# Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool

Tejinderdeep Singh
M-Tech Scholar, CSE
Sant Baba Bhag singh College of Engineering & Technology
Jalandhar, INDIA

Harpreet Kaur Arora
AP, CSE
Sant Baba Bhag singh College of Engineering & Technology
Jalandhar, INDIA

***Abstract*— Wireless Sensor Networks (WSNs) are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. In this article we discuss security issues in WSNs. In this paper we are discussing a vulnerable sinkhole attack, its implementation and correction.**

***Keywords*— Wireless Sensor Networks (WSN); Intrusion Detection (ID); Base Station (BS); Sinkhole (SH);Ad-hoc on demand Distance Vector (AoDV).***

## I. INTRODUCTION

The pervasive interconnection of wireless sensor devices has given birth to a broad class of exciting new applications in several areas of our lives.

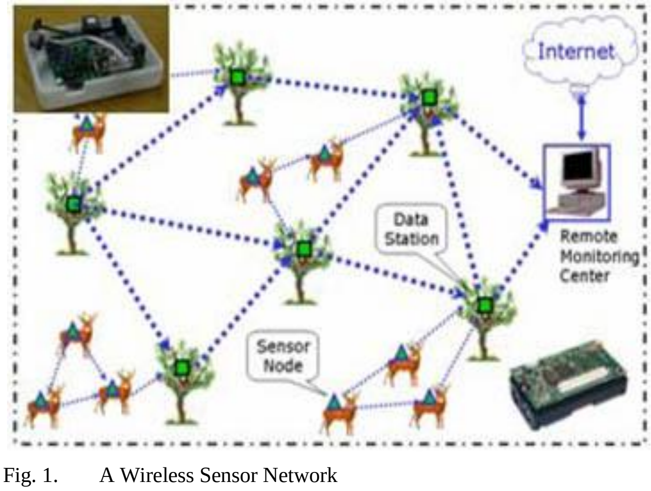

Fig. 1. A Wireless Sensor Network

However, as every network, sensor networks are exposed to security threats which, if not properly addressed, can exclude them from being deployed in the envisaged scenarios. Their wireless and distributed nature and the serious constraints in node battery power prevent previously known security approaches to be deployed and has created a large number of vulnerabilities that attackers can exploit in order to gain access in the network and the information transferred within. Securing sensor networks against these threats is a challenging research area, necessary for commercially attractive deployments. Encryption and authentication mechanisms provide reasonable defence for mote-class outsider attacks. However, cryptography is inefficient in protecting against laptop class and insider attacks. It remains an open problem for additional research and development since the presence of insiders significantly lessens the effectiveness of link layer security mechanisms. This is because an insider is allowed to participate in the network and have complete access to any messages routed through the network and is free to modify, suppress, or eavesdrop on the contents. What makes it even easier for attackers is the fact that most protocols for sensor networks are not designed having security threats in mind. As a consequence, deployments of sensor networks rarely include security protection and little or no effort is usually required from the side of the attacker to perform the attack. So, it is very important to study realistic attacker models and evaluate the practicality and efficiency of certain attacks.[1][2]

This paper investigates one of the most severe routing attacks in sensor networks, namely the sinkhole attack, from the attacker’s point of view. Our goal is to describe the most effective ways to launch this attack and demonstrate them in practice. We reveal the weaknesses of the routing protocol that is used by the research community, hoping that this will lead to a better awareness of the threats and the study of more efficient security protocol. Then we propose some countermeasures against these threats in the direction of intrusion detection. Some first intrusion detection systems have started to appear for sensor networks, but rarely do they include specific detection rules. Rules against specific attacks, like the one we present here, if properly generalized could lead to better and more realistic IDS design. [5]

## II. ROUTING PROTOCOL

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Thanks to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path.

Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination, sent using UDP/IP protocols. Header information of these control messages are explained in. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination.

## III. PROBLEM FORMULATION

A sinkhole attack prevents the base station from obtaining complete and correct sensing data, and thus forms a serious threat to higher-layer applications. It is particularly severe for wireless sensor networks given the vulnerability of wireless links, and that the sensors are often deployed in open areas and of weak computation and battery power. Although some secure or geographic based routing protocols resist to the sinkhole attacks in certain level, many current routing protocols in sensor networks are susceptible to the sinkhole attack.

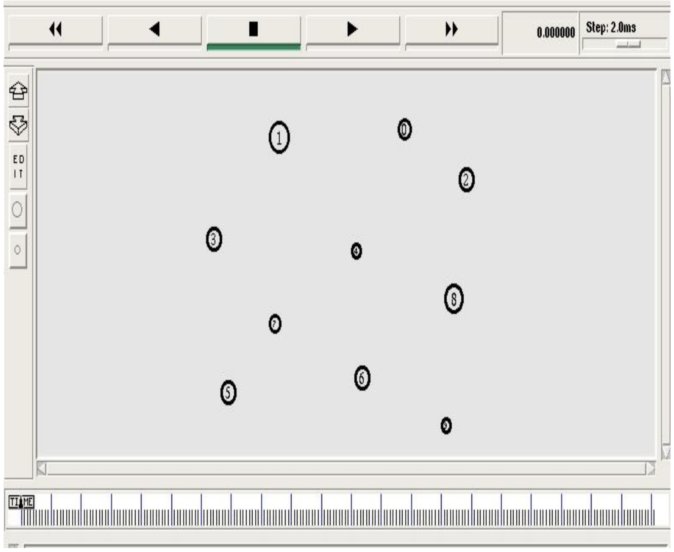

Fig. 2. A WSN Comprised Of Various Nodes

We consider a sensor network that consists of a base station (BS) and a collection of geographically distributed sensor nodes, each denoted by a unique identifier *IDv*. The sensor nodes continuously collect and send the sensed application data to the base station by forwarding packets hop-by-hop.

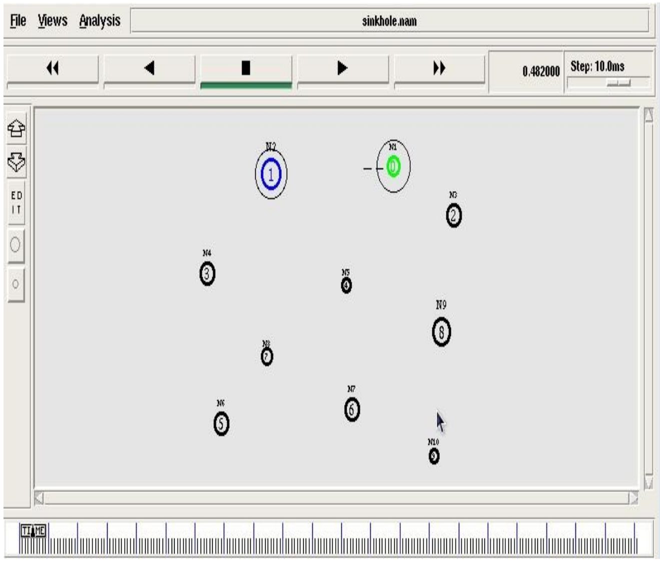

Fig. 3. Data sharing in WSN

As mentioned earlier, this commonly used many-to-one communication pattern is vulnerable to sinkhole attacks. In a sinkhole attack, an intruder usually attracts network traffic by advertising itself as having the shortest path to the base station. For example, an intruder using a wireless-enabled laptop will have much higher computation and communication power than a normal sensor node, and it could have a high-quality single-hop link to the base station (BS). It can then advertise imitated routing messages about the high quality route, thus spoofing the surrounding nodes to create a sinkhole (SH).

A sinkhole can also be performed using a wormhole, which creates a metaphorical sinkhole with the intruder being at the center. An example, where an intruder creates a sinkhole by tunneling messages received in one part of the network and replays them in a different part using a wormhole. We assume the sensor nodes are either *good* or *malicious*. The center of a sinkhole attack is a malicious node compromised by the intruder. Note that, even if there is only one compromised node providing a high quality route to the base station, it can affect many surrounding sensors. Furthermore, this intruder may also cooperate with some other malicious nodes in the network to interfere detection algorithms. In an extreme case, all the malicious nodes are colluding with the intruder. They may collaboratively cheat the base station by claiming a good node as the intruder (the victim, SH'), and thus hide the real one. In our work we implemented sinkhole attack in AODV routing protocol, that works on hop by hop method, means the request goes hop by hop till we reach the destination. The figures 2,3,4,5 shows nodes in wireless sensor networks comprised in which if some node want to send data to other, it will be destined by hop by hop method.

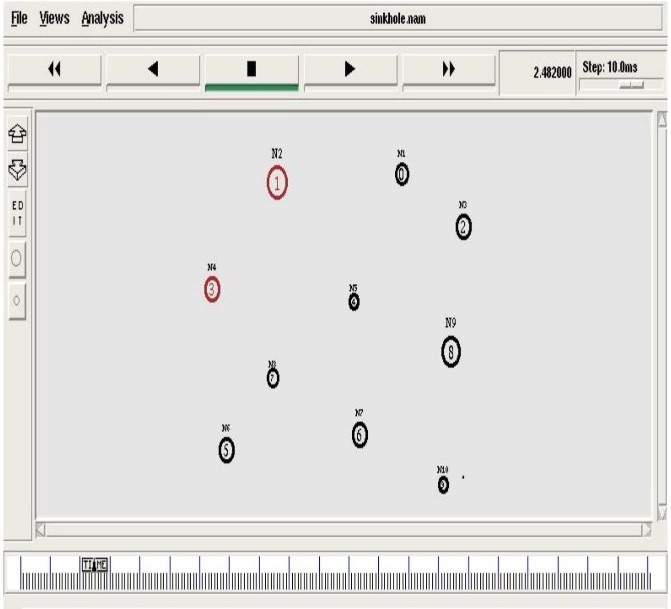

Fig. 4. A Sinkhole attack in WSN

## IV. PROBLEM SOLUTION

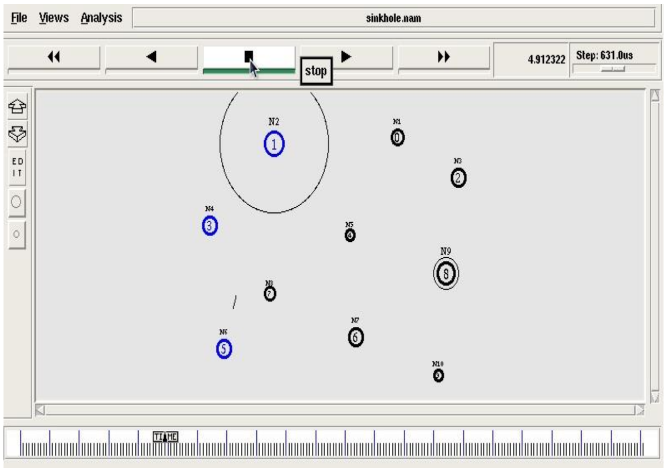

Fig. 5. Correction of Sinkhole attack

The solution proposed for SINKHOLE attacks in WSN is done in three steps. Wireless Sensor Network is an open network as it has wireless nature. The security feature becomes less when we are working in a Wireless Sensor Networks. To avoid this problem, 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. The focus of our work is to effectively identify the real intruder in the sinkhole attack in presence of colliding nodes. We assume that the base station is physically protected or has tamper-robust hardware.

Hence, it acts as a central trusted authority in our algorithm design. The base station also has a rough understanding on the location of nodes, which could be available after the node deployment stage or can be obtained by various localization mechanisms.

## V. RESULTS AND DISCUSSION

All we discussed above is Implementation of Sinkhole attack and its prevention. Now, our network is protected from sinkhole attacks. The discussion is about what happens to our network performance. As we seen in the figures, we have chosen two parameters for discussion about what happens to the network. In the first figure, the first parameter chosen is about the packet which tells how many packets lost and received during sinkhole attack and packets lost and received after correction of sinkhole attack.

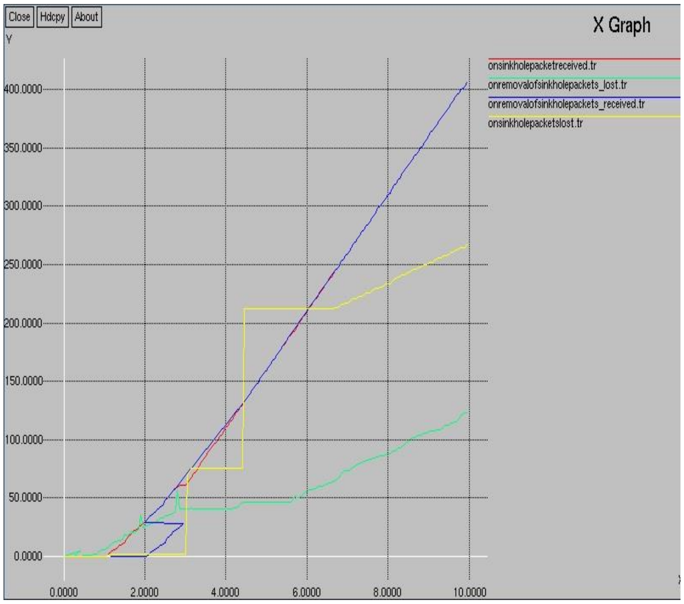

Fig. 6. Results of packet loss and packet received during and after sinkhole attack.

Here we have arranged different color combinations for various parameters. During sinkhole attack, packet lost represented by yellow line and packet received by red line whereas after the correction of sinkhole attack, packet lost are very less and denoted by green line and packets received by Blue line which are much more than the latter.

Next parameter chosen is the Latency which tells how much time a packet needs to travel from source to destination. During Sinkhole attack, main aim of the network is to reduce the network performance by delaying the routing packets. Figure shows the results of routing time or the Latency during Sinkhole attack and after correction of Sinkhole attack.

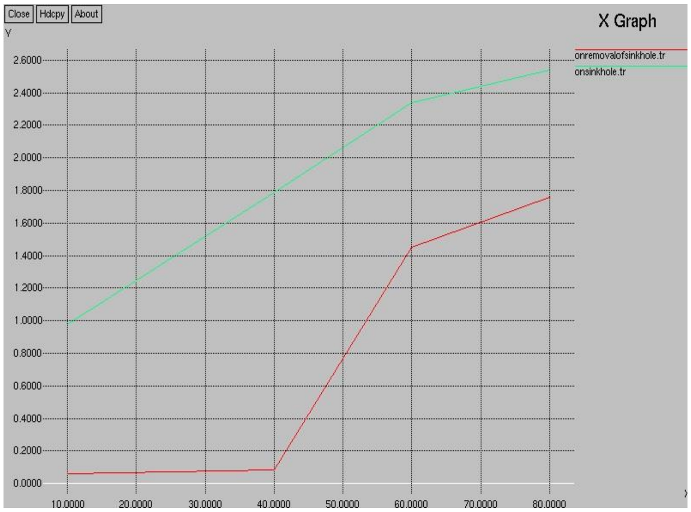

Fig. 7. Comparison of routing time while and after sinkhole attack.

Discussion ends by saying that performance of the network will be affected if there is any Sinkhole attack in the network.

## VI. Future Work

Wireless sensor network is very vast topic for new research. It discovers various steps during data sharing. As we decided Sinkhole attack for research work, several other attacks will be chosen for future work. And if someone want to choose this selected topic, then the performance of the network will be measured by choosing different parameters like routing overhead, delay, or the same attack will be implemented by choosing other protocol.

## REFRENCES

[1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:Attacks and countermeasures," *AdHoc Networks Journal*, vol. 1, no. 2–3,pp. 293–315, September 2003.

[2] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in *Proceedings of IEEE Consumer Communications and Networking Conference (CCNC '06)*, Las Vegas, USA, January 2006, pp. 640–644.

[3] G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, "Deploying a wireless sensor network on an active volcano," *IEEE Internet Computing*, vol. 10, no. 2, pp. 18–25, 2006.

[4] T. Schmid, H. Dubois-Ferri`ere, and M. Vetterli, "SensorScope: Experiences with a Wireless Building Monitoring Sensor Network," in *Proceeding of the Workshop on Real-World Wireless Sensor Networks (REALWSN '05)*, Stockholm, Sweden, June 2005.

[5] S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, "Wireless sensor networks for structural health monitoring," in *SenSys '06: Proceedings of the 4th international conference on Embedded networked sensor systems*, 2006, pp. 427–428.

[6] G. Werner-Allen, K. Lorincz, J. Johnson, J. Lees, and M. Welsh, "Fidelity and yield in a volcano monitoring sensor network," in *OSDI '06: Proceedings of the 7th symposium on Operating systems design and implementation*. Berkeley, CA, USA: USENIX Association, 2006.

[7] Hiren Kumar Dev Sharma, Ajit Kumar, Sikkim Manipal Institute of Technology 'security threats in wireless sensor networks' IEEE 2006.

[8] Piyush K. Shukla, S. Silakari. Sarita S. Bhadoria, RGVP Bhopal India 'Network security scheme for wireless sensor network using efficient CSMA MAC layer protocol', sixth international conference on Information Technology, 2009.

[9] Xiuli Ren, Norman University, Siping, China, 'Security methods for Wireless Sensor networks', International Conference on Mechatronics and Automation, June 25-28, 2006.

[10] Xiao Jiango Du, North Dakota State University 'Security in Wireless Sensor Network', IEEE August,2008 .

[11] Approaches to Wireless Sensor Network: Security Protocols, *World of Computer Science and Information Technology Journal (WCSIT)* ISSN: 2221-0741 Vol. 1, No. 7,302-306, 2011