IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Efficient Secure Data Communications for Cognitive Radio using Clustering Techniques

Padmasri Yarlagadda[1], Bosubabu Sambana[2]

Sr. Assistant Professor, Department of Computer Science and Engineering, Avanthi's Research and Technological Academy, Jawaharlal Nehru Technological University, Kakinada, India[1]

Assistant Professor, Department of Computer Science and Engineering, Avanthi's Research and Technological Academy, Jawaharlal Nehru Technological University, Kakinada, India[2]

Abstract: Secure communication of Data in cognitive radio networks is one of the challenging tasks to increase the lifetime of the network is a major constraint. The life time of the network is determined by the energy consumed by the each node and protect the data from an intrudes. In this research work we introduce a secure cluster based communication to reduce the overheads and provide the security. A special node called as centralized node collects the data from clusters and forwards them to Base station. The data is secured which authenticates the Cluster head using the shared secret key and the Digital Signature. The simulation results prove that our algorithm is more efficiently secure the data and achieves more energy savings.

Keywords: Clustering, Communication, Networks, Security, DBMS, Data Mining, Data Ware House.

I. INTRODUCTION

This paper gives us an idea about secure data communications for cognitive radio using clustering techniques. A Cognitive network consists of many sensors that are tiny in size, low rates, less computational ability and has a very less memory storage. These Nodes gather the data from the surrounding and stores it and process them within the network [1].

Cognitive Radio networks have very less rechargeable energy, this is one of the challenging factors to extended the life time of the memory since the energy efficiency is very less in overall cognitive radio network these sensor nodes can be divided into many small clutters to increase the energy efficiency and increase the network lifetime[2]. Every cluster has a cluster head(CH) and cluster members(CM) which can communicate with the defined cluster heads in order to broadcast the data to the base satiation . the cluster head collects the data from the cluster member and forwards them to the base station and the cluster heads equalize the energy between the nodes the cluster head consumes the extra energy for gathering the data and randomly selects the cluster heads

To increase the lifetime of the CRN"S and increase the energy efficiency we purpose and evaluate a security based clustering scheme. We implement distributed clustering algorithm where the cluster head is elected based on a high consuming energy of each sensor node and the distance from the base station to allocate more energy to each node here the cluster node is not selected randomly it is reelected basing of constraint to avoid the frequent selection of cluster head. A special node center node collects the data and aggregates and sends to the cluster head which has high residual energy and calculates the distance from the base station to allocate more energy for the each node the cluster head is not selected randomly. the cluster head data is authenticated for by the center head using the secret key and digital signature . this scheme effectively and efficiently manages the sensor nodes and increases the life time of the cognitive radio network lifetime [3–5].

To implement unique features, we derive the power consumption and define optimal number of clusters. We experiment and prove that minimum power communication is equal to minimum the sum of square distance between the nodes and their cluster heads.

This will overcome with clustering problems [15][16], the constrained clustering [13][14] can be deployed to cluster nodes under spectrum constraints. We propose a new approach for spectrum clustering (SC) protocol with small intra- cluster distance this will reduce the consumption communication power.

II. BACKGROUND

These below keywords are represents basic idea about conceptual concerns

2.1. **Clustering:** Cluster analysis or clustering is the task of grouping a set of objects in such a way that objects in the same group are more similar to each other than to those in other groups. Cluster analysis involves applying one or more clustering algorithms with the goal of finding hidden patterns or groupings in a dataset.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

2.2. **Communication:** Communication is the act of conveying intended meanings from one entity or group to another through the use of mutually understood signs and semiotic rules.

2.3. **Data:** Data is distinct information that is formatted in a special way. Data exists in a variety of forms, like text on paper or bytes stored in electronic memory.

2.4. **Pattern Analysis:** The phase of pattern recognition that consists of using whatever is known about the problem at hand to guide the gathering of data about the patterns and pattern classes, and then applying techniques of data analysis to help uncover the structure present in the data.

2.5. **Networks:** A computer network or data network is a telecommunications network which allows nodes to share resources. In computer networks, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media.

2.6. **Security:** Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. ... Data security is also known as information security (IS) or computer security.

2.7. **DBMS:** A database management system (DBMS) is a computer software application that interacts with the user, other applications, and the database itself to capture and analyze data. A general-purpose DBMS is designed to allow the definition, creation, querying, update, and administration of databases.

2.8. **Data Mining:** Data mining is the analysis step of the "knowledge discovery in databases" process, or KDD. The term is a misnomer, because the goal is the extraction of patterns and knowledge from large amounts of data, not the extraction of data itself.

2.9. **Data Ware House:** A data warehouse is a central repository for all or significant parts of the data that an enterprise's various business systems collect.

2.10. **Cognitive Radio:** Cognitive radio is a form of wireless communication in which a transceiver can intelligently detect which communication channels are in use and which are not, and instantly move into vacant channels while avoiding occupied ones.

III. RELATED WORK

Cognitive radio history

There have been many factors that have lead to the development of cognitive radio technology. One of the major drivers has been the steady increase in the requirement for the radio spectrum along with a drive for improved communications and speeds.

In turn this has lead to initiatives to make more effective use of the spectrum, often with an associated cost dependent upon the amount of spectrum used. In addition to this there have been many instances where greater communications flexibility has been required. Along the way, there have been several significant milestones along the road to develop cognitive radio technology.
One example that exemplified the need for flexible communications occurred in the Netherlands in 2000 when a fireworks factory exploded killing 23 people, destroying much of the town and injuring more than a thousand people. While dealing with this catastrophe, the emergency services (fire, medical, police, etc) experienced real communications difficulties because they all had different communications systems and were unable to communicate with the other services.

Another major emergency was the 9/11 terrorist attacks in the USA. Again communications difficulties were experienced. While often a variety of radios would be needed for intercommunications, this would not be viable for small groups of people, and reconfigurable radios would have enabled far more effective communications to be achieved. With spectrum becoming a more scarce resource many radio regulatory bodies started to look at how it might be more effectively used.

Similarly others had been working on the possibility of self configuring radios. In fact the term "Cognitive Radio" was coined by Joseph Mitola while he was writing his doctoral thesis on the topic in 2002.

Intelligence and flexibility

Work is under way to determine the best methods of developing a radio communications system that would be able to fulfil the requirements for a CR system. Although the level of processing required may not be fully understood yet, it is clear that a significant level of processing will be needed. The radio will need to determine the occupancy of the available spectrum, and then decide the best power level, mode of transmission and other necessary characteristics. Additionally the radio will need to be able to judge the level of interference it may cause to other users. This is an equally important requirement for the radio communications system if it is to operate effectively and be allowed access to bands that might otherwise be barred.

Cognitive radio architecture

In addition to the level of processing required for cognitive radio, the RF sections will need to be particularly flexible. Not only may they need to swap frequency bands, possibly moving between portions of the radio communications spectrum that are widely different in frequency, but they may also need to change between transmission modes that could occupy different bandwidths.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

To achieve the required level of performance will need a very flexible front end. Traditional front end technology cannot handle these requirements because they are generally band limited, both for the form of modulation used and the frequency band in which they operate. Even so called wide band receivers have limitations and generally operate by switching front ends as required. Accordingly, the required level of performance can only be achieved by converting to and from the signal as close to the antenna as possible. In this way no analogue signal processing will be needed, all the processing being handled by the digital signal processing.

The conversion to and from the digital format is handled by digital to analogue converters (DACs) and analogue to digital converters (ADCs). To achieve the performance required for a cognitive radio, not only must the DACs and ADCs have an enormous dynamic range, and be able to operate over a very wide range, extending up to many GHz, but in the case of the transmitter they must be able to handle significant levels of power. Currently these requirements are beyond the limits of the technology available. Thus the full vision for cognitive radio cannot yet be met. Nevertheless in the future the required DAC and ADC technology will undoubtedly become available, thereby making cognitive radio a reality.

Evolution from Different Analysis:

Clustering and spectrum heterogeneity and scalability is one of the challenge in cognitive radio networks. In this paper, a secondary user creates groups for locally common available channels. Which can be implemented by using distributed group maintenance algorithms? The network is partitioned into clusters by neighbor nodes which shares local common channel then the Clusters are connected to design a network. This uses the MAC protocol where access time is divided into super frames which contain the inter-cluster and intra-cluster and neighbor discovery. We implement the graph theory for spectrum clustering (SC) where local channels cluster can communicate within the cluster here Every node constructs diagraph with its nearest neighbors and checks for the available channels. A cluster in the network is formed by using the clustering technique. The intra-cluster communication is performed

We construct minimum number of clusters in cognitive radio networks using programming thermo and message-passing technique. This will form strong clusters by using inter- and intra-cluster connectivity. We suggest a spectrum aware clustering scheme that will enable efficient communication by intra-cluster aggregation and inter-cluster relaying and also finds optimal node number in a cluster.

In this paper we implement a Cryptography technique which generates public key or symmetric key with digital signature which are used communication security in Cogitative radio network [9, 14, and 15]. Symmetric key cryptography will reduce time and energy efficient. This can resolve the boundary and link reliability issues [16]. In this paper, we proposed secured communication to overcome with the nodes attacks. This scheme implements a cryptographic technique at higher layers and data at the physical layer to provide better security. An novel crypto system is proposed for data confidentiality and message authentication, etc. this approach can identify all the nearest nodes in transmission groups, if nearest nodes are less than half of the nearest clustered nodes which is not larger than that of its all neighboring clusters this will detect all the compromised nodes.

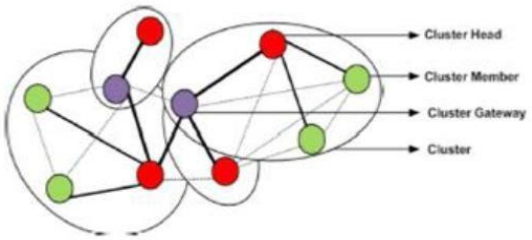

Figure 1: Proposed Cluster Based Cognitive Radio

Despite many approaches have been implemented in clustering approaches in cognitive radio networks but still it is an challenge for implementing limited energy resource usage and hardware capacity so we need and energy-efficient clustering solution to overcome with limited energy resource and spectrum access challenges. Secure data collection using CHBDC, However, the security aspect in center head -based data collection is not studied in detail. In [8] key management for secure communication and data collection in distributed CRN is discussed. The scheme ensures only confidentiality of the collected data. Identifying malicious CHBDC. Node sink is used for secure data collection. Here a fixed path is used the nodes in this path will be able to communicate with the cluster and communicate the data. The nodes in the path are overloaded with data transfer function.

Proposed algorithms spend more energy while rotating the Cluster head which gathering data from its nearest cluster member. Some of the algorithms concentrate either on security of in cresting the efficiency of energy consumption but in our paper we propose both security and effacement clustering in reducing the power consumption and also increase the efficiency of by providing.

IV. PROPOSED WORK

Extensive research has been conducted on clustering in traditional in a cognitive radio network and a comprehensive survey of the algorithms is presented in various patterns. However, the dynamic unreliable data communication availability in cognitive radio networks introduces new challenges for distributed collaboration in cognitive radio networks. In this section, we review and analyze the existing works on distributed clustering in CRAHNs. A cluster-based CR network framework and the corresponding topology management algorithm are proposed in existing pattern analysis [8], [9]. Following

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

the scheme, each un-clustered CR user chooses the channel with the largest number of neighbors as LCCC and constructs a cluster in the initial phase, which is followed by a local minimal dominating cluster merging algorithm (LMDS) to reduce cluster number. This algorithm optimizes the cluster size while guaranteeing one LCCC in each cluster. However, the robustness of the cluster structure is not considered and re-cluster is easily caused by variation in the spectrum availability, resulting in more control overhead in turn. Furthermore, the rough clustering in the initial phase limits its performance in reducing cluster numbers.

The Proposed Algorithm forms the clusters and selects the Cluster Head using high energy and number of neighbors. The cluster head can be elected when it reaches the its threshold value this will reduce the selection overheads of the cluster heads and will increase the lifetime of nodes to reserve some energy the data from the sensor nodes is transferred to the nearest cluster head and then it is forward to the BS to avoid data gathering by cluster head. A Special node Center Data Collector (CDC) collects and aggregates the from the cluster head and then it transfers it to the Base Station. The cluster head can be secured using the digital signature and cryptography

Basic Assumptions

Primary and secondary users coexist in a cognitive radio network. Primary users (PUs) can utilize their licensed bands directly, cognitive radios can operate on these bands Spectrum readings of neighbor nodes are co-ordinate since transmission range is avails to primary users [21]. These nodes are equipped with duplex receiver so that transmission done simultaneously. There are orthogonal channels which are overlapping. Which contains the unique ID with free spectrum bands which are detected by spectrum sensing which does not change the clustering structure?

Cluster Formation and Key Generation:-

TSP with Digital Signature:

After the cluster is created cluster heads is selected and CHDC is deployed for collecting the data from the cluster head. And the following operation are performed

Key Generation: In this scheme the shared key generates the key with the time stamp and digital signature for CHDC then these keys is distrusted to CH and BS [13].

Digital Signature: the data sending node generates a digital signature with the input message MSG and assigns the Time Stamp TS. Then sends the data to the cluster members in its clusters.

Private Key Generation: A sensor node generates a private key P_k associated with the node ID.

Verification: Sensor node ID, MSG and DSIG is verified whether it is authorized by the Base station. If DSIG is valid, then the node receiving an accept otherwise reject. Key initialization is done before node deployment and operates then during communication, which consists cluster formation and Key management phase for each round. The clustering structure is divided into two parts:

1. Setup phase
2. Data Transmission phase.

Those are The setup structure is again divided into three sub parts: neighbor node sensing, cluster head selection, and cluster structure design; in the data transmission phase, cluster members collect local data and transmits the data to the cluster heads and cluster heads sense the data and then aggregates them from cluster members and then sends the aggregated data to next cluster head increase the network life time we chose the nearest cluster head with reschedule energy to the next hop instead of the selecting the cluster member base station then select the key and constructs the message before deploying the CHDC preloads the key to cluster head and base station and a time stamp is assigned to it and CHDC maintains a table in which it stores all the information with unique identifier and then the digital signature is attached to each cluster head after deployment of CHDC establishes the connection with each cluster head in the avail region and the cluster heads decrypts the key and authenticates.

Algorithm for Proposed work:

1) Select a cluster head and send a message to the nearest node.
2) The nodes then send a message to the cluster head.
3) A cluster if formed the CHDC establishes a connection with the CH in the region.
4) MDC sends the beacon signal to cluster head with $ID||\{SK_i \,||\, DSIG\} \,||\, h(sk_i)$.
5) Compare the DSIG with the Digital Signature stored in the table.
6) Computes the hash function for shared key $h(sk_i)$.
7) Compare the computed hash value with the received value. If not equal, then declare that the node is malicious.

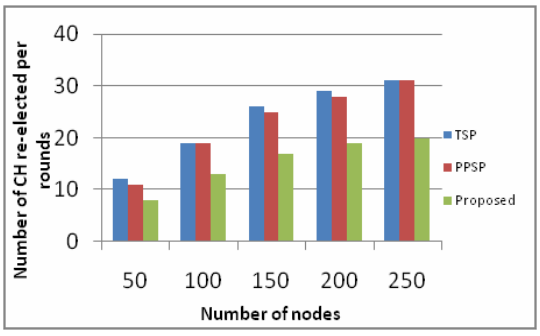

Figure 2: Shows the number of CH elected with respect to the number of nodes.

The initial energy of each node is assigned as 2 joule. The minimum energy is 0.2. This will preserve some more energy to increase the network lifetime.

Protocol Initialization:

In this scheme time is divided into different intervals Time Stamp from Base Station to node transmission by each

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

cluster member to cluster head. Then key distribution method is applied to improve communication security, the parted information is loaded to the sensor node during initialization [12].Base Station performs the following operation for key distribution to the entire nodes:

Generate a secrete key SK to encrypt the data with k € (n-1), where n is largest integer value
The CHDC sends the paired data with Ts and Sk with Uid. It also generates the function f(sk) to the cluster head along with its digital signature
The cluster head then decrypts the key Sk with Time Stamp using CH key and then validate the digital signature
After verifying the Digital signature, CH authenticates the CHDC. Paired key (Ts, Sk) which is shared to cluster heads. authorized cluster head will be authorized.
Once the CHDC is authenticated by the CH, The CH transfers the encrypted data to the CHDC using secret key (Sk). The CH generates the cluster key, which can be shared by all cluster members which can verify the data using the cluster key

SIMULATION AND RESULTS

The below diagram represents Experiential results of the proposed algorithm which shows network lifetime of each node nearer to the BS by increasing the number of nodes closer to the BS and its life time

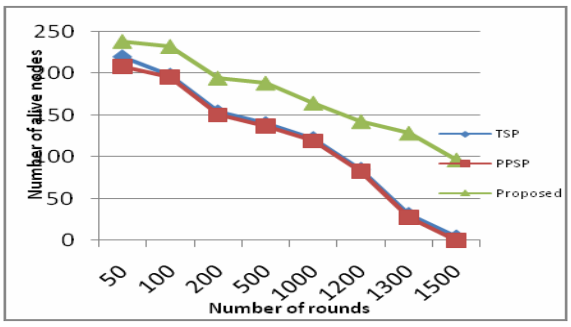

Figure 3: Number of alive nodes over time

The below Diagram represents energy consumption for sending and receiving a packet in a given time. A proposed algorithm increases when number of nodes or traffic load increases.

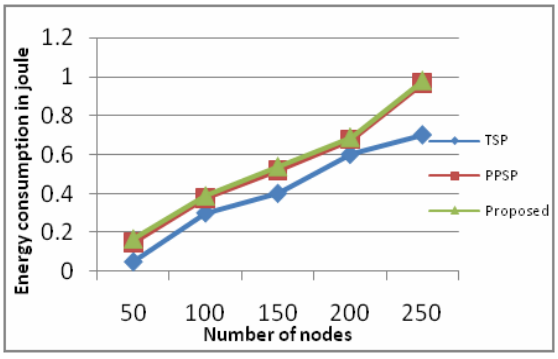

Figure 4: Energy Consumption using proposed Method

The below diagram represents percentage of packets delivered for each round using Proposed algorithms for with high packet delivery ratio.

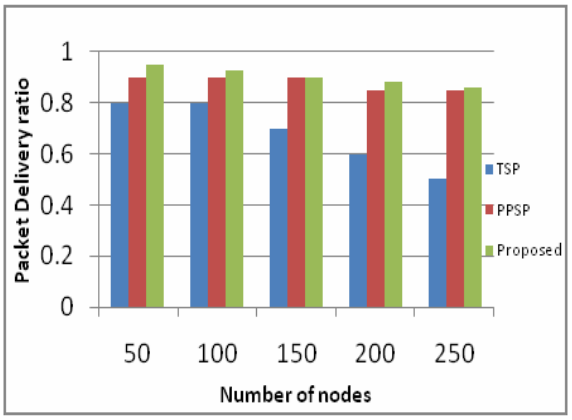

Figure 5: Packet Delivery Ratio using Proposed Method

The security of the proposed algorithm can be analyzed Fig 6 shows that the proposed algorithm can effectively determined the attacker nodes among the normal nodes.

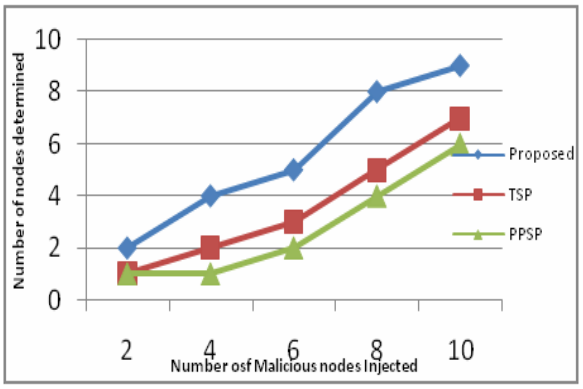

Figure 6: Security analysis Proposed Method

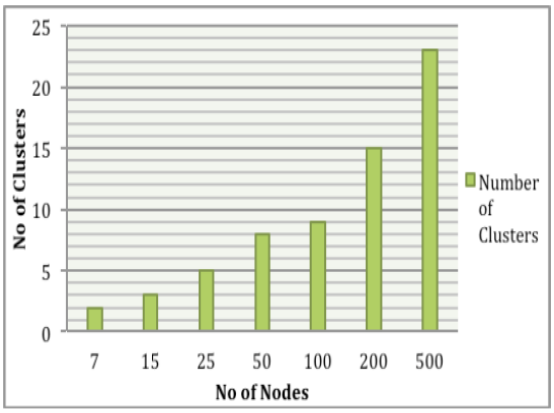

Figure.7: Node network, 2 clusters are formed with a growth of number of 1000 nodes, 25 clusters are constructed

Our experiments are done using 500 nodes that form a CRN'S. The performance setting parameters are listed Table 1.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

	Values
Network Area	200*200m
nodes	100-250
Transmission	500m
Range Network	Grid topology
Topology Initial	20J
Energy Propagation	TR
model	Model
Speed	1 m to 2m
Data packet size	512 bytes
d0	50 m
δ	0.2
a	0.5
∞	0.0

V. CONCLUSION AND FUTURE WORK

In this paper we have presented the concept of The data collection using CHDC in clustered CRN'S is one of the important concepts to increase the life time of the network and the secure data collection in clustering cognitive radio network We proposed three protocols and Proposed CHDC- based secure data collection in cognitive radio network clusters. These are designed using messy Omar key management scheme.

This has some of the important security issues like identifying malicious nodes and rewritten messages. The detailed emulation of the security with energy analysis experiments are explained and they shows that the proposed scheme shows high level of security In future research the optimization and secure routing will be implemented for better performances results

ACKNOWLEDGMENT

This paper is Heartily Dedicated to famous Educationist and Role Model **Sri. Dr. Ch. Diwakar,** Principal & Sr. Professor, Avanthi Research and Technological Academy, Vizianagaram. He gives moral support and foresight backup to every soul. Thanking you sir, gives one great opportunity in part of your vision.

REFERENCES

[1] W. Su Y. Sankarasubramaniam E. Cayirci Akyildiz, I.F. A survey on sensor- networks. IEEE Communications Magazine, pages 102{114, 2002.
[2] Y. Chen, A. Liestman and J. Liu, "Clustering algorithms for ad hoc wireless networks", IEEE Conference on communications (ICC'97), Vol.1, pp. 114-128, June, 2004.
[3] Vijay G., Bdira E., and Ibnkahla M. "Cognitive approaches in Wireless Sensor Networks: A survey," Proc. QBSC, pp.177-180, May 2010.
[4] H. Zhang, Z. Zhang, Y. Chau, "Distributed compressed wideband sens- ing in Cognitive Radio Sensor Networks," in Proc. IEEE INFOCOM WKSHPS, April 2011.
[5] M. C. Oto, and O. B. Akan, "Energy-Efficient Packet Size Optimization for Cognitive Radio Sensor Networks," IEEE Transactions on Wireless Communications, vol. 11, no. 4, pp. 1544-1553, Apr. 2012.
[6] O. Bicen, and O. B. Akan, "Reliability and Congestion Control in Cognitive Radio Sensor Networks," Ad Hoc Netw. J., vol. 9, no. 7, pp. 1154-1164, Sep. 2011.
[7] T. Chn, H. Zhang, G. M. Maggio, I. Chlamtac, "Topology Management in CogMesh: A Cluster-Based Cognitive Radio Mesh Network," Proc. IEEE ICC 2007, pp. 6516-6521, June 2007.
[8] K. E. Baddour, O. Ureten, T. J. Willink, "Efficient Clustering of Cognitive Radio Networks Using Affinity Propagation," Proc. IEEE ICCCN 2009, pp. 1-6, Aug. 2009.
[9] S. Basagni, "Distributed Clustering for Ad Hoc Networks," in Proc. I- SPAN 99, pp. 310-315, Fremantle, Australia, Jun. 1999.
[10] V. Kawadia and P. Kumar,"Power Control and Clustering in Ad Hoc Networks," in Proc. 22nd IEEE Conf. Comput. Commun., pp. 459-469, San Francisco, CA, USA, 2003.
[11] M. Chatterjee, S. K. Das, and D. Turgut, "WCA: A Weighted Clustering Algorithm for Mobile Ad hoc Networks," Journal of Cluster Computing, Special issue on Mobile Ad hoc Networking, No. 5, pp. 193-204, 2002.
[12] S. Bandyopadhyay, and E. J. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks," in Proc. INFOCOM 2003, vol.3, pp. 1713-1723, San Francisco, CA, USA, 30 March-3 April 2003.
[13] Akyildiz, W. Lee, M. Vuran and S. Mohanty, "Next Generation Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey", Computer Networks, Vol. 50, no. 13, pp. 2127-2159, 2006.
[14] Sisi Liu, Loukas Lazos and Marwan Krunz, "Cluster- based Control Channel Allocation in Opportunistic Cognitive Radio Networks" IEEE Conference on Sensor and Ad Hoc Communications and Networks (SECON), Rome, Vol. 20, pp. 479-492, June, 2009.
[15] C. Talay and D. T. Altilar, "United nodes: cluster- based routing protocol for mobile cognitive radio networks", Communications, IET Vol.5, Issue:15, pp. 529-542, April, 2011.
[16] Nafees Mansoor, A.K.M.Muzahidul Islam, Mahdi Zareei, Sabariah Baharun, and Shozo Komaki, "Spectrum Aware Cluster-Based Architecture For Cognitive Radio Ad-Hoc Networks", 2nd International Conference on Advances in Electrical Engineering, ICAEE, Vol. 9, pp. 181-185, December, 2013.
[17] S. Setia S. Zhu and S. Jajodia. Leap: efficient security.
[18] A. Chandrakasan W.R. Heinzelman and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor network. IEEE Proceedings of the Hawaii International Conference on System Sciences, pages 1{10, Jan- uary 2000mechanisms for large scale distributed sensor networks. Proceedings of the 10th ACM conference on Computer and communications security, pages 62{72,2003.ACM Press. J.G. Proakis, Digital Communications, ffith ed., McGraw-Hill, New York, NY, 2008.
[19] S.M. Alamouti, A simple transmit diversity technique for wireless communications, IEEE J. Sel. Areas Commun. 16 (1998) 1451–1458.
[20] S. Cui, A.J. Goldsmith, A. Bahai, Energy-efficiency of mmio and cooperative mimo techniques in sensor networks, IEEE J. Sel. Areas Commun. 22 (2004) 1089–1098.
[21] X. Du, M. Guizani, Y. Xiao, H.-H. Chen, A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks, IEEE Trans. Wireless Commun. 8 (2009) 1223-1229.
[22] W. Chen, M. McNeal, L. Hong, Cross-layered design of security scheme for cooperative MIMO networks, in: Proc. IEEE International Conference on Wireless Information Technology and Systems, Honolulu, HI, USA, 2010, pp. 1–4.

BIOGRAPHIES

Smt. Padam Sri Yarlagadda working as Assistant Professor, Department of CSE, Avanthi Research and Technological Academy, Vizianagaram. She is completed Bachelor of Technology in Computer Science & Engineering from Jawaharlal Nehru Technological University – Hyderabad, and Master Degree in Computer Science & Engineering from Jawaharlal Nehru Technological University – Kakinada, Andhra Pradesh,

India. She has 6 years good teaching experience and having a good Knowledge on Computer Network and Security, Future Internet Architecture, Cloud Computing, Internet of Things and Hacking along with Computer Science Subjects. She is Published 1 Research Paper in reputed International Journal. She is participated 2 international conferences and 1 national Workshop and 1 FDP.

Sri. Bosubabu Sambana working with Assistant Professor, Department of CSE, Avanthi Research and Technological Academy, Vizianagaram. He is completed Bachelor of Science from Andhra University. He is completed Master of Computer Applications and Master Degree in Computer Science & Engineering from Jawaharlal Nehru Technological University – Kakinada, Pursing Master of Science in Mathematics, Andhra University - Andhra Pradesh, India.
He has 4 years good teaching experience and having a good Knowledge on Space Research, Future Internet Architecture, Cloud Computing, Internet of Things /Services /Data, Data Analytics, Computer Network and Hacking along with Computer Science Subjects. He is Published 14 Research Papers in various reputed International and national Journals, Magazines and conferences.

He wrote 1 Textbook in Computer networks fields and have 1 Copyright and Secured 6 Certifications from NPTEL-IIT's various specifications like Algorithms for BigData, C++ Programming, Introduction to Research, Wireless Sensor Adhoc Networks, Internet Architecture, Internetwork Security, and Computer Architecture, Cloud computing etc..

He is participated 3 international and 1 national conferences. He is Participated 1 national Workshop and 2 FDP.

He is the member of SERB, Indian Science Congress, W3C, INTERNET SCOCIETY, W3C, NASA (Student), Springer, Elsevier, Science Alert, IEI, Editorial Manager, MECS-PRESS-IJMECS/ IJCSIT, W3C, manuscript central, TUBITAK-GIRIS, Internet Society, IAENG, IAAET, IJMETMR, IJECSE, IJCST, IJECSE and editorial / review member in ACM, IJMETMR, and Springer-Journal of Big Data.