Abstract— Today’s wireless sensor network (WSN) is not safe to route the information without knowing the information about the attacks occurred on data while routing in a network. There are various protocols which are used to route the data in WSN, like proactive and reactive protocols, but hybrid protocols combines the characteristics of both protocols. Sinkhole attacker attracts the data towards itself whenever data traveled through attacker node, the effects comes at data which is compromised because of such type of attack. The hypothesis used by sinkhole attack is that broadcast the false information about routes to its nearby neighbors i.e. shortest path, but in reality it is not existing. It degrades the performance of a network so that its objective is to takes place very easily. To detect sinkhole attacks on Zone Routing Protocol (ZRP), sinkhole indicator methodology is used. In this paper, Network Simulator -2 is used to simulate the result for sinkhole attack on ZRP network.

Keywords— ZRP, WSN, sequence number duplication, sinkhole attack, throughput, packet delivery ratio.

I. INTRODUCTION

Wireless Sensor network (WSN) has received lots of attentions of researchers, because of it is contributed by s latest technologies. Now a day, the usage of sensor network increases like for a Military application, Agriculture usage, rescue application, weather application, etc. Sensor Network have sensor node, with the help of such node communication is takes place. A key advantage of WSNs is their ease of deployment, in part due to their use of routing protocols that self-configure the network [1]. It enhances the communication strategies with the help of situational awareness, so that it can monitor and analyze the large scale data. Wireless Sensor network is composed of large set of homogeneous node with limited resource. The sensor nodes communicate using RF, so broadcast is the fundamental communication primitive [2].

A wireless sensor node is generally known as mote. Motes are programmed with the suitable operating parameters and security certificate before deployed. In order to obtain detailed and integrated data, a large number of sensor nodes are generally circulated over the large area and form a wireless sensor network. A sensor network has small coverage area, small battery power, small processing unit like RAM is of 4 KB and a short transmission distance of less than 100 feet. To travel the data in a network, network has to choose appropriate protocols i.e. proactive routing protocols or reactive protocols or hybrid routing protocols. The aim of Routing is to selecting best paths in a network. In the past, the term routing was also used to mean forwarding network traffic among networks. As the time gone, the definition of routing also gets changed it took place as a forwarding [3]. The categorization of routing protocols is done on the basis of their behaviour. In proactive routing, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain the up-to-date routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. In reactive routing, unlike proactive routing protocols, reactive routing protocols do not build the nodes begin a route discovery process until a route to a target is required. In reactive protocols, because route information may not be available at the time a datagram is received, the delay to determine a route can be quite significant. Furthermore, the global flood-search procedure of the reactive protocols requires significant control traffic. Hybrid protocols contain characteristics of both reactive and proactive routing protocols [4]. In this paper we have used ZRP as a routing protocol because of it aims to address the problems by combing the best properties of both approaches [6, 7]. Problem regarding proactive, it routing requires extra bandwidth to maintain acquisition information, and problem regarding reactive routing, it floods the entire network for route determination [4]. The performance of any routing protocol can be realized quantitatively by means of various performance metrics such as PDR packet delivery ratio, normalized routing load, and throughput [5].

II. OVERVIEW OF ZRP

ZRP is hybrid routing protocol, which incorporates the benefits of both pro-active and reactive protocol. To construct a routing zone, the node has to identify all its neighbours first which are one hop away and can be reached directly [8]. To do so, ZRP have a provision i.e. Neighbour Discovery Protocol (NDR). ZRP is a combination of inter-zone routing protocol (IERP) and Intra-A-zone Routing Protocol (IARP) with the help of these protocols the characteristics of reactive and proactive protocols is incorporated.

1) IntrA-zone Routing Protocol (IARP)
The route maintained from source to destination proactively within a local neighbourhood, which we refer to as a routing zone. IARP is used inside routing zones.

2) Inter-zone Routing Protocol (IERP):

If the IARP is unable to discover the destination, i.e., the destination node is out of node’s zone, at that time, IERP is called. It is a reactive protocol that enables the discovery of the destination [9].

![Image](image1.png)

Fig-1: IARP sends packet

To send a packet from source to destination in ZRP, First of all ZRP recognizes that zone, i.e. either the zone of source and destination is same or zone of source and destination is different. If source and destination nodes are both in the same zone at that time IARP is used if not in the same zone then packet is broadcasted.

![Image](image2.png)

Fig-2: ZRP Network with 25 nodes

III. SINKHOLE ATTACK

Wireless Sensor Network is affected by lots of attacks but the sinkhole attack is one of the serious attack takes place in a network to gain the information or make vulnerable network, so that the outcome of the network or the performance of the network gets decreases. Sinkhole attack is attack which attracts the neighbouring nodes toward sinkhole node or itself. By doing this type of work, the efficiency of a network throughput of a network and packet delivery ratio such parameters are gets decreases. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify[13]. In Sinkhole attack, the attacker node made a broadcast of false information so that the results are the attacker node becomes a sender and receiver, both roles are played by attacker node. By doing this, it gets traffic of the network so that it can manipulate the data flowing in the network [9].

![Image](image3.png)

Fig-3: Example of Sinkhole attack

By receiving the other’s data, the attacker node can make modification in the data or it can drop the data so that the complexity of the network get increases. In ZRP, the sinkhole attack is done by changing the sequence number in RREQ. Both IARP and IERP packet contains the sequence number, so that the changes can be taken in ZRP. Behaviour regarding node of a sinkhole node is it selects the pair of source and destination and examine that pair very carefully. The
completion of the examination process, it sends the RREQ with higher sequence number than the source node. When this bogus RREQ is reach to the destination node, the pair use the path which is developed by sinkhole node or attacker node, and the data flows from this path is under the surveillance of sinkhole node.

In this paper we have a sinkhole node named as ‘24’ which have all the characteristics of the sinkhole node and rest of the nodes numbered from ‘0’ to ‘23’ are senders and receivers in ZRP network. The scenario is shown in fig -4. There are multiple sender and receiver in this network. Suppose packet is send by any arbitrary node through this network then that packet is attracted by the sinkhole node. The normal behaviour of the node is to attract towards shortest path and higher sequence number.

IV. METHOD USED FOR DETECTION OF SINKHOLE ATTACK IN ZRP

To detect sinkhole attack in ZRP, in this paper Sinkhole Intrusion Indicator is used to detect a sinkhole attack in ZRP network. It is developed for DSR in MANET. For this paper, Sequence_Number_Discontinuity methodology is used, so that the duplication of the sequence number can be minimized and hence the performance of the network also increases. In a ZRP, the packet format of RREQ is <sender, receiver, sequence number> used. When the transmission of number of packets increases at the same time the sequence number is also increases, but affected network is not follow such behaviour and at the same time the attacker node emits higher sequence numbered packet so that packet is not thrown outside the network, it is consider as a authenticated packet. The difference in a sequence number of packet is measured on that basis the malicious node is detected. If any node having sequence number “111” is received at receiver end and the next node must have sequence number “112”, because of sinkhole node the next node is “113”, and here comes the discontinuity in sequence number.

V. PERFORMANCE EVALUATION

For simulation the simulation purpose, NS-2.34 is used to develop a simulation of a network in this paper. It provides a set of interfaces for configuring a simulation and for choosing the type of event scheduler used to drive the simulation [9]. There are number of simulation parameter which is used to determine the various aspects of the network and its characteristics.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Simulator</td>
<td>NS-2.34</td>
</tr>
<tr>
<td>2</td>
<td>Channel Type</td>
<td>Channel/WirelessChannel</td>
</tr>
<tr>
<td>3</td>
<td>Radio-propagation model</td>
<td>Propagation/TwoRayGround</td>
</tr>
<tr>
<td>4</td>
<td>Network interface type</td>
<td>Phy/WirelessPhy</td>
</tr>
<tr>
<td>5</td>
<td>MAC type</td>
<td>Mac/802.11</td>
</tr>
<tr>
<td>6</td>
<td>Interface queue type</td>
<td>Queue/DropTail</td>
</tr>
<tr>
<td>7</td>
<td>Antenna model</td>
<td>Antenna/Omni Antenna</td>
</tr>
<tr>
<td>8</td>
<td>Max packet in interface queue type</td>
<td>50</td>
</tr>
<tr>
<td>9</td>
<td>Routing protocol</td>
<td>ZRP</td>
</tr>
<tr>
<td>10</td>
<td>Dimension of the topography</td>
<td>600*600</td>
</tr>
<tr>
<td>11</td>
<td>Simulation time</td>
<td>30.0 sec</td>
</tr>
<tr>
<td>12</td>
<td>ZRP radius</td>
<td>2</td>
</tr>
</tbody>
</table>

A. Performance Metrics:
1) **Packet Delivery Ratio:**
It's a ratio of the number of packets received by the destination to the number of packets sent by the source. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means better performance of the protocol [14].

\[
PDR = \frac{\sum \text{No of packet receive}}{\sum \text{No of packet send}}
\]

Fig-5: Packet Delivery Ratio of ZRP network Vs Sinkhole attack ZRP network

2) **Network Throughput:**
Throughput is the number of data packets delivered from source to destination per unit of time. Throughput is calculated as received throughput in bit per second at the traffic destination.

Fig-6: Throughput of ZRP network vs sinkhole attack ZRP network

3) **Network Routing Overhead:** This is a ratio of number of routing protocol control packets transmitted to the number of data packets.
VI. CONCLUSION AND FUTURE WORK

In this work, we have analyzed sinkhole problem and its affect on ZRP protocol in the form of result. An acknowledged sinkhole advance can advance to abounding added kinds of attacks which can accompany down the accomplished network. We have evaluated ZRP’s performance comparatively & prove that performance of ZRP is improved after applying our mechanism which is deteriorated due to attack. We also observe variation in the values of various performance metrics such as PDR, throughput & packet loss, when we have vary number of nodes from 25 to 125 & found that the performance of ZRP is degraded heavily specially for 100 & 125 nodes under attack. Thus we say that ZRP’s performance deteriorates for higher number of nodes under attack. To improve the performance of the ZRP network the prevention mechanism has to be develop.

REFERENCES


