Volume 5, Issue 10, October-2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Avoidance of Replication Attack in Clusters through Witness Node

[1]Parveer Kaur, [2]Abhilash Sharma

[1]Research Scholar, [2]Assistant Professor

[1, 2] Department of Computer Science and Engineering

RIMT-IET, Mandi Gobindgarh, Punjab, India

Abstract - Various types of attacks occur in WSN. Attack occur in WSN is clone attack which is also known as replica attack. In this attack the node copy the id of the other node and show its predictions at different locations. A clone node can create a black hole or wormhole attack include adversary can use them in different ways. This attack can transmit false information to all legitimate nodes. The clone attack is very suitable for adversary. For this attack adversary has not to be compromise for number of nodes. The adversary can do cloning of one node and can predict other nodes through this node. It falsifies its positions at different times at different locations. Main problem in this is to detect the node having clone attack, because each and every node has same id and different locations on same interval of time. This problem has also been arising in clusters in which cluster head replicate and the main problem arises when whole cluster replicate.

Keyword: WSN, Leach, Leach-C, clone attack and clustering

I. INTRODUCTION

1.1 Wireless sensor network:

Wireless sensor network provide a very big wireless sensor nodes, which are resource constrained like energy, memory etc. A sensor node will be also referred to as just node or sensor in the sequel. There are various type of application of WSN are already present in health care, navigation, rescue, intelligent transportation, social networking, gaming application fields, and critical infrastructure protection. This system is of inhabitant went to and conveyed in unforgiving situations. WSNs are henceforth subject to a few dangers due to their temperament. In this paper we concentrate on the security of the WSN.

1.2 Types of WSN

1.2.1 Structured WSN: In this all n some of the sensors nodes are deployed in fix position in a pre-planned manner. The upside of an organized WSN is that less gadgets can be sent with lower system upkeep and administration costs.

1.2.2 Unstructured WSN: contains a thick gathering of sensor hubs, which are arbitrarily set into the field .An impromptu organization is favored over a pre-arranged sending when the system is made out of hundreds to a huge number of hubs with a specific end goal to cover a bigger region or when the Environment is not straightforwardly available by people endeavoring to develop WSN.

1.3 Routing Protocols in WSN

Energy consumption is reduced by using various techniques like data aggregation, clustering, data-centric methods etc. The routing protocols can be classified as flat, hierarchical or location-based as follow:

1.3.1 Flat networks: Equal nodes are used in this. Same role is played by every node. e. This network has no logical hierarchy. It uses a flat addressing scheme. The example of flat network is Routing Information Protocol (RIP)

1.3.2 Hierarchical networks: Nodes are partitioned into number of small group, which called cluster. Each cluster has a cluster head which is the coordinator of other nodes. These CHs perform data aggregation so that energy inefficiency may be reduced. The node which has the highest energy acts as the CH. Hierarchical routing is an efficient way to lower energy consumption within a cluster. It has major advantages of scalability, energy efficiency, efficient bandwidth utilization, reduces channel contention and packet collisions.

1.3.3 Location-based networks: In location-based clustering, the area of the sensor hubs assumes a vital part. Base station is utilized to send information to a specific area. In these conventions, the attention to position of the sensor hubs is extremely huge to exchange the information to destinations. The separation between neighboring hubs can be evaluated on the premise of approaching sign qualities. On the premise of area based convention, if there is no movement then hubs ought to go to rest to spare vitality. Area Aided Routing (LAR) and the sample of area based convention Distance Routing Effect Algorithm for Mobility (DREAM).

1.4 Applications of Wireless Sensor Network

1.4.1 Process Management: The regular utilization of WSN is region observing. In zone checking, the WSN is conveyed upon a range where some marvel is to be observed. The utilization of sensors identifies adversary interruption is military; a non military personnel illustration is the geo-fencing of gas or oil pipelines. Territory observing is most critical part.

1.4.2 Health care monitoring: Initially gadget are utilized on the body surface of a human furthermore exactly at close nearness of the client. The implantable restorative gadgets are those which are embedded inside of the human body. There are additionally numerous other application like body position estimation and area of the individual, general checking of sick patients in healing centers and at homes.

1.4.3 Environmental/Earth sensing: In observing environment there is so much application, cases of which are given beneath. They share the additional difficulties of cruel situations and decreased power supply.

1.4.4 Air pollution monitoring: Remote sensor systems have been conveyed in a few urban areas to screen the grouping of risky gasses for natives. These can exploit the specially appointed remote connections as opposed to wired establishments, which additionally make them more portable for testing readings in diverse regions.

1.4.5 Forest fire detection: A system of Sensor Nodes can be introduced in a backwoods to distinguish when a flame has begun. The hubs can be outfitted with sensors to quantify temperature, moistness and gasses which are delivered by flame in the trees or vegetation. The early discovery is vital for an effective activity of the firefighters; on account of Wireless Sensor Networks, the fire unit will have the capacity to know when a fire is begun and how it is spreading.

1.5 MWSN:

Mobile wireless sensor network (MWSNs) can basically be characterized as a wireless sensor network (WSN) in which the sensor hubs are portable. MWSNs are a littler, developing field of exploration as opposed to their entrenched ancestor. MWSNs are significantly more adaptable than static sensor systems as they can be sent in any situation and adapt to fast topology changes. On the other hand, a significant number of their applications are comparative, for example, environment checking or reconnaissance usually the hubs comprise of a radio handset and a microcontroller controlled by a battery. And additionally some sort of sensor for distinguishing light, warm, stickiness, temperature, and so forth.

II. PROTOCOL USED

LEACH protocol: Low Energy Adaptive Clustering Hierarchy ("LEACH") is a TDMA-based MAC protocol which is integrated with clustering and a simple routing protocol in wireless sensor networks (WSNs). The goal of LEACH is to lower the energy consumption required to create and maintain clusters in order to improve the life time of a wireless sensor network. LEACH is a hierarchical protocol in which most nodes transmit to cluster heads, and the cluster heads aggregate and compress the data and forward it to the base station (sink). Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round. LEACH assumes that each node has a radio powerful enough to directly reach the base station or the nearest cluster head, but that using this radio at full power all the time would waste energy. Nodes that have been cluster heads cannot become cluster heads again for P rounds, where P is the desired percentage of cluster heads. Thereafter, each node has a 1/P probability of becoming a cluster head in each round.

LEACH-C Protocol: It is the enhanced version of LEACH protocol. . It is also divided into two phases, set-up phase and steady state phase like LEACH. LEACH-C organizes the sensor nodes into clusters with each cluster a cluster head. It differs from LEACH only in that it uses a high-energy base station for the selection of cluster heads. LEACH-C, uses a centralized clustering algorithm for the election of cluster heads and for formation of clusters. It has same steady state phase as LEACH. LEACH-C protocol can increase its performance by dispersing the cluster heads in the network. Set-up phase of LEACH-C is different from LEACH. In the set-up phase of LEACH-C, each node sends information about its current location and residual energy level to the Base station. For the formation of good clusters, the base station needs to ensure that the energy distribution is same among all the nodes. To do this, Base station computes the average energy of all nodes, and determines which nodes have energy below this average energy. The nodes which have more energy than average and lesser distance from base station are selected as cluster heads. Once the cluster heads and associated clusters are found, the base station broadcasts the IDs of cluster heads to other member nodes and nodes join the cluster head by sending its information node id and location. This method can make the nodes with more energy and more chance to become the cluster head in the current round. But in this phase, every sensor node needs to send its ID and energy information to remote BS to become a cluster heads.

III. RELATED WORK

Wassim Znaidi et al [1] "Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks", Remote sensor systems (WSNs) are made out of various minimal effort, low-control sensor hubs conveying at short separation through remote connections. Sensors are thickly sent to gather and transmit information of the physical world to one or couple of destinations called the sinks. On account of open arrangement in threatening environment and the utilization of minimal effort materials, intense foes could catch them to concentrate delicate data (encryption keys, personalities, addresses, and so forth.). At the point when hubs may be bargained, "past cryptography" algorithmic arrangements must be visualized to supplement the cryptographic arrangements. This paper addresses the issue of hubs replication; that is, an enemy catches one or a few hubs and additions copied hubs at any area in the system.

Jaydeep Barad et al [2] "improvement of deterministic key management scheme for securing cluster-based sensor networks" As sensor hubs are conveyed in unfriendly or remote environment and unattended by human, they are inclined to distinctive sort of assaults. So adjustment of element key is critical for secure key administration, for scrambling messages for correspondence. As a result of the constraints of WSN like restricted memory, battery life and preparing force, utilization of bunch based remote sensor system diminishes framework deferral and vitality utilization. Drain, bunch based convention for sensor systems, accomplishes vitality productive and versatile directing. Though capacity issue in sensor system, can be diminished by utilizing deterministic key administration plan. In this setting, from all the distinctive key administration plans in WSNs, deterministic key administration plan with LEACH, called DKS-LEACH is the plan which is utilized to secure remote sensor system in productive way and gives verification, privacy and uprightness of detected information. Still vitality utilization and flexibility against hub catch is an issue with DKS-LEACH. So we proposed the plan RINGLEACH to enhance the current plan to make it stronger utilizing separation based key administration plan. Indeed, even to make it vitality proficient, one can change the current system to quit sending fake messages to BS. In this manner proposed methodology manages inside and also outside pernicious hubs.

Nayyer Panahi et al [3] "Adaptation of LEACH Routing Protocol to Cognitive Radio Sensor Networks" One of the disadvantages of LEACH convention is the uncontrolled choice of group heads which, in a few rounds, prompts the convergence of them in a constrained zone because of the irregularity of the choice strategy. Filter C is a variation of LEACH that uses a brought together grouping calculation and structures great bunches through sink control. As per test comes about, the IEEE 802.15.4 parcels are harmed by WLAN obstructions in ISM band. It appears that, sensor hubs furnished with psychological radio abilities can conquer this issue. In subjective radio sensor systems (CRSN), steering must be joined by channel designation. This requires range administration which can be lapsed to bunch heads. For this systems, new obligation cycle instruments must be outlined that mutually consider neighbor revelation, and range detecting/distribution. Group based system structural planning is a decent decision for compelling element range administration. In such construction modeling, bunch heads have a legitimate spatial dissemination and are ideally found everywhere throughout the system.

mr.suyog pawar et al [4] "design and evaluation of en-leach routing protocol for wireless sensor network" A Wireless network comprising of countless sensors with low-control handsets can be a viable device for social event information in an assortment of situations like common and military applications. The information gathered by every sensor is imparted through the system to a solitary handling focus called base station that uses all reported information to decide attributes of the earth or recognize an occasion. Bunching sensors into gatherings, so sensors impart data just to neighborhood group heads and after that the group heads convey the collected data to the handling focus, may spare a considerable measure of vitality. Filter is grouping based convention that uses randomized pivot of nearby bunch heads to uniformly appropriate the vitality load among the sensors in the system. Drain uses limited coordination to empower adaptability and power for element organizes, and joins information combination into the steering convention to lessen the measure of data that must be exchanged to the base station.

Shin-nosuke Toyoda et al [5] "Dynamic Change Method of Cluster Size in WSN" One of the significant issues in remote sensor system is adding to a vitality productive directing convention. Filter is exceptionally vitality proficient directing convention in light of the bunching of the sensor hubs. Be that as it may, vitality utilization of hubs has a tendency to wind up uneven in LEACH. Notice enhances the LEACH using so as to bunch calculation data of lingering electric force of hubs. In spite of the fact that HEED gives preferred execution over LEACH, it doesn't consider the quantity of contiguous hubs. Accordingly, the bunch head does not effectively cover the hubs in HEED. HIT depends on the little transmission reach and multi-bounce correspondence. In spite of the fact that HIT has enhanced the execution drastically, unbalance of the electric force utilization is remained. In this paper, we propose vitality proficient grouping calculation considering adjoining hubs and leftover electric force. Qualities of our methodology are stepwise grouping from a beginning bunch head and element change of bunch size.

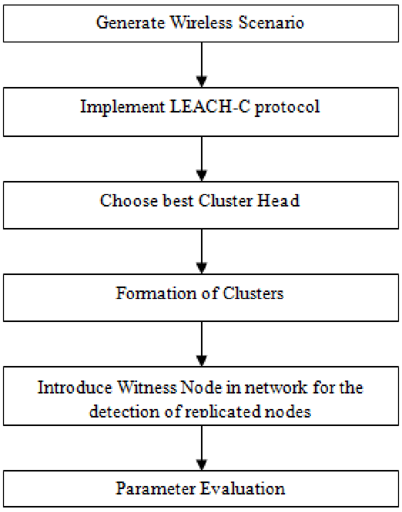
IV. PROBLEM FORMULATION

In the wireless sensor networks, the network nodes are used for sensing the information from the various types of non-reachable areas. In WSN sensor nodes has been used for sensing the information from harsh environment and communicate with each other through wireless links. In these nodes sensors of different types has been used for collecting information. Wireless sensor networks are of main two types, which are static wireless sensor nodes and mobility wireless sensor networks. In WSNs the main threat in the network is security because Sensor nodes are deployed in an open and uncontrolled environment where attackers may be present, therefore it requires secure communication. Attackers can easily capture a single node, replicate it and insert duplicate nodes at any location. If this attack is not detected, may other attacks such as Sybil or wormhole attack can be launched in the network. Attack occur in WSN is clone attack which is also known as replica attack. In this attack the node copy the id of the other node and show its predictions at different locations. This attack occurs when an attackers adds on or more nodes with node identities that are already deployed in the network i.e single identity is used by multiple nodes at different locations. If no specific detection mechanism is set up, the attackers can inject false data, revoke legitimate nodes and disconnect the network. The adversary can do cloning of one node and can predict other nodes through this node. Main problem in this is to detect the node having clone attack, because each and every node has same id and different locations on same interval of time. It can affect the network by various ways. This problem has also been arising in clusters in which cluster head replicate and the main problem arises when whole cluster replicate.

- To initialize scenarios parameters.

- Implement LEACH-C protocol for clustering.
- Introduce witness node in network for the detection of replicated nodes.
- To compare the node entry table of cluster head with other cluster heads to check duplicity.

V. PROPOSED WORK


Generate Wireless Scenario
Implement LEACH-C protocol
Choose best Cluster Head
Formation of Clusters
Introduce Witness Node in network for the detection of replicated nodes
Parameter Evaluation

VI. RESULTS AND DISCUSSION

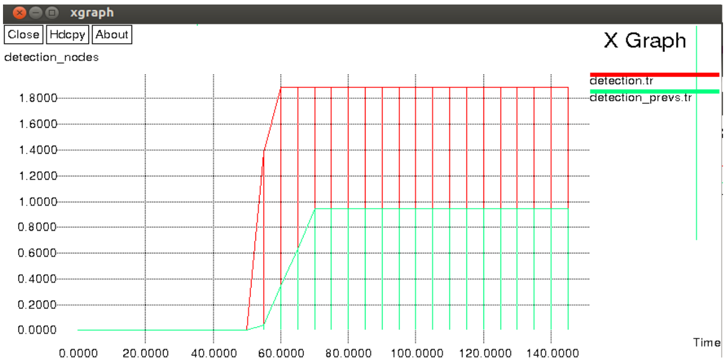


Fig 6.1: Detection

This graph is used to represent the detection of replicated nodes by using Witness node technique as compared to bloom filter technique.

Table 6.1: Detection

Time(in sec)	Previous Work	Present Work
0	0	0
20	0	0
40	0	0
60	.344	1.88
80	.944	1.89
100	.944	1.89
120	.944	1.89
140	.944	1.89

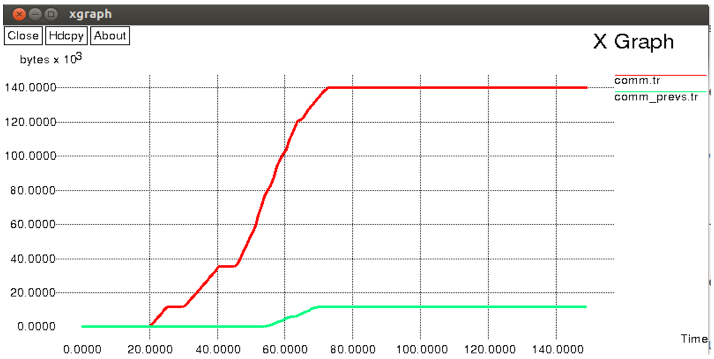


Fig 6.2: Communication

This graph is use to represent the transfer of messages between the nodes by choosing cluster member and cluster head as source node and base station as destination node, which is called communication between the nodes.

Table 6.2: Communication

Time(in sec)	Previous Work	Present Work
0	0	0
20	0	0
40	0	35
60	3.7	71
80	11	137
100	11	140
120	11.8	140.3
140	11.8	140.3

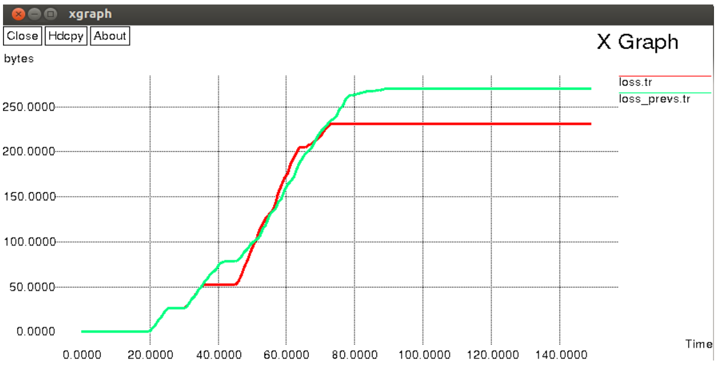


Fig 6.3: Loss

This graph is use to represent the packet loss in the network by using LEACH-C protocol as compared to LNCA protocol.

$$\text{Packets loss} = \frac{\text{Number of packets loss}}{\text{Number of packets sent}}$$

Table 6.3: Loss

Time(in sec)	Previous Work	Present Work
0	0	0
20	3.06	3.22
40	75.29	50.60
60	164.49	176.08
80	226.46	223.76
100	270.010	230.82
120	270.47	230.82
140	270.47	230.82

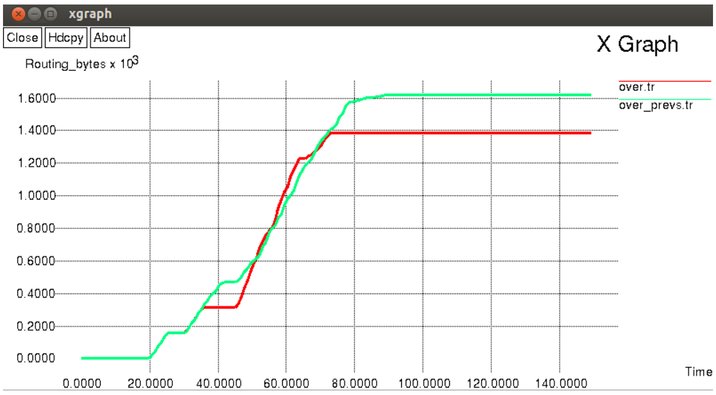


Fig 6.4: Overloading

This graph is used to represent the overloading of message by using LEACH-C protocol as compared to LNCA protocol. LEACH-C follows TDMA schedule for sending the packets in the network.

Table 6.4: Overloading

Time (in sec)	Previous work	Present Work
0	0	*0*
20	0	0
40	451.54	30360
60	986.97	1056.40
80	1582.34	1342.61
100	1622.82	1384.93
120	1622.82	1622.82
140	1622.82	1622.82

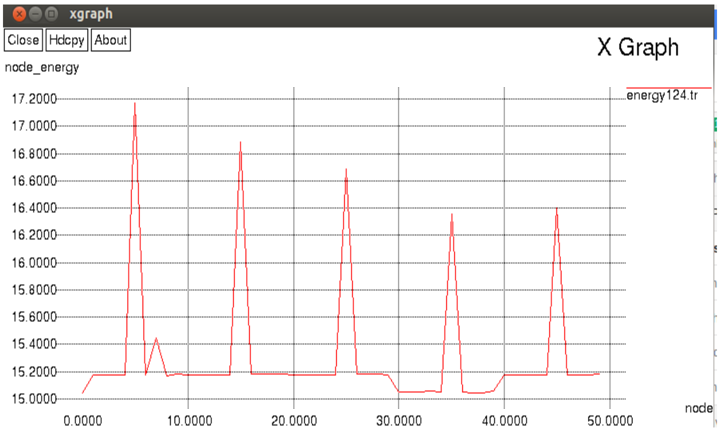


Fig 6.5: Overloading

This graph is use to represent energy required for the transmission of message. Energy is a property of objects which can be transferred to other objects or converted into different forms, but cannot be created or destroyed.

VII. CONCLUSION

In this paper, we considered a LEACH-C protocol and Witness node technique for better detection of replicated nodes. We found that by using witness node technique a whole replicated cluster can be detected. The LEACH-C clustering protocol shows better result in term of less energy consumption, communication, packets loss and packets overloading by choosing cluster head as source node and base station as destination. This shows that our technique gives better results as compared to previous technique.

REFERENCES

[1] Wassim Znaidi “Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks”, *IEEE Conf. on Personal, Indoor and Mobile Radio Communications*, 2009, pp 82 – 86.

[2] Jaydeep Barad “improvement of deterministic key management scheme for securing cluster-based sensor networks” *IEEE Conf. on Networks & Soft Computing (ICNSC),* 2014, pp 55 – 59.

[3] Nayyer Panahi “Adaptation of LEACH Routing Protocol to Cognitive Radio Sensor Networks*” IEEE Conf. on Telecommunications (IST),* 2012, pp 541 – 547.

[4] Mr.Suyog Pawar *“*design and evaluation of en-leach routing protocol for wireless sensor network*” IEEE Conf. on* Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012,pp 489 – 492.

[5] Shin-nosuke Toyoda “Dynamic Change Method of Cluster Size in WSN” *IEEE Conf. on Broadband, Wireless Computing*, 2012, pp 20 – 27.

[6] muhammad haneef “comparative analysis of classical routing protocol leach and its updated variants that improved network life time by addressing shortcomings in wireless sensor network”, *IEEE conf. On Mobile Ad-hoc and Sensor Networks (MSN)*, 2011, pp 361 – 363.

[7] Yingpei Zeng ; State Key Lab. for Novel Software Technol., Nanjing Univ., Nanjing, China ; Jiannong Cao ; Shigeng Zhang ; Shanqing Guo “Random-walk based approach to detect clone attacks in wireless sensor networks ”, 0733-8716, 677 – 691, IEEE, 2013.

[8] Sivasankar, P.T.; Ramakrishnan, M. “Active key management scheme to avoid clone attack in wireless sensor network”

[9] U. Ahmed and F.B. Hussain, “Energy efficient routing protocol for zone based mobile sensor networks”, in proceedings of the 7th international Wireless Communications and Mobile Computing conference (IWCMC), pp. 1081-1086.

[10] Y. Han and Z. Lin. “A geographically opportunistic routing protocol used in mobile wireless sensor networks”, in proceedings of the 9th IEEE international conference on Networking, Sensing and Control (ICNSC), pp. 216-221.

[11] Guanglai Chen “NoticeofRetraction the design of wireless wave height sensor network node based on Zigbee technology”, 978-1-4244-8036-4, 3683 – 3686, IEEE, 2011

[12] Vithya, G “Actuation sensor with adaptive routing and QOS aware checkpoint arrangement on Wireless Multimedia Sensor Network”, 978-1-4577-0588-5, 444 – 449, IEEE, 2011.

[13] Deshpande, V.V. “Energy efficient clustering in wireless sensor network using cluster of cluster heads”, 978-1-4673-5997-9, 2151-7681, IEEE, 2013.

[14] Xiangwen Zhang “Key Technologies of Passive Wireless Sensor Networks Based on Surface Acoustic Wave Resonators”, 978-1-4244-1685-1, 1253 – 1258, IEEE, 2008.

[15] B. Karp and H. T. Kung. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks.In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking pp.243-254.

[16] T.P.Lambrou and C.G. Panayiotou.2009.A Survey on Routing Techniques Supporting Mobility in Sensor Networks.In Proceedings of the 5th international conference on Mobile Ad Hoc and Sensor Networks (MSN'09). pp. 78-85.

[17] S. Kwangcheol, K. Kim and S. Kim. 2011. ADSR: Angle-Based Multi-hop Routing Strategy for Mobile Wireless Sensor Networks.In proceedings of the IEEE Asia-Pacific Services Computing Conference (APSCC). pp.373-376.

[18] D. Kim and Y. Chung. 2006. Self-Organization Routing Protocol Supporting Mobile Nodes for Wireless Sensor Network.In proceedings of the 1st international multi-symposiums on Computer and Computational Sciences (IMSCCS’06). pp.622-626

[19] Abinaya, P. “Dynamic detection of node replication attacks using X-RED in wireless sensor networks”, *IEEE Conf on Information Communication and Embedded Systems (ICICES),* 2014, pp 1 – 4.

[20] “Wen Tao Zhu “Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme”, *Network Computing and Information Security (NCIS),* 2011, pp 156 – 160.

[21] Yan Liang, Rui Wang “A Biologically Inspired Sensor Wakeup Control Method for Wireless Sensor Networks” *IEEE Transactions on Systems, Man and Cybernetics,* pp. 525-538, 2010.

[22] Ashlyn Antoo “EEM-LEACH: Energy Efficient Multihop LEACH Routing Protocol for Clustered WSNs” *International conference on control, Instrumentation, communication and computational technology (ICCICCT),* 2014

[23] Modares, H, Moravejosharieh, A. “Overview of Security Issues in Wireless Sensor Networks” *IEEE Third International Conference on Computational Intelligence, Modelling and Simulation,* pp. 308-311, 2011

[24] Marriwala, N, Rathee, P. “An approach to increase the wireless sensor network lifetime” *IEEE World Congress on Information and Communication Technologies,* pp. 495-499, 2012.

[25] Mittal, R, Bhatia, M.P.S. “Wireless sensor networks for monitoring the environmental activities” *IEEE International Conference on Computational Intelligence and Computing Research,* pp. 1-5, 2010.

[26] Harneet Kour “Hybrid Energy Efficient Distributed Protocol for Heterogeneous Wireless Sensor Network” *International journal of Computer Applications,* Volume 4- No.6 , 2010.