Journal of Theoretical and Applied Information Technology
30th June 2016. Vol.88. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN APPROACH FOR EFFICIENT AND SECURE COOPERATIVE WIRELESS NETWORKS USING TRANSMISSION RELIABILITY PROTOCOL

[1]APOORVA P, [2]NAGARJUN S, [3]PARVATHI T V

[1]Lecture, Department of Computer Science, Amrita Vishwa Vidyapeetham, Mysuru campus, Amrita University, India
[2]Student, Amrita Vishwa Vidyapeetham, Mysuru campus, Amrita University, India
[3] Student, Amrita Vishwa Vidyapeetham, Mysuru campus, Amrita University, India

[1]apoorvaap7@gmail.com [2]nagarjuntnp@gmail.com, [3]parvathitv2010@gmail.com

ABSTRACT

Energy efficiency and security is the major problems identified in wireless sensor networks. This work introduces the Secured Cooperative communication protocol in wireless sensor networks for establishment of cooperative clusters during transmission of data in a collective way. In the cooperation process using cooperative transmission protocol, recruitment policy helps the nodes to co-operate each other. Cluster head on one node thick path recruit neighbouring nodes to assist in communication. Proposed method aimed to build security between the intermediate cluster nodes and also minimize the overall energy consumption and increase the transmission reliability of packet delivery between a source and a sink in an unreliable wireless network by giving some level of cooperation among them. Cooperative Transmission Protocol that uses any wireless networks communications between any source node and sink node can be with optimal energy and not compromising with the reliability of transmission to decrease packet loss. In order to bring the security among the nodes inside the cluster the method called Rijndael algorithm is used as an Advanced Encryption Standard (AES). AES provides flexibility and security between the systems when compared with other cryptographic algorithms. To enhance efficiency of sensors, the existing algorithm found inefficient. Hence with all accounting of the existing systems, this work concentrates on reducing energy consumption by selecting only few/optimal node and also maintains a data cache until an acknowledgement is received from receiving cluster head upon successful transmission.

Keywords: *Rijndael Algorithm, Rijndael Managed Objects (RMO), Crypto Stream Object, Cooperative Transmission, Salt Data, Initialization Vector(IV), Cooperative Caching.*

1. INTRODUCTION

Wireless networks nodes have limited energy resources and consequently protocols designed for sensor networks should be energy-efficient. In emerged technology that allows energy saving is cooperative transmission. In cooperative transmission, the multiple nodes simultaneously receive the data, decode and retransmit data packets. In this paper, we are trying find new methodology in cooperative communication model with multiple nodes on both ends of a hop and with every data packet being transmitted only once per hop. Fuzzy Logic Based Security Level Routing Protocol (FLSL) algorithm is also imposed to build the security among the cluster.

This model of cooperative transmission, every node on the path from the source node to the sink node decided as a cluster head(CH), with the task of recruiting other nodes in its neighborhood in secured method and coordinating their transmissions. Accordingly, the classical route from a source node to a sink node is replaced with a multiple hop cooperative path, and the classical point-to-point communication is substituted with many-to-many cooperative communication. Along with this the path can then be defined as "having a width," where the "width" of a path at a specified hop is estimated by the number of nodes on each end of a hop. For the example in Fig. 1(a), the width of each intermediate hop is 3. This "width" does not need to be uniform along a path. Each hop on this path illustrates communication from many geographically near nodes, called a sending

Journal of Theoretical and Applied Information Technology
30th June 2016. Vol.88. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cluster, to another cluster of nodes, named a receiving cluster. The sensor nodes in each cluster cooperate in transmission of packets, which traverse along the path from one cluster to the next.

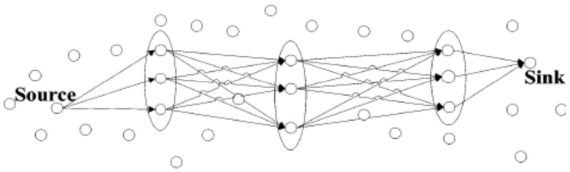
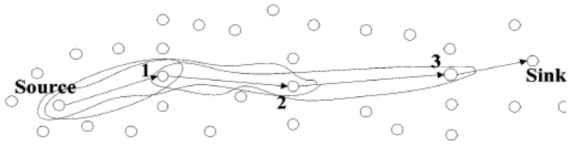


Fig-1 (a) Cooperative Transmission Protocol



(B) CAN Protocol

Proposed model of cooperative transmission for a single hop is further showed in Fig. 2(a). Each and every node in the next receiving cluster receives from every node in the sending cluster. Sending nodes are synchronized and also power level of the received signal at a receiving node/s is the summation of all the signal powers arriving from all the sender nodes. This minimizes the likelihood of a packet being received in error. We assume that some procedure for error detection is included into the packet format, so a node that does not receive a packet properly will not transmit on the next hop in the path.

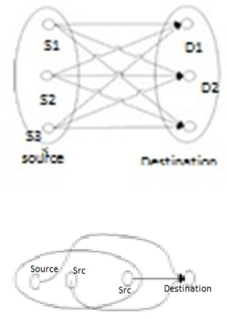


Fig-2 (A) Cooperative Reception Model (B) CAN Reception Model.

This cooperative communication model says every node on the path from the source node to next/destination node becomes a Cluster Head (CH), which performs the actions like recruiting other nodes in its neighborhood and coordinates its transmissions. We called route from a source to a sink node as having "width" path which is a multi-hop cooperative path. Fig-1 depicts a sending cluster, receiving cluster and cooperation of each cluster in transmission stage of data and model for cooperative transmission and reception for a single hop is represented where every node in the receiving cluster receives from every node in the sending cluster. Sender nodes are synchronized, and the power level of the received signal at a receiver node is the summation of all the signal powers arriving from all the sender nodes and the procedure for error detection is implemented into the packet format, so a node/s that does not receive a packet properly will not transmit on the next hop in the path. And due to that it reduces the likelihood of a packet being received in error. Here we explain two major phases cooperative transmission protocol i.e. routing phase and "recruiting-and-transmitting" phase.

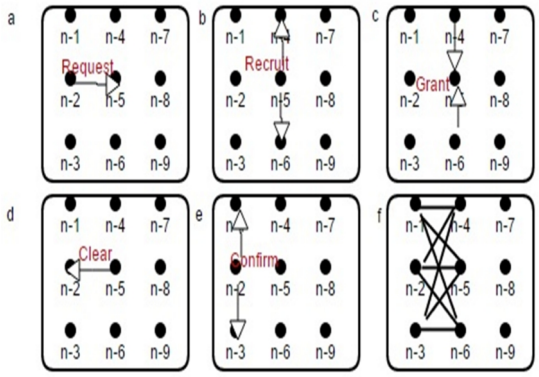


Fig. 3. Example Of The Recruiting Phase Operation (A) Request-To-Recruit (RR) Packet. (B) Recruit (REC) Packet. (C) Grant (GR) Packet. (D) Clear (CL) Packet. (E) Confirm (CF) Packet. (F) Transmission Of The Data Packet.

A. Routing Phase :

This stage find a "one-node-thick" route from the source to sink node which undergoes a thickening operation in "Recruit" and "Transmit" phase. Data regarding the energy required for transmission to neighboring nodes is calculated. This data later used for cluster establishment in the "Recruit-and-Transmit" phase for selecting nodes with lowest energy cost.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

B. Recruiting and retransmitting phase:

In this stage, the nodes on the initial path will become cluster heads, which recruit additional neighbor nodes from their neighborhood. The inter-clusters distance(s) is significantly larger than the width between nodes in the same cluster because the (CH) recruit nodes from their next instant neighborhood. Recruiting is done dynamically and per packet as the packet starts traversing the path. The cluster head initialize the recruiting by the next node on the "one-node-thick" path. Once the recruitment is completed and the receiving cluster is formed, the packet is transmitted from the sending cluster to the newly formed receiving cluster. Recruiting and transmitting of data is done dynamically per hop, initializing from the source node and progressing, multi hop, as the packet moves according to the path to the sink node. The receiving bunch of the previous hop along the path becomes the sending bunch, when data packet is received by it and forms the new receiving cluster. The next node on the "one-node-thick" path will become the cluster head of the next receiving cluster. The receiving cluster is framed by the cluster head by recruiting neighbor nodes through exchange of short control packets such as RR, REC, GR, CL, CF. Then, the sending cluster head synchronizes its nodes, at which time the node transmit the information parcel to the nodes of the accepting cluster. Medium Access Control (MAC) is done in the "recruiting-and-transmitting" phase through interchanging of short control packets between the nodes on the "one-node-thick" path and their neighbor nodes. Operation of the "recruiting-and-transmitting" phase is demonstrated in the Fig 3(a) to Figure 3(f). Selection of (CH) can be done based on the position and energy computing of node where Base node broadcasts control packets and nodes within the optimal communication range of source node and located at appropriate position correspond to Base node. These nodes will face for cluster head according to their own energy. Then the Cluster head broadcasts control packets to decide on cluster head for the next hop. Repeating above cycle till a complete route containing cluster head is formed and then cluster head performs the clustering. It executes the recruitment of cluster members according to the optimal position and residual energy of neighboring nodes.

In the *Fig: 3* demonstrate the operation of the "recruiting-and-transmitting" stage. In the present hop, node-2 is the sender and (CH) cluster head and has a packet to be sent to node-5. Node-2 transmits the request-to-recruit (RR) packet to node-5 [Fig-3(a)], causing node-5 to initiate the formation of the receiving cluster, with node-5 as the (CH) cluster head. From the routing phase, node-5 already knows that the next-hop node is node-8. Where (node-5) broadcasts to its neighbors a recruit (REC) packet [Fig-3(b)]. The Recruit packet contains, the ID of the former (node -2), the ID of the next (node-8) and the maximum time to respond, denoted as T. Every node that receives the Recruit (REC) packet, which we call potential recruits (nodes 4 and 6), computes the summation of the link costs of the following two links like, a link from the sender cluster head to itself (the receiving link) and a connection from itself to the next node, such as the receiver cluster head or the sink node (the sending link). Here (node-4) calculates the sums of the energy costs of the links (2,4) and (4,8), while (node-6) calculates the sum of the energy costs of the links (2,6) and (6,8). A potential recruit do replies to the REC packet with a Grant (GR) packet that contains the calculated sum [Fig-3(c)]. The Grant(GR) packets reports the (CH)cluster head that the nodes are reachable to cooperate in receiving on the present hop as well as in sending on the next hop. After waiting time T and collecting a number of grants, the cluster head (node-5) selects m-1 cooperating nodes with the smallest reported cost to frame the receiving cluster of nodes.

If the cluster head node received less than m-1 grants, it shapes a smaller receiving cluster with all the node/s that transmits the grants to node-5, then sends a Clear (CL) packet [Fig- 3(d)] that consists of ID of the selected cooperating nodes (4 and 6). By receiving the CL packet from node-5, node-2 transmits a (CF) confirm packet to the nodes in its sending cluster (node 1 and 3) to coordinate their transmission of the data packet [Fig-4(e)]. The CF packet consists of the waiting time-to-send and the transmission power level Pt. The transmission power level is the total transmission power divided by the number of the node/s in the sending cluster. In the case of our example, the value of Pt is divided by 3 (nodes 1&3 are cooperatively in sends). After the waiting-time-to-send expires, sending cluster nodes 1–3 transmit the data packet to receiving cluster nodes 4–6 [Fig- 3(f)].

2. RELATED WORK

Wireless sensor networks had been used [1]suboptimal algorithm for finding minimal

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

energy for cooperative wireless network using channels and receivers to reduce the optimal energy usage protocol used for organization of these clusters and for cooperatively transmitting of data. The cooperative transmission link in wireless networks as a transmission cluster and a reception cluster. This protocol reduces the energy consumption based on the communication model, which considers only the communication but not the parameters of the nodes in the cooperative networks**.** The total energy consumption can be considerably reduced by adjusting the transmit power for intra-cluster and inter-cluster transmission were suboptimal algorithms for general networks and confirmed via simulations that even these suboptimal algorithms can achieve energy savings of close to 50% in a general network. By using optimizing method in cooperative communication the energy consumption has been reduced to further extend. One more method used to reduce the error rate and energy saving in the network, so that it will increase the life time of cooperative sensor networks up to 80% in energy savings can be achieved for a grid topology [2]. The cluster algorithm technique is used reduce the energy consumption and also increase the lifetime and scalability of the network[3].Protocols also used to increase the energy efficiency and it depends upon many parameters such as lifetime, packet delivery, packet delay, and network balance[4].Main clustering technique used in this paper is Adaptive Decentralized Re-Clustering Protocol (ADRP) used to select the cluster head and next head based on the residual energy in the each node and average energy of cluster in the wireless network[5]. Study of different routing protocols for wireless sensor network and also compare their strength and limitations [6]. Another method is used to increase both energy and security in wireless sensor network. And also discussed various security issues energy efficient data transmissions in the wireless sensor networks[7]. New method used to wakeup scheme that is Pipelined Tone Wakeup(PTW) scheme for sensor networks, which helps to achieve the balance between energy saving and end-to-end delay[8].

Trust based framework model are designed for cluster based networks for each nodes have unique local IDS.[9].Integrated approach is used secure wireless sensor network and also analyze security issues solve that issues to get a secure network[10].FLSL algorithm used a protocol that leads to reduce error rate and consuming energy in cooperative sensor network[14].One of the new protocol used with two schemes such as non cooperative and cooperative scheme. These schemes are reduce the error rate and saving energy in the sensor network [16].

Another method used to estimate the performance of cooperative transmission between sender cluster node and receiver cluster node in the wireless sensor network. [17]Optimization technique used cluster cooperative network for save energy. [19][20] There is some method to propose Packet level data compression algorithm. Using this algorithm even better compression ratio has been accomplished and also found that deficiency in the symmetric key management for clustering the nodes for that problem they have found the solution with Identity Based Crypto Logical Approach (IBCLA).

3. METHODOLOGY

The proposed system consists of five phases like *Cluster formation phase, Neighbor recruitment phase, Node selection phase, Cooperative Data Transmission phase, Cooperative Caching phase.*

Cluster formation: In this cluster formation phase we discuss about how the cluster forms to communicate with another sensor. Cluster is made on the basis of the optimal path for the next transmission of the data. In order to form the cluster head in the cluster and also to build the security among the nodes in the cluster, we impose Authenticated Broadcast Mechanism where any node broadcast HELLO message inside the cluster, as soon as the node/s receive the HELLO message the node will response for the request. Here each node will maintain the data cache were counter will be recorded inside the cache, based on the maximum number of HELLO counts received by the any of the node, counter will be maintained in every node and will decided as the Cluster Head. Here the security methods are incorporated in the form of Cryptographic methods, as we mentioned above security is given to each and every node/s inside the cluster through some authentication process, while forming the cluster nodes inside the cluster will be having common shared key, if any kind of message is broadcasted in encrypted form by any sender node, the receiver nodes has to decrypt with the shared key, if not the sender node is considered as an Anti-node/s. Nodes are

Journal of Theoretical and Applied Information Technology
30th June 2016. Vol.88. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

verified and Authenticated using methodologies called Hash Function and Message Authentication Code (MAC).

Neighbor recruitment: Before the neighbor recruitment happens, the source sensor node or the secured node interact with the COM-port, the data packets will be encrypted with the encryption algorithm called *Rijndael* algorithm as an Advanced Encryption Standard (AES), were this algorithm creates new symmetric block cipher that reinforce the key size in the huge bits where an attack is not practical. During neighbor recruitment phase for encrypted data packet transmission, nodes starts communication with all the neighboring nodes by sending the request packet to neighbors and CH to *Recruit* the nodes with *Recruit* packets. We say by sending the request from the secure node to the neighbor CH it tends to send the Recruit packet and each nodes give the *Grant signal* to *Cluster head.*

Node selection: Node selection is all about the recruiting forwarding nodes to forward data packet between clusters and from source node to base station. While recruiting the node's battery residual energy is also vigorously considered, then the CH selects only few nodes among many available and nodes are listed based on their residual energy, then the selected nodes list confirms to requester.

Data Transmission: In data transmission phase, once after the source node receives CONFIRM packet from next hop CH, it gets information about all forwarding nodes. Source node then uses Selective Repeat Protocol and multicast encrypted data packet to all forwarding nodes along with next hop CH. Upon receiving data packet, the next hop CH performs *Neighbor recruitment phase* and *Node selection phase* step to recruit the next neighbor and select forwarders and continue forwarding the data packet towards the destination or base station. Among CH and non CH nodes in a cluster who is receiving data packet from previous cluster, initially only CH node involve in forwarding such data packet to next cluster and every non CH node will multicast to next cluster forwarder only if it has not received acknowledgment (ACK) packet from current CH node within some timeout.

Cooperative Caching: Each non CH node receiving data packet from previous cluster stores received data as cache and runs a timer waiting for ACK packet from current CH node. Upon receiving ACK from current CH node within timeout, each non CH node will clear data packet from cache.

Algorithmic module (*Rijndael Algorithm*)

Step-1: Convert plain text/cipher text to plain Bytes/cipher Byte.

Step-2: Set Rfc2898DeriveBytes with secret key and salt data.

Step-3: Create Rijndael Managed Object (RMO) with 32 Byte main key and 16 Byte Initialization Vector (IV) using RFC2898DeriveBytes.

Step-4: Create encryptor or decryptor using Rijndael Managed Object.

Step-5: Perform encryption or decryption of message using Crypto Stream (CS) object.

Step-6: Convert Plain Byte/cipher Byte back to plain Text/Cipher text.

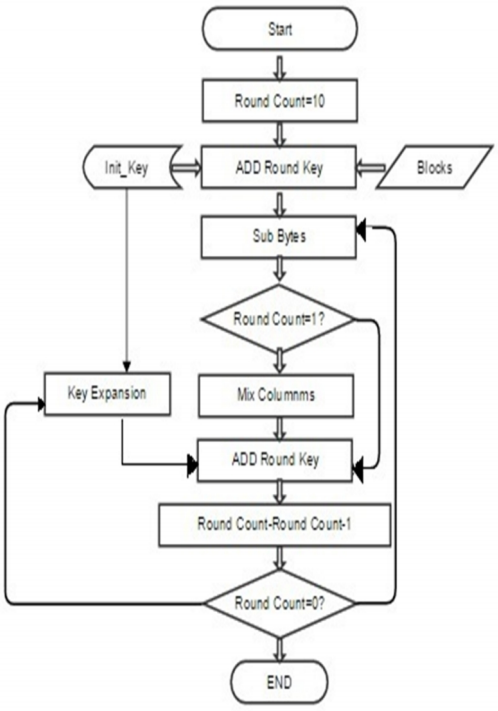


Fig: 4. Flow of Rijendael Algorithm

4. EXPERIMENTAL RESULTS

In this experimental set up selection of the nodes is done and an optimal path is being established

Journal of Theoretical and Applied Information Technology
30th June 2016. Vol.88. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for the data transmission. In order to do this process, initially confirmation has to be done about the node/s are secured or not, to authenticate the nodes the procedure is explained in (*Cluster formation phase)* The cryptographic method helps in securing the nodes which is achieved in (*Neighbor recruitment phase*) and in the *Cooperative Data Transmission phase* the data is transmitted after the CH gets ACK from the receivers cluster and then starts sending the data to the next cluster, if CH fails to get ACK within the give time interval, non-CHs starts transmitting the data cooperatively. A small data cache memory is maintained in every node inside the cluster, because every node consist of sender's address in the cache, as soon as the cooperative data transmission starts the node/s automatically clears the cache after the completion of process. The transmission of data at the single instant of time is reduced and the life of sensor is maintained and traffic congestion is avoided, but while the CH waits for ACK from receiver's node the delay occurs and it can be neglected.

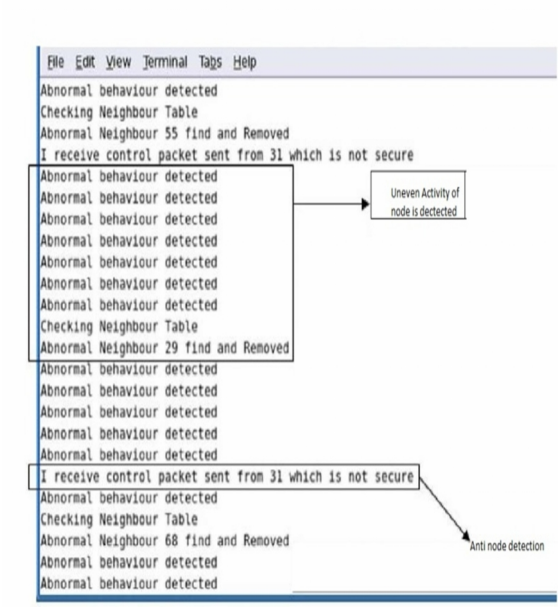


Fig:5 Results On Behavior And Detection On Anti-Node.

In the *Fig: 5* it shows the simulation results on security among each and every node. The node is said to be secured only if it is authenticated. By incorporating cryptographic authentication process, while forming the cluster nodes inside the cluster will be having common shared key.
Broadcasted message will be in encrypted form by any sender node, the receiver nodes has to decrypt with the shared key. If not the sender node is considered as an Anti-node/s and based on the behavior of the node/s so that the node is insecure.

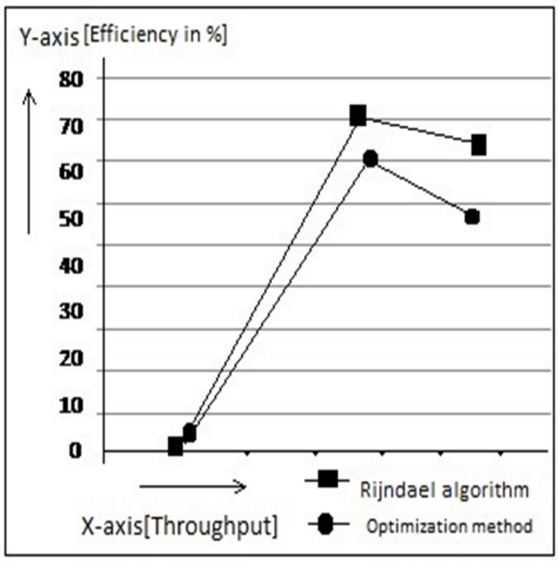


Fig: 6. Calculation Of Energy Efficient And Throughput.

Comparative study is achieved by estimating efficiency and throughput with the previous work (optimization technique) and cooperative communication. The reduction in failure rate and energy consumption translates into increased lifetime of cooperative sensor networks.

5. CONCLUSION & FUTURE WORK

In this work, we carried the methodology to build the security among the nodes using cryptographic method called *Rijndael algorithm*. It detects the anti-node and to avoid intrusion of non-essential signals from an anti-node which creates the extra traffic congestion while transmitting the data through cooperative communication.
This proposed work computes energy efficiency of the cooperative and direct transmission schemes in WSN, also studied and compared. In "*recruiting-and-transmitting*" phase, the cluster

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

on the initial path recruits only optimal nodes from their neighborhood hence form a secured cluster. The data cache is maintained in every node/s so the sender's details will be recorded in the cache memory. The results show that our proposed cooperative transmission protocol reduces the energy consumption and failure rate and delay time in the data transmission phase with Single Input Multiple Output (SIMO) format throughput is increased.

In future, the propagation delay can be estimated for the cooperative transmission in order to accomplish that work the activity of and behavior of the node has to be study.

REFERENCES

[1] Amir Ehsan Khandani, Jinane Abounadi, Eytan Modiano, and Lizhong Zheng,"Cooperative Routing in Static Wireless Networks", *IEEE Transactions on communications*, vol. 55, no. 11, November 2007, pp.2185-2192.

[2] Mohamed Elhawary and Zygmunt J. Haas," Energy-Efficient Protocol for Cooperative Networks", *IEEE/ACM Transactions on*, *19*(2), April 2011, pp.561-574.

[3] Li Qing , Qingxin Zhu, Mingwen Wang," Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks",*Computer communications*, *29*(12),2006, pp.2230-2237.

[4] Farzad Kiani, Ehsan Amiri, Mazdak Zamani,Touraj Khodadadi,4 and Azizah Abdul Manaf," Efficient Intelligent Energy Routing Protocol in Wireless Sensor Networks", *International Journal of Distributed Sensor Networks,2015,p.15.*

[5] Fuad Bajaber and Irfan Awan," Adaptive decentralized re-clustering protocol for wireless sensor Networks", *Journal of Computer and System Sciences*, *77*(2), 2011,pp.282-292.

[6] Shio Kumar Singh, M P Singh, and D K Singh," Routing Protocols in Wireless Sensor Networks – A Survey", *International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1*, November 2010, pp. 63-83.

[7] Shilpy Ghai1, Prof.V.K.Katiyar2,"Energy Efficient Data Transmission Schemes in Wireless Sensor Networks*", International Research Journal of Innovative Engineering Vol. 1.*

[8] Xue Yang,and Nitin H.Vaidya," AWakeup Scheme for Sensor Networks: Achieving Balance between Energy Saving and End-to-end Delay", In *Real-Time and Embedded Technology and Applications Symposium, 2004. Proceedings. RTAS 2004. 10th IEEE*,2004,pp.19-26

[9] Garth V. Crosby, Niki Pissinou,and James Gadze," . In *Dependability and Security in Sensor Networks and Systems, 2006. DSSNS 2006. Second IEEE Workshop on,2006,*pp. 10-pp.

[10] Fei Hu, Jim Ziobro, Jason Tillett,and Neeraj K. Sharmand ," Secure Wireless Sensor Networks: Problems and Solutions", *Rochester Institute of Technology, Rochester, New York, USA*,2004.

[11] Bikramaditya Das,and Susmita Das," Efficacy of Multiband OFDM Approach in High Data Rate Ultra WideBand WPAN Physical Layer Standard using Realistic Channel Models",*I nternational Journal of Computer Applications* 2.2,2010,pp.81-87

[12] Kiyani, Farzad, H. Tahmasebirad, Hadi Chalangari, and Sajjad Yari. "DCSE: A dynamic clustering for saving energy in wireless sensor network." In *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*, 2010,pp. 13-17.

[13] Thangam, R. Parimala, and G. Wiselin Jiji. "Reliable and Energy Efficient Protocol for Cooperative Wireless Sensor Networks." *International Conference on Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012) Proceedings published in International Journal of Computer Applications® (IJCA),2012.*

[14] Pandey, K. K., Purohit, N.and Agarwal,"Efficient Clustering Technique for CooperativeWireless Sensor Network", *International Journal of Computer Network and Information Security*, *6*(10), 2014,p.40.

[15] Sagiraju Srinadh Raju and K.Ramesh²," Energy-Efficient Cooperative Protocol for Wireless Networks",.Sagiraju Srinadh Raju et al ,Int.J.Computer Technology & Applications,Vol 3 (4), 1455-1462.

[16] Karthikeyan.S, Sairam.N, Manikandan.G, and Sivaguru.J," A Parallel Approach For Improving Data Security" *Research*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Journal of Applied Sciences, Engineering And Technology, *4*(6),2012, pp.603-607.

[17] U.Sandhya and S.Vikram Phaneendra, "Optimization of energy usage in Cooperative Networks, International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 9– Sep 2013,2013.

[18] M. Ramesh Kumar and Suresh Gnana Dhas," An Expedited Triple Key Broadcast Authentication Scheme Based On Tesla, ECDH,and ECDSA", *Journal of Theoretical and Applied Information Technology*, *58*(3),2013.

[19] S.Jancy,and Dr . C. Jaya Kumar, PACKET LEVEL DATA COMPRESSION TECHNIQUES FOR WIRELESS SENSOR NETWORKS, *Journal of Theoretical and Applied Information Technology*, *75*(1),2015 May.

[20] A.Jegatheesan,DR.D.Manimegalai,AND G.Thanusha, "a novel identity based cryptological approach for cluster employed secure wireless sensor network." Journal of Theoretical and Applied Information Technology, 68(2).2014.

.