A SURVEY: Detection and correction of sinkhole attack in wireless sensors networks by leach protocol

Akash Verma[1], Mr. Pranjal Khare[2]

[1]M.Tech Scholar of Computer Science Engineering, BTIRT College Sagar, (M.P.) India
[2]Asst. Prof. of Computer Science Engineering, BTIRT College Sagar, (M.P.) India

---***---

Abstract - *Wireless Sensor Networks (WSNs) are self-configuring, interconnected sensor nodes that communicate and gather data without the use of wires. It is made up of a large number of inexpensive sensors. However, due to the low computing capacity and energy capacities of Wireless Sensor Networks, maintaining protection is extremely difficult. Because of these features, the network is vulnerable to a variety of attacks, including the Sinkhole attack. Sinkhole Attacks are carried out by either hacking a network node or using a fake node. This paper employs a novel technique to protect WSN from Sinkhole Attack. We can also use LEACH protocol to secure a Wireless sensors network from non-sinkhole attacks such as Sybil attack, wormhole attack, and so on by examining the graphical results of LEACH protocol. We will use the LEACH protocol in both sinkhole and non-sinkhole attacks in this article. This will be used to evaluate the efficiency of the LEACH Protocol. The easiest way to evaluate output is to use a graphical representation. The security priorities, risks, attacks, and constraints associated with Wireless Sensors Networks are also discussed in this paper.*

***Key Words*: Sinkhole Attack, Wireless Sensor Network (WSN), low energy adaptive clustering hierarchy (LEACH), Cluster Head (CH).**

1. INTRODUCTION

Wireless Sensor Network (WSN) is a collection of various small sensors. These Sensors garner information about a particular environment. These sensing devices are also known as nodes. Wireless Sensor Network (WSN) is used in various areas such as military activities, to keep the track of their enemy and this information is very helpful for authorities [1]. Sensor nodes are used to detect physical or environmental conditions, such as temperature, sound, pressure, etc. Due to the necessity for low energy consumption and least cost, Wireless Sensor Network is the best solution. Wireless Sensor Network (WSN) is nothing but simply a collection of nodes and it performs certain important functions such as monitoring, sensing, capturing, processing and controlling [2]. Now-a-days Wireless Sensor Network is also used in various fields such as in health care system, precision agriculture, defense system, environmental monitoring etc. The aim of this paper is to study existing solutions used to detect sinkhole attack. The noxious hub attempts to manage the traffic from different hubs towards itself. This not just draws in every one of the hubs close to the sinkhole yet in addition every single hub nearer to the base station. The Sinkhole can then effectively change the information. Remote sensors are inclined to different assaults, for example, Selective Forwarding, Sybil Attack, Sinkhole assault and so on [5]. Wireless Sensor Network has no centralized control but it is a self organized [6]. Sinkhole attack can be commenced from within the network as well as from outside. Firstly, the attackers may utilize a vexed hub to start the interruption and also the trespasser may shape an immediate way to the base station through it enticing different hubs to send their traffic through it. In Sinkhole assault insider attack, an interloper bargains a hub inside the organization and starts an attack. At that point the trade off hub attempt to draw in all the rush hour gridlock from neighbor hubs dependent on the steering metric that utilized in directing convention. At the point when gatecrasher gets achievement in this, it will initiate an attack. Remote sensor network has numerous to one correspondence where every hub send information to base station, makes this WSN inclined to sinkhole attack. [3]. Wireless remote sensor networks are fundamentally utilized in unstable conditions where security is the essential concern and these organizations are helpless against assault. For a huge scope network it is absurd to expect to notice every single hub. At the point when the security is upset this organization quickly reaction back with a message which needs an unexpected consideration [4].

Following are the various security principles of wireless sensor network [4]:

- **Confidentiality**: The data should be kept private and not accessible to unauthorized user.
- **Authentication**: It ensures the identity of the node with which it is communicating.
- **Integrity**: It verifies the correctness of the data.
- **Availability**: The service should be approachable all the time.
- **Non-repudiation**: A node cannot deny sending a message which it has previously sent.
- **Authorization**: It ensures that only verified user can use the resources.

Table I : WIRELESS SENSOR NETWORK ATTACK ON DIFFERENT LAYERS [4].

Layers	Attacks
Transport Layer	Flooding,de-synchronization
Network Layer	Black Hole, Sybil Attack
Data Link Layer	Collision, Exhaustion
Physical Layer	Jamming

2. SINKHOLE ATTACK

Sinkholes attacks operate by making a compromised node appear particularly appealing to nearby nodes in terms of the routing algorithm. An adversary might, for example, spoof or replay an advertisement for a very high-quality route to a Base Station. End-to-end acknowledgements containing reliability or latency information can be used by certain protocols to verify route consistency. In this scenario, a laptop-class adversary with a strong transmitter may provide a high-quality route by transmitting with enough power to reach the Base Station in a single hop or by employing a wormhole attack. It causes the network's output to deteriorate over time. It's a black hole assault with a twist [4]. The many-to-one nature of WSNs is the primary cause of Sinkhole attacks. All of the sensor nodes want to communicate with the base station directly. In the WSN, there is no node synchronization and no global id assignment for sensor nodes. Furthermore, due to memory limitations, node information for the entire network cannot be stored in each node. WSNs are vulnerable to external threats because of these factors. Because of the broadcasting existence of WSNs, sinkhole attacks occur. During connection creation, the sensor nodes send Router request and Route reply messages to each other. When a node wants to send a message to a sink, it sends path discovery request messages to its neighbors. When the neighbor node receives the request from the sender node, it determines which route to the base station is the shortest [14]. The figure 1 depicts a diagrammatic view of a sinkhole that attracts all nearby traffic to the malicious node, with the path through the malicious node being the most effective. As a result of all of the surrounding nodes sending data packets to the malicious nodes, a sinkhole forms in the middle. As seen in the diagram, the malicious node drops traffic from the source node [4].

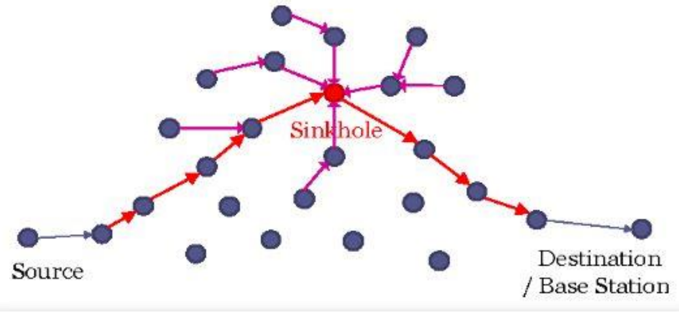

Fig-1: Sinkhole Attack

3. PROBLEM STATEMENT

This paper conducts a systematic review of the security classification literature. In this paper, we'll look at a variety of wireless sensor network problems. Sinkhole attack, Sybil attack, and Wormhole attack are three major problems that we are attempting to solve. We can solve these problems by applying, but the main issue is efficiency, which we must boost in this job. Wireless sensor networks are commonly used networks, but when their output deteriorates, it poses a significant security risk [3].

4. LEACH PROTOCOL

Wireless sensor networks operate in a resource-constrained setting, necessitating mechanisms that use fewer resources. The Low-Energy Adaptive Clustering Hierarchy protocol is a clustering-based protocol with low resource consumption. The protocol's working phase is split into two phases: setup and steady-state. Clusters are created during the set-up process by selecting cluster heads. The cluster head is chosen from among the cluster members with the highest likelihood and energy level. The member nodes send data to their Cluster head in their assigned slot during the steady-state period. The Cluster Head collects data from the member nodes and transmits it to the Base Station (BS). Many routing attacks, such as sinkhole, wormhole, sybil, and selective forwarding, are vulnerable to the LEACH protocol, and there are few solutions to address the protocol's security threats. To protect the clustered network, a lightweight mechanism is needed [7].

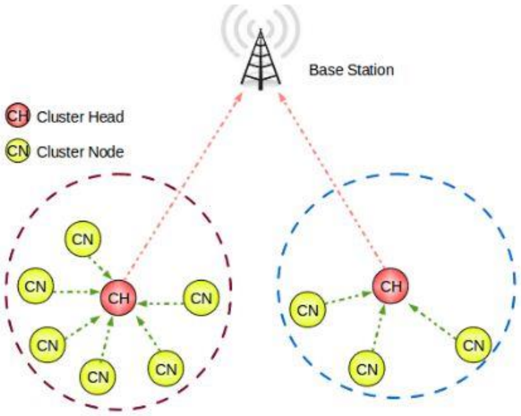

Fig -2: LEACH Protocol

5. RESEARCH METHODOLOGY

The different steps of proposed algorithm are given below:

1. **Network Deployment:-** In this the sensors node can sense the environment and collect information about the vulnerabilities and pass to the base station.

2. **Distribution of key:-** It requires a software for the detection of malicious node which affect the performance of technique for the detection of malicious node.

3. **Detection of malicious node:-** The base station is ready to give its ID however the malignant hub can't give its recognizable proof. The keys which are distributed in a network is a concept of Armstrong number. It is a unique 16 digit number which is generated from color combination. This number is hard to crack and unique identification of each node is concentrated with the key to form final key.

4. **Isolation of malicious node:-** To remove malicious node completely multiple routing path is used at ends. By this we can easily correct malicious node and protect our network.

6. FUTURE WORK

In our future work, we can expect the calculation rose ceaselessly and widely, where there are as yet numerous issues existing. In the mean time, we will improve the re-enactment all the more outwardly. By analyzing the graphical results of LEACH protocol we can also use LEACH protocol to protect a Wireless sensors network from non sinkhole attacks such as Sybil attack, wormhole attack etc.

7. CONCLUSIONS

This paper recommended an examination to distinguish a sinkhole assault in remote sensor organization. Remote sensor networks are the climate where security assumes a significant part in the presentation of the organization. Sinkhole attack decays the organization execution by dropping the bundles and lessens the productivity of filter convention. The proposed SSLEACH calculation is utilized for interruption discovery and adds greater security to the Filter convention to ensure the organization with least energy utilization, calculation and most extreme parcel conveyance proportion than the current S-Drain and MS-Filter plans. The proposed calculation can recognize an assault in an organization if hop count=1 to BS.

REFERENCES

[1]. Hoon Kim, Member, and Sang-wook Han, "An Efficient Sensor Deployment Scheme for Large-Scale Wireless Sensor Networks", In IEEE communications letters, VOL. 19, NO. 1 January 2015 IEEE.

[2]. Ankit Solanki Sarvajanik College of Engineering and Technology, Niteen B. Patel Sarvajanik College of Engineering and Technology, 4th ICCCNT IEEE-2013.

[3]. Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network", In International Conference on Space Science and Communication Melaka, Malaysia e 2013 IEEE

[4]. Manpreet kaur, Amarvir singh, "Detection and Mitigation of Sinkhole Attack in wireless sensor network", In 2016 International Conference on Micro-Electronics and Telecommunication Engineering.

[5]. Fang-Jiao Zhanga,b , Li-Dong Zhaia,* , Jin-Cui Yangb, , Xiang Cuic "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks", In Procedia Computer Science 31 (2014) 711 – 720.

[6]. Asaduzzaman and Hyung Yun Kong, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network", In journal of communications and networks, VOL. 12, No. 4, August 2010.

[7]. S.Ranjeeth Kumar , A.Umamakeswari, "SSLEACH: Specification based Secure LEACH Protocol for Wireless Sensor Networks", In School of Computing, SASTRA University, Thanjavur, India IEEE WiSPNET 2016 conference.

[8]. Changlong Chen, Min Song, and George Hsieh, "Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks", In George Hsieh is with the Department of Computer Science, Norfolk State University, Norfolk, VA 23504, USA 2010 IEEE.

[9]. Liping Teng and Yongping Zhang, "SeRA: A Secure Routing Algorithm against Sinkhole Attacks for Mobile Wireless Sensor Networks", In 2010 Second International Conference on Computer Modeling and Simulation Department of Computer Science and Technology China University of Mining and Technology Xuzhou, China.

[10]. Prakash kala, Arun Prakash Agrawal, Rishi Rajan Sharma, "A novel approach for isolation of sinkhole attack in wireless sensor network", In 10th International Conference on Cloud Computing, Data Science & Engineering 2020 IEEE.

[11]. Nazli Siasi, Adel Aldalbahi, Mohammed A. Jasim, "Reliable Transmission Scheme Against Security Attacks in Wireless Sensor Networks", In Department of Electrical Engineering, University of South Florida, Tampa, FL, USA 2019 IEEE.

[12]. Deepali S. Patil1 Shailaja C. Patil2, "A Novel Algorithm for Detecting Node Clone Attack in Wireless Sensor Networks", In Department of Electronics and Telecommunication Engineering, Rajarshi Shahu College of Engineering, Pune University 2017 IEEE.

[13]. Divya Bharti, Neha Nainta, Prof. Himanshu Monga," Performance Analysis of Wireless Sensor Networks under adverse scenario of attack", 6th International Conference on Signal Processing and Integrated Networks (SPIN)2019 IEEE.

[14]. Arya, Dr. Binu G S, "Cross Layer Approach for Detection and Prevention Of Sinkhole Attack Using A Mobile Agent", 2nd International Conference on Communication and Electronics Systems 2017 IEEE.

[15]. D. Sasirekha, Dr. N. Radha, "Secure And Attack Aware Routing In Mobile Ad Hoc Networks Against Wormhole And Sinkhole Attacks", In 2nd International Conference on Communication and Electronics Systems 2017 IEEE.

[16]. Reenkama Kaur Gill1, Priya Chawla and Monika Sachdeva, "Study of LEACH Routing Protocol for Wireless Sensor Networks" In International Conference on Communication, Computing & Systems (ICCCS–2014).

[17]. Sibo Liu, Liaojun Pang†, Qingqi Pei, Hua Ma, Qingquan Peng, "Distributed Event-triggered Trust Management for Wireless Sensor Networks", In 2009 Fifth International Conference on Information Assurance and Security.

[18]. Walid Elgenaidi, Thomas Newe, Eoin O'Connell, Daniel Toal, Gerard Dooly and Joseph Coleman., "Memory Storage Administration of Security Encryption Keys for Line Topology in Maritime Wireless Sensor Networks", In 2016 Tenth International Conference on Sensing Technology.

[19]. Hailin Feng, Guoying Wang and Guanghui L, "Efficient Secure in-network Data Aggregation in Wireless Sensor networks", In 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing 2010 IEEE.

[20]. Jiann-Liang Chen , Yin-Fu Lai1 , Hsi-Feng Lu, and Quan-Cheng Kuo, "Public-key Based Security Scheme for Wireless Sensor Network", In Department of Computer Science & Information Engineering, National Dong Hwa University 2008 IEEE.