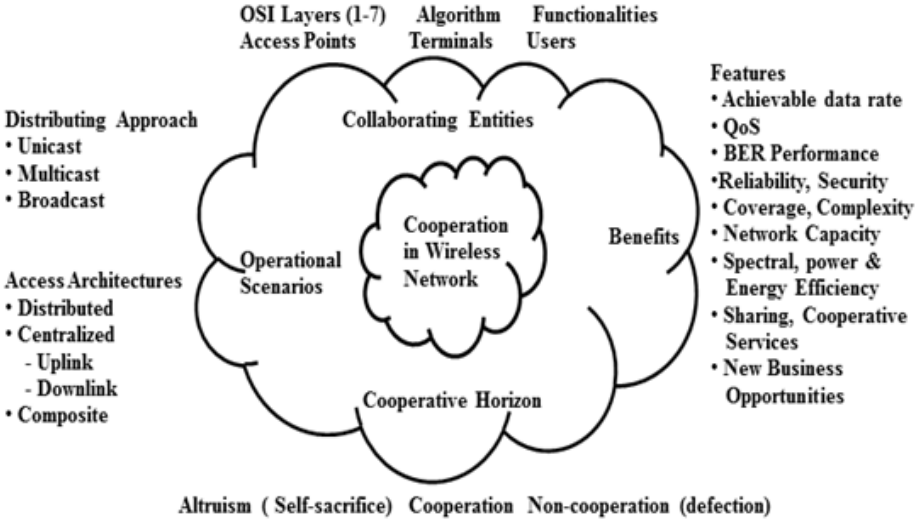

Figure 1.4 – Conceptual view of Cooperative Wireless Communication (CWC)

The radio nodes negotiate about their cooperation strategies as shown in figure 1.5. In cooperative transmission case, numbers of relays cooperatively transfer the message from source to destination. While cooperating with each other, the relays may negotiate about channel usage of each other or for sharing of other resources.

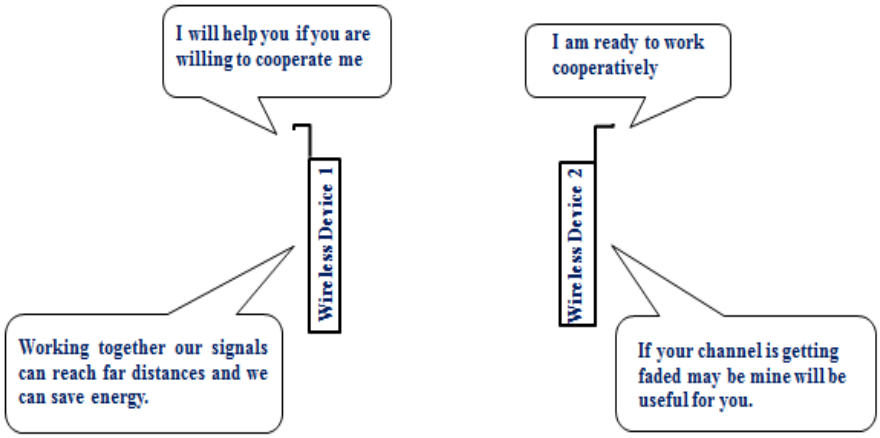

Figure 1.5- Cooperation between radio nodes

1.1 Cooperative Wireless Communication

The origin of cooperative communication concept dates back to the work on three terminal relay channels by Vander Meulen in 1971 [3]. In this work, the author has proved that the channel capacity of the relayed communication channel in time sharing mode is far better than the channel capacity of direct communication. This work was further extended by Cover and El Gamal in 1979 for deriving the capacity theorems based on Information theoretic mutual information in between the source-receiver and source-

relay-receiver scenario [4]. Here, the authors have shown that the channel capacity for the relayed cooperative communication channel is supremum over all joint distributions in case of traditional multihop communications.

Cooperative communication exploits the overheard information at the surrounding radio nodes for increasing the throughput and reducing the bit error rates at the receiving ends. Also, different channel coding techniques are described which can provide the diversity advantage of cooperation. Cooperative communication takes different forms at different protocol layers in the OSI model and hence there are various openings for cross-layer benefits through various design techniques and optimization parameters [5]. Cooperation provides considerable improvements in the throughput and overall robustness of the communication system with significant reductions in the delay and interference. Laneman *et. al.* in their research work [6], have proposed low complexity fixed relaying cooperative protocols including amplify-and-forward and decode-and-forward techniques. The authors have analysed these protocols for outage probability performance under the assumption of high-SNR conditions. Large energy and power savings are achieved through cooperation by making use of these protocols but at the cost of high bandwidth requirements due to half-duplex operations.

Scaglione *et. al.* in the research work of [7] has defined two prospective architectures for cooperation in MANETs. Out of these two cases, one is completely based on presently available clustered infrastructure wherein the cooperating relay nodes are centrally controlled by cluster heads. The second approach is visualized in terms of decentralized scenario without clustering in which case, the cooperation links are formed according to request from source node in the ad hoc network. Based on the rate information stored at each cooperating entity, the total time requirement for cooperative two-hop transmission is found to be less as compared to the direct transmission [8]. Novel approaches for video streaming and multimedia applications like multiple description coding (MDC) and scalable video coding (SVC) are presented in the work of [9]. Combined cooperative cellular short range network architecture concept is coupled with MDC and SVC techniques for achievement of robust wireless transmission with energy efficiency. By making use of GPRS technology for the cellular communication and Bluetooth for the short range, almost 50% power saving gain is observed to be achieved.

Direct and cooperative transmission can be compared by making use of rate of information, signalling required for setting up a transmission and the amount of data to be transmitted. These infrastructures are shown to provide improved wireless link abstractions with trade-off in complexity at

physical and higher layers. Single hop architecture for the cooperative wireless sensor networks is proposed in [10] and by making use of theory of random arrays, distributed beam forming gain performance is analysed. With the application of Ricean distribution, average loss in the directivity gain at the receiving end is investigated. The authors have shown that the high directive gains can be achieved in WSN by exploiting cooperation among the sensor nodes. In the research work of [11], the authors have projected new and generic model for a multi antenna channel with application of Gaussian noise, flat fading, path loss and co-channel interference. By making use of asymptotic free probability approach, capacity limit of the channel under assumption is calculated.

To accomplish the reliability similar to SISO, cooperative transmission is the ultimate solution. Employing number of relays in the cooperative system increases the reliability of transmission but at the same time, malicious behaviour becomes more prominent. In the research work of [12], the authors have analysed performance evaluation of cooperative transmission by considering the parameters like path loss exponent, relationship between intermediate relays, number of hops and successful transmission probabilities. Here, the authors have shown that MISO system outperforms SISO in terms of successful transmission probability when the network node is surrounded by more honest nodes than that of cooperating entities.

Network coding is a technique where the intermediate network nodes are allowed to perform coding operations over multiple received data streams. In network coding, the redundancy information is transmitted for the erasure correction purpose. For cooperative wireless communication, network coding and cooperative channel coding are the essential techniques. The research work in [13] proposes a new technique for the construction of network codes as an integral part of the channel codes with diversity order analysis of the employed cooperative protocol. The joint network channel coding (JNCC) proves to be efficient in terms of reliability and diversity order.

Misha Dohler *et.al.*in [14] have appropriately explained cooperation mechanism, wireless relay channel and their modelling, transparent relaying techniques, regenerative relaying techniques and hardware issues in the design of cooperative transceivers for different application scenarios like 3G UMTS Voice / HSDPA Relay and LTE / WiMAX Relay systems. They have also demonstrated some of the real implementations of cooperative diversity mechanisms.

Cooperative diversity in terms of distributed antenna system was first analysed in the research work of [15]. Here two or more information sources form a cooperative group and transmit common information

to a single sink. The distributed antenna system was evolved initially for the cellular communication system. With spatial diversity, the advantages of the distributed antenna system are signal strength and channel capacity improvement. For making the transition from traditional cellular system to a cooperative cellular network, authors in [16] have put forth new techniques such as distributed antenna system, multi-cell coordination, group cell mechanism including multiple point transmission and reception (CoMP). These are the stepping stones towards bringing 3GPP LTE-Advanced (LTE-A) into reality.

The research work in [17] has shown that with the coverage range enhancement and improvement in the channel capacity, the cooperative relaying can expressively increase the spectrum efficiency and overall performance of the system. Two intra-cell coordinated multipoint schemes for LTE-Advanced are taken into consideration and it is shown that the network capacity can be considerably improved with the cooperation. Since the transmissions in the cooperative communication are from the nodes at different locations, they may not be time or frequency synchronized. And it becomes difficult to achieve full diversity for the collocated MIMO systems.

Reliable communication with reduced energy consumption is the hot issue in the resource constrained networks like WSN and CRN. Cross layer cooperation is the best suited solution for achievement of energy efficiency and reliability in wireless communication. In [18], distributed cross layer technique is proposed which makes use of opportunistic relaying mechanism to achieve quality of service (QoS) in the cooperative communications. Energy savings and low bit error rates can be achieved with the help of cross layer cooperation as shown in Figure 1.6. Some parts of the routing functions are executed at the physical layer. The diversity provided by the MIMO space time codes can help in the performance improvement at the MAC and upper layers [19]. Due to this, the physical layer system cooperates with higher layers in the protocol stack and gets benefits in terms of improvements in the system robustness, throughput, delay and interference reduction with the coverage range extension.

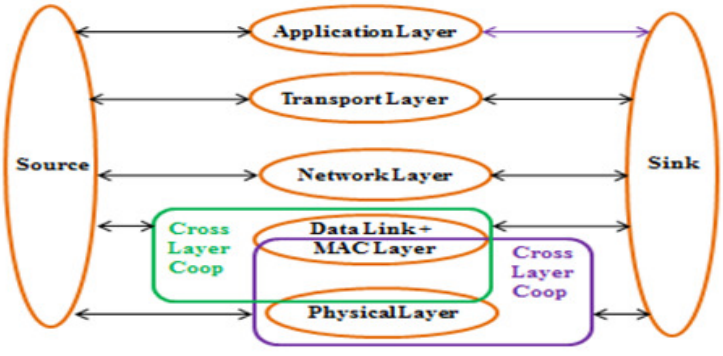

Figure 1.6 - Cross Layered Cooperative Communication

The research work of [20] puts forth a new distributed weighted cooperative routing algorithm in which relay selection is based on the weights of the relays. The metrics used for the decision of relay weights are residual energy and channel state information (CSI) at each source-relay-receiver link. Here, the authors have made use of Destination Sequenced Distance Vector (DSDV) routing protocol with consideration of the difficulties due to time synchronization and data packet reduplication. To achieve energy efficient long range communication, cooperative beamforming is the ultimate solution. In the work of [21], a cross layer framework for cooperative communication is proposed which brings the concept of cooperative beamformimg. Here, the cooperative beamforming mechanism is applied for the analysis of the spectrum efficiency of the cooperative communication system. For the study of delay characteristics of the source messages, queuing theory is used.

The cooperative communication techniques developed uptill now lack in consideration of security aspects. Many researchers have paid attention towards the power allocation, energy efficiency, localization problems and many other aspects. But security in cooperative communication is very hot issue because the cooperative communication is more prone to eavesdropping attacks.

1.2 Cooperation Strategies

Independent paths in between source and sink are generated by introducing relay channel in between them in the cooperative communication paradigm. Based on how the signal received form the source is processed at relay, there are different cooperative communication protocols. Main classes include fixed and adaptive relaying mechanisms as depicted in Figure 1.7. In case of fixed relaying, the channel resources are distributed in between source and relay in deterministic way. All four techniques under the fixed relaying category work in the predefined deterministic or fixed manner [22]. Adaptive relaying technique containing selective and incremental relaying mechanisms has inbuilt flexibility in the sense that during the adverse conditions like severe channel fading or low SNR conditions, the relay can idle itself.

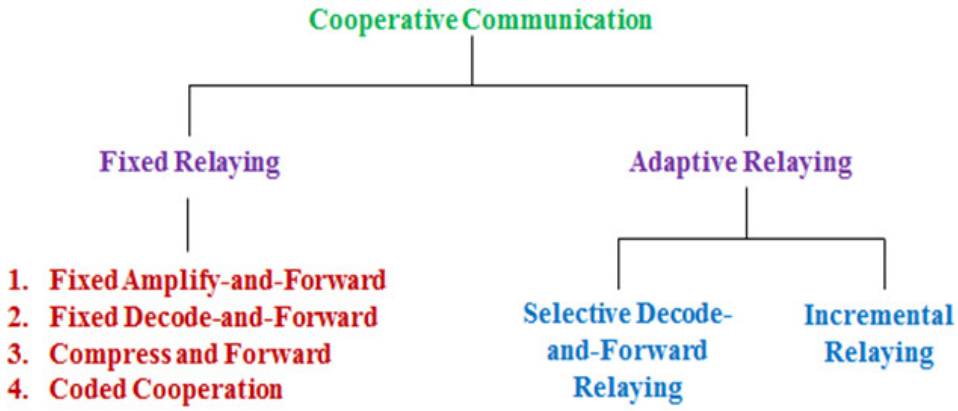

Figure 1.7 - Cooperative Relaying Techniques

For optimum diversity gains, proper relay selection plays a vital role in the cooperative communication. The research work of [23] presents a survey of the distributed relay selection schemes for adhoc cooperative wireless networks. These relay selection schemes include opportunistic relaying, power aware relay selection, switch and examine node selection, opportunistic relaying with limited feedback, simple relay selection, geographical information based relay selection, threshold based relay selection for detect-and-forward, opportunistic AF relaying with feedback, incremental transmission relay selection, outage optimal relay selection, energy efficient relay selection, random priority based relay selection, receive SNR priority list based relay selection, fixed priority transmission protocol, generalized selection combining multiple relay selection scheme and output threshold multiple relay selection. Different performance metrics like objectives, mechanisms, performance, advantages and drawbacks of each of them are illustrated in the tabular way [23].

1.3 Opportunistic Large Array Approach

Opportunistic Large Array (OLA) is nothing but a cluster of network nodes which use active scattering mechanism in response to the signal of the source called leader. The intermediate nodes opportunistically relay the messages from the leader to the sink [24]. The authors have suggested an optimal power allocation mechanism in [25]. It includes a class of diversity protocols for multi-node wireless network utilizing relaying strategies depending on the distance of relay either with source or sinks. Higher data rates at the reduced transmit power can be converted to an increase in cell coverage [26]. Relaying and cooperative diversity essentially creates a virtual antenna array. All of the cooperative diversity protocols are efficient in terms of full diversity achievement and optimum performance except fixed decode-and-forward approach. Distributed antennas can provide the powerful benefits of space

diversity without need for physical arrays. Although prior to Laneman [27], the work on relay and cooperative channels utilized full duplex approach, he has constrained the cooperative communication to employ half duplex transmissions. Also the Channel State Information (CSI) is employed in the receiver instead of transmitter.

For cooperative transmission, OLA selects the nodes which have the received signal SNR above some threshold figure and the resonance generated by relay nodes carries the actual messages to the desired sinks without causing interference. For the abolition of the routing and multiple access overheads, OLA as shown in Figure 1.8, is a competent physical layer broadcasting algorithm. Multiple clusters of *ad hoc* wireless nodes can form a multi-OLA system, constructing a multiple access system with the cluster of nodes acting as a team through cooperative transmission rather than transmitting independent data from each node. OLAs can either be with regenerative or non- regenerative [28]. With decode and forward cooperation strategy and selection threshold criterion, OLA can be regenerative by decoding the received data and encoding it again.

OLA utilizes the cooperative transmission of the AdHoc network nodes to reach back a far distant node or sink. Applications of OLA can be: Joint control systems and secure military scenarios where delay can't be tolerated. OLA is a cooperative mechanism which is simple and scalable.

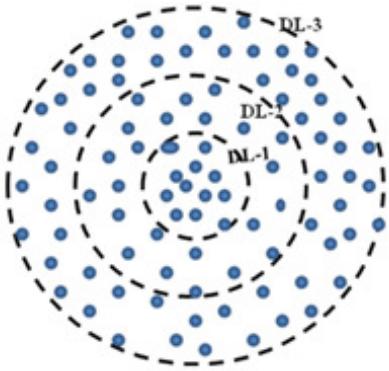

Figure 1.8 - Basic OLA Structure with Decoding Levels

For a network of 100 nodes, having square meter area of 350m, the coverage area obtained could be one km. In more general sensor network practical applications, the reach back issue plays an important role. With direct transmission, the quick draining of energy resources takes place which is called as reach back problem. Cooperative transmission is necessary for successful information conveying to the far distant sink. Opportunistic Large Array with Concentric Routing Algorithm (OLACRA) includes more flooding as

compared to basic OLA. With optimum ganging of levels, OLACRA yields the diversity gains up to 75% [29].

A-OLA-T as depicted in Figure 1.9 is the alternating OLA with threshold. It requires slightly less than double the power of basic OLA but A-OLA-T doubles the network life compared to basic OLA [30].

Table 1.2 – State-of-the-art of OLA algorithms

Parameter/ Technique	Delay	Energy saving / life extension	Reliability	Node Density /Scalability	Authentication and Authorization	Merit/ Demerit
Basic OLA [28] The avalanche of responses to the leader node is like the ola in a sports stadium.	Constant	60% of the radiated power savings as compared to non-cooperative broadcasting	With increased SNR values, BER reduces.	Reasonable node density with high scalability	**NOT ADRESSED UPTILL NOW**	With cooperative TX, reach-back problem is solved
OLA-T [28] The node participation in each OLA is controlled by the power transmission threshold in Rx.	Constant delay	32% of the transmitted energy as compared to Basic OLA	Highly reliable coop communication for high SNR cases	For constant threshold values, ρ=2.65 nodes/m^2 with less scalability as compared to basic OLA		With full flooding approach, energy saving is 50%
OLA-VT [29] OLA with variable threshold, which optimizes thresholds as a function of level.	slightly variable	25% of the transmitted energy as compared to Basic OLA	**NOT CONCENTRATED ON RELIABILITY ISSUES**	Less scalable as compared to basic OLA		
A-OLA-T [30] Broadcast protocol alters between the sets of OLAs for each broadcast.	Variable delay	Can offer a 17% life extension as compared to Basic OLA and OLA-T		Highly scalable		Almost double power as compared to OLA is required.
OLACRA [30] It exploits the concentric ring shapes of broadcast OLAs to limit flooding on upstream connection.		75% as compared to full flooding approach		Possesses highest scalability		Level Ganging
OLACRA-T [30] The criterion to be met for OLACRA is that their received power should be less than a specified threshold.				Highly scalable		

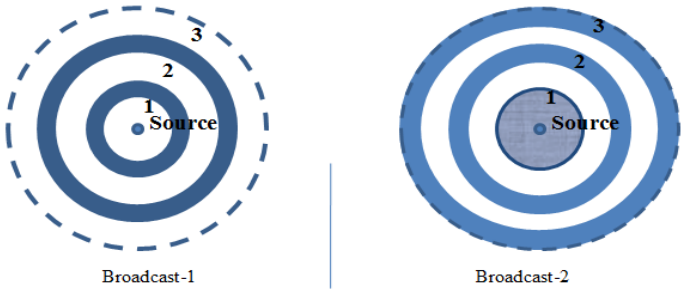

Figure 1.9 - Two set Alternating OLA-T

The OLA broadcasting is a spread spectrum technology and therefore it is possible to have multiple OLA networks transmitting simultaneously to the same remote receiver. A-OLA-T can offer a 17% life extension as compared to basic OLA technique. OLACRA-T and OLA-VT are available which are nothing but the threshold and variable threshold respectively. OLA based protocol does not need a global positioning system for knowledge of the geographical position of the node due to the assumption of full channel state information (CSI) and distributed synchronization strategy at each node [30].

1.4 Motivation

Wireless communication is a great revolution but it still suffers from limited battery life, broken connections from multi-path fading, insufficient coverage and security threats due to its open nature. Simple cooperation can make a big difference in coverage range, energy and battery life. In CWC, the active nodes may increase their effective QoS via cooperation. Out of two most popular cooperative relaying strategies, Amplify and forward mechanism results in the noise amplification and is not suitable for the scalable networks like wireless sensor networks. Decode-and-forward mechanism is well suited for WSN provided that the channels should be strong enough. In cooperative communication, the information overheard by neighbouring nodes is intelligently used to provide the healthy communication between a source and the destination called as sink. The sink node or destination receives numerous editions of the message from the source, and relay(s) and it estimates these inputs to obtain the transmitted data reliably with higher data rates.

The cooperative broadcasting is prone to eavesdropping attacks due to its multi-node wireless connectivity. Nowadays everybody wish to use their wireless equipment to make wireless security sensitive transactions like online banking, stock trading and shopping. In such cases, the protection of personal and

business data is very much important. When a receiver receives a message, it may be concerned about who is the real sender and whether the content of the message has been changed illegally by somebody in the transmission. Message secrecy problem become the important aspect of information security in modern times.

1.5 Challenges

The challenges relating to cooperative wireless communication, investigated in the scope of this thesis, are listed below:

- Multi-node cooperative connectivity for wireless sensor networks.
- Malicious behaviour detection in cooperative wireless communication.
- Authentication and authorization mechanism for CWC.
- Energy efficient light weight cryptographic solution for opportunistic cooperative communication.
- Obtain integrated solution for security and reliability.

Cooperative communication is a promising technique that would enhance the design of WSN. Security of private key cryptosystems depends on the secrecy of the secret key. In case of public key systems, it is infeasible to extract private key from the public key. Breaking or knowing of a public key is a complex and timely task. Lot of work is in progress in the direction of enhancement of energy efficiency. But certain issues such as Trusted, Authenticated and Reliable connectivity in multi-node cooperative communication networks in addition with energy efficiency are the real forthcoming challenges.

Authentication is the mechanism whereby systems may securely identify their users. Authentication systems provide answers to the questions:

- Who is the user?
- Is the user really who he/she represents himself/herself to be?

Authorization, by contrast, is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system. The importance of protecting the secrecy of sensitive messages has been realized by people since ancient times. By making use of strong techniques, the storage and transmission of information become cheap and simple in modern times. A huge amount of information is transformed in a way that almost anyone may access it. A lot of

new problems related to cryptology appear. For example, an enemy might not only have the means to read transmitted messages, but could actually change them, or the enemy could produce and send a false message to the receiver and hope that this would initiate some action as shown in Figure 1.10 below.

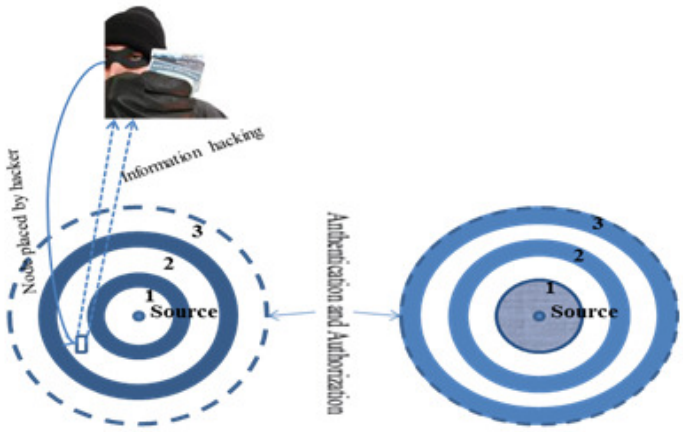

Figure 1.10 – Security Issues for Cooperative Wireless Connectivity

Now consider another example in which, we imagine a sensor node who has stolen an access to a bank's outgoing telephone line. When the user visits the bank and deposits 100 Euros on its account, the bank sends a message to a central computer, telling the computer to add 100 Euros to the user's account. By changing the content in the message, the sensor node can add a different amount, for example 1000 Euros, to user's account. Another possibility would be to record the message transmitted by the bank and then send the same message several times, each time adding 100 Euros to the account. This example shows that it is necessary to have some mechanism to check that only messages sent by the bank will be accepted by the central computer. Here, the message needs to be authenticated.

The traditional cryptographic algorithms such as AES, DES, and NTRUE etc. include complex mathematical calculations. Since next generation networks like CRNs and WSNs are making use of resource constrained miniature network nodes, these traditional higher layered cryptographic solutions are not feasible for them. Light weight cryptographic solutions with Physical layer security employing information theoretic source and channel coding techniques has potential to provide energy efficient security solutions for these networks.

1.6 Problem Statement and Research Objectives

To design energy efficient and reliable authentication and authorization mechanism for the multi-node cooperative connectivity by making use of light weight cryptography for resource constrained networks like wireless sensor networks and cognitive radio networks.

The problem statement can be divided into different sub-problems as below:

- Is there possibility of multi-node cooperative connectivity for WSN and CRN?
- Are these systems energy efficient?
- Is there any consideration of Authentication and Authorization issues in cooperative communication?
- Is cooperative communication considerably security and reliable?

Research objectives are as shown in the figure 1.11 below.

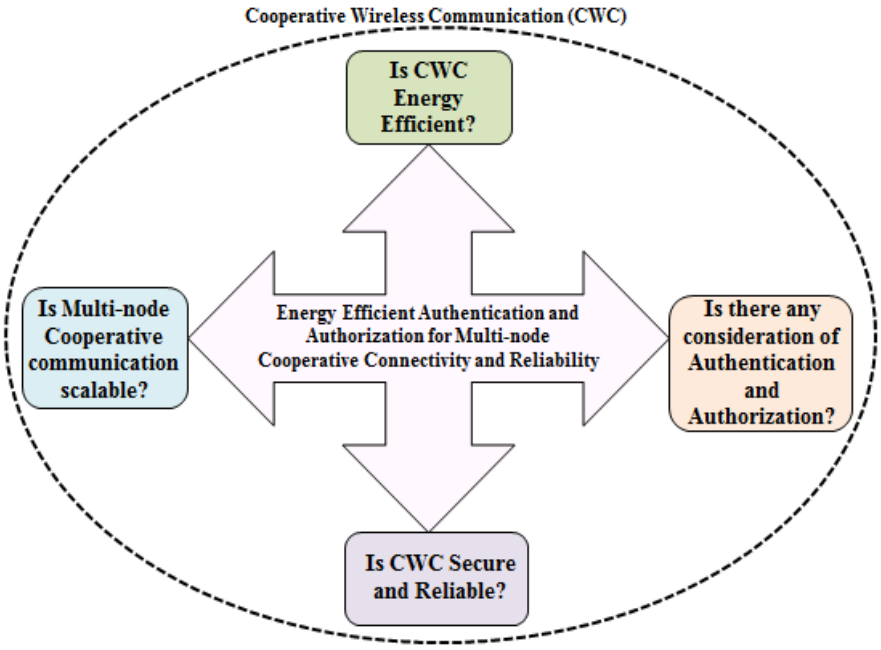

Figure 1.11 – Problem Statement and Research Objectives

1.7 Novelty and Contributions

This PhD study contributes to solving the challenges listed in Section 1.5 by proposing novel methods applicable in the area of cooperative wireless communication and Figure 1.12 provides an overview of the contributions presented in this thesis.

The first contribution of the thesis is the extension of the opportunistic large array approach in the direction of achieving energy efficiency and scalability for resource constrained networks like cognitive radio networks and wireless sensor networks. Also, the basic OLA work is extended for the malicious behaviour detection in the cooperative IoT scenario which is the second contribution of the thesis. As a third contribution, analysis of the cooperative OLA approach is carried out for QoS parameters like throughput, delay and energy consumption. For this, the basic work is extended with actual cooperative scenario building with network simulator version 2.

The next contribution is the novel concept of cooperative web of trust for the cognitive radio networks. The authentication and authorization techniques are developed on the basis of trust levels achieved by the individual radio nodes in the network. With trust levels, role based access control is used for developing authorization mechanism. Primary user emulation attack in CRN is taken into consideration while designing the security technique. Since the cryptographic techniques are found to be energy consuming, the next contribution aims towards physical layer security for further energy efficiency and reliability.

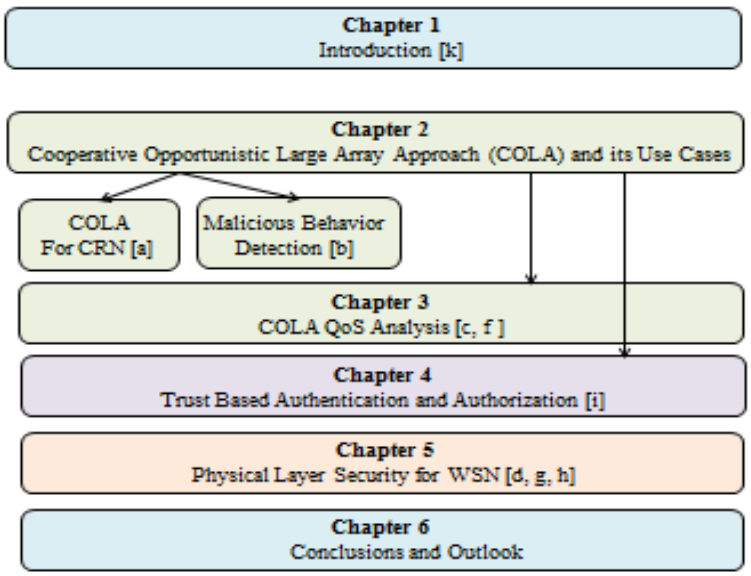

Figure 1.12 – Overview of contributions and correlation of thesis chapters

The last contribution is also the innovative work which combines information theoretic security with cooperative jamming technique to improve the secrecy capacity of the main channel as compared to the eavesdropper's channel. Information source and channel coding techniques are employed to achieve

reliability combined with security. Mutual information in between source, receiver and eavesdropper are analysed by building a total functioning communication link with Matlab.

The contributions have been, or are in the process of being, validated through peer-review and publication in journals and conference proceedings. The relevant publications are:

Conference Papers

a - Vandana Rohokale, Nandkumar Kulkarni, Horia Cornean, Neeli Prasad, "Cooperative Opportunistic Large Array Approach for Cognitive Radio Networks", 8th IEEE International Conference on Communications, Bucharest, Romania, pp.513-516, June 2010. (Published)

b - Vandana Rohokale, Neeli Prasad, "Receiver Sensitivity in Opportunistic Cooperative Internet of Things (IoT)", Second International Conference on Ad Hoc Networks, Victoria, British Columbia, Canada, pp. 160-167, August 2010. (Published)

c - Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring and Control", Wireless Vitae 2011, 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, Chennai, India, pp. 1-6, Feb-Mar 2011. (Published)

d - Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Jamming for Physical Layer Security in Wireless Sensor Networks", Proceedings of 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, pp.455-459, Sept 24-27, 2012. (Published)

Journal Papers

e - Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Wireless Communications and Physical Layer Security: State of the Art", Journal of Cyber Security and Mobility", Vol.1, pp. 227-249, 2012. (Published)

f - Vandana Rohokale, Sandeep Inamdar, Neeli Prasad, Ramjee Prasad," Energy Efficient Four Level Cooperative Opportunistic Communication for Wireless Personal Area Networks (WPAN)", Springer Journal of Wireless Personal Communications, Vol. 69, Issue 3, pp. 1087-1096, April 2013. (Published)

g - Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Reliable and Secure Cooperative Communication for Wireless Sensor Networks Making Use of Cooperative Jamming with Physical Layer Security", Springer Journal of Wireless Personal Communication, 2013. (Published Online)

h - Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Jamming for Physical Layer Security in Wireless Sensor Networks", Wireless Personal Communication Journal of Springer Verlag, 2013. (Accepted)

i - Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Web of Trust for Security in Cognitive Radio Networks", Journal of Mobility and Cyber Security, 2013. (Accepted)

Book Chapters

j **-** Vandana Rohokale, Rajeev Prasad, Neeli Prasad, Ramjee Prasad," Interoperability, Standardisation, Governance in the era of Internet of Things (IoT)", River Publications, European Commission Cluster Book 2011, Edited by Ovidiu Vermesan and Peter Friess, pp. 257-28.(Published)

k- Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Information Theoretic Security for Cooperative Communication", River Publications, Internet of Things and M2M Communications Book, 2013, Edited by Dr. Fabrice Theoleyre and Pr. Ai-Chun Pang, pp. 161-181. (Published)

1.8 Thesis Outline

The following section provides an outline of the thesis with a brief description of the individual chapters.

Chapter 2: Cooperative Opportunistic Large Array Approach and its Use cases

This chapter presents a cooperative opportunistic large array (COLA) approach which is the extension of basic OLA approach. The main difference in between these two approaches is that the basic OLA approach was designed for infinite coverage concept. But the COLA is designed for the limited coverage networks like CRN and WSN. With some extension work, this COLA approach is applied to two different use cases like spectrum sensing in cognitive radio networks and malicious behaviour detection in cooperative IoT [31, 32].

Chapter 3: Cooperative OLA QoS Analysis

Cooperative OLA approach is analyzed for QoS parameters such as energy, throughput and delay. Cooperative OLA scenario is built with simulation platform with four cooperation levels to cover larger area. Initially COLA is built with hundreds of network nodes into consideration. But for the experimental convenience, later we have built the same scenario with few network entities and four cooperation levels [33, 36, 40]. The reason for increasing cooperation levels was to check network performance for more cooperative relay levels.

Chapter 4: Trust Based Authentication and Authorization for COLA

Innovative cooperative web of trust (CWoT) is proposed and analysed in this chapter. Authentication and authorization techniques are built based on the trust levels acquired by the radio node with its previous behaviour. Received signal strength and energy consumption parameters are analysed with and without

cooperation [39]. Primary user emulation attack is taken into consideration for analysis of the proposed security techniques.

Chapter 5: Physical Layer Security for Wireless Sensor Networks

The new concept with the combination of information theoretic security and cooperative jamming is proposed and analyzed in this chapter. Information theoretic source and channel coding techniques with modulation are used to develop a full functioning communication link. Then the mutual information and secrecy capacities of source, receiver and eavesdropper are analyzed [34, 37, 38, and 41]. Authentication and authorization mechanisms built with the combination of cryptographic techniques proposed in chapter 4 are found to be somewhat more energy consuming. Physical layer techniques are proposed here for the further saving in the consumption of network resources.

Chapter 6: Conclusions and Outlook

This chapter provides the summary of the overall thesis and discusses future research scope.

1.9 Conclusions

After taking a glance on the literature review, it is clear that there are certain issues, which are untouched by the research community till date as mentioned below.

- For cooperative communication, many issues are taken into consideration by the researchers including throughput, delay, energy efficiency etc. But the less attention is paid towards energy efficient security solutions.
- The readily available solutions from cellular or Wi-Fi techniques cannot be directly applied to wireless sensor networks and cognitive radio networks.
- The security techniques based on traditional cryptographic techniques demand considerable energy consumption due to key generation and management techniques.
- Also, wireless physical layer security with information theoretic aspects is least attended issue in the literature.

References

[1] Katiyar H., Rastogi A., Agarwal R., " Cooperative Communication: A Review", IETE Tech Review 2011; vol. 28, pp. 409-417.

[2] E.C. van der Mullen, "Three-terminal communication channels", in Advances in Applied Probability, vol. 3, 1971, pp. 120-154.

[3] T. M. Cover and A. A. E. Gamal, "Capacity Theorems for the relay channel", IEEE Transactions on Information Theory, vol. 25, no. 5, pp. 572-584, Sept 1979.

[4] R. Gallager, "Communications and Cryptography: Two Sides of One Tapestry", Series in Engineering and Computer Science, Kluwer, 1994.

[5] J. Nicholas Laneman, David N. C. Tse, Gregory W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior", IEEE Transactions on Information Theory, vol. 50, no. 12, December 2004, pp. 3062-3080.

[6] Anna Scaglione, Dennis L. Goeckel and J. Nicholas Laneman, "Cooperative Communications in Mobile Ad Hoc Networks: Rethinking Link Abstraction", IEEE Signal Processing Magazine, September 2006, pp. 18-29.

[7] Shivendra S. Panwar, Pei Liu and Zhifeng Tao, "Cooperative Wireless Communications", US Patent No. US 7,330,457 B2, Feb 2008.

[8] Federico Albiero, Maros Katz, Frank H.P. Fitzek, "Energy Efficient Cooperative Techniques for Multimedia Services over Future Wireless Networks", IEEE International Conference on Communications ICC 2008, May 2008, pp. 2006-2011.

[9] A. G. Kanatas, A. Kalis and G. P. Efthymoglou, "A Single Hop Architecture Exploiting Cooperative Beam Forming for Wireless Sensor Networks", Physical Communications, vol. 4, issue 3, September 2011, pp. 237-243.

[10] S. Chatzinotas and B. Ottersten, "Free Probability Based Capacity Calculation of Multi antenna Gaussian Fading Channels with co-channel interference", Physical Communications, vol. 4, issue 3, September 2011, pp. 206-217.

[11] Hassanzadeh, A., Stoleru, R., "Towards Optimal Monitoring in Cooperative IDS for Resource Constrained Wireless Networks", 20th International Conference on Computer Communications and Networks (ICCCN), 2011, pp. 1-8.

[12] Dieter Duyck, Daniele Capirone, Michael Heindlmaier, Marc Moeneclaey, "Towards full-diversity joint network-channel coding for large networks", European Wireless 2011, April 27-29, 2011, Vienna, Austria, pp. 554-561.

[13] Sushant Sharma, Yi Shi, Jia Liu, Y. Thomas Hou, Sastry Kompella, and Scott F.Midkiff, "Network Coding in Cooperative Communications: Friend or Foe?" , IEEE Transactions on Mobile Computing, vol. 11, no. 7, July 2012, pp. 1073-1085.

[14] Misha Dohler, Yonghui Li, " Cooperative communications Hardware, Channel and Phy", John Wiley and Sons Ltd. Publication, 2010.

[15] A. Saleh, A. Rustako, and R. Roman, "Distributed Antennas for Indoor Radio Communications," IEEE Trans. Commun.,vol. 35, no. 12, Dec 1987, pp:1245–51.

[16] Qian Li, Hu, R.Q. , Yi Qian, Geng Wu,"Cooperative Wireless Communications

for Wireless Networks: Techniques and Applications in LTE-Advanced Systems", IEEE Wireless Communications, vol.19, Issue. 02, pp. 22-29, April 2012.

[17] WANG Hui Ming and XIA Xiang Gen, "Asynchronous Cooperative communication systems: A survey on signal Designs" Science China Information Sciences, vol. 54, Issue. 08, pp. 1547–1561, August 2011.

[18] Chen Yongrui, Yang Yang, Yi Weidong," A cross layer strategy for cooperative diversity in wireless sensor networks", Journal of Electronics, China, vol. 29, Issue.1/2, pp. 203-208, March 2012.

[19] Vandana Rohoakale, Neeli Prasad, "Receiver Sensitivity in Opportunistic Cooperative Internet of Things (IoT)", Second International Conference on Ad Hoc Networks, pp.160-167, August 2010, Victoria,British Columbia, Canada.

[20] Chao Chen, Baoyu Zheng, Xianjing Zhao, Zhenya Yan, "A Novel Weighted Cooperative Routing Algorithm Based on Distributed Relay Selection" 2nd International Symposium on Wireless Pervasive Computing, 2007, ISWPC '07, pp. 224-229.

[21] Lun Dong, Athina P. Petropulu, H. Vincent Poor, "Cross-Layer Cooperative Beamforming for Wireless Networks", Cooperative Communication for Improved Wireless Network Transmission-IGI Global, pp. 1132-1138, 2010.

[22] K. J. Ray Liu, Ahmed K. Sadek, Weifeng Su and Anders Kwasinski, "Relay Channels and Protocols", Cooperative Communication and Networking, Cambridge University Press, 2009.

[23] S. Abdulhadi, M. Jaseemuddin, A. Anpalagan, "A Survey of Distributed Relay Selection Schemes in Cooperative Wireless Ad hoc Networks", Wireless Personal Communications, vol. 63, pp. 917–935, 2012.

[24] A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation – part i: System Description, part ii: Implmentation Aspects and Performance Analysis," IEEE Transactions on Communication, vol. 51, no. 11, pp.1927– 48, Nov. 2003.

[25] J. N. Laneman, D. Tse, and G. W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behaviour," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3063 80, Dec. 2004.

[26] Ahmed K. Sadek, Weifeng Su and K.J.Ray Liu," Multinode Cooperative Communications In Wireless Networks", IEEE Transactions on Signal Processing, Volume 55, Issue 1, pp. 341-355, January 2007.

[27] Anna Scaglione and Yao-Win Hong, "Opportunistic Large arrays: Cooperative Transmission in Wireless Multihop Ad-Hoc Networks to Reach Far Distances", IEEE Transactions on Signal Processing, vol.51, no.8, pp. 2082-2092, August 2003.

[28] Arvind Kailas and Mary Ann Ingram," Alternating Opportunistic Large arrays in Broadcasting for Network Lifetime Extension", IEEE Transactions on Wireless Communication, vol. 8, no. 6, pp. 2831-2835, June 2009.

[29] Y. W. Hong and A. Scaglione, "Energy-efficient broadcasting with cooperative transmissions in Wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 5, no. 10, pp. 2844–55, Oct. 2006.

[30] Lakshmi V. Thanayankizil, Aravind Kailas, Mary Ann Ingram, "Energy-Efficient Strategies for Cooperative Communications in Wireless Sensor Networks," sensorcomm, 20th International Conference on Sensor Technologies and Applications (SENSORCOMM 2007), pp.541-546, 2007.

[31] Vandana Rohokale, Nandkumar Kulkarni, Horia Cornean, Neeli Prasad, "Cooperative *Opportunistic* Large Array Approach for Cognitive Radio Networks", 8th IEEE International Conference on Communications, Bucharest, Romania, pp. 513-516, June 2010.

[32] Vandana Rohokale, Neeli Prasad, "Receiver Sensitivity in Opportunistic Cooperative Internet of Things (IoT)", Second International Conference on Ad Hoc Networks, Victoria, British Columbia, Canada, pp. 160-167, August 2010.

[33] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring and Control", Wireless Vitae 2011, 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, Chennai, India, pp. 1-6, Feb-Mar 2011.

[34] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Jamming for Physical Layer Security in Wireless Sensor Networks", Proceedings of 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, pp.455-459, Sept 24-27, 2012.

[35] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Wireless Communications and Physical Layer Security: State of the Art", Journal of Cyber Security and Mobility", Vol.1, pp. 227-249, 2012.

[36] Vandana Rohokale, Sandeep Inamdar, Neeli Prasad, Ramjee Prasad," Energy Efficient Four Level Cooperative Opportunistic Communication for Wireless Personal Area Networks (WPAN)", Springer Journal of Wireless Personal Communications, Volume 69, Issue 3, pp. 1087-1096, April 2013.

[37] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Reliable and Secure Cooperative Communication for Wireless Sensor Networks Making Use of Cooperative Jamming with Physical Layer Security", Springer Journal of Wireless Personal Communication, 2013. (Published Online)

[38] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Jamming for Physical Layer Security in Wireless Sensor Networks", Wireless Personal Communication Journal of Springer Verlag, 2012. (Accepted)

[39] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Web of Trust for Security in Cognitive Radio Networks", Journal of Mobility and Cyber Security, 2013. (Accepted)

[40] Vandana Rohokale, Rajeev Prasad, Neeli Prasad, Ramjee Prasad," Interoperability, Standardisation, Governance in the era of Internet of Things (IoT)", River Publications, European Commission Cluster Book 2011, Edited by Ovidiu Vermesan and Peter Friess, pp. 257-285.

[41] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Information Theoretic Security for Cooperative Communication", River Publications, Internet of Things and M2M Communications Book, 2013, Edited by Dr. Fabrice Theoleyre and Pr. Ai-Chun Pang, pp. 161-181.

2

Cooperative Opportunistic Large Array (COLA) Approach and its Use Cases

The goal of this chapter is to present a cooperative opportunistic large array (COLA) approach which is the extension of basic OLA technique. The main difference in between these two approaches is that the basic OLA approach was designed for infinite or very large coverage concept. But the proposed COLA mechanism is designed for limited coverage networks like CRN and WSN. With some extension work, this COLA approach is applied to two different use cases like spectrum sensing in cognitive radio networks and malicious behaviour detection in cooperative IoT.

2.1 Introduction

The opportunistic large array approach for cooperative wireless communication is studied and applied for two different use cases namely spectrum sensing in cognitive radio networks and malicious behaviour detection in the cooperative IoT. In the data transmission phase, decode and forward relaying mechanism is considered. Here, the equations for the coverage radius and critical network density are modified for the limited broadcast coverage of the wireless sensor networks. Also the new equations are derived for the fraction of energy savings with the cooperative OLA approach and receiver sensitivity for intrusion detection. Equation for the fraction of energy savings (FES) is developed based on the network entities taking part in the actual cooperative communication out of many relays present in the vicinity of the system.

2.2 Proposed System Model for COLA

For cooperative transmission, OLA selects the nodes which has the received signal SNR above some threshold figure and since the resonance generated by relay nodes carries the actual messages to the desired sinks without causing interference. For the reduction in the routing and multiple access overheads, OLA is a competent physical layer broadcasting algorithm. Multiple clusters of ad hoc wireless nodes can form a multi-OLA system, constructing a multiple access system with the cluster of nodes acting as a team through cooperative transmission rather than transmitting independent data from each node. OLAs can either be with regenerative or non- regenerative based on the use of selective decode and forward cooperative technique. OLA utilizes the cooperative transmission of the Ad Hoc network nodes to reach back a far distant node or sink. OLA can apply either to existing or newly designed modulation techniques that exploit the positioning diversity of the ad hoc radio nodes. OLA can also be easily built on top of any existing ad hoc systems without changing their original structure [1, 2].

The consumer radio devices which are half-duplex in nature are assumed to be uniformly and randomly distributed over a continuous area with average density ρ. The deterministic model is assumed, which means that the power received at a Consumer Premise Equipment (CPE) is the sums of powers form each of the CPE. In this model, the network node transmissions are orthogonal to each other network node transmissions. The orthogonality is approximated with direct sequence spread spectrum (DSSS) modulation and RAKE receiver. Also the nodes can delay their transmissions by a random number of chips. It is assumed that a CPE can decode and forward a message without error when it's Signal to Noise ratio

(SNR) is greater than or equal to modulation-dependent threshold λ [1]. Due to noise variance assumption of unity, SNR criterion is transformed into received power criteria and λ becomes a power threshold. Let P_s be the source transmit power and the relay transmit power be denoted by P_r, and the relay transmit power per unit area be denoted by $\overline{P}_r = \rho P_r$. The assumed continuum model is as shown in Figure 2.1 below. In this figure, the node which is at the far distance form source is considered and it is out of coverage area indicated by circle boundary for very large radius coverage implication. Another limited radius node is shown inside the circle.

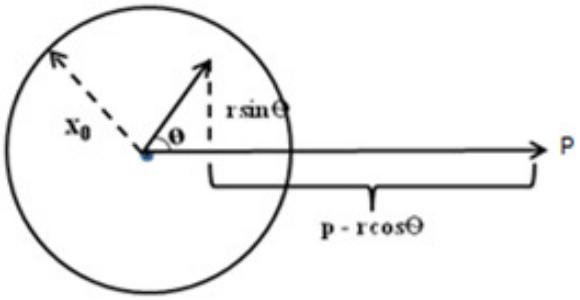

Figure 2.1- Illustration of path loss model $f(x_0, p)$

Suppose that every transmission with power P is received with power $P.l(d) = P/d^2$ at distance d, where $l(.)$ is a path loss attenuation function, which in general is assumed to be continuous and non-increasing. Path loss exponent is assumed to be 2. The squared path loss function in Cartesian coordinates is written as $l(x, y) = (x^2 + y^2)^{-1}$ where x, y are the normalized coordinates at the receiver. For the ease of presentation, a bounded network is assumed. The aggregate path loss from a circular disc of radius x_0 at an arbitrary distance $p > x_0$ from the source is given by,

$$f(x_0, p) = \int_0^{x0} \int_0^{2\pi} l(p - r\cos(\theta), r\sin(\theta))\, r dr d\theta \text{ ------- (2.1)}$$

$$= \pi \ln \frac{p^2}{|p^2 - x_0^2|}$$

Let $r_0, r_1, \ldots\ldots$ denote the solution of the recursive formula.

$$f(r_{k-1}, r_k) - f(r_{k-2}, r_k) = \frac{\lambda}{\overline{P}_r}, \quad k = 2,3,4 \text{ -------- (2.2)}$$

with initial conditions r_0=0, and $r_1 = l^{(-1)}(\frac{\lambda}{\overline{P}_r})$. If the solution of above equation exists then each level set is a disk shaped region with inner and outer radii given by r_{k-1} and r_k respectively. Hence $\overline{P}_r [f(r_{k-1}, r_k) - f(r_{k-2}, r_k)]$ is the received power at a node with distance r_k from the source, when the disc between r_{k-2} and r_{k-1} transmits.

Theorem: If $\mu = \text{detection threshold} \triangleq e^{(\lambda/\pi\rho P_r)}$ [2] and $\mu > 2$,

Then

$$r_k = \sqrt{\frac{P_S(\mu-1)}{\lambda(\mu-2)}}\left(1-\frac{1}{(\mu-1)^k}\right) \text{ --------- (2.3)}$$

$$\text{and } \lim_{k\to\infty} r_k = r_\infty = \sqrt{\frac{P_S(\mu-1)}{\lambda(\mu-2)}} \text{ -------- (2.4)}$$

For ($\mu \leq 2$), the broadcast reaches to the whole network i.e. $lim_{k\to\infty} r_k = \infty$. For ($\mu > 2$), the total area reached by the broadcast is limited i.e. $r_k < r_{total}$. Instead of infinite radius, we are considering some practical scenarios where the radius is limited.

For wireless LAN, the maximum radius covered is found to be approximately 100 meters. The cellular coverage areas for different cell structures are as follows:

1. Pico cells: 100m x 100m
2. Micro cells: 1000m x 1000m
3. Macro cells: Up to several kilometres.

Minimum node density requirement for particular transmission is obtained with the help of following equations.

$$\text{For } \mu > 2, \frac{\lambda}{\rho P_r \pi} > \ln 2 \text{ ---------- (2.5)}$$

$$\rho < \frac{\lambda}{\ln 2 P_r \pi} \text{ ---------- (2.6)}$$

$$\text{Also, } r_\infty = \sqrt{\frac{P_s(e^{\frac{\lambda}{\rho P_r \pi}}-1)}{\lambda(e^{\frac{\lambda}{\rho P_r \pi}}-2)}} = \frac{N_{\max}}{\pi r_{\max}^2} = \rho_{\max} \text{ -------- (2.7)}$$

$$r^2 = \frac{P_s(\mu-1)}{\lambda(\mu-2)} \text{ ------- (2.8)}$$

$$\lambda r^2\mu - 2\lambda r^2 = P_s\mu - P_s \text{ -------- (2.9)}$$

$$(\lambda r^2 - P_s)\mu = 2\lambda r^2 - P_s \text{ ------- (2.10)}$$

Then the detection threshold μ is given by,

$$\mu = \frac{2\lambda r^2 - P_s}{\lambda r^2 - P_s} \text{ ------- (2.11)}$$

Similarly, we can write,

$$\frac{\lambda}{\rho P_r \pi} = \frac{2\lambda r^2 - P_s}{\lambda r^2 - P_s} \text{ -------- (2.12)}$$

Now we can write equation for node density as below.

$$\rho = \frac{\lambda}{P_r \pi} \frac{1}{\ln(\frac{2\lambda_r^2 - P_S}{\lambda r^2 - P_s})} \text{ ---------- (2.13)}$$

Then to find out total number of network entities present in the network,

$$\frac{\lambda}{\rho P_r \pi} > ln2\rho < \frac{\lambda}{\pi(ln2)P_r}$$

$$\frac{N_{total}}{\pi r_{total}^2} \geq \frac{\lambda}{\pi(ln2)P_r} \text{ ---------- (2.14)}$$

Where N_{total} is the maximum number of active nodes utilized for particular cooperative transmission for the radius r_{total} as shown in Figure 2.2 below.

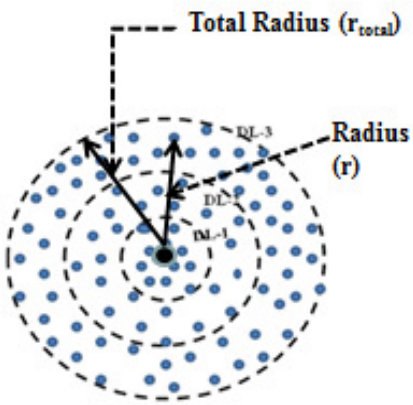

Figure 2.2 - Proposed OLA structure for Numerical Analysis

Also for (μ > 2), from eq. (2.3), the critical density could be obtained as follows,

$$\rho_{critical} = \frac{\lambda}{P_r \pi \ln(\frac{2\lambda r^2 - P_S}{\lambda r^2 - P_S})} \text{ ---------- (2.15)}$$

If the network's active node density ρ is smaller than $\rho_{critical}$ then the signal transmitted from source will not reach to the destination receiver. Out of total radio nodes, the radio nodes utilized for particular cooperative transmission can be calculated with the help of plot in between total nodes in the radio network (N) and radius till that level (*r*). The Fraction of Energy Saving (FES) with the OLA approach can be written as a ratio of

$$\text{FES} = 1 - \frac{\substack{number\ of\ active\ radio\ nodes\ utilized \\ for\ cooperative\ transmission}}{\substack{Total\ number\ of\ nodes \\ in\ the\ OLA\ network}} \text{ ---------- (2.16)}$$

Depending on the active radio nodes taking part in the cooperative transmission, the energy savings equation is derived based on selective decode and forward technique. The relay node which has the SNR more than or equal the threshold value can only take part in the further cooperative transmission.

2.3 Use Case 1 – Spectrum Sensing in Cognitive Radio Networks

The emergence of new wireless technologies has created huge demand of radio spectrum. The radio spectrum is a scarce natural resource. Due to the limitations of radio spectrum it becomes obvious that the present fixed frequency allocation schemes cannot accommodate the new emerging multimedia technologies. The actual measurement of radio spectrum utilization clearly shows that the licensed radio spectrum is underutilized continuously across time and space [3]. As a result innovative techniques which can offer new approaches of exploiting the available radio spectrum are needed. Cognitive Radio (CR) seems to be a promising solution to the radio spectrum congestion problem by opportunistic uses of the spectral holes [4]. The cooperative wireless communication (CWC) concept is more applicable to wireless sensor networks and Cognitive ad-hoc networks than that of cellular networks due to scalable nature of these networks.

For improvement in the QoS of CRN, CWC approach may be applied. There are two main cooperative approaches towards CR viz. Commons Model and Property Rights Model. In commons model, primary terminals are unaware about the presence of secondary users, thus behaving as if no secondary activity was present. Instead, secondary users sense the radio environment for finding out spectrum holes and then take advantage of the detected transmission opportunities. For the property rights model, the primary nodes may accept to lease their bandwidth for a fraction of time, in exchange for the concession, they benefit from the superior QoS in terms of rate of outage probability and improvement in energy savings [5] [6]. Cooperative relaying of primary packets through secondary nodes is proved to be a promising technique to improve the secondary throughput by utilizing the idle periods of the primary nodes.

An opportunistic large array (OLA) is a group of forwarding nodes that operate without any mutual coordination, but naturally fire together in response received from a single source or other OLA. These OLAs do not need location information for routing. Due to the assumption of perfect channel state information (CSI) at each node, there is no need of addressing due to which the protocol becomes scalable with maximum node density. Not needing location knowledge for routing makes the protocol suitable for

applications where location information is either not available or too expensive or energy consuming to exploit [7]. With the help of OLAs, the cognitive network can be built without GPS.

A cognitive radio adapts its services according to the changes in its surrounding, due to which, spectrum sensing has become an important requirement for the realization of CR networks [8]. The major necessary functionalities for spectrum sensing in cognitive radio ad hoc networks are as follows:

- Primary User (PU) Detection: the CR node continuously monitors and analyses its local radio environment, for determining holes in the spectrum.
- Cooperation: the observed information in each CR node is exchanged with its neighbouring network nodes for the improvement in sensing accuracy in case of hidden node problems.
- Sensing control: it enables each CR node to perform its sensing operations adaptively to the dynamic radio environment. Also, it coordinates the sensing operations of the CR nodes and its neighbours in a distributed manner, which prevents false alarms in cooperative sensing.

2.3.1 Proposed COLA Model for Spectrum Sensing in CRN

Opportunistic Large Array (OLA) is nothing but a cluster of network nodes which use active scattering mechanism in response to the signal of the source. The intermediate nodes opportunistically relay the messages from the leader to the sink. Either secondary users or combination of primary as well as secondary users can form OLAs for the good coordination among network entities. The proposed COLA approach for CRNs is as shown in Figure 2.3 below.

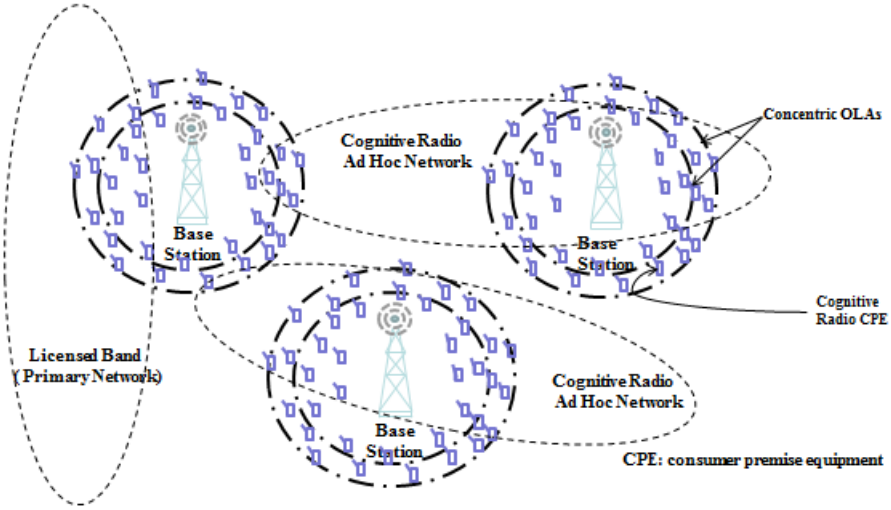

Figure 2.3 - Cooperative OLA for CRNs

Cognitive relaying concept is employed through the cooperative OLA model, in which cooperative relaying of primary traffic takes place through secondary users. In this scenario, supporting the primary traffic to increase its throughput results in a decreased transmission time of the primary, which in turn leads to more transmission opportunities for the secondary. As shown in figure 2.3, the secondary users form the OLA structure and cooperate each other in data transmission as well as information sharing. As soon as primary user gets back to use the network resources, the secondary users immediately pass this information to other nodes and find out the spectrum hole for the secondary user to continue the data transmission. For cooperative transmission, OLA selects the nodes which has the received signal SNR above some threshold figure and since the resonance generated by relay nodes carries the actual messages to the desired sinks without causing interference.

2.3.2 Performance Evaluation of Use Case - 1

As observed from Figure 2.4, for lower threshold values like lambda (SNR threshold) = 0.5, maximum energy savings of 85% are observed. Also for threshold values of lambda=1.5, considerable energy savings are observed. For this case, the FES value is observed to be around 57% which is higher than non-cooperative systems like multihop communication. Less value of SNR threshold is indication of participation of maximum number of nodes in the cooperation. If the lambda (SNR threshold) value is increased, then the number of nodes taking part in cooperative communication is less.

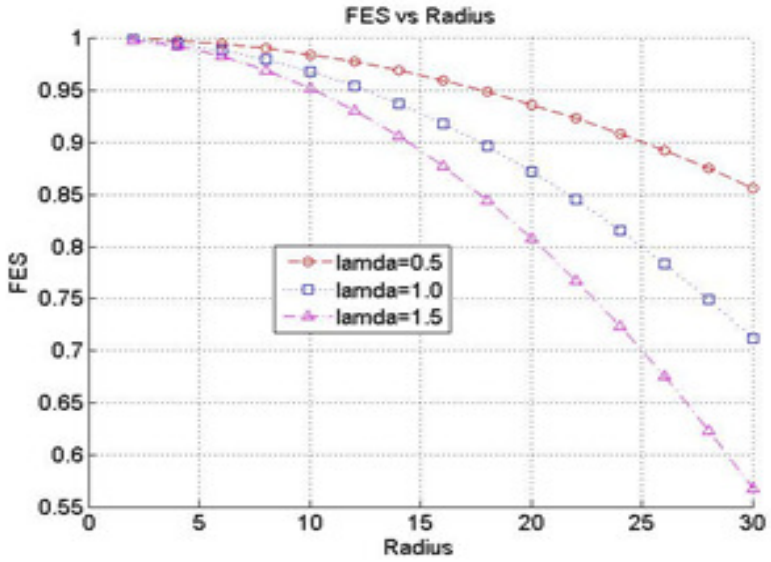

Figure 2.4 - Fraction of Energy Saving (FES) as a function of Radius and SNR threshold Lambda

From Figure 2.5, it is observed that after certain radius value, the network node density seems to be almost constant. This indicates that for particular node density, the broadcast beyond certain radius is meaningless. This is the indication of the restriction on cooperation levels and ultimately coverage radius in the network. Beyond 15 meters radius as shown in this figure, the node density remains constant indicating almost no cooperation after that.

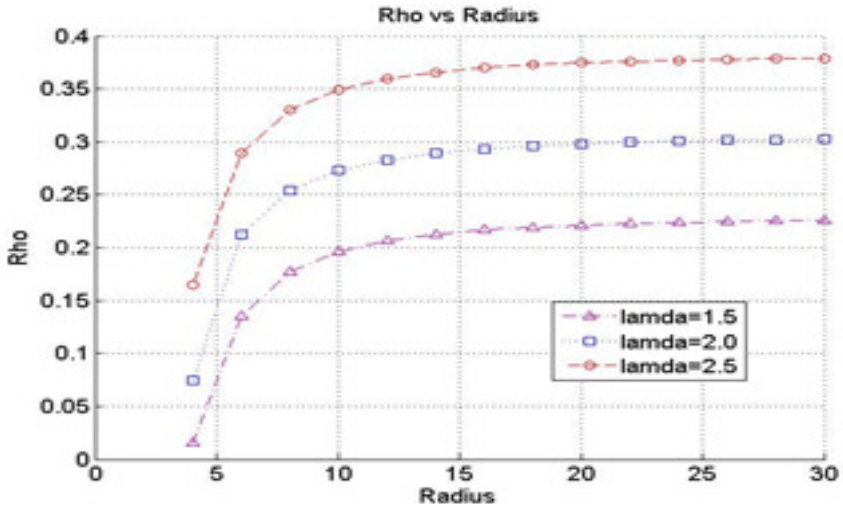

Figure 2.5 - Radio node density as a function of Radius and SNR threshold (Lambda)

For lower SNR threshold values, considerable energy savings are observed from Figure 2.6. Coverage extension is observed due to cooperation. For broadcast radius of 15 and threshold of 3, the energy savings observed is almost 68%. For less radius coverage, the energy savings is very high almost equal to 97% which ultimately means that there is very less or no cooperation at the low distances where the nodes can directly communicate with their respective receivers. The relationship between number of nodes participating for particular transmission and radius is interesting. From Figure 2.7, for threshold (Lambda)=0.5 and radius=30, the maximum node participation is around 400 to 420. For threshold (Lambda)=1.5 and radius=30, the maximum node participation is observed to be almost 1300. This indicates that cooperation requires large number of nodes in the network. For moderate radius values, cooperation gives good results.

This use case presents an energy-efficient opportunistic large array approach for CRNs. It seems to prove a promising solution for the spectrum sensing issues of secondary radio nodes in the CRNs. This kind of mechanism can be applied to cognitive applications like wireless LAN, cellular pico-cells in hot spot situations and Bluetooth. For limited radii broadcasting, the minimum energy consumption by the network has been achieved. Fraction of energy saving factor is observed to be 57% for the radius of 30 meters as compared to the traditional non-cooperative multi-hop communication techniques.

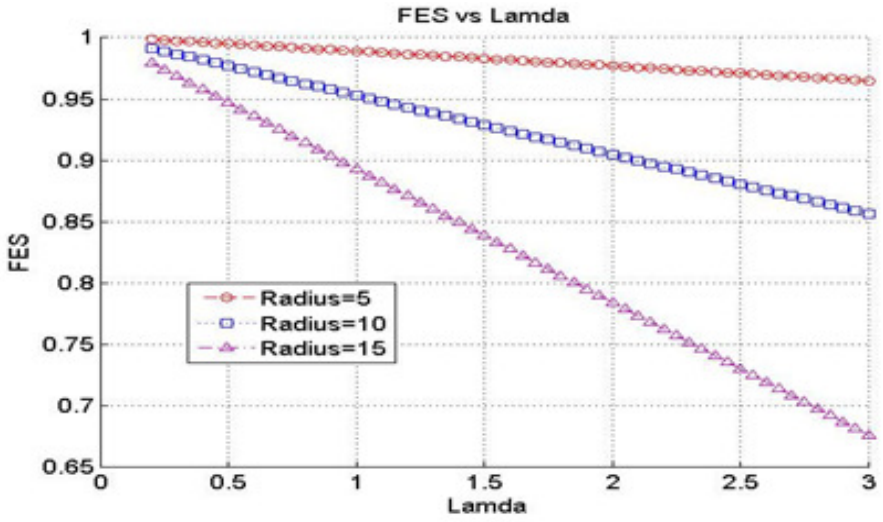

Figure 2.6 - Fraction of Energy Saving (FES) as a function of Lamda (Threshold) and Radius

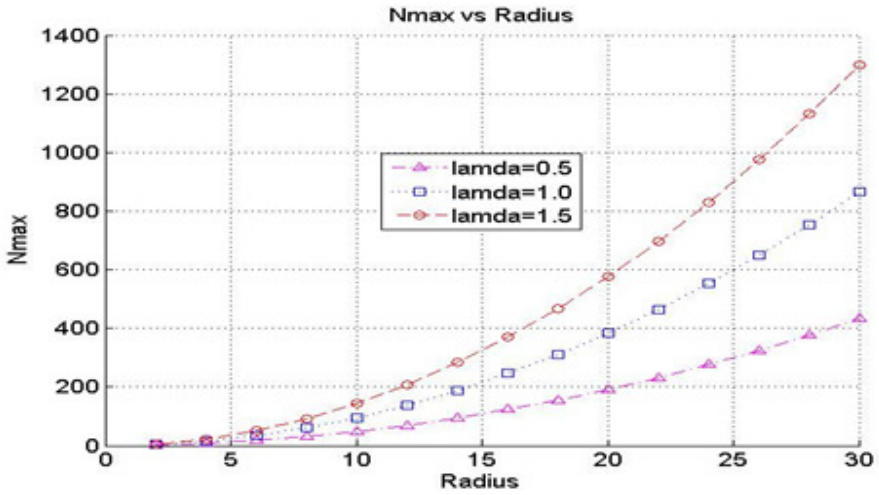

Figure 2.7 - Node participation in CWC as a function of Radius and SNR threshold

2.4 Use Case 2 – Cooperative IoT for Malicious Behavior Detection

In Cooperative communication, a source message is relayed through a locally connected network by means of cooperating network nodes. Recently, the cross layer cooperative schemes have been shown to offer multiple advantages over the single layer approaches at the cost of some overheads including security threats. In distributed cooperation schemes, the cooperating nodes make transmission decisions based on quality of the received signal, which is the only parameter available locally. Receiver sensitivity is the most important parameter of the physical layer and has a direct impact on the MAC layer. This case study

proposes a novel cooperative approach for analysis of receiver sensitivity and exploitation of receiver sensitivity statistics to detect the presence of malicious behavior in the cooperating systems.

The strength of the cooperative OLA approach is that it does not require GPS equipment for identification of the location of the network node entities. The energy savings achieved in WSNs are the result of cross-layer interactive cooperative communication. Routing functions are partially executed in the physical layer. The diversity provided by MIMO space-time codes can improve performance at the MAC, network and transport layers. Physical layer parameters such as modulation technique, transmit power, hop distance and receiver sensitivity significantly affect the MAC protocol. Choice of the medium access scheme is the important aspect of WSNs [9].

2.4.1 Proposed COLA System Model for Malicious Behaviour Detection

In order to maximize the information transfer among network nodes, the optimal receiver sensitivity is the prime requirement. The noise floor of a receiver determines its sensitivity to low-level signals and its capability of detecting and demodulating those signals. Cooperation allows independently faded radios to collectively achieve robustness to severe fades while keeping individual sensitivity levels of each intermediate receivers and actual receivers close to the nominal path loss. Furthermore, a small number of radios (10-20) are enough to achieve practical sensitivity levels [10]. The proposed cooperative IoT model is depicted in Figure 2.8. The nodes which are participating in particular communication are shown with solid fill.

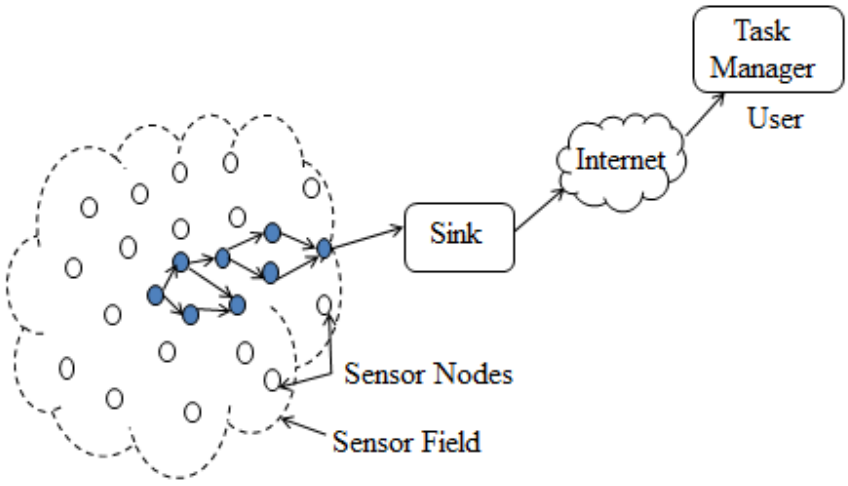

Figure 2.8 - Proposed Cooperative IoT model

The receiver sensitivity [11] is given by,

$$S_R = K\,(Ta+Trx)\,B\,(SNR) \quad [\text{mdB}] \qquad \text{---------- (2.8)}$$

where S_R = receiver sensitivity

K= Boltzman's constant

Ta=equivalent noise temperature in [k] of the source eg. antenna at the input of the receiver

Trx = equivalent noise temperature in [k] of the receiver referred to the input of the receiver

B = bandwidth

SNR = required SNR at the output

2.4.1 Performance Evaluation of Use Case - 2

The sensor coverage metric surveillance that is coverage radius is used as a measurement of the QoS provided by a certain sensor network [12]. From the plot of Figure 2.9, it is observed that for high QoS values, the network node requirement is high. But for low threshold values like SNR Threshold (Lambda)=0.4, the maximum number of node requirement is reduced to 600 for the range of 40 meters.

As seen from the plot of Figure 2.10, for moderate QoS (Coverage Radius) values, considerable energy savings are observed. For decoding SNR threshold (Lambda)=1.5, the energy savings of 75% is observed for the range of 40 meters. Figure 2.11 indicates that for high radius values, the sensitivity is considerably decreased. It indicates better sensitivity of the receiver for distant nodes. Lower power for a given SNR means better sensitivity. Radio devices that fail in unknown ways or may be malicious, introduce a bound on achievable sensitivity reductions [13].

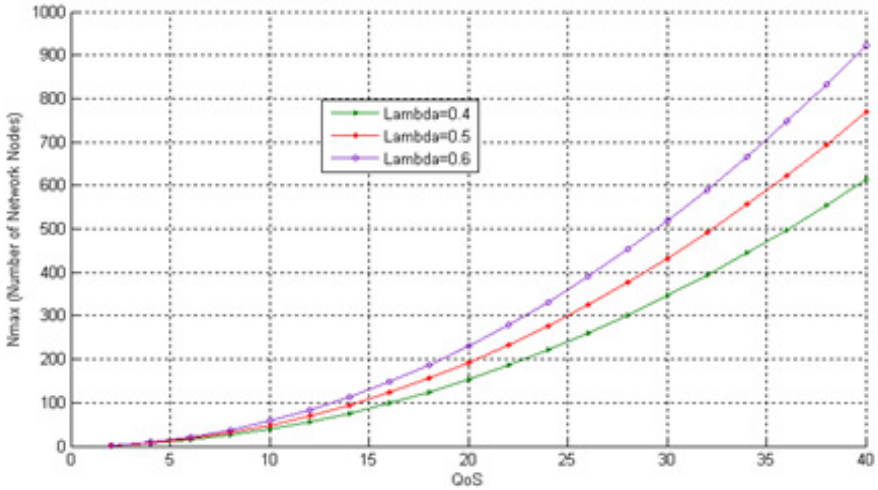

Figure 2.9 - Nmax versus QoS

The energy savings are considered on the basis of minimum number of nodes participating in a particular communication purpose out of the total deployed network nodes. As seen from Figure 2.11, for small radius, the sensitivity achieved is around -90 dBm, but for the higher values of radius, sensitivity reaches up to -62dBm.

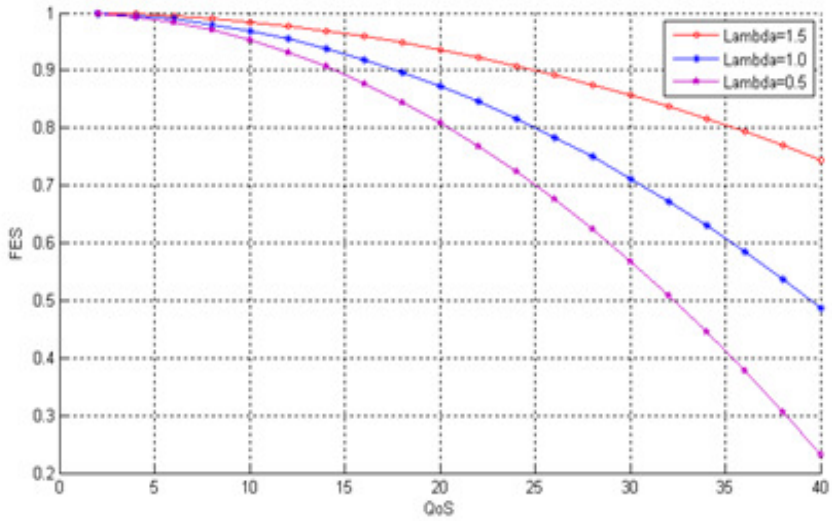

Figure 2.10 - FES versus QoS.

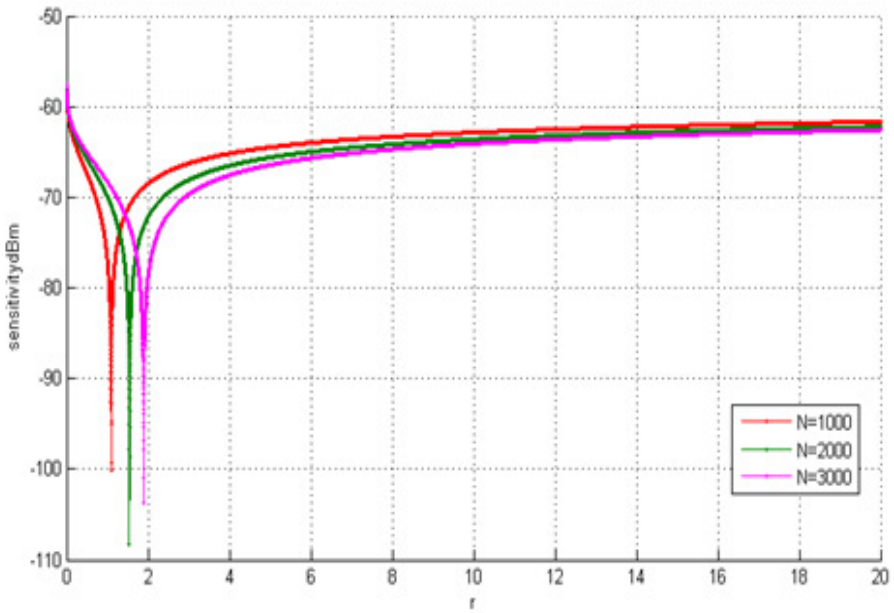

Figure 2.11 - Sensitivity versus radius.

When the channel condition is severely faded, then the receiver sensitivity values are going to get affected. Channel may suddenly get faded due to certain malicious action initiated by eavesdropper. For detection of malicious behavior in the communication system, periodic measurement of receiver sensitivity

values may be the better solution. Lesser sensitivity figures indicate good and robust system. But due to intruders entered in the system or severe channel fading, the sensitivity figures get changed considerably.

In this case study, the cooperative behaviour of WSNs is analysed. The observed high QoS values indicate that our proposed cooperative IoT model is highly reliable and scalable. For decoding threshold values of Lambda=1.5, the fraction of energy savings obtained is almost 75%. Since receive sensitivity indicates how faint an input signal can be successfully received by the receiver, the lower the power level, the better is the receiver. Better sensitivity figures are obtained for radius of up to 20 meters. For e.g, sensitivity achieved for 10 meters radius it is around -65dBm. In future works, these results may be extended for the nodes which are malicious or which fail in unknown ways.

2.5 Conclusions

- For first use case, the performance is evaluated by considering the fraction of energy savings parameter. FES equation is newly written by taking into consideration the active number of radio nodes communicating cooperatively with respect to the total number of radio nodes present in the OLA structure. The performance of the system is compared with the conventional non-cooperative multi-hop techniques.
- In the second use case, receiver sensitivity equation is newly developed for the intrusion detection purpose. In normal situation, the receiver sensitivity values are observed to stay in between -90 to -100 dBs. But when the malicious behavior is detected by the network, suddenly, sensitivity values rise by 30 dBs. And thereafter stays at the same value around -65 dBs.
- To the best of author's knowledge, the COLA mechanism has been firstly applied for spectrum sensing in CRN. Also, the application of receiver sensitivity for malicious behavior detection has been done firstly for the cooperative transmission.

References

[1] Anna Scaglione and Yao-Win Hong, "Opportunistic Large arrays: Cooperative Transmission in Wireless Multihop Ad-Hoc Networks to Reach Far Distances", IEEE Transactions on Signal Processing, vol.51, no.8, pp. 2082-2092, August 2003.

[2] L. Thanayankizil, A. Kailas, and M. A. Ingram, "A simple cooperative transmission protocol for efficient broadcasting over multi-hop wireless networks", KICS/IEEE Journal of Communications and Networks, vol.10, no.2, pp.213-220, June 2008.

[3] FCC, "Spectrum Policy Task Force Report (ET Docket no. 02-135)," Nov. 2002

[4] Mitola J., "Cognitive radio:making software radios more personal", IEEE Pers Commun,1999, vol. 6, Issue. 4, pp. 13-18.

[5] J. M. Peha, "Approaches to spectrum sharing", IEEE Communications Magazine, vol. 43, issue. 2, pp. 10–12, Feb. 2005.

[6] G. Faulhaber and D. Farber, "Spectrum management: Property rights, markets and the commons", in Proceedings of the Tele-communications Policy Research Conference, Oct. 2003, pp. 1-25.

[7] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran , Shantidev Mohanty," NeXt generation /dynamic spectrum access/cognitive radio wireless networks: A survey" I.F. Akyildiz et al./Computer Networks 50 (2006), pp. 2127–2159.

[8] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, Shantidev Mohanty," NeXt generation /dynamic spectrum access/cognitive radio wireless networks: A survey" I.F. Akyildiz et al. Computer Networks, 50 (2006), pp. 2127–2159.

[9] Ferrari, G. Tonguz, O.K. Bhatt, M. "Impact of receiver sensitivity on the performance of sensor networks" 59th IEEE Vehicular Technology Conference, 2004, pp. 1350-1354, VTC 2004-Spring. 2004.

[10] Birsen Sirkegi Mergen, Anna Scaglione, Gokhan Mergen, "Asymptotic analysis of multi-stage cooperative broadcast in wireless networks", 2004 International conference on Acoustics, Speech and Signal Processing, pp. 2531-2550.

[11] Matt Loy, "Understanding and Enhancing Sensitivity in Receivers for Wireless Applications", Technical Brief SWRA030, Texas Instruments, Digital Signal Processing Solutions, May 1999, pp. 1-77.

[12] Shridhar Mubaraq Mishra, Anant Sahai and Robert W. Brodersen," Cooperative Sensing among Cognitive Radios", IEEE International Conference on Communications, 2006. ICC '06, pp. 1658 – 1663.

[13] J. Pasley, "How BPEL and SOA are changing web services development", IEEE Internet Computing, vol.9, issue. (3) (2005), pp. 60–67.

3

Cooperative OLA QoS Analysis for IEEE 802.15.4 WPAN

The goal of this chapter is to present QoS analysis of the cooperative opportunistic large array (COLA) approach. The performance of wireless network mainly depends on the QoS parameters like throughput, end to end delay and energy consumption. In this chapter we are going to present the simulation scenario of cooperative OLA network with Network Simulator version 2. In this work, the cooperative OLA approach is applied for IEEE 802.15.4 WPAN networks and network performance is analysed through QoS parameters with simulation platform.

3.1 Introduction

To establish a real time wireless communication network scenario is really difficult. Development of test beds is a time consuming and costly affair. Simulators are helpful for the developer to check the real time performance of the system. Due to the use of simulators, both time and cost are saved with the ease of implementation [1]. Initially the cooperative scenario for 425 wireless sensor nodes is simulated with the help of network simulator version 2 and the system performance is studied for the QoS parameters like throughput, delay and energy consumption. After that the cooperative OLA scenario is built for IEEE 802.15.4 WPAN with 11 sensor nodes and four levels of cooperation. Due to limited battery resources, the energy consumption is the critical issue for the transmission as well as reception of the signals in the wireless communication. WSNs are infrastructure-less shared networks demanding more energy consumption due to collaborative transmissions. The concept of four levels of cooperation for data transmission from source to destinations proposed for improvement in the network coverage with energy efficiency.

3.2 Network Simulator Version 2 (NS2)

Network simulator is an object oriented discrete event simulator mainly developed for wired and wireless networking research community. It supports development of simulation scenario of TCP, routing, and multicast protocols. Network simulator version 1 was developed in 1995 by the Defense Advanced Research Project Agency (DARPA). DARPA also supported the network simulator version 2 (NS2) through the Virtual Inter-Network Testbed (VINT) project and released version 2 in 1996. Version 2 consists of a scripting language called Object Oriented Tcl (OTcl). It is an open source software package available for both Windows 32 and Linux platforms. NSF has taken initiatives in the direction of strong development of NS2 [2].

NS2 supports various protocols at the application layer, and mainly TCP and UDP at the transport layer and includes models for simulation of wired and wireless physical layers. Network simulation2 offers an implementation for the IEEE 802.11 protocol, regarding its wireless physical layer implementation. The main aim of recent research in the field of wireless communication and networks using ns 2 is to evaluate and understand the performance of new protocol and new wireless physical layer, which is obviously very important for many research groups. Since NS2 is an open source software and can be expanded in true sense while evaluating the performance of wireless protocols on a complex topology such as 802.11 in a

multi-hop scenario, our interest lies in cooperative MAC design in wireless networks and retransmission implementation.

CMU Monarch group is the main developer for the NS2 wireless networking support. The wireless node entity in NS2 is capable of computing its own position and velocity as a function of time which also follows the ISO Network Stack. Network layer is implemented in terms of a routing agent in the NS2. Data link layer contains medium access control (MAC) protocol and address resolution protocol (ARP). Physical layer consists of radio propagation model and radio interfaces with different adjustable parameters like transmission power and receiver sensitivity. All these layers are connected together in the NS2 wireless network node [3].

Creating wireless topology in NS2 is nothing but designing a mobile node which is the heart of the wireless model. Wireless model in NS2 essentially contains a mobile node with supporting features due to which the simulations of multi-hop adhoc networks, Wireless LANs, Wireless Sensor Networks etc. is possible. Mobile node is a basic node object with ability to move within a given topology and ability to receive and transmit signals to and from a wireless channel. There are five ad-hoc routing protocols which are supported by NS2 like Destination Sequence Distance Vector (DSDV), Dynamic Source Routing (DSR), Temporally ordered Routing Algorithm (TORA), Adhoc On-demand Distance Vector (AODV) and Protocol for Unified Multicasting Through Announcements (PUMA). In NS-2, physical layer makes use of Radio-propagation model, Propagation/ TwoRayGround. The proposed Coop-MAC algorithm is designed based on the widely adopted IEEE 802.11 MAC for practical simulations.

3.3 Related Work

In the research work of [4], a medium access control (MAC) algorithm is proposed which is named as Cooperative diversity MAC (CD-MAC). It makes use of cooperative diversity to ensure robust communication for wireless adhoc networks. The authors have analysed bit error rate (BER) and frame error rate (FER) performance for the cooperative scenario with the provision of relay selection mechanism. Distributed asynchronous cooperation based cross layered MAC (DSC-MAC) protocol is proposed in [5]. With this protocol, multiple relays can schedule parallel transmissions with packet level synchronization. The trade-off is observed in between enhancement in cooperative diversity gain with the deterioration in the multiplexing opportunities. This protocol is shown to improve throughput and delay performance of the simulated cooperative scenario.

WSNs support the wireless communication without any fixed infrastructure. In the work of [6], the authors have presented a new clustering based approach which makes use of the network node activity to lower the overall energy consumption by the network. The energy consumption utilized for data transmission is considered as a key performance measure for the location based topology control and power save mechanisms. The detailed comparison is illustrated in the Table 3.1 below.

Table 3.1 - Comparison of Energy conservation Protocols for WSN

Energy Conservation Protocol/Algorithm		**Characteristics**	**Energy Efficiency**
Location Based Topology Control [6]	R & M Protocol	Initially some energy is spent to build the topology.	Much more energy efficient for large size networks.
	Local Minimum Spanning Tree (LMST)		More energy consuming but the topology is more robust and preserves connectivity in the worst case with fully distributive working style.
Power Save Algorithms [6]	Geographic Adaptive Fidelity Protocol (GAF)	Grouping sensor nodes into clusters reduces the overall energy usage in the network.	Slightly less than CPSP because it utilizes information about the geographical location of the nodes (Node Equivalence Principle).
	Coordination Based Power Save Control (CPSP)		Greater that GAF due to large number of sleeping nodes.

Ana Moragrega et al in [7] have proposed a more realistic energy consumption model for cooperative WSNs. Node inactivity is considered as a prime factor for the analysis of cooperative WSN energy consumption and the outage performance. Various operating modes are considered like: 1) Transceiver mode where the nodes are active and are able to transmit or receive the data. 2) Idle mode in which the radio node neither receives nor transmits and 3) Sleep mode where the nodes are inactive or the radio nodes are considered as off. The cooperative protocol with a fixed number of active nodes performs well only for levels up to $\geq 10^{-4}$ values of the outage probability and the performance goes poor with less outage probability levels. With the consideration of node inactivity, for WSN, the diversity gain obtained through cooperation is deteriorated as compared to non-cooperation.

Hong et al in [8] have discussed energy efficiency of a new cooperative form of broadcast called Opportunistic Large Arrays (OLA). OLA cooperation helps the receiver in detection by providing the receiver with the accumulation of the entire transmitter's signal energy. Although OLA provides considerable energy savings, the authors prove the optimum energy assignment for cooperative networks as an NP-complete problem which involves high computational complexity. For this reason, the authors have

proposed two algorithms as suboptimal solutions named as Cumulative Increment Algorithm (CIA) and Cumulative Sum Increment Algorithm (CSIA) for illustrating the energy savings by OLA. The authors have proved that Cooperative Wireless Advantage (CWA) outperforms the Wireless Multicast Advantage (WMA) in terms of energy efficiency.

Opportunistic Large Array (OLA) is nothing but a cluster of network nodes which use active scattering mechanism in response to the signal of the source called leader. The intermediate nodes opportunistically relay the messages from the leader to the sink [9]. The authors have suggested an optimal power allocation mechanism in [10]. It includes a class of diversity protocols for multi-node wireless network utilizing relaying strategies depending on the distance of relay either with source or sinks. Higher data rates at the reduced transmit power can be converted to an increase in cell coverage [11]. Relaying and cooperative diversity essentially creates a virtual antenna array. All of the cooperative diversity protocols are efficient in terms of full diversity achievement and optimum performance except fixed decode-and-forward approach. Although prior to Laneman [10], the work on relay and cooperative channels utilized full duplex approach, he has constrained the cooperative communication to employ half duplex transmissions. Also the Channel State Information (CSI) is employed in the receiver instead of transmitter. Table 3.2 describes the various cooperative OLA algorithms with respect to the energy savings or life extension to the cooperative WSN.

Table 3.2 - Energy Efficiency of Cooperative OLA algorithms

OLA Technique	Energy saving / Life extension
Basic OLA [12] The avalanche of responses to the leader node is like the ola in a sports stadium.	60% as compared to non-cooperative multi-hop systems.
OLA-T [13] The node participation in each OLA is controlled by the power transmission threshold in Rx.	32% of the transmitted energy as compared to Basic OLA
OLA-VT [13] OLA with variable threshold, which optimizes thresholds as a function of level.	25% of the transmitted energy as compared to Basic OLA
A-OLA-T [13] Broadcast protocol alters between the sets of OLAs for each broadcast.	Can offer a 17% life extension as compared to Basic OLA and OLA-T
OLACRA [13] It exploits the concentric ring shapes of broadcast OLAs to limit flooding on upstream connection.	75% as compared to full flooding approach

3.4 Proposed Cooperative WPAN Simulation Scenario and Performance Analysis

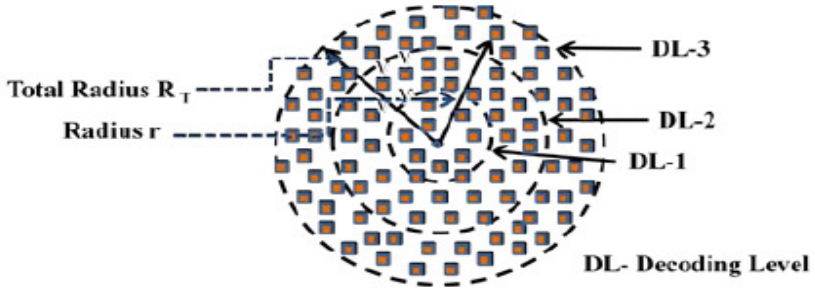

Figure 3.1 Proposed Two Level Cooperative OLA for Simulation Scenario (425 Nodes)

The goal of the experimentation is to reveal the tradeoffs of energy, latency, and throughput in S-MAC. S-MAC protocol is specifically designed for wireless sensor networks with NS2. All simulations of S-MAC are done using ns-2.34 where the energy model for S-MAC is updated. The radio power values used to compute energy consumption in idle, transmitting, receiving, and sleeping state are in accordance with the RFM TR3000 radio transceiver on Mica Motes. Simulation parameter and node configuration parameter set are given in Table 3.3 and Table 3.4 respectively.

Table 3.3 -Simulation Parameters

Simulation Area	75mx75m
Energy Model	EnergyModel
Initial energy	100J
Transmitting Power	36.00mW
Receiving Power	14.4mW
Sleep Power	15µW
Transmission Range	100m
Number of Nodes	425

Table 3.4 - Node Configuration Parameters

Channel Type	WirelessChannel
Radio Propagation Model	TwoRayGround
Antenna Model	OmniAntenna
Network interface type	WirelessPhy
MAC Type	SMAC
Interface Queue Type	PriQueue
Buffer size of IFq	50
Routing Protocol	DSDV

Figure 3.2 shows decrement in the energy consumption due to cooperation. Since while cooperating with other radio nodes, the relay nodes also transmit their own data, the overall energy consumption gets reduced due to collaborative efforts. For initial values of interarrival time in between packets, the energy consumption is more. But when cooperation starts in the intermediate phases, then the energy consumption has been reduced. Very less energy consumption at the interarrival time in between packets=6*10^-2sec is the indication of less nodes participation in the cooperation due to selection threshold criterion.

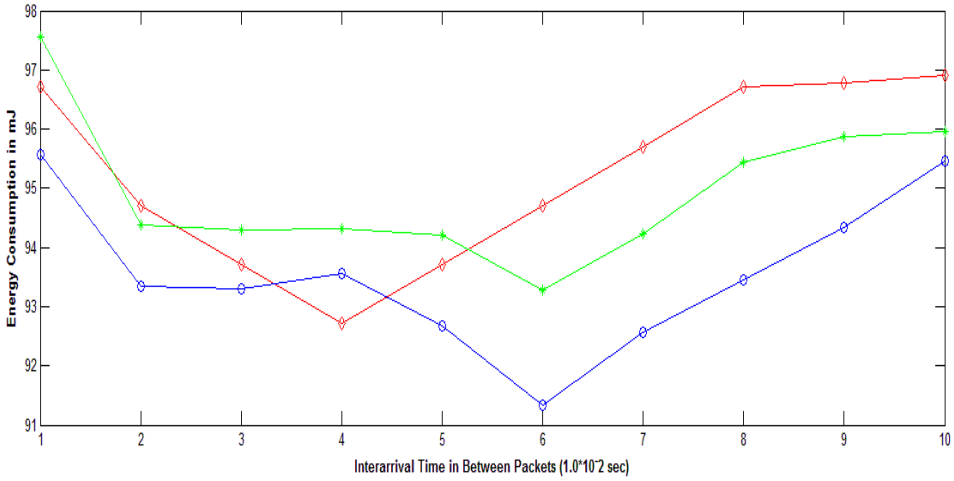

Figure 3.2 - Energy consumption versus Inter-arrival time

In Figure 3.3, the end-to-end delay graph is shown. The increased amount of delay due to cooperation is the limitation of this system. In general, delay is the critical parameter for indoor scenarios. It reveals from the plot that the end-to-end delay is slightly increased but the total communication delay can be reduced through cooperation. Least delay figures at the interarrival value of 4*10^-2 shows more number of idle nodes in the cooperative communication system. Plot of Figure 3.4 shows the significant improvement in the system throughput. Due to cooperation, throughput gets noticeably improved. Many intermediate relay nodes cooperate in the data transmission from source to receiver and it results into increase in throughput. After interarrival time of 6*10^-2, the throughput starts decreasing due to the fact that till certain cooperation level or coverage area, cooperation works well but after certain figures, it is difficult to achieve good cooperation.

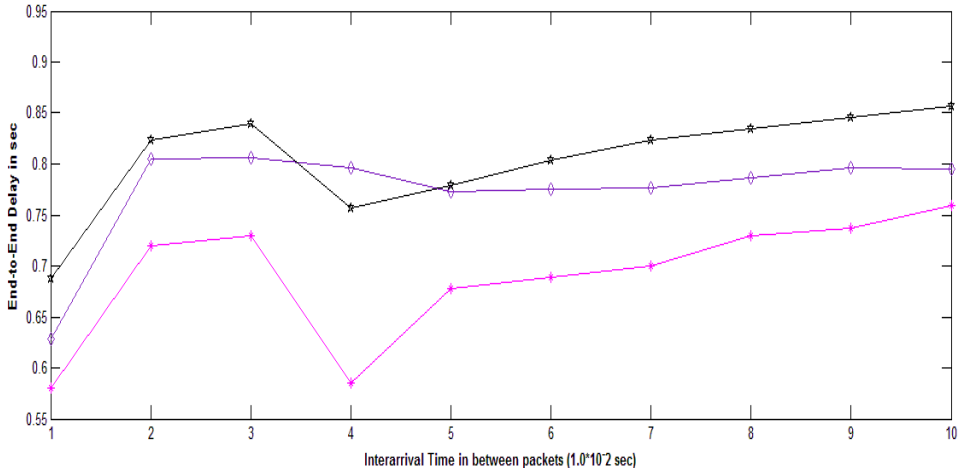

Figure 3.3 - End-to-End Delay versus Inter-arrival Time

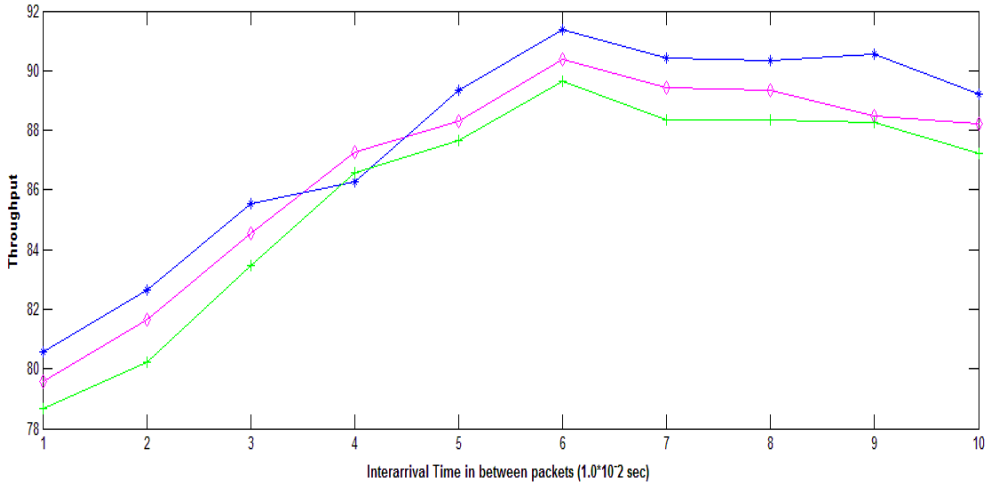

Figure 3.4 - Throughput versus Inter-arrival time

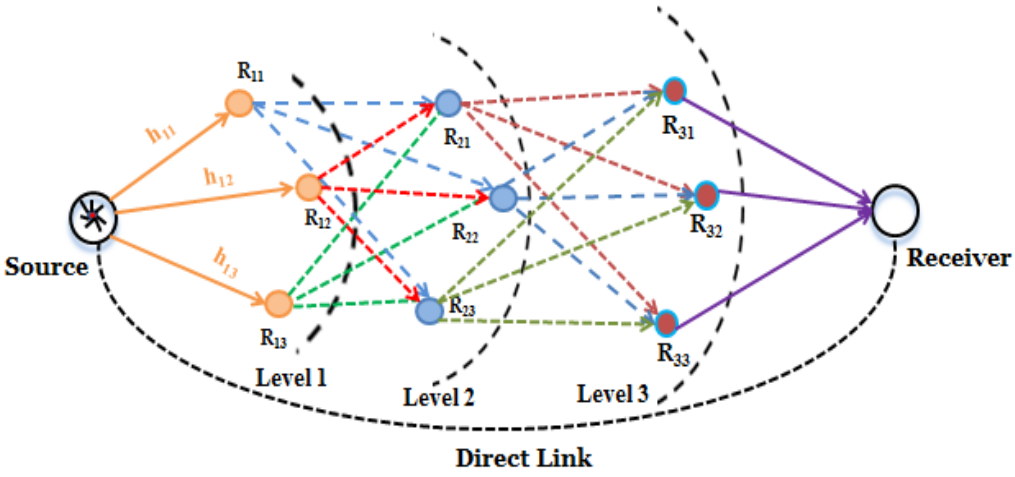

Figure 3.5 - The Proposed Cooperative Relaying Model

Four layer opportunistic cooperative wireless sensor network WPAN scenario is taken into consideration as depicted in Figure 3.5. When the source broadcasts the data to be transmitted, the nodes in vicinity of it opportunistically form the OLA structure and based on the received signal strength, selectively participate in the further data transmission. Selective Decode and Forward cooperative technique is practiced at each relay node. The curvy coloured dotted lines in the Figure 3.5 indicate different OLA levels. Levels 1 to Level 3 are the deterministic sets of sensor nodes based on regenerative OLA protocol. The data broadcasted by source is overheard by neighbouring nodes in the first layer i.e. R_{11}, R_{12} and R_{13}. The received signal strength at these nodes is compared with SNR threshold. If this signal strength at particular node is greater than or equal threshold value, then that node can decode the data, encode it again and can involve itself in further communication. Otherwise it stays idle. Similar is the case for all other layered relay nodes. Due to the selective decode and forward mechanism, the message flooding is under control for cooperative communication among the nodes and also the cooperative transmission becomes energy efficient. Because for the particular transmission, if out of eleven total nodes, only five nodes for eg., are actually taking part in cooperative transmission, the fraction of energy savings achieved is almost about 50% [14]. As per the analytical model in [14], for $\mu > 2$, the total area reached by the broadcast is limited i.e., $r_k < r_{Total}$. The cooperative channel is assumed to be flat fading channel for simplicity. Then we get at the relaying nodes,

$$y(s) = \sum_{n=1}^{N} h_n(s)\, s_n + w(s) \quad \text{----------} \qquad (3.1)$$

Where s_n is the symbol of n-th message and n-th source cooperative channel gain is given by,

$$\mathrm{h}_{\mathrm{n}}(s) = \sum_{i \in c_n} h(i,s)\sqrt{P_r^{s_n}} \quad \text{----------} \qquad (3.2)$$

Where c_n is the cooperating OLA group. At the relay transmitting end, superposition coding takes place which can be analytically represented as,

$$\sum_{j \in N_k(s)} \sqrt{P_r^{S_j} S_j} \text{ provided that } \sum_{j \in N_k(s)} P_r^{s_j} = P_r \text{ ----------} \quad (3.3)$$

Received signal at k-th level is given by,

$$y_{k+1}(s) = \sum_{n=1}^{N} \sum_{B: n \in b} \sum_{i \in c_k B} \sqrt{P_r^{s_n} h(i,s) s_n + w_{k+1}(s)} \quad \text{---------} \quad (3.4)$$

Especially for WSN, the energy model is used and we are performing cooperative relaying mechanism for 802.15.4 (WPAN). In the energy model the receive power, transmit power, idle power and sleep power values are initially set to particular values. And after simulation, due to communication among the nodes, these energy consumption values for the communication are changed. The analysis is done based on the

trace file contents. Table 3.5 and Table 3.6 presents the simulation parameters and the node configuration parameters for NS2.

Table 3.5- Simulation Parameters (Four levels of Cooperation)

Simulation Area	50mx50m
Energy Model	Energy Model
Initial energy	100J
Transmitting Power	31.32e-3W
Receiving Power	35.28e-3W
Sleep Power	144e-9W
Idle Power	712e-6W
Transmission Range	50m
Number of Nodes	11

Table 3.6- Node Configuration Parameters (Four levels of Cooperation)

Channel Type	Wireless Channel
Radio Propagation Model	TwoRayGround
Network Interface	Wireless Physical/802.15.4
Antenna Model	OmniAntenna
MAC Type	Mac/802.15.4
Interface Queue Type	PriQueue
Buffer size of IFq	50

NS2 simulations are performed for different values of CBR intervals ranging from 0.1 to 1. Figure 3.6 shows the variations in total energy consumption according to node functionalities. We observe that for the CBR interval of 0.6, the minimum energy consumption is there. Here the meaning of less energy consumption may be the less node participation in the cooperation due to various reasons like energy draining, idle condition or selfishly inactive behaviour. For the CBR interval values from 0.1 to 0.9, we observe total energy consumption less than 2 but for CBR interval 1.0, it goes beyond the value of 2. For high CBR values, we get higher energy consumption. Per node energy consumption is depicted in the Figure 3.7. Source node consumes less energy as compared to receiver node. This is because of the fact that source merely broadcasts the message but the receiver has to decode and then forward it. At node 5 and 6, the energy consumption is observed to be decreased may be due to the non-cooperation behaviour of these nodes or due to selection threshold condition, it has less energy and hence is not able to participate in the cooperation.

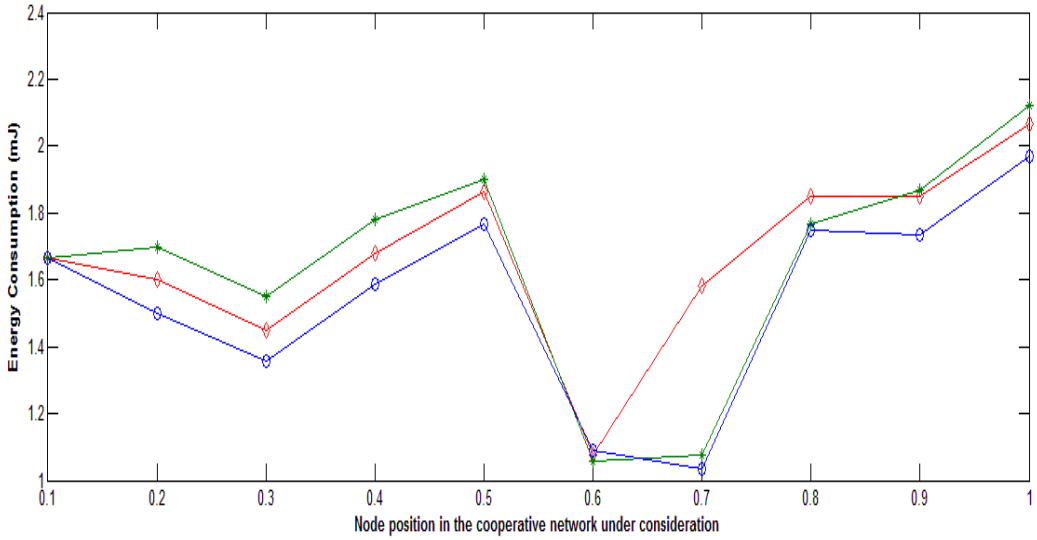

Figure 3.6 - Total Energy Consumption per CBR Interval

As compared to energy consumption at CBR interval of 0.1, the energy consumption at CBR interval of 1.0 is more as shown in Figure 3.8. No number 5, 7 and 8 have least energy consumption indicating their absence in the cooperative data transmission for this particular network scenario. Small CBR interval indicates the large traffic and high CBR intervals are the signs of small traffic. According to our results, we can comment that the cooperative relaying mechanism proves to be more energy efficient at high traffic loads. Per node energy consumption for all the CBR intervals ranging from 0.1 to 1.0 are shown in the bar graph of Figure 3.9.

Receiving nodes consume slightly more energy. But the overall energy consumption of cooperative communication is less as compared to other protocols like Broadcasting Incremental Power (BIP) and Local Minimum Spanning Tree (LMST), which are based on the minimum energy broadcasting using minimum spanning tree (MST) development. In [15], for LMST protocol, the energy usage for transmission in the whole WSN was observed to be 1.1 mJ for WSN of 50 nodes. Here in our case, for four level cooperation model of 11 nodes, the energy consumption is observed to be only around 0.2mJ which means good energy savings. Also, it is interesting to observe that at CBR interval of 0.6, the energy consumption is constant at all the node locations. It is indication of the fact that may be no any data transmission taking place at this CBR value.

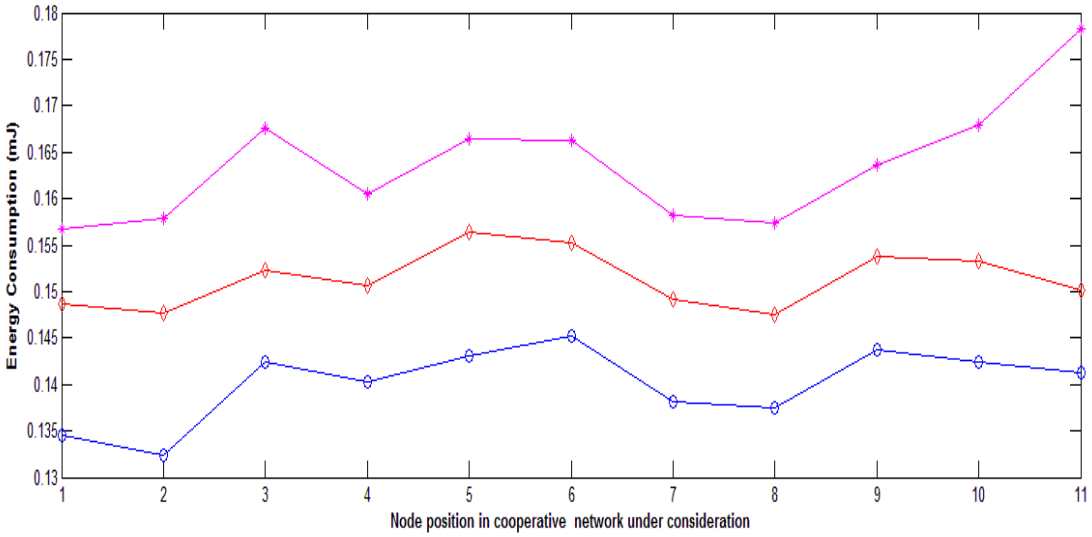

Figure 3.7 - Per Node Energy Consumption at CBR Interval=0.1

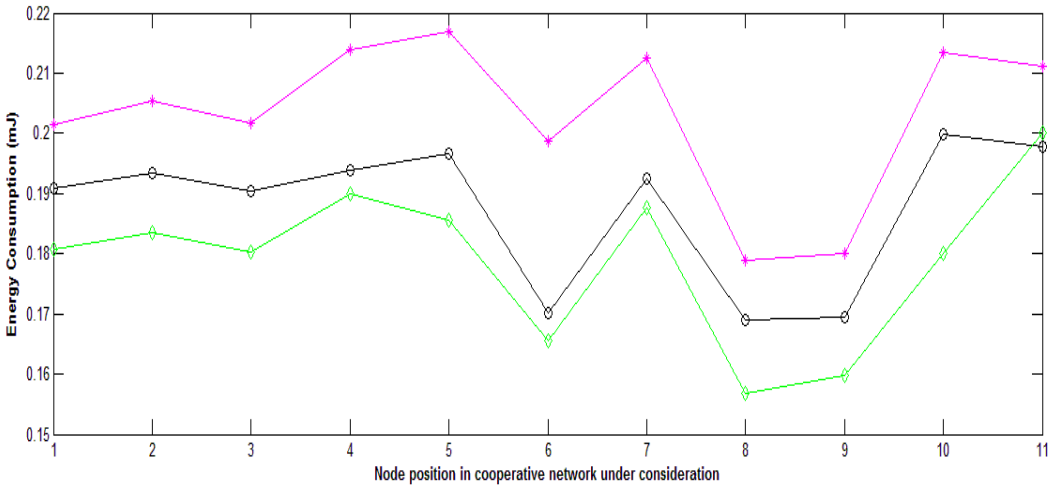

Figure 3.8 - Per Node Energy Consumption at CBR Interval=1.0

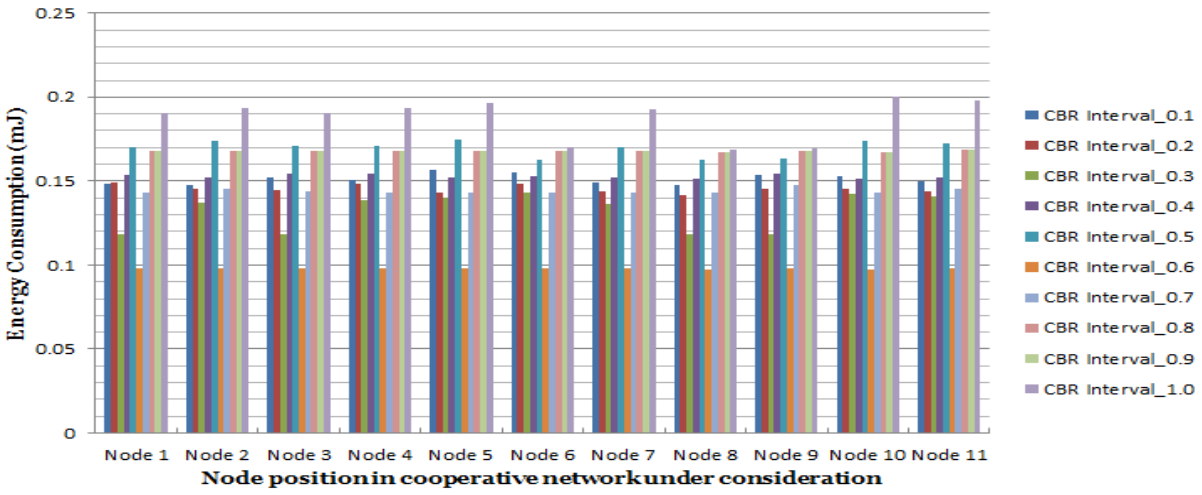

Figure 3.9 - Energy Consumption Per Node for CBR Intervals from 0.1 to 1.0

Due to the unity noise variance assumption, the received power becomes received signal to noise ratio (SNR) [14].

$$SNR=Prx=\frac{\overline{P_r}}{d^2}=\frac{\rho Pr}{d^2} \quad \text{----------} \quad (3.5)$$

$$SNR=\frac{NPr}{pi\, r^2 d^2} \quad \text{----------} \quad (3.6)$$

$$\text{SNR in Decibels (dB)} = 10log_{10}(\text{SNR}) \quad \text{----------} \quad (3.7)$$

Outage Probability is given by [16],

$$\text{Outage Probability} = \frac{1}{\sigma_{s,r}^2}\frac{2^{2R_S}-1}{SNR} \quad (3.8)$$

Where $\sigma_{s,r}^2$ = variance

R_S= Spectral efficiency

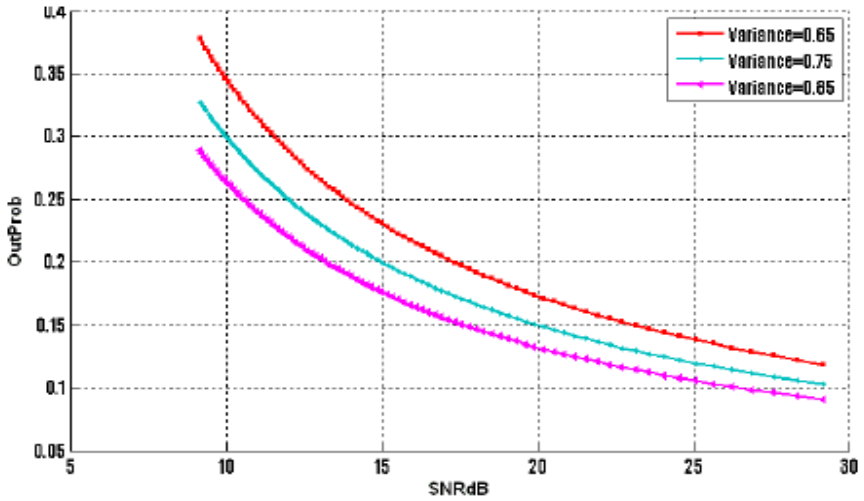

Figure 3.10 – Outage Probability Analysis for Decode and Forward Cooperative Strategy

The outage probability analysis is depicted in figure 3.10 below. As seen from figure, the decode and forward cooperative mechanism gives approximately the same performance as that of amplify and forward cooperative strategy.

3.5 Conclusions

The NS-2 experimentation has shown substantial enhancement in the system throughput. Simulation results reveal the trade-off between energy consumption, latency and throughput in S-MAC operation. Simulation results reveal the trade-off between energy consumption, latency and throughput in S-MAC operation. The outage behaviour for decode and forward cooperative technique is observed to be almost same as that of amplify and forward technique. Also, it reveals from the simulation results of the four level cooperative

OLA that opportunistic cooperative relaying mechanism is capable to provide the benefits of the MIMO antenna arrays. Energy is the scarce resource parameter for the tiny sensor nodes and cooperation ultimately results in lifetime extension of the individual sensor nodes as well as the whole network.

References

[1] Mrs. Saba Siraj, Mr. Ajay Kumar Gupta and Mrs Rinku-Badgujar, "Network Simulation Tools Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, pp. 201-210, June 2012.

[2] The Network simulator ns-2 http://www.isi.edu/nsnam/ns/

[3] Almargni Ezreik, AbdallaGheryani, "Design and Simulation of Wireless Network using NS-2", 2nd International Conference on Computer Science and Information Technology (ICCSIT'2012) Singapore, pp. 157-161, April 28-29, 2012.

[4] Sangman Moh, Chansu Yu, Seung-Min Park, and Heung-Nam Kim," CD-MAC: Cooperative Diversity MAC for Robust Communication in Wireless Ad Hoc Networks", IEEE International Conference on Communications, ICC '07, pp. 3636 – 3641, 2007.

[5] Xinyu Zhang and Kang G. Shin, "DAC: Distributed Asynchronous Cooperation for Wireless Relay Networks", Proceedings of the 29th conference on Information communications, INFOCOM'10, pp.1064-1072, 2010.

[6] Ewa Niewiadomska-Szynkiewicz, Piotr Kwaśniewski, and Izabela Windyga, "Comparative Study of Wireless Sensor Networks Energy-Efficient Topologies and Power Save Protocols", Journal of Telecommunications and Information Technology, pp. 68-75, March 2009.

[7] Ana Moragrega, Christian Ibars, Yan Geng, "Energy Efficiency of a Cooperative Wireless Sensor Network", Second IEEE International workshop on Cross Layer Design, IWCLD '09, pp. 1-5, June 2009.

[8] Yao-Win Hong and Anna Scaglione, "Energy-Efficient Broadcasting with Cooperative Transmissions in Wireless Sensor Networks", IEEE Transactions on Wireless Communications, Volume 5, Issue 10, October 2006.

[9] A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation – part i: System Description, part ii: Implmentation Aspects and Performance Analysis," IEEE Transactions on Communications, Volume 51, Issue 11, pp.1927– 1948, Nov. 2003.

[10] J. N. Laneman, D. Tse, and G. W. Wornell, "Cooperative Diversitry in Wireless Networks: Efficient Protocols and Outage Behaviour", IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3063-80, Dec. 2004.

[11] Ahmed K. Sadek, Weifeng Su and K.J.Ray Liu," Multinode Cooperative Communications In Wireless Networks", IEEE Transactions on Signal Processing, Volume 55, Issue 1, pp. 341-355, January 2007.

[12] Anna Scaglione and Yao-Win Hong, "Opportunistic Large arrays: Cooperative Transmission in Wireless Multihop Ad-Hoc Networks to Reach Far Distances", IEEE Transactions on Signal Processing, Volume 51, Issue 8, August 2003.

[13] Arvind Kailas and Mary Ann Ingram, "Alternating Opportunistic Large arrays in Broadcasting for Network Lifetime Extension", IEEE Transactions on Wireless Communications, Volume 8, Issue 6, pp. 2831-2835, June 2009.

[14] Vandana Rohoakale, Nandkumar Kulkarni, Horia Cornean, Neeli Prasad, "Cooperative Opportunistic Large Array Approach for Cognitive Radio Networks", 8th IEEE International Conference on Communications, Bucharest, Romania, pp.513-516, June 2010,

[15] Niewiadomska-Szynkiewicz, E., Kwa´sniewski, P., & Windyga, I. ,"Comparative study of wireless sensor networks energy-efficient topologies and power save protocols", Journal of Telecommunications and Information Technology, Vol. 3, pp.68–75, 2009.

[16] Y. W. Hong and A. Scaglione, "Energy-efficient broadcasting with cooperative transmissions in wireless sensor networks," IEEE Transactions on Wireless Communication., vol. 5, no. 10, pp. 2844–55, Oct. 2006.

4

Trust Based Authentication and Authorization for CRN

Spectrum is a scarce and very essential resource for the ever growing mobile communication applications. Cooperative spectrum sensing is a well-known and proven mechanism in the Cognitive Radio Networks (CRNs). As compared to other traditional radio networks, CRNs are more delicate and more open to the wireless environments. Therefore, the CRNs have more security threats than the conventional wireless networks. The spectrum sensing and sharing mechanisms are inherently vulnerable to the malicious behaviors in the wireless networks. This chapter proposes an energy efficient light weight cryptographic Cooperative web of trust (CWoT) for the spectrum sensing in cognitive radio networks which is proved to be appropriate for the resource constrained wireless sensor networks (WSNs). Received signal strength (RSS) values obtained can be utilized to avoid Primary user emulation attacks (PUEAs).

4.1 Introduction

Wireless communication and relative mobile computing applications is a boom in the telecom market but the available spectrum and its allocation is not appropriate to satisfy the highly increasing demands by mobile applications. Cognitive radio technology is a hopeful evolution for the solution towards scarce radio spectrum [1]. Cognitive radio entities continuously sense the spectrum holes which are utilized for the opportunistic communication. CRNs provide the spectrum reuse concept. Since the CRN evolves from the hybrid combination of many heterogeneous networks, it is much more prone to the wireless open media vulnerabilities [2]. Consumer premise equipment (CPE) which has the inbuilt cognition capability, continuously monitors the spectrum, senses the white spaces in the spectrum and occupies the spectrum according to the availability and it can vacate the occupied spectrum immediately after sensing the comeback of the licensed user.

CPE is a mobile equipment with cognition capabilities which can sense radio environment eg., spectrum white spaces, information about geographic location, available wireless or wired networks around and available services, analyze and get information regarding the secondary user's needs and reconfigure itself by adjusting some specific parameters to make sure that rules and regulations of CRN are strictly followed. Whenever the CPE senses spectrum holes, CRN sends Request to send (RTS) kind of packets on the network to initiate the communication [3].

Cooperation is the vital characteristic of CRNs because the secondary nodes of CRN basically cooperate with each other for finding out the spectrum white spaces in the available spectrum for the successful and timely wireless communication. With cognitive environment, it is very much essential that the information bearing secondary nodes should exchange their data through multicast communication. Safety of the secondary user's communication data from intruder is a critical issue for CRNs. Because of these reasons, Group Security is necessary for secondary users of CRN [4]. The group based security with collaborative advantages is possible with the concept of Cooperative Web of Trust (CWoT).

CRN is a multi-user environment where multiple secondary and primary users are present in the system. Spectrum sensing for such multi-user case becomes more complicated wherein the sensing of spectrum holes and the interference estimation are the complex tasks. A collaborative effort by secondary users is the attractive solution. The research work in [5] proposes a new cooperative spectrum sensing mechanism for multi-user CRNs in which each user's contribution is weighted by taking into account

the parameters like received power and path loss components.

4.2 Related Work

For wireless communication, a signal has to be transmitted through open media with a virtual connection. Since the CRNs are built with numerous heterogeneous wired and wireless networks, the chances of the data being hijacked are more. Figure 4.1 below depicts the security threat taxonomy for CRN [6] wherein the possible security threats to CRN are mentioned.

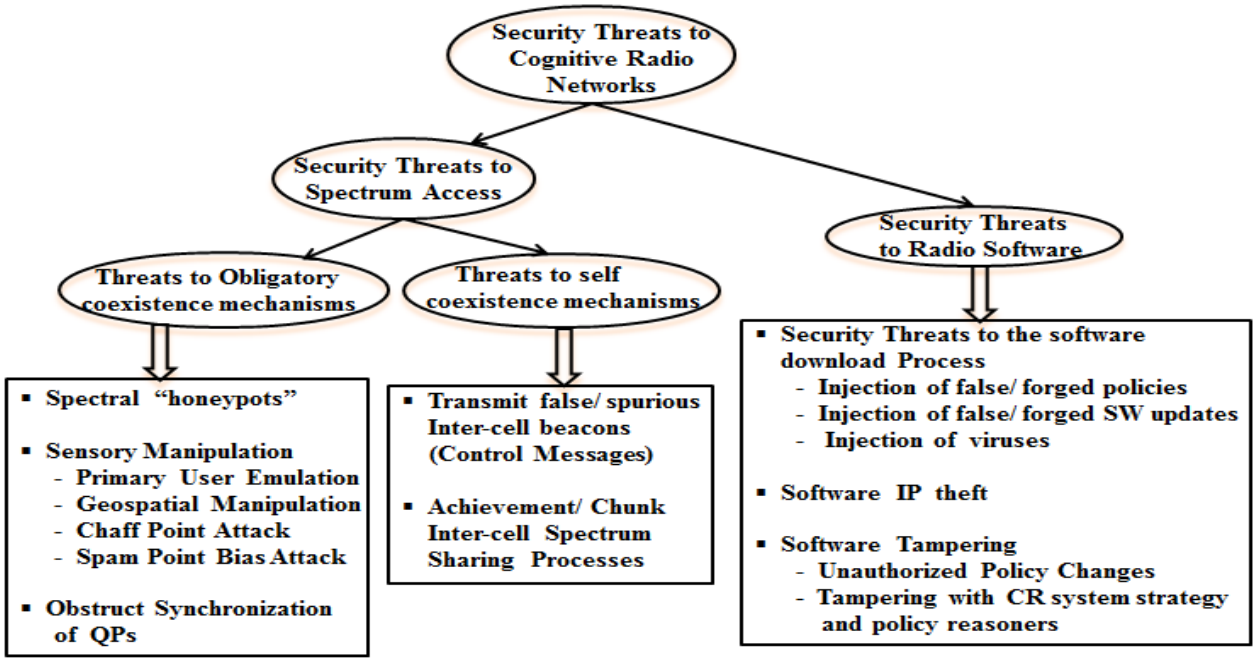

Figure 4.1- Security Threats Taxonomy for CRNs

In the research work of [7], the authors have calculated trust depending on various communications attributes and it is compared with the threshold value of trust. Helena et. al. in [4] have presented a good combination of wireless physical layer security, private key cryptography and one way hash functions. They have proposed a security protocol for a centralized system where the authenticity is verified at the data fusion center which they claim as the robust mechanism against the location disclosure attacks.

The research work in [8] proposes a trust methodology for secrecy in cooperative spectrum sensing (TM-SCSS) wherein the data fusion centre assigns and updates the trust value to each entity according to the sensing results. The secondary cooperating radio nodes are classified into categories like malicious node, pending node and trusted node based on their recent trust values updated according to the data fusion centre.

Cooperative spectrum sensing is a dominant technique for the detection mechanism in the CRN. It makes use of cooperative spatial diversity to exploit benefits like energy efficiency, cooperation efficiency and wideband sensing capability. But the advantages come with certain overheads like security challenges due to heterogeneous nature of CRN, sensing time and delays, mobility management and channel impairments as depicted in Figure 4.2. The techniques used for spectrum sensing include Energy Detector based Sensing, Cyclostationary based sensing, Radio Identification based sensing and matched filtering. For energy detection based sensing, cooperation is the best suited technique since it results into appropriate received signal strength values.

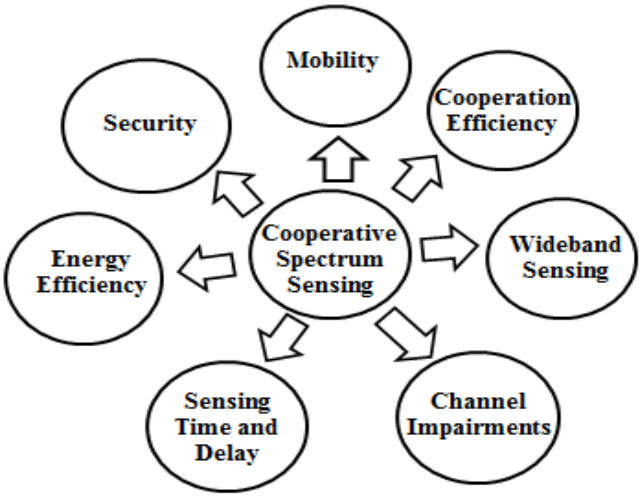

Figure 4.2 - Gain and Overheads in Cooperative Spectrum Sensing [9]

4.2.1 Primary User Emulation Attack (PUEA)

An attacker imitates the characteristics of a primary signal transmitter and pretends as being primary user as shown in Figure 4.3. Proper identification mechanisms are very much essential for the prevention of the PUEA attacks in CRN. The problems associated with the PUEA attack are security, trust and performance related. So, for the prevention of the critical threat like PUEA, some kind of strong security mechanism is vital [6].

This chapter proposes a light weight cooperative web of trust for the prevention of primary user emulation attacks in the spectrum sensing technique for the heterogeneous cognitive radio networks. The facts with CWoT's considerably improved received signal strength (RSS) figures ensure the security against identity thefts of the primary users.

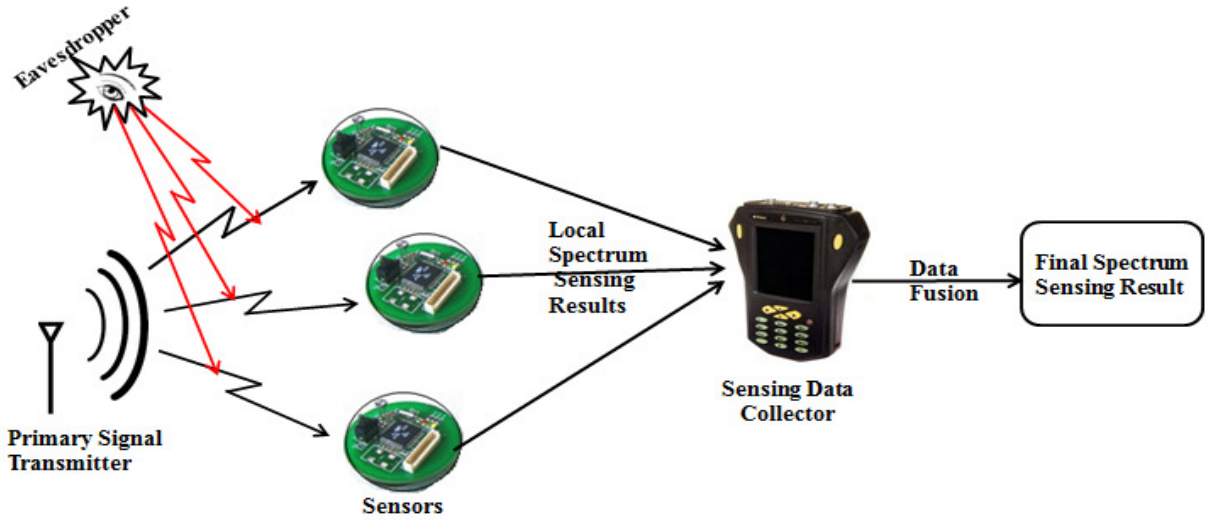

Figure 4.3 - Primary User Emulation Attack in CRN

With the CWoT mechanism, authentication and authorization techniques are proposed which are based on trust levels. The secondary user's cognitive radio equipment forms an opportunistic large array (OLA) like structure to communicate the information broadcasted by any source to its intended receiver. The CWoT mechanism is found to be efficient in terms of QoS parameters for the adhoc networks in terms of reliability, energy efficiency and delay issues.

4.3 Cooperative web of trust for cognitive radio networks

The proposed CWoT security mechanism considers following model, which is a part of the Cooperative Opportunistic Large Array (OLA), as shown in Figure 4.4. The model illustrates various layers. The coverage limits of the various layers of the cooperation are shown with different levels.

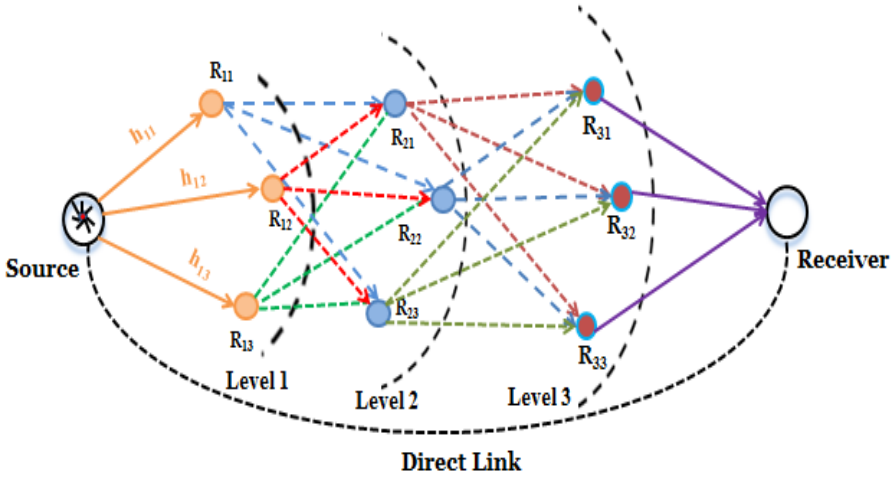

Figure 4.4 - Proposed CWoT Model for Secondary users of CRN

The analytical model for cooperative opportunistic large array (OLA) approach is considered same as in the works of same authors in [10]. Accordingly, the consumer radio devices (secondary user's sensor nodes) which are half-duplex in nature are assumed to be uniformly and randomly distributed over a continuous area with average density ρ. As in [10], the deterministic model is assumed, which means that the power received at a Consumer Premise Equipment (CPE) is the sums of powers from each of the CPE. In this model, the network node transmissions are orthogonal to the other node's transmissions. It is assumed that a CPE can decode and forward a message without error when it's Signal to Noise ratio (SNR) is greater than or equal to modulation-dependent threshold λ_d. Due to noise variance assumption of unity, SNR criterion is transformed into received power criteria and λ_d becomes a power threshold. Let P_s be the source transmit power and the relay transmit power be denoted by P_r, and the relay transmit power per unit area be denoted by $\overline{P_r} = \rho P_r$. Instead of infinite radius, we are considering some practical scenarios where the radius is limited.

Theorem: If $\mu \triangleq e^{(\lambda/\pi\rho P_r)}$ [11] and $\mu > 2$,

then $r_k = \sqrt{\frac{P_s(\mu-1)}{\lambda(\mu-2)}}\left(1 - \frac{1}{(\mu-1)^k}\right)$ -------- (4.1)

and $\lim_{k\to\infty} r_k = r_\infty = \sqrt{\frac{P_s(\mu-1)}{\lambda(\mu-2)}}$ --------- (4.2)

For ($\mu \leq 2$), the broadcast reaches to the whole network i.e. $lim_{k\to\infty} r_k = \infty$.

For ($\mu > 2$), the total area reached by the broadcast is limited i.e. $r_k < r_{total}$.

where r_k= radius of the kth level of the OLA structure.

Some preliminary assumptions for the proposed system are as below:

- All the nodes will have a unique identification, or UID, which will be utilized in the authentication of the nodes.
- All nodes are capable of transmitting and receiving information or data, if the minimum threshold for the received message is satisfied.

In communication in CWC it is important for a receiver to know the following information: Who the actual sender of the message is (i.e. where the message originated)Who delivered the message to me (i.e. if the message is coming directly from the sender or via intermediate nodes). This information can be given by the usage of bit patterns in the packets of the data being sent.

The packet contains two layers of information as shown in figure 4,5:

G-value of intermediate sender	S-value (G-value of original sender)	Sender	Receiver	Intermediate Sender	Intermediate receiver	Payload

Figure 4.5 - Packet Structure

The first field stores the value of G (derived from UID and the Public key of the recipient) of the intermediate node. If the sender is directly sending this packet to the receiver, its G value is stored here.

The second fields store the G-value of the original sender that is the node where the message originated. Note that in case of direct communication (i.e. no intermediate nodes are used), the first two fields will bear the same data and will facilitate in the receiver knowing that sender is directly sending the information.

The payload contains the information that is to be sent to the other node. The frame may additionally contain information like timestamp. This will help in time-analysis of the performance of the network.

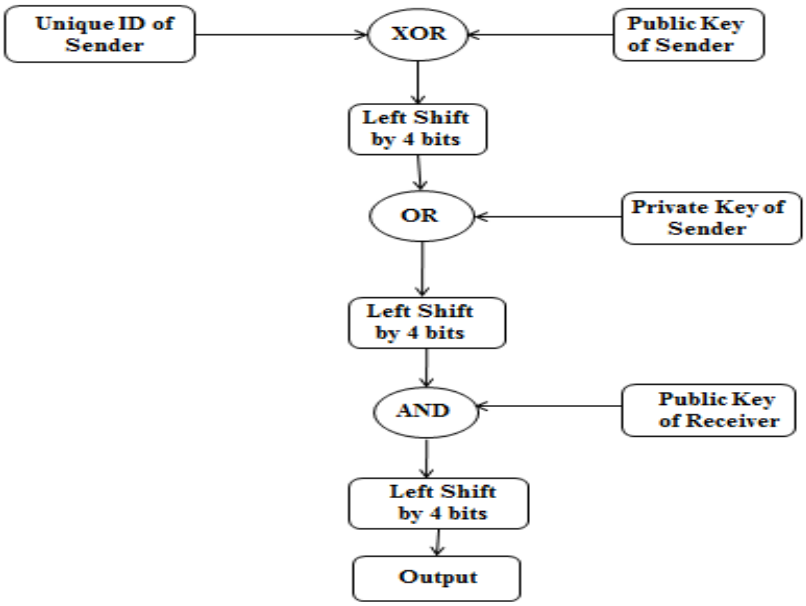

Figure 4.6 - One Way Function Generation

One way function is generated by making use of the steps as shown in figure 4.6. To make our security mechanism light weight, we have used only 4 bit left shifts. One way functions are not easy to break. So for security purpose, it is of most importance.

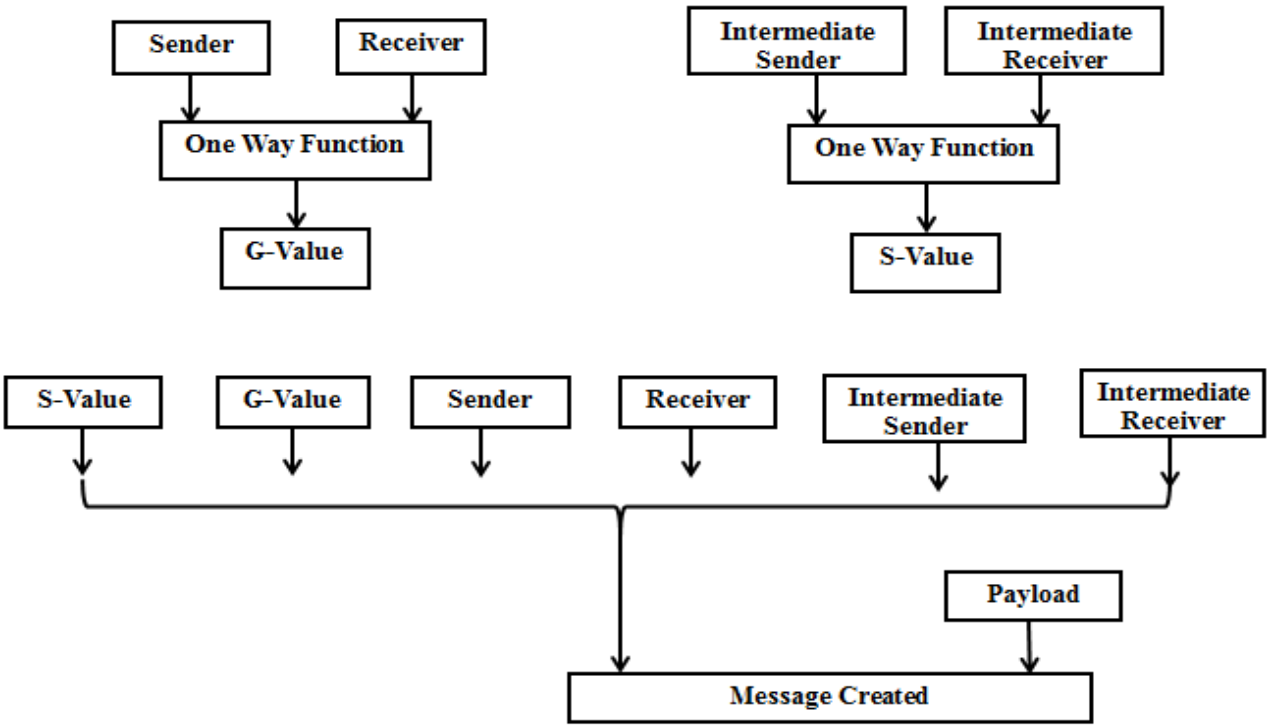

Figure 4.7 - Message Creation Mechanism

Taking into account the typical flow of messages using the RTS-CTS-Message-ACK, the information about the nodes with the authentication details is transmitted cooperatively to the destination. The messages being relayed by the intermediate nodes or relays are considered on the basis of decode and forward, since the other technique amplify and forward amplifies the noise, thus degrading the signal that is received at the other end. It is in general considered that such cooperative relay of messages may present a problem of message flooding in the network. Figure 4.7 shows the message creation mechanism. This situation is normally avoided by restricting the transmission of messages that fall below a given criteria (received SNR threshold) for the signal-to-noise ratio (SNR) of that message, as explained by [10]. The noise variance is assumed to be unity and hence the SNR criterion in transformed into a minimum criteria for power. Hence if the power with which the message is received is less than the threshold λ_t, the corresponding secondary relay node is not eligible for further retransmission of the signal. Such node stays idle during the communication.

4.4 Authentication

Let us consider an array of n nodes, depicted by N_i for i=1 to n. Whenever a node, say N_A wants to communicate with N_B, N_A will send a Request to send (RTS) to N_B. Depending on whether the nodes are communicating for the first time or not, two scenarios are generated as explained below.

Scenario 1: This is the first time that N_A is communicating with N_B: When N_A is communicating for the first time with N_B, it would require an external entity to assure the authenticity of the node. The proposed model assumes that the network nodes trust each other to some basic level at the beginning of the communication, and later verifies the credibility of each node using trust values from other nodes. The basis of web-of-trust is used. For the aforementioned scenario i.e. if the nodes are communicating for the first time, some trust is to be assumed. In such a situation there is no way for N_A to verify that the person claiming to be N_B really is N_B. Hence N_A will, for the time being, trust N_B for the communication. An Asymmetric key exchange mechanism is considered. The public key is known to all the nodes in the network, whereas individual private key is retained by the corresponding node. Newer key exchange mechanisms for 802.11ae and 802.11af, based on groups have been discussed in the research work published in [11, 12, 13].

When N_A wants to communicate with N_B, it will use the public key of N_B, K_{public}, and will pass this, with its own UID to a one way function**,** F ($K_{public,}$ UID). One way function is generated as shown in Figure 4.5. The output of this function, **G**, will then be sent to N_B. The use of one way function is beneficial as follows: any node other than N_B, will not be able to decipher the UID of N_A because of the use of the one way function. This is then attached to the RTS frame, which is to be sent to N_B. N_B, upon receipt of this frame recognizes that this is the first time N_A, or, for that communication, someone claiming to be N_A, is communicating with him/her.

Since there is no previous record of the authenticity of the identity of N_A, N_B will flag this node, and will try to confirm its identity later, as and when possible with cooperation from neighbouring nodes**.** This value G received from N_A is then given to another function F_D which will generate a corresponding value for the UID, called as K. Note that the UID itself is never disclosed to any other node. This value, K, is then stored in the memory of N_B. Based on feedback about this node from the neighbouring nodes, N_B may at a later stage delete this node, or set it to a higher priority.

In the packets that will follow, i.e. the ones containing the actual data from N_A, all N_B has to do is to extract the value of K of the sender from these packets. It may be noted that this value of K will be in encrypted format, if possible using the one way function only. N_B then extracts the K of the sender and matches it with K that it has received from the RTS packet. If the two keys match, the packet is considered as authentic and an acknowledgement is sent back to N_A. In the case that the value of K of the sender and the received packet do not match, the packet is discarded, with no notification being sent to the sender.

Scenario 2: N_A or someone claiming to be N_A has already communicated with N_B: In such a scenario, N_B has an idea about the identity of N_A. So all that N_B has to do is to confirm a match between the stored value of K of N_A and the value of K derived from the incoming packet. If a match occurs, the packets are processed and an acknowledgement is sent, otherwise the packet is discarded.

4.5 Trust Building

Cooperation itself has offered many of its benefits in the field of communication. The overheads of authentication can be reduced with the help of the cooperation from neighbouring nodes, i.e. by maintaining a web of trust (WoT). Consider a situation where N_A is a known party to N_B, i.e. they both trust each other. In a situation, where a third node, say Cairn, wants to contact with N_B. It is also known that N_A knows Cairn, that is, N_A trusts Cairn. This fact can be used to avoid unnecessary expenses that would be required to authenticate Cairn. As N_B trusts N_A, and N_A trusts Cairn, then a direct relation that N_B trusts Cairn can be made. Here, N_A is standing as a guarantor for Cairn.

It may be noted that this cooperation comes with its own drawbacks. Consider a situation where one of the nodes in the system is malicious. If this node stands as a guarantor for many other malicious nodes, then the security of the system can be compromised. One solution to this problem can be the use of trust-ranking of nodes. Based on the performance of nodes, ranks can be assigned to the nodes. If a node is a suspect, that is if many packets being sent via that node are not being delivered to the destination and this fact can be confirmed by some cooperation, then the node can be blacklisted, or its rank can be decreased by one.

If the rank of a node reaches zero, its entry of K and node name is deleted and cooperatively notified to other nodes. If such a node has a guarantor, then the guarantor can be blacklisted and its priority be

decreased as well. In the above example, N_A stood as a guarantor for Cairn. In the event that packets being routed through Cairn are not reaching the destination, or for that matter, if any crooked activity is suspected at Cairn then cairn can either be blacklisted or its rank can be decreased, depending upon the seriousness of the malicious nature being observed at that particular node. The message building mechanism uses one way function as shown in Figure 4.7. The complete CWoT security mechanism is depicted as in the flowchart shown in Figure 4.8.

In the event that a particular node has come up and is interacting with other nodes for the first time, the authenticity can be established based on the fact that if the new node is giving good performance with most number of neighbouring nodes, with no problems regarding identity of that node, the node's rank can be increased, indicating the increased level of trust. We can do one more thing that trusted nodes can be added only at level 1, that is,

- A trusts B & B trusts C then A trusts C
- A trust B, B trusts C & C trust D then A trust D is not possible in this case.

In this scenario, we are assuming that by reducing the number of middle agents (secondary relays) will help us in improvement of security protocol.

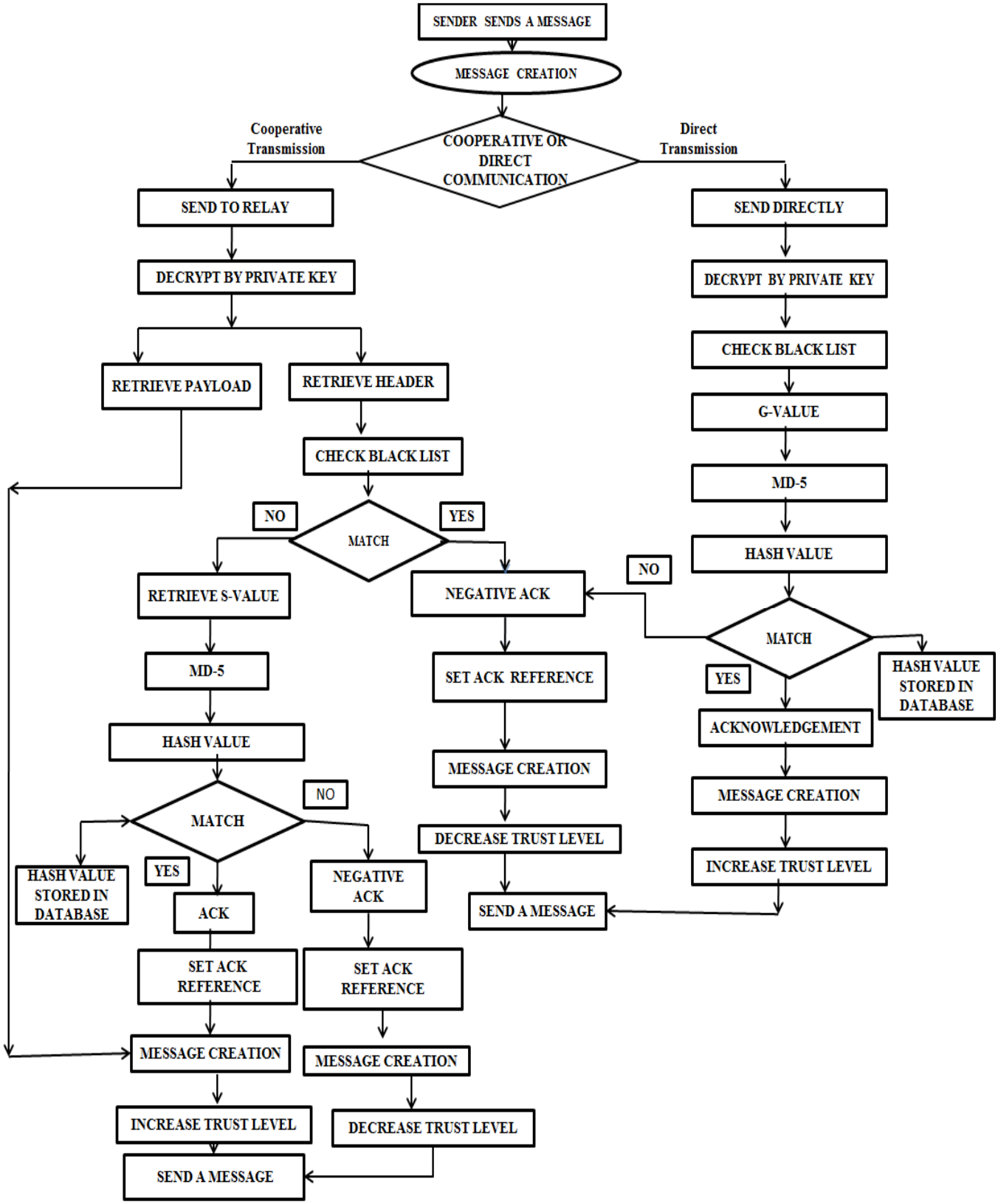

Figure 4.8- Flowchart for Cooperative Web of Trust (CWoT) Security Mechanism

4.6 Authorization

The role based access control technique is considered, wherein the participant radio nodes are classified according to various roles assigned to them. After the message is received, based on the reputation of that node, appropriate trust level is assigned to it. Based on the achieved trust level, the role is assigned to that particular node. Lastly, the access rights for that node are validated. The system divides the communicating nodes into three types of roles: sender, relay and receiver. Depending on the amount of information required for successful transmission of the message, appropriate access rights are assigned to these roles. Though this scheme may look suitable for implementation, an obvious drawback of the previously implemented mechanisms is the static nature of the access roles that is provided to the participants. Therefore the roles are desired to be flexible. This can be achieved by the use of reputation based role assignment, as defined in [14]. In contrast to the multi-level approach of the technique proposed in the previous works, a decentralized approach is utilized here because of highly mobile nature of the nodes in the WSN. This gives equal priority to all the nodes, and reduces the central point of failure. On the basis of the trust level of the node that is communicating, a role is assigned to the node. It must be noted that since the role is being assigned at the necessary host, one node may have many roles assigned to it in context with different nodes. This may be thought of as a problem, but such a problem is easily eliminated as the trust information of the nodes is shared by all communicating parties. Thus, the trust value maintains appropriate reputation of the nodes, which in turn provides the suitable role to the node.

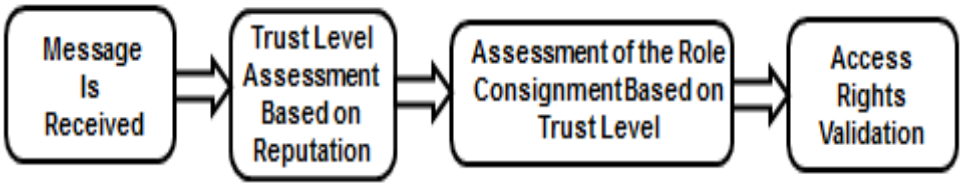

Figure 4.9 - Authorization Process

Proposed CWoT security system works for the detection and isolation of malicious nodes, based on the distance estimation of the values generated by broadcasting nodes, and gathering information about the same signal from neighbouring nodes. It is assumed that in replayed messages if the data that is presented, i.e. distance is incorrect and if such fact is brought to the notice of the node by the neighbours, then the nodes may diagnose it as a malicious node and thus eliminate it as shown in the authorization process of Figure 4.9.

In case, the identity of the adversarial relay (eavesdropper) is not diagnosed, then it can be pinpointed for detection by mechanism proposed in [15]. However it may be noted that only adversarial relay can be detected using this mechanism. The method involves the inclusion of some symbols. Based on the key shared between the sender and the receiver, the key that is unknown to the relay nodes, some symbols are generated. These symbols are called as trace symbols. The function explained above for the generation of the values of *K* (G value) can be used, along with some pseudo random number generator to produce unique values and the location where these symbols are to be added. At the receiving end, the receiver using the shared key extracts the symbol from the location. A mathematical function corresponding to the function used for the generation of the symbols is used at the receiving end to establish the ground truth whether these symbols were indeed generated on the basis of the tracing key, and then compare it with the received values. In case, the signal is garbled, or modified by a malicious relay, such malicious behaviour can be detected. Tracing mechanisms are provided in [15] for detection of the adversarial node.

The aforementioned topics give an insight to the basic mechanism that is to be implemented for this work. As every communication is bound to change the status of the network, it can be expressed as

$$M(n') \rightarrow < \alpha > M' \text{ ---------- (4.3)}$$

When radio node of the network configuration M transforms into another network configuration M' by execution of the action/communication/message**.** M is a table maintaining the trust information of the various participating nodes in the network. Each node stores the trust information about other nodes in its vicinity. A trust handling unit keeps on updating the trust level *T(n)* of the neighbouring nodes. The trust levels can be categorized into ***blacklisted < not trusted < acquaintance < trusted < medium < highly trusted***. During initialization, the nodes are assigned a trust value of acquaintance. Thereafter, those are the communication messages that alter the trust level *T(n)* of the neighbours. If a communication from node A to B delivers a corrupt message or the identity of the sender cannot be verified, it takes the network to a state that invokes decrease in the trust level of that node. As a node can act as the guarantor for other nodes that are less trusted, the guarantor stands liable for any false trust that it may have stood for.

This can be expressed as:

$$M(i) \rightarrow (\alpha)M' \text{ } - - - - (4.4)$$

$$M'(T(i)-1) - - - - \quad (4.5)$$

Where M' = Broadcast trust

If the step (4) results into a trust of blacklist, that is $T(i) < \theta$, the node is removed or banned from communication. θ is the minimum value below which the node is blacklisted. There may be two scenarios existing after this case: (1) If it is observed that the blacklisted node is blacklisted by a node that is still trusted, that node's trust is decreased by one. (2) If the blacklisted node is blacklisted by many other networks, its trust level is decreased as well. Based on the trust $T(i)$ for the node i , roles are assigned. The role is represented as,

$$R\big(I, T(i)\big) - - - -(4.6)$$

Where the role R is assigned to node i at trust level $T(i)$. The participants during communication will be assessed against this role at the receiving node. If it is found that the access requested is given in the role at the trust level $T(i)$, the action is permitted, otherwise rejected. The security is ensured as below: at the time of establishing communication, a trusted node at some trust level j will never communicate with another node at a trust level below some trust level k. This trust level k may vary from one node to another depending on the importance of the functionality of that node. In such manner, as proved by [16], malicious nodes are isolated from the communication network.

4.7 Simulation Results

After inclusion of security mechanisms in the communication system, it is general observation that the energy consumption of the system increases by large amount. As compared to the research work implemented in [11], the fraction of energy savings is slightly reduced with the addition of security in the system. As can be seen from the Figure 4.10, the energy consumption goes on increasing with the coverage area extension. It is interesting to note that for higher values of the SNR threshold (received SNR value at the secondary node), the energy consumption is observed to be reduced. The cooperative wireless communication is inherently energy efficient. By exploiting the cooperative diversity, the coverage range of the communicating nodes can be extended. Due to range extension capability, the received signal strength values are observed to be considerably better values compared to that without cooperation. This is very encouraging result for the protection against primary user emulation attack.

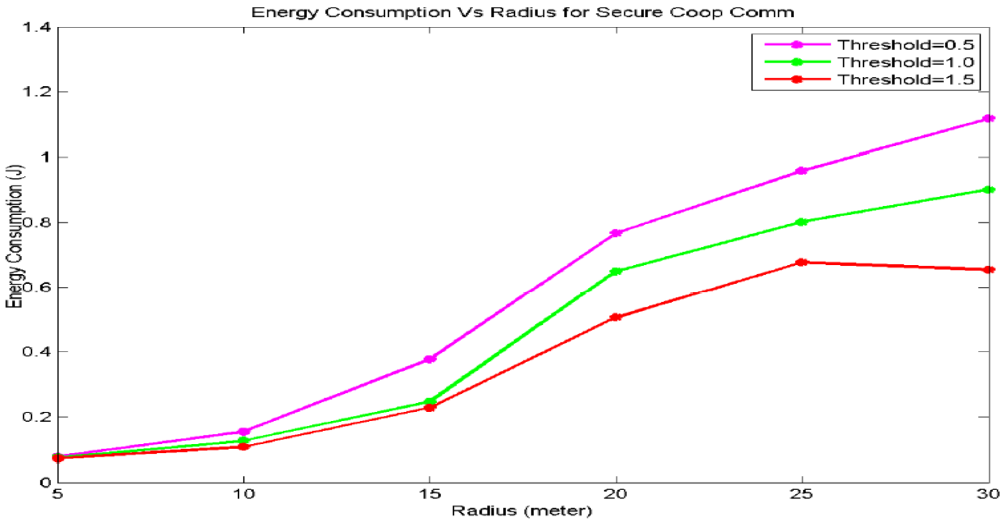

Figure 4.10 - Energy Consumption Vs Coverage Radius for Secure Cooperative CRN

Received signal strength (RSS) at the secondary relay nodes is depicted in the Figure 4.11 below. It can be clearly seen that as compared to without cooperation, the RSS valus is much better with cooperation. At the coverage radius of 30 meters, the RSS value is almost zero without cooperation whereas at the same value, the RSS value is found to be around 0.14 with cooperation. Secondary users can recognize each other's RSS signals and share a common protocol and are able to identify each other. Also due to increase or decrease in the trust levels due to the behavior in the cooperative system, the secondary users are unable to emulate primary users. If any of the secondary user tries to misbehave and emulate primary user, its trust level gradually decreases and at the last, the node is blacklisted from the total communicating network entities. The RSS value with cooperation is promising figure for the secondary entities in the cognitive radio networks. As in [6], the fraction of energy saving (FES) is given by,

$$\text{FES} = 1 - \frac{\substack{number\ of\ active\ radio\ nodes\ utilized \\ for\ cooperative\ transmission}}{\substack{Total\ number\ of\ nodes \\ in\ the\ OLA\ network}} \text{ --------- (4.7)}$$

It is clearly observed from the figure that the FES value with security mechanism differs from the Cooperative system without security by almost 10%. Since the proposed system makes use of light weight cryptography and cooperative web of trust, the cost for the cooperative web of trust mechanism inclusion is less almost 10% as shown in Figure 4.12. Security inclusion cost of 10% is the promising result. Because the traditional cryptographic techniques are very much costly in terms of energy and computing power. Also, it is interesting to note that for higher values of threshold, the fraction of energy savings is considerably higher as compared to the low threshold situations.

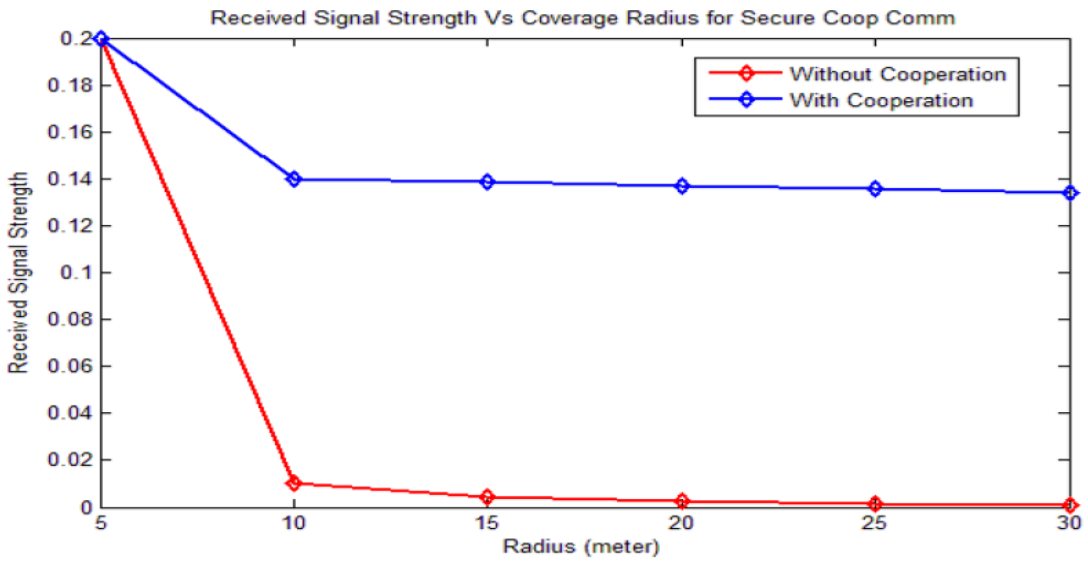

Figure 4.11 - Received Signal Strength vs. Coverage Radius for Secure Web of Trust with and without Cooperation

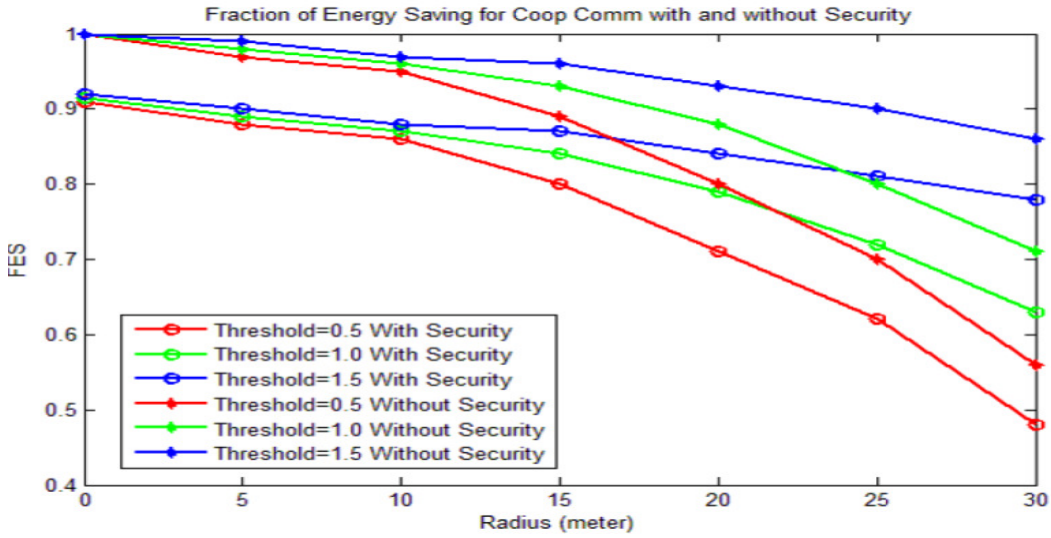

Figure 4.12 - Fraction of Energy Savings Vs Coverage Radius with and without application of Secure Web of Trust and Cooperation

4.8 Conclusions

The cooperative web of trust seems to provide promising energy efficient security solution for the spectrum sensing technique in cognitive radio networks. Also, the RSS values obtained are observed to be the effective result in the direction of improvement in the energy detection mechanism for spectrum sensing. Web of trust mechanism with cooperative diversity provides appropriate security solution for the primary user emulation attacks. Depending on the trust levels acquired through reputation in the system, the nodes immediately get either rewards for good behaviour or get blacklisted due to extreme

misbehaviour. However, some improvements are needed in the present system. The storage of hash values is also a resource consuming prospect. Using proper function by light weight cryptography, the hash values can be computed at the run time, without consuming much time, thus eliminating the overheads of space and time requirements. Also since each broadcast consumes some energy, only relevant acknowledgements should be propagated, so that the system assumes the presence of an end-to-end logical channel, without having to bother about the intermediaries and the overhead such as acknowledgement sending to them. The authorization implemented assigns the role dynamically on the basis of reputation of the node.

References

[1] J. Mitola, "Cognitive radio architecture evolution," Proc. IEEE, vol. 97, no. 4, pp. 626–641, Apr. 2009.

[2] J. L. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network".

[3] Chen K-C et al, "Cognitive radio network architecture: part I—general structure", In the Proceedings of the 2nd international conference on ubiquitous information management and communication, Suwon, Korea, 2008a, pp.114–119.

[4] Sazia Parvin , Farookh Khadeer Hussain, Omar Khadeer Hussain , SongHan, Biming Tian, Elizabeth Chang," Cognitive radio network security: A survey", Journal of Network and Computer Applications, Elsevier, July 2012.

[5] Shahid MIB, Kamruzzaman J.," Weighted soft decision for cooperative sensing in cognitive radio networks", 16th IEEE international conference on networks (ICON), New Delhi, 2008, pp. 1–6.

[6] A. M. Wyglinski, M. Nekovee, Y. T. Hou, "Cognitive Radio Communications and Networks: Principles and Practice", Elsevier, Dec 2009.

[7] Sazia Parvin, Song Han, Farookh Khadeer Hussain, Md. Abdullah Al Faruque, " Trust Based Security for Cognitive Radio Networks", ACM iiWAS '10 Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services, pp 743-748.

[8] Helena Rifà-Pous, Carles Garrigues," A Secure and Anonymous Cooperative Sensing Protocol For Cognitive Radio Networks", ACM SIN '11 Proceedings of the 4th international conference on Security of information and networks, pp 127-132.

[9] Ian F. Akyildiz, Brandon F. Lo, Ravikumar Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey", Elsevier Science Direct Physical Communication 4, 2011, pp. 40-62.

[10] Vandana Rohokale, Nandkumar Kulkarni, Neeli Prasad, Horia Cornean, "Cooperative Opportunistic Large Array Approach for Cognitive Radio Networks", 8th IEEE International Conference on Communications, Bucharest, Romania, pp.513-516, June 2010.

[11] Wu Guo-feng, Zhu Shi-lei, Hu Xiao-ning and Hu Han-Ying, " A Trust Mechanism-based Secure Cooperative Spectrum Sensing Scheme in Cognitive Radio Networks", ESEP 2011: 9-10 December 2011, Singapore.

[12] Jiang Hong, Yu Qing-song, Lu Hui, "Simulation and Analysis of MAC Security Based on NS2", IEEE International Conference on Multimedia Information Networking and Security, 2009.

[13] Sudip Misra , Ankur Vaish, "Reputation-based role assignment for role-based access control in wireless sensor networks", Computer Communications 34 (2011) ,pp.281–294,2011.J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility (Periodical style)," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34–39, Jan. 1959.

[14] Donggang Liu, Peng Ning, "Security for Wireless Sensor Networks", pg.177, 2007 Springer Science+Business Media.,2007.

[15]Yinian Mao, Min Wu, "Tracing Malicious Relays in Cooperative Wireless Communications", IEEE Transactions on Information Forensics and Security, Vol. 2, No. 2, June 2009.

[16] Massimo Merro and Eleonora Sibilio, "A Calculus of Trustworthy Ad-hoc Networks", Springer-Verlag Berlin Heidelberg 2010, pp. 157–172, 2010.

5

Physical Layer Security and Cooperative Jamming for Wireless Sensor Networks

Interference is generally considered as the redundant and unwanted occurrence in wireless communication. The research work in this chapter proposes a novel cooperative jamming mechanism with information theoretic security for scalable networks like Wireless Sensor Networks (WSNs) which makes use of friendly interference to confuse the eavesdropper and increase its uncertainty about the source message. The whole communication link is built with the help of Information theoretic source and channel coding mechanisms. The whole idea is to make use of normally inactive relay nodes in the selective Decode and Forward cooperative communication and make them work as cooperative jamming sources to increase the equivocation of the eavesdropper. In this work, eavesdropper's equivocation is compared with the main channel in terms of mutual information and secrecy capacity.

5.1 Introduction

The performance of wireless networks is greatly affected by some of the channel parameters such as bandwidth and power scarcity, multi-user interference, non-reliability due to signal fading, vulnerability to the attacks, etc. The cooperative diversity mechanism makes use of the benefits of wireless sensor network scalability in terms of cooperative resource sharing in which multiple diversity channels are created resulting into the higher transmission rates, increased throughput and coverage range, improvement in reliability and end-to-end performance and much more. Cooperative wireless communication (CWC) greatly improves the cross layer optimizations.

Wireless sensor nodes are inherently memory and energy constrained. Today's commonly utilized algorithms such as RSA, Diffie-Hellman, NTRU and Elliptic Curve Cryptography make use of large numbers multiplication in their encryption and decryption mechanisms. Due to their huge demand of memory and energy, these cryptographic algorithms cannot be employed to wireless sensor nodes. These higher layer cryptographic protocols are complicated and costly solutions for the distributed ad hoc networks like WSN. This research work proposes a cooperative jamming technique for physical layer security with the help of Information Theoretic source and channel coding mechanisms. In CWC, the active nodes may increase their effective QoS via cooperation. Among three popular cooperative relaying strategies, Amplify and forward mechanism results in the noise amplification and is not suitable for the scalable networks like wireless sensor networks. Decode-and-forward mechanism is well suited for WSN provided that the channels are strong enough. Cooperative Jamming is designed to mystify the eavesdropper.

Wireless sensor nodes are resource constrained miniature devices and energy reservation for lifetime extension is crucial for them. Most of the energy consumption occurs due to the transmissions. Hence, reduction in the amount of data transmissions can result in energy savings. Information theoretic communication concept was born after the evolutionary paper by Cloud Shannon titled "A Mathematical Theory of Communication" [1]. Physical layer security and Information Theory are closely related to each other and it is extensively studied in [2,3], which opened the doors for the security considerations at physical layer. Information theoretic analysis of cryptosystems was kicked off by Shannon in [4] where he has shown that the number of different keys like private and public keys must be at least as

large as the number of messages to achieve perfect secrecy. According to Shannon, the system is considered to be perfectly secure if the a posteriori probabilities of source X given eavesdropper E are equal to the a priori probabilities of X for all E, that is, $P(X/E)=P(X)$. WSN is a low data rate system. To limit the data rates, efficient compression is necessary. Channel coding mechanisms like LDPC, Convolution coding, BCH coding and Reed Solomon are proven to be reliable which can provide the lower values of BER rates.

Relaying and cooperative diversity essentially creates a virtual antenna array. All of the cooperative diversity protocols are efficient in terms of full diversity achievement and optimum performance except fixed decode-and-forward approach. Although prior to Laneman [3], the work on relay and cooperative channels utilized full duplex approach, he has constrained the cooperative communication to employ half duplex transmissions. Also in this case, the Channel State Information (CSI) is employed in the receiver instead of transmitter.

Wire-tap channel was introduced by Wyner where the eavesdropper's channel is assumed to be degraded as compared to the legitimate receiver's channel. The positive perfect secrecy was achieved for the single user wire-tap channel [4]. Csiszar and Korner in [5] studied the single user eavesdropping channel which was not necessarily degraded and obtained the secrecy capacity. They introduced superposition coding technique for the broadcast channels. Physical layer security intends to make use of the inherent randomness in the wireless channels to provide the additional security at physical layer. Statistical independence between the eavesdropper's observation and the actual message is an important measure for the Information Theoretic Security (ITS). ITS is measured by the Eve's uncertainty about the message given the code word, called the Eve's equivocation [6].

As compared to the conventional cryptosystems, the secrecy assured by the Information theoretic mechanisms is more cost effective solution because it avoids the key generation and management tasks and results into the significantly lower complex solutions which are proven to provide the savings in the resources like memory and battery supply which are the critical issues for the resource constrained wireless sensor networks. Also the information theoretic security mechanisms are less prone to the man-in-the-middle attack as compared with the public key cryptosystems because of the inherent randomness shared by

the communicating radio nodes [7, 8, 9, 10, 11]. The ITS mechanisms are shown to be robust for the dominant eavesdroppers which possess unlimited computational resources and have access to the communication systems either through perfect or noisy channels.

Matthieu Bloch and Joao Barros in their work [12] have shown adorable results with the appropriate combination of Information Theoretic Security and Cryptography. They have shown that source and channel coding techniques with small cryptographic one time pads can achieve perfect information theoretic secrecy. The authors have proposed a key pre-distribution scheme which makes use of a mobile node for the task completion of key distribution process blindly using network coding techniques. This methodology has shown to reduce the memory requirements. For secure communication, cryptography is not the only solution. By exploiting the intrinsic randomness of the channels and state-of-the-art error correcting codes, we can implement reliable and insensible data transfer which is the building block of the secure multi-node communication.

The research work by Liang Chen in [13] shows that the physical layer security can be achieved even though the relays possess lower security clearance values when the compress and forward cooperating mechanism is used. The authors propose the combined version of decode and forward with compress and forward for ripping the benefits from the advantages of both of them. They propose that when the channels are better and the relay nodes have higher security clearance figures then decode and forward scheme works better and for other conditions compress and forward scheme is the best choice. With these cases, the high transmission rates and physical layer security can be achieved.

In the research article by Yi Sheng Shiu et.al. [14], physical layer security issues for wireless communication are discussed in the tutorial fashion. Secret channel capacity and the computational capacity are considered as the metrics for the comparison among different physical layer tactics. The authors have classified the existing physical layer security techniques into five major categories based on their characteristic features. These classes can be listed as: theoretical secure capacity, the power, the code, channel and signal detection methodologies. Shuangyu Luo et. al. in their research work [15], have proposed an optimally organized Gaussian noise for cooperative jamming which results in the maximum secrecy rate. The authors have presented that when the optimal solution requires global channel information, the suboptimal solution requires only local channel information. The suboptimal

solution almost reaches close to the optimal solution for the achievement of secrecy rate. Uncoordinated cooperative jamming mechanism is proposed wherein no eavesdropper channel information is needed for the secure communication.

Cooperative jamming protocol system design for secure wireless communication with the consideration of a relay with multiple antennas is proposed in [16] for determining the antenna weights and transmit power of source and relay, so that the system secrecy rate is maximized with the considerable decrease in the transmit power. Relay equipped with multiple antenna can provide degrees of freedom for the relay channel and thus can exclude the effects of jamming at the receiving end. In the research work of [17], the authors have proposed a novel full cooperative jamming and partial cooperative jamming methodologies for two hop decode and forward wireless MIMO relay systems in the presence of the eavesdropper. Full cooperative jamming and partial cooperative jamming depends on whether the transmitter and helper are transmitting the jamming signals at the same time. With these proposed cooperative jamming schemes, the source and destination nodes act as momentary helpers for transmission of the jamming signals during their inactive phases.

Shyamnath Gollakota and Dina Katabi in their research work of [18] have presented a new physical layer approach called iJam for secret key generation which they claim to be fast and channel independent. The iJam mechanism works as follows. The transmitter sends its transmission twice. The receiver works as the jammer too. The receiver cum jammer jams gratis (some kind of alternate) samples from the original transmitted signal and its repeated version. At the time of decoding at the receiving end, the receiver combines together the unjammed samples from both the received signals to reconstruct the original exact transmitted signal. The working principle behind the iJam technique is that receiver jams the transmissions so that the information about the undisclosed key is kept secret from the eavesdropper while the intended recipient is allowed to extract the secret key perfectly by stitching the unjammed received symbols. The eavesdropper cannot imagine jammed samples of every transmission and hence jamming is a powerful technique but it is costly affair due to the task of continuous transmission of jamming signals.

In [19], the use of cooperating relays for the performance improvement of secure wireless communication with the eavesdropper's presence is proposed. The authors have taken into consideration three cooperative protocols namely decode-and-forward, amplify-

and-forward and cooperative jamming. With these cooperative protocols, two practical problems like transmit power allocation at the source and relays and relay weight determination for the achievable secrecy rates are analyzed. The improvement is observed in the limitations of channel conditions and the overall system performance with cooperation as compared to without cooperation strategies.

This chapter proposes joint source and channel coding mechanism for the physical layer security in resource constrained cooperative wireless communications. LZW source coding technique is used for secure data compression which will result in the low data rates and ultimately low energy consumptions. BCH and Reed Solomon channel coding method is utilized to achieve the appropriate reliability values. For modulation DSSS modulation with Gold codes and BPSK modulation is considered which proves to be inherently secure modulation technique. Friendly cooperative jamming mechanism is employed at the cooperating relay which sends jamming signals for the eavesdropper whereas at the same time, the source transmits the information signal intended to the receiver.

5.2 Physical Layer Security (PLS)

The importance of protecting the secrecy of sensitive messages has been realized by people since ancient times. By making use of strong techniques, the storage and transmission of information has become cheap and simple in modern times. A huge amount of information is transformed in a way that almost anyone may access it. A lot of new problems related to cryptology appear. For example, an adversary might not only have the means to read transmitted messages, but could actually change them, or the enemy could produce and send a false message to the receiver and hope that this would initiate some action. The transactions with the help of wireless networks such as credit card transactions or banking related data exchange communications are prone to the malicious behaviour due to the open nature of wireless medium. Adversaries can easily get access to the wireless transactions and can modify the data therein [20].

Traditional cryptographic techniques include symmetric (private) and asymmetric (public) key systems which are further classified into different mechanisms such as DES, AES, RSA, Diffie-Hellman, etc. as shown in the Figure 5.1. The main problem associated with these

cryptographic techniques is that they include complex mathematical calculations which consume considerable part of the resources which are very much crucial for wireless sensor nodes or the consumer radio nodes of the cognitive radio networks.

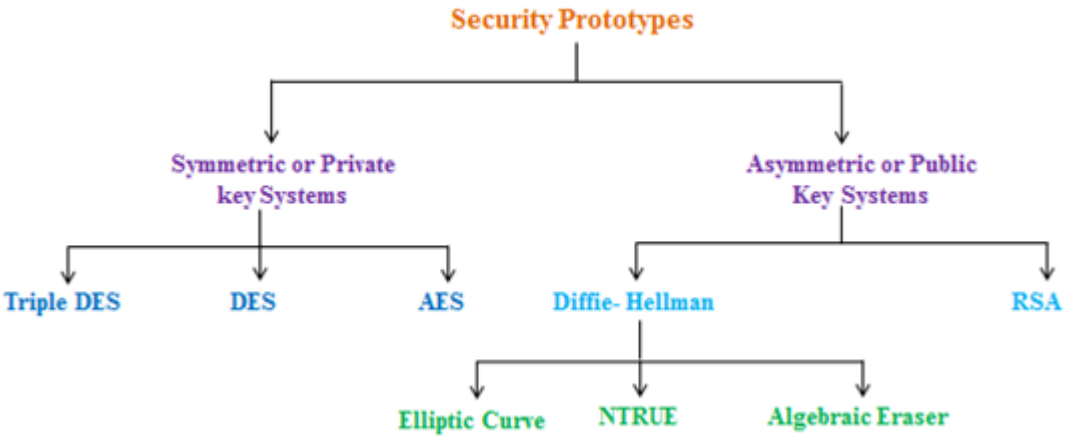

Figure 5.1 - Classification of Security Mechanisms

For establishment of a communication link in between sender and receiver, traditional cryptographic encryption block making use of public and private keys is required at the transmitting end while at the receiving end, channel decoding and decryption blocks are separately used. With the help of information theoretic security, encryption and channel coding blocks are combined in a single secure encoding block as depicted in Figure 5.2.

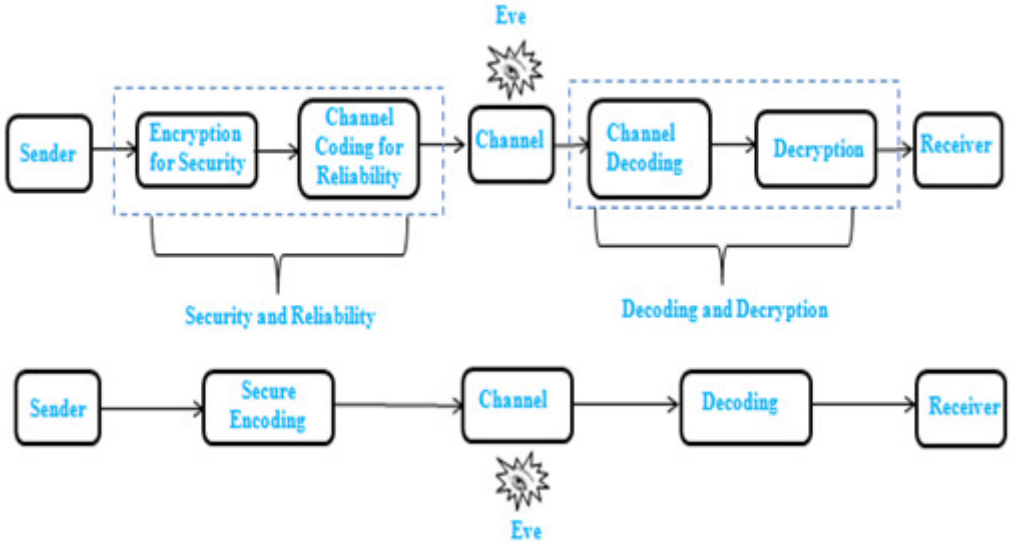

Figure 5.2 - Information Theoretic Security combines Security and Reliability Functions in a single block

Also, at the receiving side, channel decoding and decryption blocks are combined to form decoding block. This greatly reduces resource consumption because of relief from the

key management functionality which is most costly affair. With the basic wiretap channel, and variants of it like Gaussian, MIMP, compound wiretap, feedback wiretap and wiretap channel with side information are considered for the detail analysis in their work. They have further extended their work from basic wiretap channel to broadcast channels, multiple access channels, interference channels, relay channels and two-way channels [21].

In the research work of [22], a tutorial is presented on the security improvement techniques at the physical layer in wireless networks. Depending on their characteristic features, these are classified into further subclasses as shown in Figure 5.3. Two metrics considered for the security analysis include secret channel capacities and computational complexities in comprehensive key search.

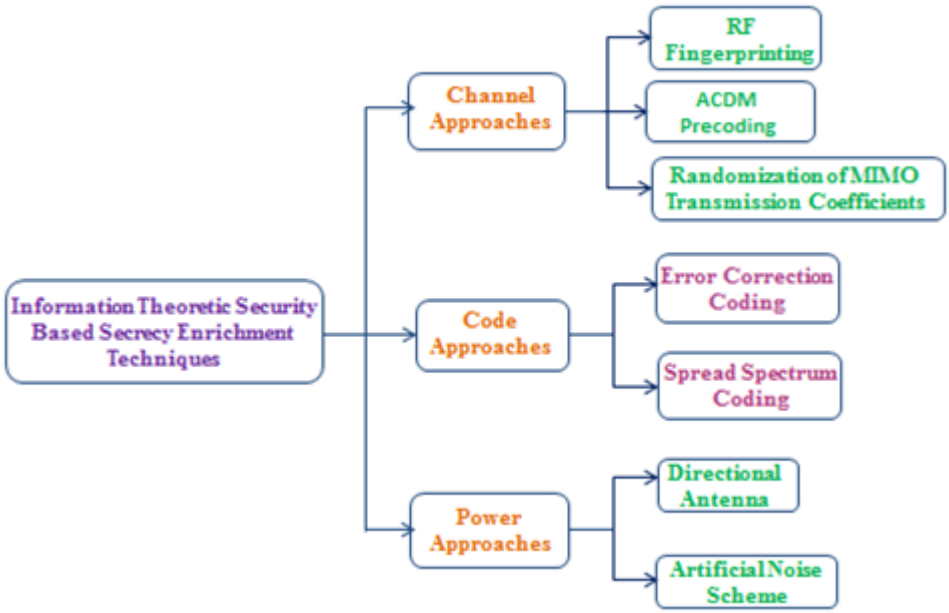

Figure 5.3 - Security Enhancement Techniques based on Information Theoretic Mechanisms

Built in physical layer security is nothing but the capacity of the transmission channel. It is called secret channel capacity. It is defined as information theoretic secrecy because the eavesdropper's received signal does not give any information about the original transmitted signal. It just keeps on purely guessing. Information theoretic secrecy is in fact equivalent to perfect secrecy. In the research work of [23], cooperative jamming technique is used to confound the eavesdropper and relay is cooperatively sending jamming signals towards the eavesdropper to confuse it about the actual transmitted signal. Here, the secrecy capacity observed is almost equal to the perfect secrecy.

Traditional application layer cryptographic mechanisms cannot go beyond detection of signal corruption to determine the eavesdroppers. For the detection of malicious behaviour by the compromised relay node in the cooperative communication, the authors in the work of [24] have proposed a cross-layer technique which makes use of adaptive signal detection at the physical layer with the statistical signal detection scheme making use of pseudorandom tracing symbols at the application layer. In [25], two different cooperative techniques are introduced viz. cooperative relaying and cooperative jamming for gaining the security. Power allocation of relay with cooperative relaying and jamming is studied for the achievement of optimum secrecy rate with the available source transmit power. Secrecy capacities of cooperative relaying and cooperative jamming techniques are compared with and without eavesdropper's channel state information.

Imperfect channel condition is the challenging issue for consideration of physical layer security in wireless communications. Cooperative decode and forward approach is considered to combat channel fading and achieve security in the information transmission in [26]. For the assumption of the presence of one eavesdropper, optimal solution is achieved with the help of iterative solution for transmit power minimization consideration. For the assumption of multiple eavesdroppers, due to the problem of secrecy capacity maximization with transmit power minimization, suboptimal solution is proposed by considering the restriction of complete nulling of signals at all the eavesdroppers.

Synergy MAC protocol for now a days Wi-Fi security framework is nothing but the extension of cooperative communication protocol at physical layer to the MAC sublayer. It results into the advantage of spatial diversity with increased transmission rates. For security adjustment in the cooperative scenario, two new security schemes are proposed for 802.11i viz. WPA and WPA2. Various security algorithms such as WEP, WPA and WPA2 are appropriately analysed in the work of [27] to function with Synergy MAC. The speciality of Synergy MAC is that it has multi-rate capability for packet transmission.

For establishing secure connection in between source and cell edge destination users in the presence of an eavesdropper, relay placement is observed to be more advantageous. Also when path loss is more severe, relay transmission is found to be beneficial. In the randomize-and-forward (RF) relaying mechanism, different randomization is introduced in each hop which is proved to be better physical layer security solution as compared to the traditional

decode-and-forward (DF) relay technique [28]. For achievement of physical layer security, two cooperative relaying schemes are analysed in [29] namely Decode-and-forward (DF) and Cooperative Jamming (CJ). For cell edge users, relays in between decode the received signal and again encoded and weighted signal is transmitted to the receiver. While the source is transmitting the weighted information signal to the receiver, some of the cooperating relay nodes are transmitting weighted noise signal to misperceive the eavesdropper. Two objectives are taken into consideration viz. maximization of the achievable secrecy rate and minimization of total transmit power.

Due to open nature of multi-hop cooperative communication networks, they are inherently prone to the security threats such as impersonation attacks and message integrity at the receiving end. In the work of [30], the authors have put forth a prevention based technique for secure relay selection for cooperative wireless communication which includes authentication protocol designed with hash chains and Merkle trees. The proposed security system can enhance the number of messages in the Merkle tree and at the same time it can appropriately select secure relay nodes for cooperative communication with significant improvement in the throughput QoS. Throughput attained by using this technique is observed to be higher than the systems without security provision.

In [31], secure cooperative transmission technique making use of physical layer security which considers the presence of passive eavesdroppers. The channels under consideration are frequency flat and frequency selective channels. By exploiting the local information available at individual nodes, full diversity and prevention against malicious behaviour is achieved by keeping intact the transmitter efficiency. The proposed protocol is named as Anti-Eavesdropping Space Time Network Coding (AE-STNC) which works on the principle of randomizing the signals being received at the eavesdroppers with best channel quality so that it becomes difficult for the eavesdropper to capture the messages under transmission. The AE-STNC protocol is extended further to design AE-STFNC for the broadcast asynchronous cooperative communication networks which is also provides the flexible diversity with security.

Due to highly mobile nature of the mobile adhoc networks, they suffer from imperfect channel conditions and frequently changing topology. The important network design parameters such as security and throughput are simultaneously analysed in the research work

of [32] for mobile adhoc networks. The authors have projected a topology control mechanism with authentication for throughput enhancement by combining higher layer security techniques with physical layer security techniques for CWC. The proposed system combines the authentication protocol technique from the upper layers in the protocol stack and transmission methodology from the physical layer to improve the overall cooperative system's throughput.

5.3 Proposed Secure CWC System Model

The simplified cooperative relaying is depicted in Figure 5.4 with only one relay and two eavesdroppers, one on the main channel and the other on the relay channel. In first time slot, source transmits the message to relay as well to the sink. At the same time slot, the relay will transmit the corresponding jamming signal intended towards the eavesdropper.

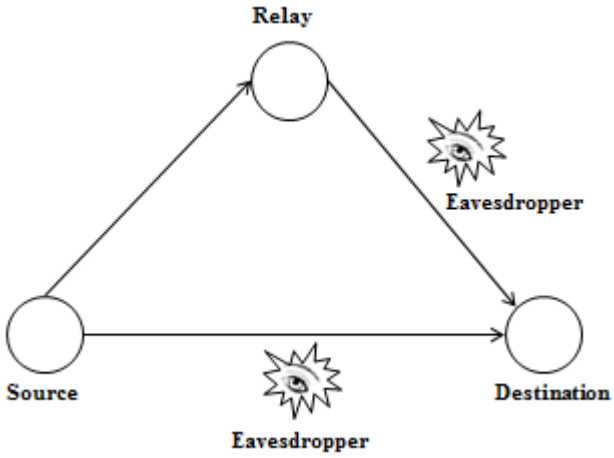

Figure 5.4 - Simplified Cooperative Relay Model with Eavesdropper

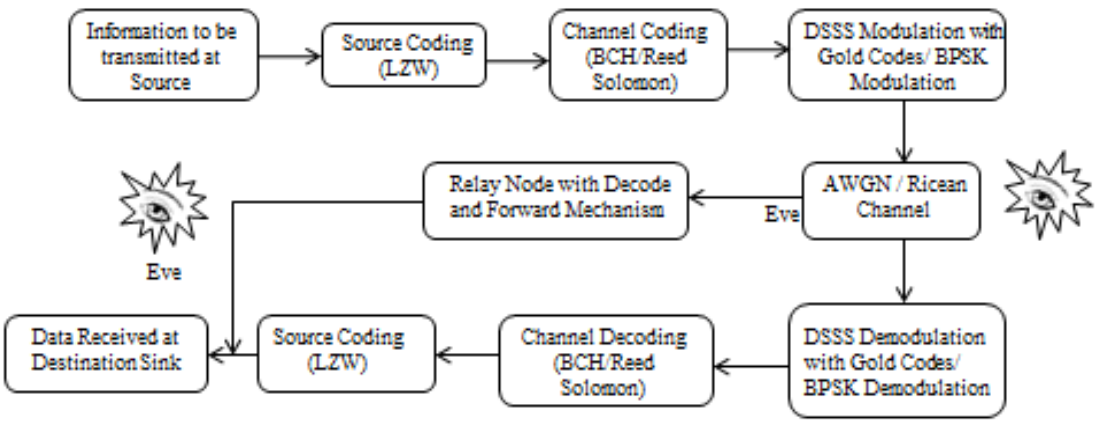

Figure 5.5 - Block Diagram of the proposed Information Theoretically Secure CWC

The complete functional block diagram is shown in Figure 5.5. It includes the source coding (decoding), channel coding (decoding) and the modulation (demodulation). Information theoretic mechanism with guaranteed secrecy has an added advantage due to relief from key management issues which results into considerable resource savings as compared to traditional cryptosystems. Key generation and key management tasks are the most expensive tasks in terms of resource usage. As compared to the public key cryptosystems, information theoretic security approaches are found to be less prone to man-in-the-middle attack due to the inherent randomness shared by the nodes [33].

Since the cooperative wireless sensor network nodes are battery limited devices, energy is the crucial parameter for their lifetime. Most of the energy consumption in wireless communications is due to the radio communication among the node entities. For limiting transmission data rates, the data compression mechanism is proved to be an energy efficient tool [34]. Out of all the available data compression algorithms, the LZW source coding mechanism seems to be inherently secure. Lempel Ziv technique can be modified to provide proper authentication requirement by the CWC for sensor networks. Good compression ratios ultimately result in considerable energy savings. BCH channel coding and decoding mechanism is utilized here. AWGN and Ricean channel is used for this purpose. Light weight version of the LZW and BCH coding is utilized here for cooperative WSN.

Cooperative jamming mechanism is implemented in this work. When the source transmits the actual information, at the same time, relay sends random jamming signal. Jamming signal received at the receiver is cancelled by making use of Interference cancellation technique [35]. And the jamming signal received by the eavesdropper is treated as the actual transmitted signal and it tries to decode it. Cooperative Jamming is a costly affair because some of the radio network nodes have to remain continuously busy sending jamming signals. This may result in quick draining of energy for these nodes.

After successful implementation of the above block diagram as shown in Figure 5.5, many simulations are performed for this case and then the probabilistic entropies, Mutual Information and channel secrecy capacities are calculated. The following parameters are taken into consideration like:

1. Entropy of the system as a whole $H(X, Y)$ – average information per pairs of transmitted and received characters.

$$H(x,y) = \sum_{i=1}^{n} \sum_{j=1}^{m} p(x_i, y_j) \log \frac{1}{p(x_i,y_j)} \quad \text{------ (5.1)}$$

2. Entropy of the source $H(X)$ – average information per character of the source.

$$H(x) = \sum_{i=1}^{n} p(x_i) \log \frac{1}{p(x_i)} \quad \text{---------- (5.2)}$$

3. Entropy at the receiver $H(Y)$ – average information per character at the destination.

$$H(y) = \sum_{j=1}^{m} p(y_j) \log \frac{1}{p(y_j)} \quad \text{---------- (5.3)}$$

4. Conditional Entropy $H(Y|X)$ – a specific character x_k being transmitted and one of the permissible y_j may be received (a measure of information about the receiver, where it is known what was transmitted). $H(Y|X)$ gives an indication of the noise (errors) in the channel.

$$H(y|x) = H(x;y) - H(x) \quad \text{---------- (5.4)}$$

5. Conditional Entropy $H(X|Y)$ – a specific character y_j being received; this may be a result of transmission of one of the x_k with a given probability (a measure of information about the source, where it is known what was received). $H(X|Y)$ gives a measure of equivocation (how well one can recover the input content from the output).

$$H(x|y) = H(x;y) - H(y) \quad \text{---------- (5.5)}$$

The mutual information for main channel is given by,

$$I(x;y) = H(x) - H(x|y) \quad \text{---------- (5.6)}$$

6. Similarly, mutual information for the Eavesdropper's channel is given by,

$$I(x;e) = H(x) - H(x|e) \quad \text{---------- (5.7)}$$

7. The maximum amount of mutual information is nothing but the secrecy capacity for that particular channel.

$$C_{SM} = \max [\, I(x;y) \,] \quad \text{---------- (5.8)}$$

Ultimate aim is to prove that $H_{E/X} > H_{Y/X}$ and $C_{sE} < C_{sM}$

where C_{sE}= Secrecy capacity of Eavesdropper's channel

C_{sM}= Secrecy capacity of the Main or Direct channel

Maximum amount of eavesdropper's equivocation (uncertainty of eavesdropper about the source message) indicates the system security.

5.3.1 LZW Source Coding and Decoding

Lempel-Ziv-Welch (LZW) is the most popular dictionary based lossless data compression technique. LZW is the algorithm where Welch has added some modifications to the prior available methodologies by Lempel and Ziv known as LZ77 and LZ78 [36, 37]. As compared to Shannon-Fano and Huffman coding techniques, LZW mechanism provides better compression ratios with improved coding efficiency.

Table 5.1 - LZW algorithm for sequence 0100111110010100000101010110011000

Numerical Positions	Subsequence (Parsed Data)	Codebook (Numerical Representation)	Binary Encode Blocks	Decoded Data with Dictionary Bits Numerical Position in bracket
1	**0**			**0** (1)
2	**1**			**1** (2)
3	01	12	00011	01 (3)
4	00	11	00010	00 (4)
5	11	22	00101	11 (5)
6	111	52	01011	111 (6)
7	001	42	01001	001 (7)
8	010	31	00110	010 (8)
9	000	41	01000	000 (9)
10 (A)	0101	82	10001	0101 (A)
11 (B)	01011	A2	10101	01011 (B)
12 (C)	0011	72	01111	0011 (C)
13 (D)	0000	91	10010	00

LZW source encoding is skilled by parsing the source data sequence into the fragments that are the shortest sub sequences not encountered previously [38]. Let's consider one example data sequence to illustrate this algorithm as follows:

0100111110010100000101010110011000

The binary symbols 0 and 1 are assumed to be dictionary bits which are assumed to be codebook. So, we get,

Codebook/Dictionary Bits: 0, 1

Data to be fragmented: 0100111110010100000101010110011000

Data Parsing: 0, 1, 01, 00, 11, 111, 001, 010, 000, 0101, 01011, 0011, 0000

5.3.2 BCH Channel Encoding and Decoding

BCH codes form the subclass of cyclic codes which are powerful random error correcting codes. It is the good generalization of the Hamming codes for multiple error correction. BCH codes were simplified by making use of Galois field and primitive polynomials by Gorenstein and Zierler [39]. Berlekamp's iterative algorithm and Chien's search algorithm are the most efficient BCH decoding algorithms. The most common binary BCH codes are known as primitive BCH codes and are characterized as follows:

Block Length: $n = 2^m - 1$

Number of message bits: $k \geq n - mt$

Minimum Distance: $d_{min} \geq 2t + 1$

Each BCH code is and t-error correcting code which can detect and correct up to *t* random errors per codeword. Let α be a primitive element of $GF\ (2^m)$. The generator polynomial *g(x)* of *t* error correcting BCH code of length $2^m - 1$ is the lowest degree polynomial over GF(2) which has $\propto, \propto^2, \propto^3 \ldots\ldots \propto^{2t}$ as its roots. Let $f_i(x)$ be the minimal polynomial of $\propto^i$. Then *g(x)* must be the LCM of $f_i(x)$ as follows:

$$g(x) = LCM\{f_1(x), f_2(x), f_{2t}(x)\} \text{ ------- (5.9)}$$

Since the BCH codes are a subclass of the cyclic codes, any standard decoding procedure for cyclic codes is also applicable to BCH codes. Many efficient algorithms have been designed specifically for BCH codes. Here we have applied Gorenstein-Zierler decoding algorithm which is the generalized form of the binary decoding algorithm first proposed by Petersen. Here, we have utilized *t* error correcting BCH decoding algorithm. Various BCH decoding algorithms are available in literature. Most of them follow the general steps of error detection and error correction as below.

- Calculate syndromes for the received code vector.
- Decide the number of errors *t* and the error locator polynomial from the syndromes.
- Find out the roots of error locator polynomial to find out the exact error locations.
- Calculate error values corresponding to respective error locations.
- Correct the detected errors at respective locations.

The whole decoding procedure can be illustrated as shown in figure 5.6 below.

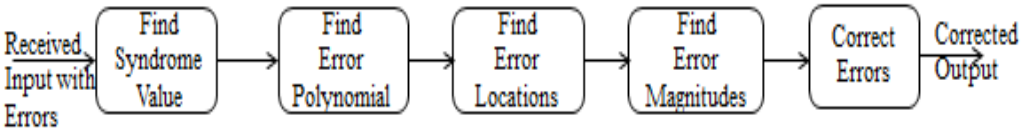

Figure 5.6 - BCH Decoding Mechanism

Here we assume t_c error correcting BCH code. Suppose a BCH code is constructed based on the field element α. Consider the error polynomial

$$e(x) = e_{n-1}x^{n-1} + e_{n-2}x^{n-2} + ...e_1x + e_0 \quad \text{------- (5.10)}$$

where at most t_c coefficients are non-zero. Suppose that p errors have actually occurred, for which, $0 \le p \le t_c$.

Let these error polynomials can then be written as,

$$e(x) = e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + ...e_{i_p}x^{i_p} \quad \text{--------- (5.11)}$$

Here we are considering the general case. For binary codes, $e_{i_k} = 1$. For error correction, we must know the error locations and error magnitudes. Thus the unknowns are $i_1, i_2, i_3, ..., i_p$ and $e_{i_1}, e_{i_2}, e_{i_3}, ...e_{i_p}$ which signify the error locations and error magnitudes respectively. The syndrome can be obtained by evaluating the received polynomial at α.

$$\begin{aligned} s_1 &= p(\alpha) = c(\alpha) + e(\alpha) = e(\alpha) \\ &= e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + ...e_{i_p}x^{i_p} \quad \text{-------- (5.12)} \end{aligned}$$

Now, the error magnitudes are needed to be defined like $y_k = e_{i_k}$ for *k=1, 2, ….p,* where i_k is the location of the k^{th} error and x_k is the field element associated with this location. Now the syndrome can be written as,

$$s_1 = y_1x_1 + y_2x_2 + ... + y_px_p \quad \text{------- (5.13)}$$

We can evaluate the received polynomial at each of the powers of α that has been used to define $g(x)$. We define the syndromes for $j = 1,2,.....2t_c$ by

$$s_j = p(\alpha^j) + c(\alpha^j) + e(\alpha^j) = e(\alpha^j) \quad \text{-------- (5.14)}$$

Thus we have the following set of $2t_c$ simultaneous equations, with p unknown error magnitudes $y_1, y_2, ...y_p$.

$$\begin{aligned} s_1 &= y_1x_1 + y_2x_2 + ... + y_px_p \\ s_2 &= y_1x_1^2 + y_2x_2^2 + ... + y_px_p^2 \\ &\vdots \\ s_{2t_c} &= y_1x_1^{2t_c} + y_2x_2^{2t_c} + ... + y_px_p^{2t_c} \end{aligned} \quad \text{------- (5.15)}$$

Now we need to define the error locator polynomial.

$$e(x) = e_px^p + e_{p-1}x^{p-1} + ... + e_1x + 1 \quad \text{------- (5.16)}$$

The zeros of this polynomial are the inverse error locations x_k^{-1} for $k = 1,2,....p$. That is,

$$e(x) = (1 - xp_1)(1 - xp_2).....(1 - xp_k) \quad \text{---------- (5.17)}$$

So, if we know the coefficients of the error locator polynomial *e(x),* we can obtain the error locations $x_1, x_2, ..., x_p$. After some algebraic manipulations, we get,

$$e_1 s_{j+p-1} + e_2 s_{j+p-2} + \ldots\ldots\ldots + e_p s_{j+p} \text{ for } j = 1,2,\ldots., p \text{ -------- (5.18)}$$

These are nothing but the set of linear equations that relate the syndromes to the coefficients of *e(x).* This set of equations can be written in the matrix form as below.

$$\begin{bmatrix} s_1 & s_2 & \ldots\ldots & s_{p-1} & s_p \\ s_2 & s_3 & \ldots\ldots & s_p & s_{p+1} \\ s_p & s_{p-1} & \ldots\ldots & s_{2p-2} & s_{2p-1} \end{bmatrix} \begin{bmatrix} e_p \\ e_{p-1} \\ e_{p-2} \end{bmatrix} = \begin{bmatrix} -s_{p+1} \\ -s_{p+2} \\ -s_{2p} \end{bmatrix} \text{ ------- (5.19)}$$

The values of the coefficients of the error locator polynomial can be determined by inverting the syndrome matrix. This is possible only if the matrix is non-singular. After finding out error locations, the error magnitudes are determined and then those many number of errors are corrected.

5.3.3 Reed Solomon Channel Encoding and Decoding

Reed Solomon codes are an important subclass of the non-binary BCH codes with a wide range of applications in mobile communication and data storage. Irving S. Reed and Gustav Solomon in their paper [40], introduced the idea of burst error correcting RS codes. In this subclass of BCH codes, the symbol field (sub-field) *GF(q)* and the error locator field $GF(q^m)$ are the same, i.e., *m=1*. Hence, for this case,

$$n = q^m - 1 = q - 1 \text{---------- (5.20)}$$

The minimal polynomial of any element β in the same field *GF(q)* is

$$f_{\beta(x)} = x - \beta \text{ ---------- (5.21)}$$

Since the symbol field and error locator field are the same, all the minimal polynomials are linear. The generator polynomial for a *t* error correcting code will be given by,

$$g(x) = LCM[f_1(x) f_2(x), \ldots\ldots., f_{2t}(x)] \text{---------- (5.22)}$$

$$= (x - \propto)(x - \propto^2) \ldots\ldots (x - \propto^{2t-1})(x - \propto^{2t}) \text{ ---------- (5.23)}$$

Hence the degree of the generator polynomial will always be *2t.* Thus, the RS code satisfies $n - k = 2t$.

5.3.4 DSSS Modulation and Demodulation with Gold Codes

For Indoor scenario, DSSS is the best choice because it is inherently secure due to the use of pseudo noise codes used for modulation. Gold Codes are the type of binary sequences

which use number of PN sequences to increase the security in WSN. Noisy nature of the wireless medium is exploited to improve the security of overall communication system. Gold codes have restricted small cross correlations within a set, which is useful when multiple devices are broadcasting in the same range. Steps for Gold code generation are as follows:

- Choose two maximum length sequences of the same length $2^{m}-1$ such that cross correlation is less than or equal to $2^{\frac{(m+2)}{2}}$, where *m* is the size of the Linear Feedback Shift Register (LFSR) used to generate the maximum length sequence.
- The set of the $2^{m}-1$ EX-ORs of the two sequences in their various phases is a set of Gold codes. The highest absolute cross-correlation in this set of codes is $2^{\frac{(m+2)}{2}}+1$ for even m and $2^{\frac{(m+1)}{2}}+1$ for odd m. The EX-OR of two Gold codes from the same set is another Gold code in some phase [41].

5.4 Performance Evaluation

The total communication link is prepared with Matlab codes. The parameters taken into consideration are listed in the table 5.2. For simulation purpose, the sequence of 300 bits is randomly generated and applied as an input to the LZW source coding block. The input to the BCH coding block is the binary sequence of 448 bits. Then (511, 448) BCH coding is applied with the error correcting capability of seven bits. The output of BCH coding block is containing 511 bits which is the input to DSSS modulation block. Twenty bit lengthy PN sequence is used for the construction of the Gold Codes. Accordingly the 511 bits data is spreaded to 10220 bits after the DSSS modulation. The AWGN channel is taken into consideration for this experimentation.

Table 5.2- Communication Link Design Parameters

Parameter	Technique Used	No. of input bits	No. of output bits
Input Data sequence	Binary data	300	
Source Coding	LZW Coding	300	448
Channel Coding (n, k, t)	BCH Coding (511, 448, 7)	448	511
Modulation	DSSS with Gold Codes	Gold code length = 20 bits	10220
Channel	AWGN channel With Noise addition	10220	10220
Demodulation	DSSS Demodulation	10220	511
Channel Decoding	BCH Decoding	511	448
Source Decoding	LZW Decoding	448	300

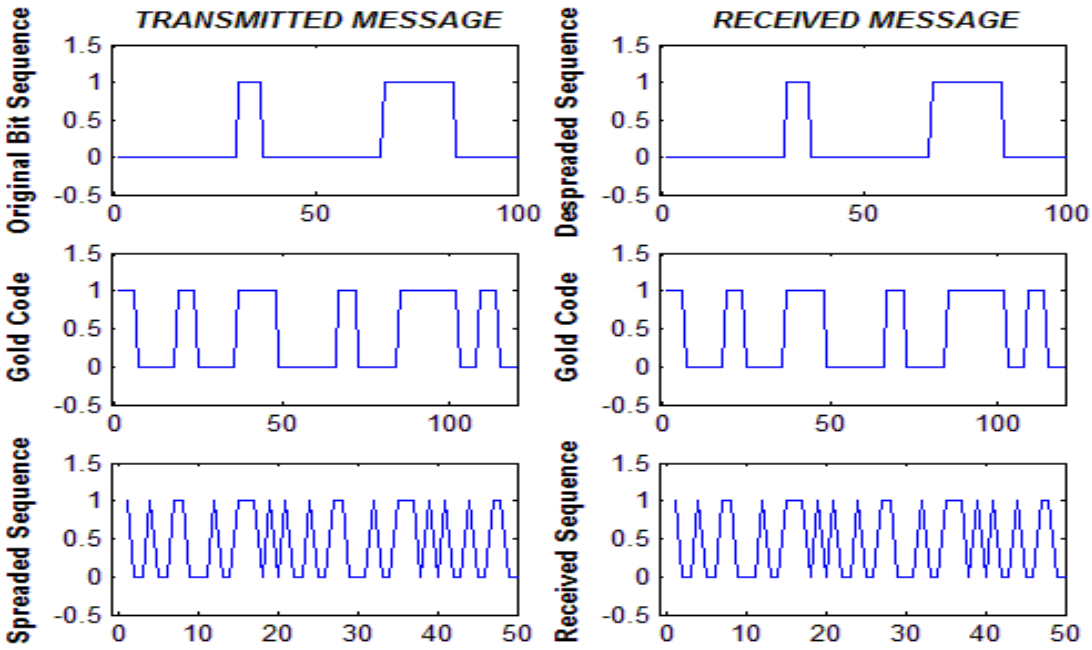

Figure 5.7 - BCH encoded Input data, Spreaded sequence, Despreaded sequence and Recovered data after demodulation

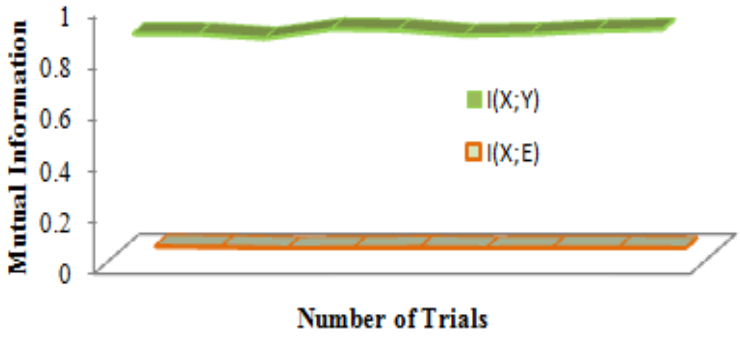

Figure 5.8 - Secrecy Capacities of Main and Eavesdropper's Channel in terms of Mutual Information with BCH channel coding mechanism

Figure 5.7 shows the BCH encoded data, its spreaded and despreaded version and data recovered after DSSS demodulation. BCH encoded data and BCH decoded data look exactly same. The secrecy capacities of the Main and Eavesdropper's channel are shown in the Figure 5.8 in terms of Mutual Information. The error correcting capability of RS and BCH codes is revealed from Figure 5.9 and Figure 5.10. Figure 5.9 shows that twenty eight errors are introduced through the Ricean Channel with the RS codec and all the errors are corrected by the RS decoding mechanism showing the BER value as zero. On the other hand, as shown in Figure 5.10, eleven errors are introduced through the Ricean channel with the BCH codec and again it corrects all the errors giving the BER value as zero. The zero bit error rate indicates

the maximum mutual information and maximum secrecy capacity. The error correcting capability of Reed Solomon mechanism is found to be approximately 40% greater than the BCH methodology. Hence it has been proved that the RS channel coding technique is more reliable as compared to the BCH technique. This is really promising result.

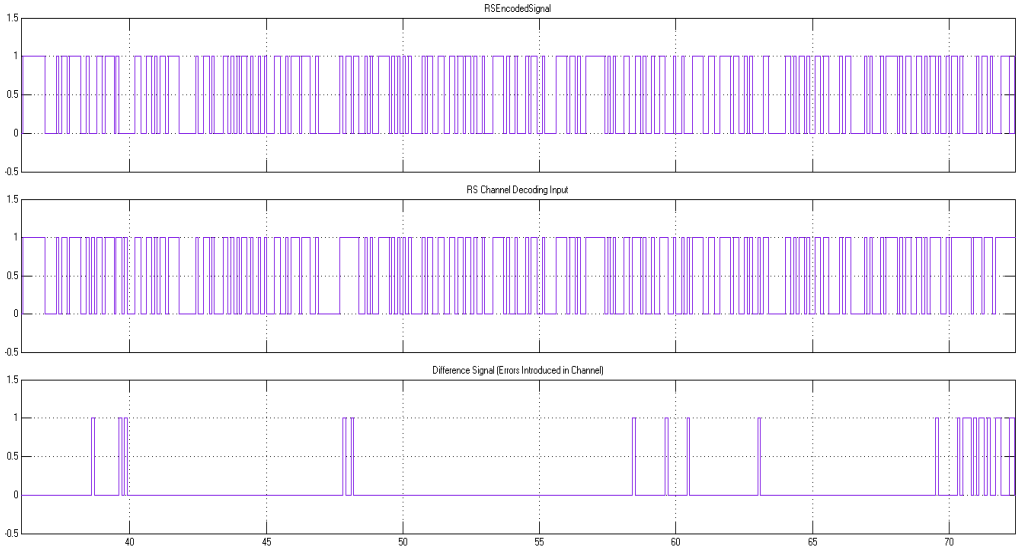

Figure 5.9 - Errors introduced in the RS encoded signal through Ricean Channel and noise

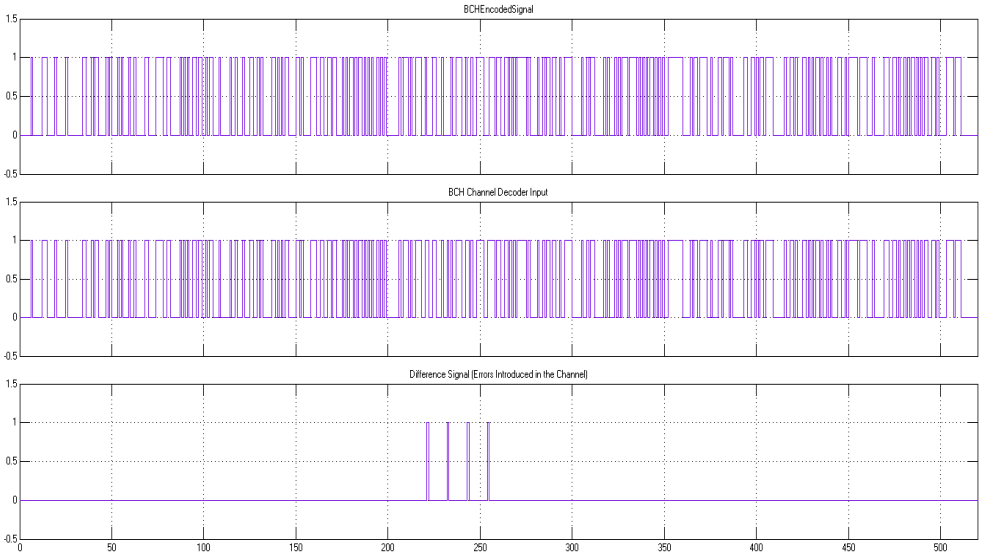

Figure 5.10 - Errors introduced in the BCH encoded signal through Ricean Channel and noise

Information to be transmitted at the source input and the recovered data at the final receiver or sink block are shown in the Figure 5.11. The original data is successfully recovered at the receiving end. First part of Figure 5.11 is the input to the LZW source coding block and the second part of the Figure 5.11 is the output of the LZW source decoding block. We observe the exactly same input and output bit sequences at the source coding input and

the source coding output blocks. This indicates zero error probability which is the indication of maximum mutual information and ultimately it results into the maximum secrecy capacity.

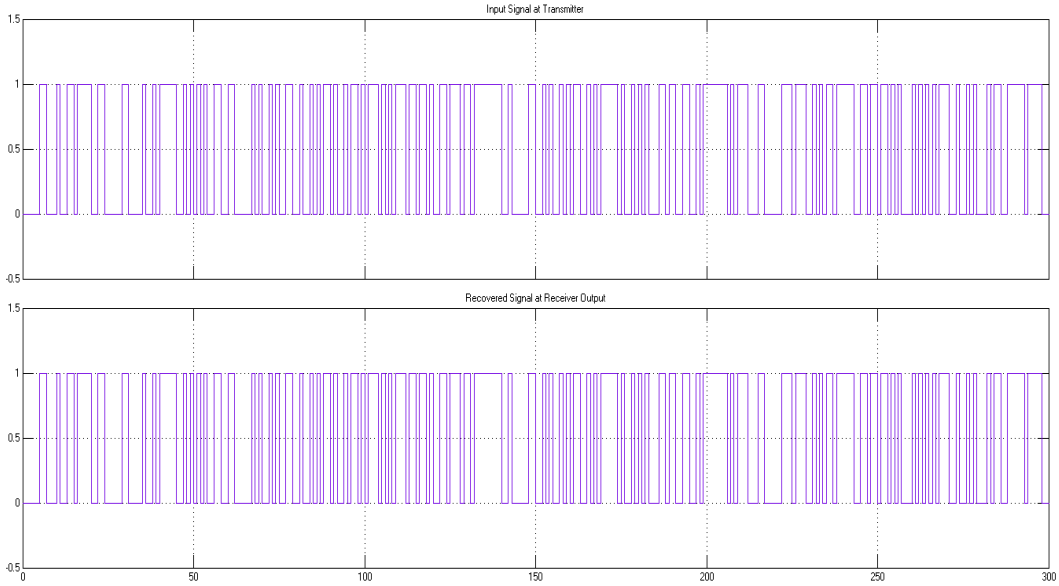

Figure 5.11 - Input signal at Transmitter and Recovered signal at Receiver output

If the probability of error is zero, then the data rate at which the transmitter communicates to the receiver is given by,

$$\text{Data Rate} = \frac{\log_2(\text{Number of Messages})}{n} = \frac{nR}{n} = P \text{ bits/sec} \quad (5.24)$$

And then channel capacity becomes

$$C = \max I(x; y) \quad (5.25)$$

Shannon's result states that "What can be achieved by the best strategy over *n* channel uses is given by the maximal mutual information for a single channel use" [2]. Secrecy capacity of a communication channel is nothing but the maximum amount of mutual information shared between source and receiver entities.

Figure 5.11 shows the transmitted signal at the input end of the communication link and the signal recovered at the receiver output. It is revealed from the plots that both input and output signals are exactly same and BER value is zero. The mutual information in between source and receiver *I (X; Y)* is depicted in the plot of Figure 5.12. It is observed from the figure that the mutual information between the source and receiver has much higher value. It is slightly less than one, the ideal value, which shows that the secrecy capacity of the main channel is high. On the contrary, the mutual information between the source and eavesdropper as shown in Figure 5.13 bears very less values which are less than 0.01. Also, the

eavesdropper's equivocation value is observed to be very high. This indicates that the secrecy capacity of the eavesdropper's channel is very low. So, the communication link built with the source and channel coding technique is proved to be secure one.

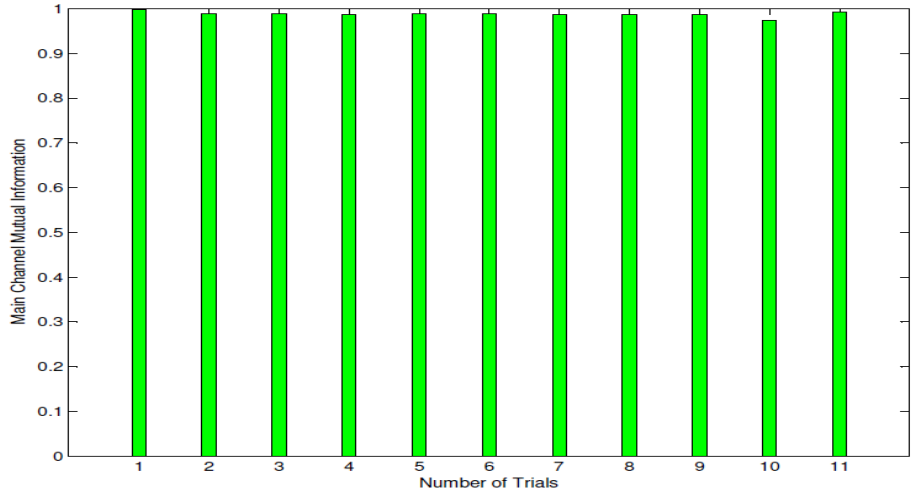

Figure 5.12 - Mutual Information in between Source and Receiver

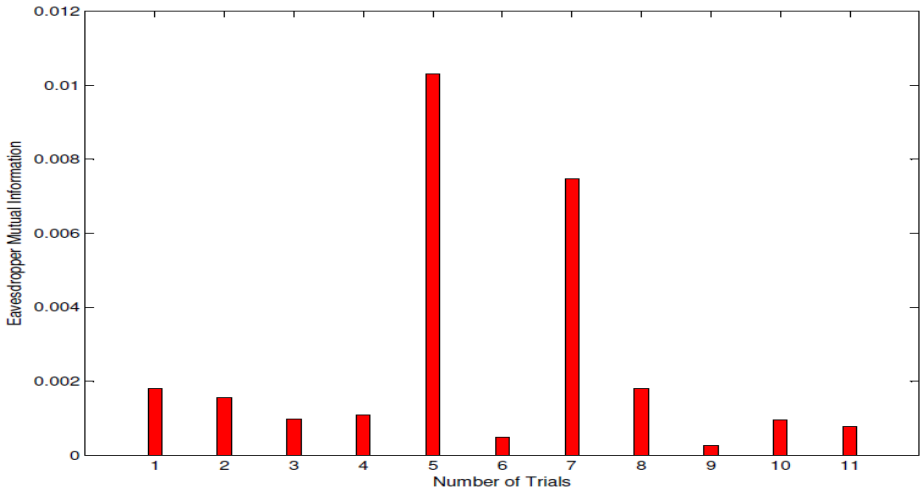

Figure 5.13 - Mutual Information in between Source and Eavesdropper

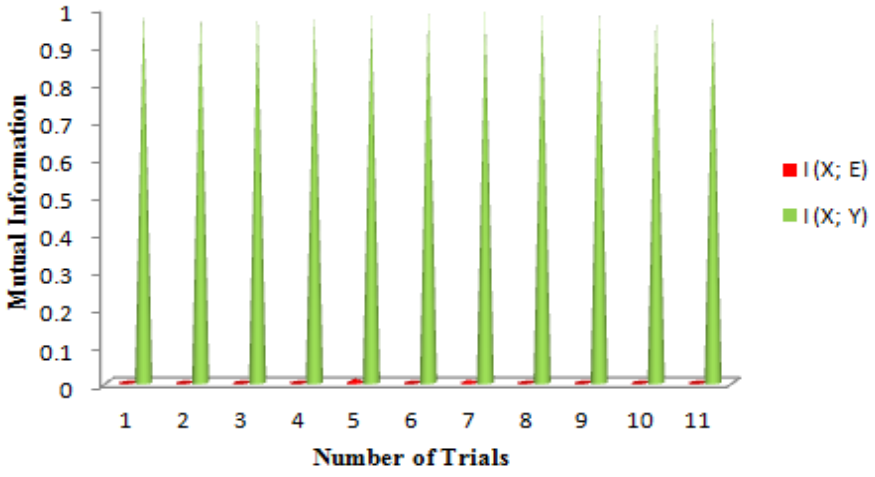

Figure 5.14 - Secrecy Capacities of Main channel and Eavesdropper's channel

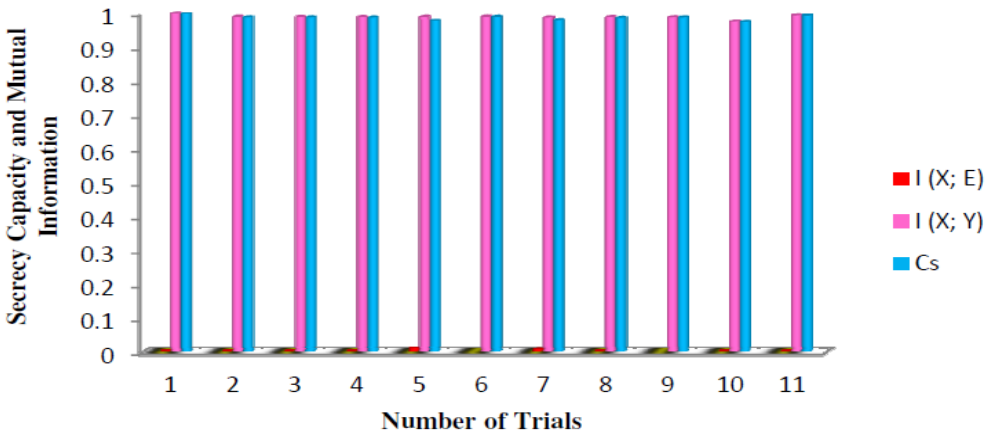

Figure 5.15 - Secrecy Capacity and Mutual Information of Direct Channel and Eavesdropper's Channel

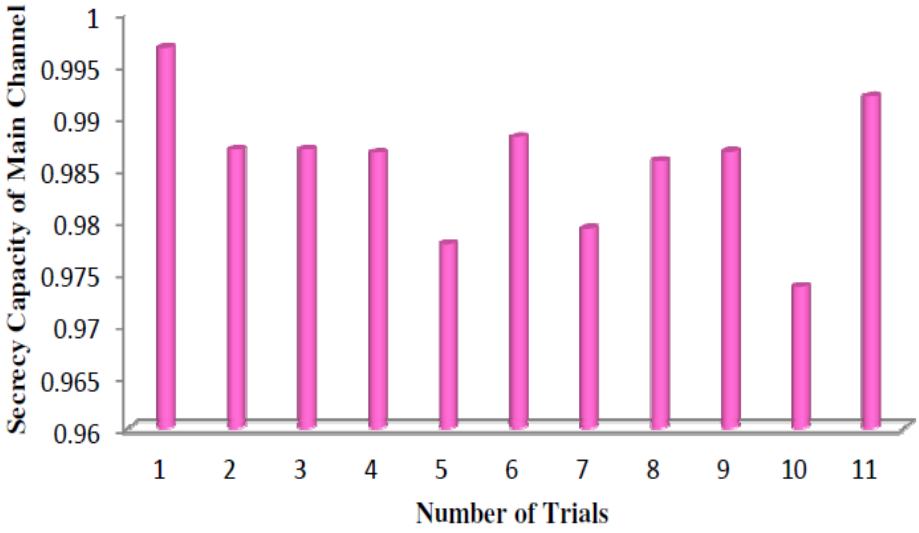

Figure 5.16 - Secrecy Capacity of the main channel

The mutual information for both the channels viz. eavesdropper's and main channels versus number of trials is shown in the Figure 5.14. For both the RS and BCH channel coding techniques, we have observed the maximum secrecy capacity for the main channel. And the eavesdropper's channel's equivocation is very high showing the least secrecy capacity, which indicates that our communication link is secure one. As is revealed form Figure 5.14, Mutual Information of the main (source-receiver) channel $I(X;Y)$ is much higher than the mutual information of the Eavesdropper's channel $I(X;E)$. According to Ciszar and Korner [5], the special case in which the eavesdropper is less capable that is,

$$I(X;E) \leq I(X;Y) \quad \text{---------- (5.26)}$$

Then Secrecy Capacity of a communication link can be given by,

$$C_s = \max_{P_X}[I(X;Y) - I(X;E)] \text{ ---------- } (5.27)$$

This shows that the secrecy capacity of the main channel is greater than the secrecy capacity of the eavesdropper's channel due to the jamming effect by the cooperating relay node. Hence, the Eavesdropper's Equivocation is much higher than the main channel. This is really encouraging result for the physical layer security. Also, the source and channel coding mechanisms taken into consideration are likely to consume fewer resources as expected by wireless sensor networks. From the plot of Figure 5.15, it reveals that the secrecy capacity of a system is almost equal to the maximum amount of the mutual information in between source and receiver which indicates the maximum amount of secrecy of the communication system. Figure 5.16 indicates the secrecy capacity of the main or direct channel in the presence of cooperative jamming relay with eavesdropper's presence. From the figure, it can be observed that the secrecy capacity's maximum value reaches almost 0.998 and at the same time the minimum value of the secrecy capacity is merely 0.96. This is very powerful result showing that the communication link built with the information theoretic blocks such as source and channel coding decoding mechanism with modem gives utmost security to the communication system.

5.5 Conclusions

Physical layer security mechanism comprising source and channel coding techniques is presented in this chapter. The whole communication link is built with the help of information theoretic source and channel coding techniques such as LZW source coding and BCH and RS channel coding methods. Maximum amount of uncertainty for eavesdropper's channel is the indication of the communication link security. Also, secrecy capacity of the main communicating channel is found to be far greater than the eavesdropper's channel which is the promising result for further work. The communication link built with the Reed Solomon channel coding and decoding technique is found to be more reliable as compared to the BCH channel coding decoding method. As compared to BCH technique, Reed Solomon mechanism is observed to possess almost 40% more error correcting capability. This work can be extended for selective decode and forward cooperative relaying technique while taking into consideration weights and polarization mechanisms at the relays.

References

[1] C. E. Shannon, “A Mathematical Theory of Communication”, The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.

[2] C. E. Shannon, “Communication Theory of Secrecy Systems”, The Bell System Technical Journal, Vol. 28, pp. 656-715, October, 1949.

[3] A. Wyner, “The Wire-tap Channel”, Bell System Technical Journal, vol.54, pp. 1355-1387, 1975.

[4] I. Csiszar and J. Korner, ”Broadcast Channels with Confidential Messages”, IEEE Transactions on Information Theory, vol. IT-24, no.3, pp. 339-348, May 1978.

[5] Anna Scaglione and Yao-Win Hong, “Opportunistic Large arrays: Cooperative Transmission in Wireless Multihop Ad-Hoc Networks to Reach Far Distances”, IEEE Transactions on Signal Processing, vol.51, no.8, pp. 2082-2092, August 2003.

[6] Y. Liang, H.V. Poor, S. Shamai (Shitz), “Information Theoretic Security”, Foundations and Trends in Communications and Information Theory, Vol.5, Nos. 4-5, pp. 355-580, 2008.

[7] L. Lai, H. El Gamal, and H.V. Poor, “Authentication over noisy channels”, IEEE Transactions on Information Theory, vol.55, pp. 906-916, February 2009.

[8] J. L. Massey, “Contemporary Cryptography-An Introduction”, in Contemporary Cryptography – The science of Information Integrity, pp. 533-549, Piscataway, NJ, USA:IEEE Press, 1992.

[9] U. M. Maurer, “Authentication Theory and Hypothesis Testing”, IEEE Transactions on Information Theory, vol. 46, pp. 1350-1356, July 2000.

[10] U. Rosenbaum, “A lower bound on authentication after having observed a sequence of messages”, Journal of Cryptology, vol. 6, no. 3, pp. 135-156, 1993.

[11] G. J. Simmons, “Authentication Theory/Coding Theory”, IN Proceedings of the CRYPTO’84 on Advances in Cryptography, pp. 411-431, Lecture Notes in Computer Science, New York, NY, USA: Springer - Verlag, 1985.

[12] M. Bloch, J. Barros, “Physical Layer Security: from Information Theory to Security Engineering”, Cambridge University Press, 2011.

[13] Liang Chen, “Physical layer security for cooperative relaying in broadcast networks”, Military Communications Conference - MILCOM 2011, USA, pp. 91-96.

[14] Yi-Sheng Shiu, Shih Yu Chang , Hsiao-Chun Wu, Huang, S.C.-H., Hsiao-Hwa Chen, “ Physical layer security in wireless networks: a tutorial”, IEEE Wireless Communications Journals and Magazines, vol. 18, Issue: 2, pp. 66-74, April 2011.

[15] S. Luo, J. Li and A. Petropulu, "Physical Layer Security with Uncoordinated Helpers Implementing Cooperative Jamming" in Proc. 7th IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM2012), pp. 97-100, Hoboken, NJ, June 2012.

[16] Zhu Han, A.P. Petropulu, H. V. Poor, " Cooperative jamming for wireless physical layer security", IEEE/SP 15th Workshop on Statistical Signal Processing, 2009. SSP '09, pp. 417-420.

[17] Jing Huang, "Cooperative Jamming for Secure Communications in MIMO Relay Networks", IEEE Transactions on Signal Processing, vol. 59, No. 10, pp. 4871-4884, October, 2011.

[18] Shyamnath Gollakota and Dina Katabi, "Physical layer wireless security made fast and channel independent", IEEE Conference, INFOCOM, pp. 1125 - 1133 April 2011.

[19] Lun Dong, Zhu Han, Athina P. Petropulu, and H. Vincent Poor, "Improving Wireless Physical Layer Security via Cooperating Relays", IEEE Transactions on Signal Processing, vol. 58, no. 3, pp. 1875-1888, March 2010.

[20] C. S. R. Murthy and B. S. Manoj, "Adhoc Wireless Networks Architecture and Protocols", Prentice Hall PTR, 2004.

[21] Yingbin Liang and H. Vincent Poor and Shlomo Shamai (Shitz) "Information Theoretic Security", Foundations and Trends in Communications and Information Theory: Vol. 5: No 4–5, pp 355-580, 2009.

[22] Yi-Sheng Shiu, Shin Yu Chang, Hsiao-Chun Wu, Scott C.-H. Huang, Hsiao-Hwa Chen, "Physical Layer Security in Wireless Networks: A Tutorial", IEEE Wireless Communications, April 2011.

[23] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Jamming for Physical Layer Security in Wireless Sensor Networks", 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, Sept 24-27, 2012.

[24] Yinian Mao, Min Wu, "Tracing Malicious Relays in Cooperative Wireless Communication", IEEE Transaction on Information Forensics and Security, vol.2, Issue:2, pp. 198-212, June 2007.

[25] Ling Tang, Xiaowen Gong, Jianhui Wu and Junshan Zhang, "Secure Wireless Communication via Cooperative Relaying and Jamming", IEEE GLOBECOM Workshop on Physical Layer Security, Dec 2011, pp. 849-853.

[26] Lun Dong, Zhu Han, Athina P. Petropulu and H. Vincent Poor, "Secure Wireless Communication via Cooperation", Fourty Sixth IEEE Annual Allerton Conference, USA, Sept 2008.

[27] Santosh Kulkarni and Prathima Agarwal, "Safeguarding Cooperation in Synergy MAC", 42nd IEEE Southeastern Symposium on System Theory (SSST), USA, PP. 156-160, March 2010.

[28] Jianhua Mo, Meixia Tao and Yuan Liu, "Relay Placement for Physical Layer Security: A Secure Connection Perspective", IEEE Communication Letters, vol.16, no.6, pp. 878-881, June 2012.

[29] Jiangyuan Li, Athina P. Petropulu, Steven Weber, "On Cooperative Relaying Schemes for Wireless Physical Layer Security", IEEE Transactions on Signal Processing, vol. 59, no.10, pp. 4985-4997, October 2011.

[30] Ramya Ramamoorthy, F. Richard Yu, Helen Tang, Peter Mason, Azzedine Boukerche, "Joint Authentication and Quality of Service Provisioning in Cooperative Communication Networks", Elsevier Journal of Computer Communications, 2012, vol.35, pp. 597-607.

[31] Zhenzhen Gao, Yu-Han Yang and K. J. Ray Liu, "Anti-Eavesdropping Space-Time Network Coding for Cooperative Communications", IEEE Transactions on Wireless Communications, vol. 10, no. 11, Nov 2011, pp. 3898-3908.

[32] Quansheng Guan, Yu, F.R., Shengming Jiang, Leung V.C.M., " A Joint Design for Topology and Security in MANETs with Cooperative Communications", IEEE International Conference on Communications (ICC), pp. 1-6, June 2011.

[33] Y. Liang, H.V. Poor, S. Shamai (Shitz), "Information Theoretic Security", Foundations and Trends in Communications and Information Theory, Vol.5, Nos. 4-5, 2008, pp. 355-580.

[34] J. L. Massey, "An introduction to contemporary cryptology", Proceedings of the IEEE, vol. 55, issue. 5, pp. 533-549, May 1988.

[35] U. M. Maurer, "Authentication Theory and Hypothesis Testing", IEEE Transactions on Information Theory, vol. 46, pp. 1350-1356, July 2000.

[36] Francesco Marcelloni and Massimo Vecchio, "An Efficient Lossless Compression Algorithm for Tiny Nodes of Monitoring Wireless Sensor Networks", The Computer Journal Advance Access, pp. 1-19, April 30, 2009.

[37] T.A. Welch, "A technique for high-performance data compression", Computer, vol.17, pp. 8–19, (1984).

[38] Simon Haykin, "Fundamental Limits in Information Theory", Communication Systems, 4th Edition, Wiley Publications, 2001.

[39] Morelos-Zaragoza, Robert H. and Lin, Shu, "On Primitive BCH Codes with Unequal Error Protection Capabilities" IEEE Transactions on Information Theory, Vol. 41, Issue. 3, pp. 788-790, May 1995.

[40] I. S. Reed and G. Solomon, "Polynomial Codes over Certain Finite Fields", Journal of the society for Industrial and Applied Mathematics, Vol.8, No.2, pp. 300-304, June 1960.

[41] M. George, M. Hamid, and A. Miller," Gold Code Generators in Virtex Devices", XILINX XAPP217, v1.1, pp. 1-9, Jan 2001.

6
Conclusions and Future Scope

This chapter concludes the thesis and puts forth new research directions which are based on performance evaluation of the proposed techniques and algorithms in this research work. Security, reliability and energy efficiency issues related to cooperative wireless communication are analysed in this thesis. Some of the important problems in the deployment of authentication and authorization for reliable and energy efficient cooperative communication are identified during this research work which are mentioned and future solutions are proposed.

6.1 Conclusions of the Thesis

In this thesis, we initially explored analytical and simulation model for Cooperative Opportunistic Large Array (COLA) for Wireless Communication with the limited radius for the coverage limited wireless sensor networks. Then we focussed on the execution of mechanism for the malicious behaviour detection in the cooperative wireless sensor networks with the help of receiver sensitivity figures. Subsequently, we analysed and simulated the cooperative environment for the outage probability analysis and QoS analysis. Next we investigated the experimentation on the cooperative web of trust (CWoT) for security in cognitive radio networks. Then we evaluated the performance of the cooperative jamming mechanism for physical layer security in wireless sensor networks.

Initially, introduction to the cooperative wireless communication field is presented. Direct and cooperative transmission techniques are compared. Next part includes the benefits of cooperation, different applications of cooperative transmission and various aspects of CWC. Then, State-of-the-art techniques in the field of cooperative communication are investigated here. The cooperative wireless communication is put forth in pretty details. Also, the opportunistic large array approach is discussed in details presenting the detail comparison of OLA algorithms with reference to parameters like energy efficiency, network lifetime, network scalability, delay, reliability, authentication and authorization. The parameters which have not been investigated in the research field until now are highlighted in the table and discussions thereafter. Motivation for the research work and real challenges for bringing CWC in reality are mentioned with proposed research methodologies. Scientific contributions are mentioned at the last of this chapter.

Next, the opportunistic large array approach for cooperative wireless communication is studied and applied for the cognitive radio networks. In the data transmission phase, decode and forward relaying mechanism is considered. Here, the equations for the coverage radius and critical network density are modified for the limited broadcast coverage of the wireless sensor networks. Also the new equations are derived for the fraction of energy savings with the cooperative OLA approach based on the network entities actually taking part into the cooperative communication. Here the cognitive relaying concept is worked out through the cooperative OLA model, wherein, relaying of primary traffic takes place through secondary

users. Under these circumstances, supporting the primary traffic to increase its throughput results in a decreased transmission time of the primary, which ultimately results in more transmission opportunities for the secondary. For cooperative transmission, OLA selects the relay nodes which have the received signal SNR above some threshold figure. The uniqueness of this algorithm is that node location information and high source transmit powers for data transmission is not needed. This kind of mechanism can be applied for applications like wireless LAN, cellular pico-cells in hot spot situations and Bluetooth.

Then, receiver sensitivity is used to detect malicious behavior in opportunistic cooperative internet of things (IoT). Here, the new equation is derived for the receiver sensitivity calculations with and without presence of malicious behavior. In distributed cooperation schemes, the cooperating nodes make transmission decisions based on the quality of the received signal, which is the only parameter available locally. Receiver sensitivity is the most important parameter of the physical layer and has a direct impact on the MAC layer. In order to maximize the information transfer among network nodes, the optimal receiver sensitivity is the prime requirement. The noise floor of a receiver determines its sensitivity to low-level signals and its capability of detecting and demodulating those signals. Cooperation allows independently faded radios to collectively achieve robustness to severe fades while keeping individual sensitivity levels close to the nominal path loss. In this work, it is observed that normally, the receiver sensitivity figures are found to be below -90 dB without presence of the malicious behavior in the cooperative IoT scenario. As soon as some malicious behavior is present in the system, the receiver sensitivity value is suddenly increased by approximately 30 dB.

In Subsequent work, the outage probability analysis is performed for the cooperative IoT mechanism. Also, the QoS parameters like energy, delay and throughput are studied through the network simulation. With cooperative wireless communication, the wireless node entities can increase their effective quality of service (QoS) via cooperation. Fraction of energy savings achieved in this case is the first step towards green cooperative communication. The outage behavior for decode and forward cooperative scheme is almost same as that of amplify and forward technique but the energy savings achieved at the low threshold values is the added advantage of this system.

Following, cooperative web of trust (CWoT) is studied for the security in cognitive radio networks. Radio spectrum is a scarce and very essential resource for the ever growing mobile applications. Cooperative spectrum sensing is a well-known and proven mechanism in the Cognitive Radio Networks (CRNs). But the spectrum sensing and sharing mechanisms are inherently vulnerable to the malicious behaviors in the wireless networks. This work has proposed the light weight cryptographic Cooperative web of trust (CWoT) for the security in cognitive radio networks. Authentication and authorization are analytically modeled and simulated to study the performance evaluation of the system. Trust levels are modified according to the radio node's behavior in the cooperative network. Accordingly, the authorization mechanism is developed. With the security inclusion also, the system performance is observed to be good with very less energy consumption.

In the succeeding work, physical layer security and cooperative jamming technique is applied for the physical layer security in resource constrained wireless sensor networks and the system performance is analysed with information theoretic measures. The system makes use of friendly interference to confuse the eavesdropper and increase its uncertainty about the source message. The whole communication link is built with the help of Information theoretic source and channel coding mechanisms. The whole idea is to make use of normally inactive relay nodes in the selective Decode and Forward cooperative communication and make them work as cooperative jamming sources to increase the equivocation of the eavesdropper. Here, the total communication link is built by making use of information theoretic source and channel coding techniques such as LZW, BCH and RS coding decoding with DSSS and BPSK modem. Source, receiver and eavesdropper's individual entropies, conditional entropies, mutual information and finally secrecy capacities are calculated. Mutual Information of the main channel $I(X;Y)$ is much higher than the mutual information of the Eavesdropper's channel $I(X;E)$. This shows that the secrecy capacity of the main channel is greater than the secrecy capacity of the eavesdropper's channel due to the jamming effect by the cooperating relay node. Hence, the Eavesdropper's Equivocation is found to be much higher than the main channel.

In consequence, this thesis proposed a cooperative OLA approach for indoor scenario with consideration of limited coverage like wireless sensor networks and cognitive radio networks. Also, malicious behaviour detection is proposed which is based on receiver sensitivity figures. Further cooperative scenario is built with the network simulator for WSN. QoS

analysis and outage probability analysis is done for four level of cooperative relaying. Then novel cooperative web of trust is proposed which makes use of trust levels based on behaviour reputation of the radio nodes and based on trust nodes, the authentication and authorization mechanism is built. Lastly, innovative and responsive Information theoretic cooperative jamming mechanism is proposed that makes use of communication link built with information theoretic source and channel coding techniques.

6.2 Future Research Scope

The research work related to Cooperative OLA approach for CRNs can be extended to wireless sensor networks and various IoT scenarios. The OLA approach considered here employs spread spectrum coding mechanism with RAKE receiver. This work can be extended further with orthogonal frequency division multiplexing (OFDM) technique for extended coverage applications. The radio network entities which are malicious or which fail in unknown ways can be detected by making use of receiver sensitivity. This work can be extended to build a security system for various applications of cooperative transmission.

Cooperative diversity with web of trust technique provides effective solution for the primary user emulation attacks. Depending on the trust levels acquired through the reputation in the system, the nodes immediately get either rewards for good behaviour or get blacklisted due to extreme misbehaviour. The blacklisted node also can get chance to work hard to achieve good reputation and can be included after certain test in the CWoT. However, some improvements are needed in the proposed technique. The storage of hash values is also a resource consuming prospect. Using proper function by light weight cryptography, the hash values can be computed at the run time, without consuming much time, thus eliminating the overheads of space and time requirements. Also since each broadcast consumes some energy, only relevant acknowledgements should be propagated, so that the system assumes the presence of an end-to-end logical channel, without having to bother about the intermediaries and the overhead such as acknowledgement sending to them. The authorization implemented assigns the role dynamically on basis of the reputation of the node. In case the sender does not have an idea about the reputation it has with respect to the receiving node(s), it results in unnecessary transmission in the network, thus consuming system resources. This research work of CWoT can be extended by making use of these improvement directions.

Physical layer security mechanism comprising source and channel coding techniques which are proposed can be restructured according to the particular applications. Various source and channel coding techniques are there in literature, but the researchers should choose the one which is best suited for the QoS parameters and the system design depending on specific application. The system designed with Ricean channel for indoor scenario can be redesigned for outdoor applications with the help of Rayleigh fading channel. Instead of DSSS and BPSK, OFDMA can be used for comparative large coverage areas. Also, selective decode and forward technique can be employed for the designed mechanisms with the relay weight functions. Polarization effects can be added to get the optimal power allocation at the transmitter.

Appendix A: List of Publications

Book Chapters

[1] Vandana Rohokale, Rajeev Prasad, Neeli Prasad, Ramjee Prasad," Interoperability, Standardisation, Governance in the era of Internet of Things (IoT)", River Publications, European Commission Cluster Book 2011, Edited by Ovidiu Vermesan and Peter Friess, pp. 257-285 .

[2] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Information Theoretic Security for Cooperative Communication", River Publications, Internet of Things and M2M Communications Book, 2013, Edited by Dr. Fabrice Theoleyre and Pr. Ai-Chun Pang, pp. 161-181.

Journal Papers

[3] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Wireless Communications and Physical Layer Security: State of the Art", Journal of Cyber Security and Mobility", Vol.1, pp. 227-249, 2012.

[4] Vandana Rohokale, Sandeep Inamdar, Neeli Prasad, Ramjee Prasad," Energy Efficient Four Level Cooperative Opportunistic Communication for Wireless Personal Area Networks (WPAN)", Wireless Personal Communications, Volume 69, Issue 3, pp 1087-1096, April 2013.

[5] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Reliable and Secure Cooperative Communication for Wireless Sensor Networks Making Use of Cooperative Jamming with Physical Layer Security", Springer Journal of Wireless Personal Communication, 2013. (Published Online)

[6] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Jamming for Physical Layer Security in Wireless Sensor Networks", Wireless Personal Communication Journal of Springer Verlag, 2013. (Accepted)

[7] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Web of Trust for Security in Cognitive Radio Networks", Journal of Cyber Security and Mobility, 2013. (Submitted)

Conference Papers

[8] Vandana Rohokale, Nandkumar Kulkarni, Horia Cornean, Neeli Prasad, "Cooperative Opportunistic Large Array Approach for Cognitive Radio Networks", 8th IEEE International Conference on Communications, Bucharest, Romania, pp.513-516, June 2010.

[9] Vandana Rohokale, Neeli Prasad, "Receiver Sensitivity in Opportunistic Cooperative Internet of Things (IoT)", Second International Conference on Ad Hoc Networks, Victoria, British Columbia, Canada, pp. 160-167, August 2010.

[10] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring and Control", Wireless Vitae 2011, 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, Chennai, India, pp. 1-6, Feb-Mar 2011.

[11] Vandana Rohokale, Neeli Prasad, Ramjee Prasad, "Cooperative Jamming for Physical Layer Security in Wireless Sensor Networks", Proceedings of 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, pp.455-459, Sept 24-27, 2012. (Published)

Contribution of Publications to Thesis Chapters:

	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5	Chapter 6
Publication [1]		Yes	Yes			Yes
Publication [2]		Yes	Yes			Yes
Publication [3]		Yes	Yes			Yes
Publication [4]		Yes	Yes			Yes
Publication [5]		Yes		Yes		Yes
Publication [6]		Yes			Yes	Yes
Publication [7]		Yes			Yes	Yes
Publication [8]		Yes			Yes	Yes
Publication [9]		Yes			Yes	Yes
Publication [10]		Yes			Yes	Yes
Publication [11]		Yes				Yes

Appendix B: Short CV

Vandana Milind Rohokale received her B.E. degree in Electronics Engineering in 1997 from Pune University, Maharashtra, India. She received her Masters degree in Electronics in 2007 from Shivaji University, Kolhapur, Maharashtra, India. She has recently obtained her PhD degree from CTIF, Aalborg University, Denmark under the guidance of Prof. Ramjee Prasad. She is presently working as Associate Professor in Sinhgad Institute of Technology, Lonavala, Maharashtra, India. Her research interests include Cooperative Wireless Communications, AdHoc and Cognitive Networks, Physical Layer Security, Information Theoretic security and its Applications.