*International Journal of Engineering Science Invention*
*ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726*
*www.ijesi.org Volume 3 Issue 6ǁ June 2014 ǁ PP.12-14*

# Detection Techniques of Sinkhole Attack in WSNs: A Survey

**Rajakumaran L[1] Thamarai Selvi R[2]**
*[1]M.Phil. Scholar [2]Asst. Professor, Department of Computer Applications,*
*Bishop Heber College (Autonomous), Trichirappalli-620 017*
*[1]rajkumaranmca@gmail.com [2]thams_shakthi@yahoo.co.in*

***ABSTRACT:*** *Wireless Sensor Networks (WSNs) are widely used in many areas of non-commercial like military, health care, environmental monitoring, and commercial products like house holding, vehicles etc. WSN are placed in the harsh environment and due to the wireless nature of communication they are vulnerable to various security attacks like Sinkhole attack, Black hole attack, Sybil attack and Wormhole attack, Jamming attack etc,. The sinkhole attack is one of the most destructive routing attacks in WSN. This paper discus about various detection techniques for the sinkhole attacks in WSN.*

***KEYWORDS:*** *wireless sensor network, sinkhole attack, Intrusion detection.*

## I. INTRODUCTION

Wireless sensor network (WSN) is a collection of sensor nodes which are capable of sensing and processing data and send them to a base station as shown in the figure 1. These sensor nodes are small in size. They are deployed in an unattended environment which is not physically protected. They are used for monitoring of that environment and send back the collected data to the Base Station (BS). WSN are light weighted and have limited power sources, limited memory storage, limited computational capability and transmission range. They are vulnerable to various security threats as they use the wireless medium for transmission of the data to the BS. There are several attacks in each layer of the sensor networks. The physical layer attacks are jamming, tampering, Data link layer attacks are Jamming and collision; Network layer attacks are selective forwarding attack, sinkhole attack, Sybil attack, black hole attack, wormhole attack; Transport layer attacks are flooding attack, de-synchronization attack. One of the most dangerous and very difficult to detect the attack is sinkhole attack because using this attack we can perform any type of attack in the WSN.

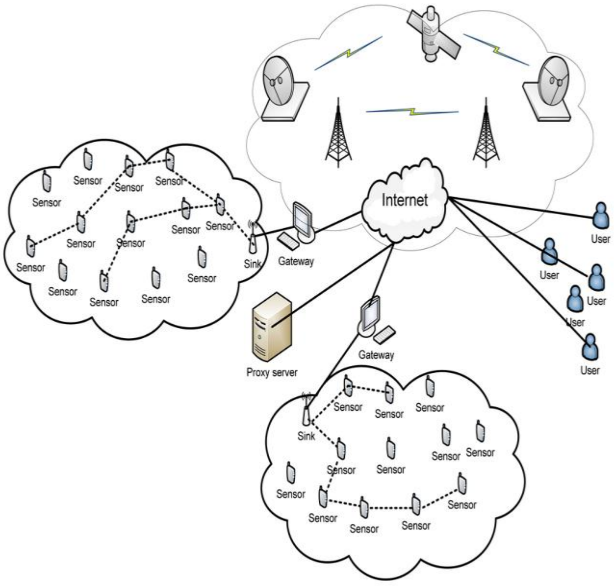

**Figure 1 wireless sensor network**

### Sinkhole attack

The sinkhole attack in WSN is that an intruder uses a compromised node in the sensor network of a particular area and lures some or all the traffic of that particular area and makes a sinkhole. Sinkhole attacks are carried out by making the compromised node look more attractive to all the neighboring nodes which have an effective routing path to the destination with high rate of energy.

For example that node may be any laptop with high energy and high performance power. First it just advertise that it have a high quality single hop connection with the BS to its neighboring nodes. After that all the nodes divert all their traffic to pass through the intruder node to the BS. Thus sinkhole attack is launched. Sinkholes attacks are difficult to be detected because of the routing information provided by each node are difficult to verify. Once the attacker made the sinkhole attack he can perform any type of attack in the WSN as the entire traffic flows through that sinkhole node so he can collect all the data through the node and misuse the collected data. He even drop all the packets or some of the packets also can perform Selective Forwarding attack, Wormhole attack, Flooding attack, Sybil attack, Black hole attack.

## II. RELATED WORK

**Udaya Suriya Rajkumar. D., et al., [1** proposed a LBIDS (Leader Based Intrusion Detection System) solution to detect and defend against the sinkhole attack in WSN. The proposed solution consists of three algorithms a Leader Election Algorithm, Algorithm for Avoid Malicious, CheckIDS Algorithm. In this approach a region wise leader is elected for each group nodes within the network. That leader performs the intrusion detection mechanism by comparing and manipulating the behavior of each node within the cluster and monitors each node behavior for any sinkhole attack to occur. When a compromised node gets detected the leader informs other leader within the WSN, about the sinkhole node so all the leaders in the network stops communication with that particular sinkhole Node. The energy efficiency and intrusion detection rate is high.

**D. Sheela., et al., [2]** proposed routing algorithm based on mobile agents to defend against sinkhole attacks in WSN. Mobile agent is a self controlling software program that visits every node in the network either periodical or on required. By using the collected information the mobile agents make every node alert of the entire network so that a valid node would not listen to the wrong information from malicious or compromised node which leads to sinkhole attack. The important feature of the proposed mechanism is that does not require any encryption or decryption mechanism for detecting the sinkhole attack. Very less energy is enough for this mechanism than the normal routing protocols.

**Maliheh Bahekmat., et al., [3]** discussed about a novel algorithm for detecting sinkhole attacks in WSNs in terms of energy consumption. The proposed algorithm works by comparing the control fields of the received data packets with the original control packet, whenever a node needs to send data to the BS, it first sends a control packet directly to the main BS. Then it begins to send data packets in form of hop by hop routing to the BS. After the data packet arrives at the BS, it compares the control fields of the received data packets with the original control packet. If any manipulations have been detected to these control fields or loss in the data packet, the BS detects that there is a malicious node in that path by using the proposed strategy. Advantage of this method is very less energy consumed for the detection mechanism. This algorithm can also be used for detection of wormhole attacks. The performance of the proposed algorithm is examined in MAT lab stimulation.

**Tejinderdeep Singh and Harpreet Kaur Arora [4]** proposed a solution for Sinkhole attacks detection in WSN using Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol. This system consists of three steps. The sender node first requests the sequence number with the rreq message, if the node replies its sequence number with rrep message. Transmitting node will match sequence number in its routing table. If matches then data will be shared otherwise it will be assign the sequence number to the node. If the node accepts the sequence number then the node will enter in the network otherwise it will be eradicated from the network.

**S.Sharmila and Dr G Umamaheswari [5]** proposed a solution for Detection of sinkhole attack in wireless sensor networks using message digest algorithms. Detecting the exact sink hole by using the one-way hash chains is the main aim of this protocol. In the proposed method destination detects the attack only when the digest obtained from the trustable forward path and the digest obtained through the trustable node to the destination are different. It also ensures the data integrity of the messages transferred using the trustable path. The algorithm is also robust to deal with cooperative malicious nodes that attempt to hide the real intruder. The functionality of the proposed algorithm is tested in MAT lab stimulation.

**Ahmad Salehi S., et al., [6]** proposed a light weight Algorithm to detect the sinkhole attack node in the WSN the algorithm consist of two step process. The first step is to find a list of affected nodes in that area by checking the data consistency and the second step to then effectively identifies the intruder in the list by analyzing the network flow information. The algorithm is also robust to deal with multiple malicious nodes that cooperatively hide the real intruder. The proposed algorithm's performance has been evaluated by using numerical analysis and simulations**.**

**Murad A. Rassam., et al., [7]** proposed fuzzy rules based detection mechanism of sinkhole in Mintroute WSNs. This detection system is first distributed in each and every node to keep monitoring the entire network which assures a high detection possibility; second the deciding of finding the attacker is done by the sink by the cooperation mechanism after receiving id of the suspected sinkhole from each node; which causes cutback of communication with all sensor nodes by broadcasting the suspected nodes ID. In this system the sink is involved in making the decision about the attack based on the alarms received from the nodes. This scheme has the ability of detecting sinkhole attack in small scale WSNs.

## III. SUMMARY

This paper surveyed the various detection and prevention mechanisms of sinkhole attacks in the wireless sensor networks. The detection of sinkhole attacks are very difficult problem. Still there are many other approaches and challenges in detection of sinkhole attack in WSN.

## REFERENCES

[1] Udaya Suriya Rajkumar, D and Rajamani Vayanaperumal, "A Leader Based Monitoring Approach for Sinkhole Attack in Wireless Sensor Network", *Journal of Computer Science 9 (9): 1106-1116, 2013,* pp 1106-1116. ISSN: 1549-3636

[2] D. Sheela, et al, "A non Cryptographic method of Sink hole attack Detection in Wireless Sensor Networks", *IEEE-International Conference on Recent Trends in Information Technology, June 3-5 2011,* pp 527-532,

[3] Maliheh Bahekmat, et al, "A novel algorithm for detecting Sinhole attacks in WSNs", *International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012,* pp 418-421.

[4] Tejinderdeep Singh and Harpreet Kaur Arora, "Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool", *International Journal of Advanced Computer Science and Applications, Vol. 4, No. 2, 2013,* pp 32-35.

[5] S.Sharmila and Dr G Umamaheswari; "Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms" International Conference on Process Automation, Control and Computing (PACC) 2011, pp. 1-6

[6] Ahmad Salehi S., et al., Detection of Sinkhole Attack in Wireless Sensor Networks "*Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace)*", 1-3 July 2013, pp 361-365.

[7] Murad A. Rassam., et al., A Sinkhole Attack Detection Scheme in Mintroute Wireless Sensor Networks "*1st IEEE International Symposium on Telecommunication Technologies" 26-28 Nov 2012,* pp 71-75.