



## International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

# The Survey of Removal of Network Attacks with Energy Efficient Approach in WSN -A Review

Kiran Bansule, Prof. Kalyani Pendke, Prof. Rashmi Jain

Scholar Student, Dept of CSE, Rajiv Gandhi College of Engineering and Research, Nagpur, India

Assistant Professor, Dept of CSE, Rajiv Gandhi College of Engineering and Research, Nagpur, India

Assistant Professor, Dept of CSE, Rajiv Gandhi College of Engineering and Research, Nagpur, India

**ABSTRACT:** A Wireless Sensor Network is the collection of large number of sensor nodes, which are technically or economically feasible and measure the ambient condition in the environment surrounding them. The difference between usual wireless networks and WSNs is that sensors are sensitive to energy consumption. Energy saving is the crucial issue in designing the wireless sensor networks. In this paper, energy efficient technique is used to improve the lifetime of WSN. This proposed energy efficient technique is builds to evaluate in detecting and preventing compromised node become cluster head. K-LEACH uses the K-medoids clustering algorithm to obtained highly uniform clustering of nodes and very good choices of cluster heads and it is very well known fact energy retention of a WSN is highly dependent on the grouping or clustering of transmitting and receiving nodes. K-LEACH protocol improves the clustering and cluster head selection procedure. The proposed system will detect a malicious node and also attack made by that node in the network. Then this system will find the alternate path to send the data packets to the receiver. In this way the effect of attack will be removed from the network. In this paper incorporates efficient estimation to determine honest nodes during packets transmission phase. A proposed energy efficient technique is design to provide a secure data transfer.

**KEYWORDS:** Wireless Sensor Network (WSN); Cluster head(CH); Energy Efficiency; Network Lifetime.

### I. INTRODUCTION

Wireless Sensor Networks is a large network of sensors which have the ability to communicate with each other. The WSN which are distributed in a ad-hoc manner. A wireless sensor network consists of geologically distributed autonomous sensor to monitor and control over physical or environmental condition, like temperature, sound, pressure etc. Wireless sensor network (WSN) is one of the evolving technologies. Sensor nodes are able to monitor physical environment, compute and transmit this information to core network. These sensors can communicate with each other and also to some external Base station. In WSN, sensor nodes use wireless communication to send packets. Due to limited transmission range, a sensor node uses multi-hop transmission to deliver the packet to a base station. Hence a packet is forwarded through so many nodes to reach the destination.

Wireless Sensor network usually consist of one base station able to manage all the communication. Energy efficiency is an important factor in wireless sensor network . The main aim is to improve the lifetime of wireless sensor network using an energy efficient technique. In a wireless sensor network, the sensor consumes more energy. The proposed system is design to overcome this problem using an energy efficient technique and it also improve the life time of wireless sensor network. This paper proposes energy efficient technique that selects most optimal Cluster Head (CH) with maximum residual energy at each round of CH selection mechanism along with preventing compromised node to become CH, which leads to better performance than LEACH . The malicious node and attacks made by that node in the network will be detected by the proposed system. Then the proposed system will remove the attacked node and find the alternate shortest path to send the data packets



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Security is main concern in WSNs along with the energy efficient approach. The difference between usual wireless networks and WSNs is that sensors are sensitive to energy consumption. Energy saving is the crucial issue in designing the wireless sensor networks. The proposed system, overcome this problem using energy efficiency technique. The main aim is to improve the lifetime of wireless sensor network using an energy efficient technique. In a wireless sensor network, the sensor consumes more energy. The proposed system is design to overcome this problem using an energy efficient technique and it also improve the life time of wireless sensor network.

Security is very important in a Wireless sensor network. Very few techniques are available for data transfer in WSN. The data are not securely transferred from source to destination. The proposed system will overcome this problem using encryption technique and securely transfer data from source to destination.

## II. RELATED WORK

An efficient clustering algorithm [1] with position based multihop clustering technique is used to choose closed CH and forward packets to BS using round robin technique which makes network energy efficient to select the CH of minimum energy. The protocol improves the network performance with respect to delay and energy consumption. Energy efficient hierarchal routing protocols[2], developed from conventional LEACH routing protocol. Main focus on to increase the life time and how quality routing protocol is improved for the wireless sensor network.

An energy efficient dynamic clustering algorithm for WSNs [3] that automatically organizes the sensors into appropriate number of clusters in network to select best set of CHs. Mobile agent as security solution that will defense against Black-Hole attack for WSNs. The proposed scheme is build to overcome the impact of Black-Hole attack using multiple BS by using mobile agents. The author proposed a mobile agent which is a program segment which is self-controlling. They implement in their paper a simulation-based model of their solution to recover from Black Hole attack in WSNs [4].

Jaspreet Kaur, Vinod Kumar has suggested a secure routing protocol to minimize the impact of Gray-Hole attack in WSN[5]. They proposed system used local monitoring technique to defense against the Gray-Hole attack in WSNs. In this paper proposed a new algorithm-PDCH[6], on the bases of PEGASIS to make every nodes load balance and extent the network lifetime. Protocol PEGASIS is based on the chain structure, every chain have only one cluster head, it is in charge with every node's receiving and sending messages who belong to this chain, the cluster head consumes large energy and the times of every round increasing.

Junwhan Kim has proposed a new routing protocol opportunistic real time routing (or ORTR)[7] that guaranteed delivery of data under time constraints with efficient power consumption. Author compared existing routing protocols against ORTR through a set of simulation experiments. Presented simulation results illustrate that ORTR provides guaranteed real-time service with optimal transmission power without degrading the energy balance.

In the Linked Cluster Algorithm [8], a node becomes the cluster head if it has the highest identity among all nodes within one hop of itself or among all nodes within one hop of one of its neighbors. Security is an important feature for the deployment of Wireless Sensor Networks.[9] This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks.

Noor Zaman, Tung Jang Low, Turki Alghamdi, has suggested a modified algorithm for Low Energy Adaptive Clustering Hierarchy(LEACH) protocol proposed. the modified protocol called "Kmedoids-LEACH protocol(K-LEACH)[10]for clustered WSN is aimed to improving the lifetime of the sensor network by balancing the energy consumption of the nodes. This protocol uses the K-Euclidean distance and maximum residual energy(MRE) is used to select the cluster head.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

## A. Comparison of LEACH and K-LEACH protocol :

LEACH	K-LEACH
In LEACH protocol cluster formation is random and this may lead to non-uniform cluster sizes as well as poor formation of cluster.	K-LEACH uses the K-medoids clustering algorithm to obtained highly uniform clustering of nodes and very good choices of cluster heads and it is very well known fact energy retention of a WSN is highly dependent on the grouping or clustering of transmitting and receiving nodes.
LEACH protocol does random selection of CH, this again may lead to poor to very poor selection of CH which will consequently lead to highly inefficient energy retention by the network.	K-LEACH considers least distant from the centre of cluster as a criterion for a node to be chosen as a cluster head(CH) during cluster head selection procedure.
LEACH protocol select a nodes randomly.	K-LEACH protocol improves the clustering and cluster head selection procedure.

### III. FLOWCHART DESCRIPTION

1. Create a Network: In first module to create a network.
2. Cluster Head formation: : In the second module is to create a cluster using a energy efficient technique, this technique improve the lifetime of wireless sensor network
3. Encryption: Security is very important in a Wireless sensor network. Very few techniques are available for data transfer in WSN. The data are not securely transferred from source to destination.
4. Detect attacks: In forth module , The malicious node and attacks made by that node in the network will be detected.
5. Remove attacks: In fifth module, system will remove the attacked node and find the alternate shortest path to send the data packets.

### IV. FLOWCHART

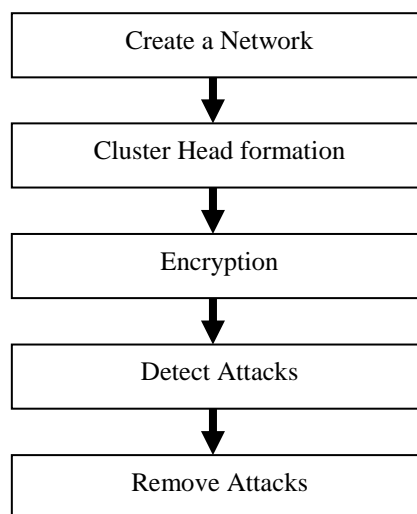


FIG.1: PROPOSED ARCHITECTURE

### V. CONCLUSION

Energy efficient and secure data transmission technique for defense against attacks in wireless sensor network is mainly the purpose of the proposed approach which can improve the lifetime of wireless sensor network using An



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

energy efficient techniques. K-LEACH uses the K-medoids clustering algorithm to obtain highly uniform clustering of nodes and very good choices of cluster heads and it is a very well known fact energy retention of a WSN is highly dependent on the grouping or clustering of transmitting and receiving nodes. This paper is built to evaluate in detecting and preventing compromised nodes to become cluster heads. The system will detect a malicious node and also attack made by that node in the network. Then the system will find the alternate path to send the data packets to the receiver and also provide secure data transfer using encryption technique.

## REFERENCES

1. Itika Gupta, A. K. Daniel, "An Energy Efficient Position Based Clustering Protocol for WSNs using Round Robin Scheduling Technique", 3<sup>rd</sup> International Conference on Advanced Computing and Communication Technologies, 10.1109/ACCT. 2013.
2. M. Aslam, N. Javaid, A. Rahim, U. Nazir, A. Bibi, Z. A. Khan, "Survey of Extended LEACH-Based Clustering Routing Protocols for Wireless Sensor Networks" arXiv:1207.2609 V1. [cs.NI] 11 Jul 2012.
3. Mahmoud M. Salim, Hussein A. Elsayed, Salwa H. El Ramly, "PR -LEACH: Approach for Balancing Energy Dissipation of LEACH Protocol for WSNs" in 31<sup>st</sup> National Radio Science Conference (NRSC2014), April 28-30, 2014.
4. Sheela. D, Srividhya.V. R. , Asma Begam, Anjali and Chidanand G. M. "Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent", International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012) July 15-16, 2012
5. Jaspreet Kaur, Vinod Kumar, "An Effectual Defense Method Against Gray-Hole Attack in Wireless Sensor Networks" International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (3), 2012,
6. Wang Linping, Cai Zhen, "Improved algorithm of PEGASIS protocol introducing double clusterheads in wireless sensor network", vol.10, pp.148-151, IEEE, 2011.
7. Junwhan Kim, "opportunistic real-time routing in multi-hop wireless sensor networks", sac'09 March 812, 2009.
8. D. J. Baker and A. Ephremides, "The Architectural Organization of a Mobile Radio Network via a Distributed Algorithm", IEEE Transactions on Communications, Vol. 29, No. 11, pp. 1694-1701, November 1981
9. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009
10. Noor Zaman, Tung Jang Low, Turki Alghamdi, "Energy Efficient Routing Protocol for WSNs", 3<sup>rd</sup> International Conference on advance in Computing Technologies, ISBN 978 -89968650 - 3-2, February 16- 9, ICACT, 2014
11. Nidhi Chhajed, Mayank Sharma, "Detection and Prevention technique for Black hole Attack in Wireless Sensor Networks: A Review" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 11, November 2014
12. Osama Moh'd Alia, Zyad Shaaban, Ahmad Basheer, Alaa AlAjouri, Ahme Alsswey, "Musician Inspired Clustering Protocol for Efficient Energy in WSNs", Sensor Networks and Cellular Systems (SNCS) Research center, Saudi Arabia, 2014
13. M. S. Fareed, N. Javaid, M. Akbar, S. Rehman, U. Qasim, Z. A. Khan "Optimal Number Of Cluster Head Selection for Efficient Distribution of Sources in WSNs", 7<sup>th</sup> International Conference on Broadband, Wireless Computing, Communication and Application, 2012
14. M. Natranjan, R. Arthi, K. Murugan, "Energy Aware Optimal CH Selection in WSNs", in IEEE 4<sup>th</sup> ICCCNT, Tiruchengode, India, July 4-6, ICCCNT 2013.
15. Snehal P. Dongare, Ram S. Mangrulkar, "Implementing Energy Efficient Technique for Defense against Gray-Hole and Black-Hole Attacks in Wireless Sensor Networks" International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India, 2015
16. Dokurer, Seimih "Simulation of Black hole Attack in wireless ad-hoc Networks" Master's Thesis Atihm University, September 2006.
17. X. H. Wu, S. Wang, "Performance comparison of LEACH and LEACH-C protocols by NS2," Proceedings of 9<sup>th</sup> International Symposium on Distributed Computing and Applications to Business, Engineering and Science. Hong Kong, China, pp. 254-258, 2010
18. Shalli Rani, Jyotish Malhotra, Rajneesh Talwar, "Energy Efficient Protocol for Densely Deployed Homogeneous Network" in International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)-2014.
19. Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2<sup>nd</sup> International Conference on , vol.3, no., pp.V3-672-V3-676, 21-24 May 2010.
20. Payal N. Raj and Prashant B. Swadas, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.
21. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient routing protocols for wireless microsensor networks," in Proc. 33<sup>rd</sup> Hawaii Int. Conf. System Sciences (HICSS), Maui, HI, Jan. 2000.