ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Sinkhole Attack Detection and Prevention in WSN & Improving the Performance of AODV Protocol

Neelam Janak kumar Patel, Dr. Khushboo Tripathi

[1]Ph.D. Research Scholar, Dept. of CSE, ASET, Amity University Haryana, India

[2]Assistant Professor, Dept. of CSE, ASET, Amity University Haryana, India

ABSTRACT: Wireless sensor networks are useful and important in information and communication technology in recent years, and they contain deploying a large number of small nodes. The nodes then sense environmental changes and report them to other nodes over a flexible network planning. Sensor nodes are in coordinate for deployment in hostile environments or over large geographical areas. Energetic nature of this network makes routing protocols to play a conspicuous role in setting up efficient route among pair of nodes. There are proactive, reactive & hybrid types of routing protocols have been proposed, among which one of the well-known is AODV algorithm due to its high performance gain. Supportive nature of nodes discover to various kinds of passive and active attacks. Sinkhole is one of the most destructive kinds of attack which tries to attract most of network traffic towards it & degrade the performance of network. This paper mainly focuses on sinkhole problem, its consequences & present mechanism for detection & prevention of it on the context of AODV protocol. It also shows performance of AODV with no sinkhole attack, under attack & after applying our mechanism in the form of simulation result obtained for certain variation of nodes in network, by considering performance metrics as throughput, packet delivery ratio (PDR) and Packet loss. Simulation is carried out using widely used simulator NS2.34.

KEYWORDS: AODV; WSNS; Sinkhole; Throughput; Packet loss; PDR.

I. INTRODUCTION

A wireless sensor network (WSN) is comprised of a large number of sensors that collaboratively monitor various environments. The sensors all together provide global views of the environments that offer more information than those local views provided by independently operating sensors. There are numerous potential applications of WSNs in various areas such as residence, industry, military and many others. For instance, people can use WSNs to build intelligent house, to gather machine information for real-time control in factories, and to track enemy movements in battle fields [1].

WSNs have some special characteristics that distinguish them from other networks such as the Internet. The characteristics, listed as follows, demand careful considerations for protocol and algorithm designs that can lead to the use of WSNs in the real world:

- Sensors have limited resources, such as energy, memory and computation capacity. Light-weight protocols and algorithms are preferred to achieve longer sensor life.
- Sensors have limited reliability, partially because of the resource constraints.
- WSNs usually have dynamic topologies. A side from sensors' leaving the network for reliability issues, new sensors may be added or activated and join the WSNs.
- WSNs can well have a large number of sensors.
- WSNs are usually centralized in terms of data processing and sometimes control as well. Data flow from sensors towards a few aggregation points which further forward the data to base stations of a fewer number. Base stations could also broadcast query/control information to sensors [4].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Among the designs of WSNs, security is one of the most important aspects that deserve great attention, considering the tremendous application opportunities. In most of the routing protocols for WSNS, in order to communicate outside their broadcast range nodes takes cooperation to forward packets to each other which depictions them to a wide range of security attacks, which can be categorized into two types as passive & active attack, such as flooding, wormhole, black hole planning miserable, location disclosure under which performance of AODV is already evaluated. But a sinkhole is one of undecorated representative attack in WSNS under which AODV needs to be evaluated, where malicious node tries to draw all network traffic towards it by propagation fake routing information & modify or drops packets sent for forwarding which leads to performance degradation of network. The enactment of any routing protocol can be realized quantitatively by means of various performance metrics such as packet delivery ratio (PDR), end to end delay, and throughput & packet loss.

The rest of the paper is organized as follows: Section 2 presents Literature survey. Section 3 presents Overview of AODV protocol describing its working, while section 4 describe sinkhole problem in detail. Section 5 Explain the proposed algorithm. Section 6 presents implementation of detection & prevention mechanism & Results section 7 concludes this paper & finally presents our future work.

II. LITERATURE SURVEY

In [1] authors provided a survey on various countermeasures for sinkhole attack in mobile ad hoc network and different-different techniques for sinkhole attack. Also discuss sinkhole attack causes problem in on-going communication between different nodes and also effect of routing protocol. AODV protocol to solve the duplicate sequence number problem is a challenging research area. In [2] authors focus on exploring and analysing the existing solutions which used to detect and identify sinkhole attack in wireless sensor network. The analysis is based on advantages and limitation of the proposed solutions. In [3] authors proposed a combined CAM-PVM (compare and match-position verification method) with MAP (message authentication and passing) for detecting, eliminating, and eventually preventing the entry of Sybil nodes in the network. They propose a scheme of assuring security for wireless sensor network, to deal with attacks of these kinds in unicasting and multicasting. In [4] a mechanism is proposed against sinkhole attacks which detect malicious nodes using hop counting. The main advantage of the proposed technique is that, a node can detects malicious nodes only collaborating with the neighbour nodes without requiring any negotiation with the base station. Simulation result shows that, the proposed technique successfully detects the sinkhole nodes for large sensor field. In [5] authors mainly focuses on sinkhole problem, its consequences & presents mechanism for detection & prevention of it on the context of AODV protocol. It also shows performance of AODV with no sinkhole attack, under attack & after applying our mechanism in the form of simulation result obtained for certain variation of nodes in network, by considering performance metrics as throughput, PDR, End to end delay & Packet loss. Simulation is carried out using widely used simulator NS2. In [6] a light weight detection scheme is proposed for detecting the sinkhole attack in wireless sensor network. The new message digests algorithm with high complexity and less collision resistant is proposed in order to identify the sinkhole attacks. The scheme detects the sinkhole, when the digest transmitted in the trustable route and new route are different. The functionality of the detection scheme is tested and the performance is analysed in terms of detection accuracy. Thus the digest method of detection meets the security goals such as data integrity, data authenticity, data availability, confidentiality and time synchronization. In [7] the main contribution is to propose a new Sinkhole detection algorithm based the multi-path selection. The simulation also proves the feasibility of the approach. In [8] authors concentrated on the sinkhole attack against Mint Route and Multihop LQI protocol in Tiny OS. Various detection schemes are also discussed which can correctly locate sinkhole in the network. In [10] a proportional study has been given about the sinkhole attach and wormhole attack. Existence of the wormhole nodes in the network is one of the major security difficulties occurred so far. The work is concerned with the comparison of sinkhole attack and wormhole attack with the techniques and modes of wormhole attacks.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

III. OVERVIEW OF AODV

AODV routing protocol is developed as an improvement to the Destination-Sequenced Distance-Vector (DSDV) routing algorithm [5]. The aim of AODV is to reduce the number of broadcast messages sent throughout the network by discovering routes on-demand instead of keeping complete up-to-date route information. A source node seeking to send a data packet to a destination node checks its route table to see if it has a valid route to the destination node. If a route exists, it simply forwards the packets to the next hop along the way to the destination. On the other hand, if there is no route in the table, the source node begins a *route discovery* process. It broadcasts a *route request* (RREQ) packet to its immediate neighbors, and those nodes broadcast further to their neighbors until the request reaches either an intermediate node with a route to the destination or the destination node itself. This route request packet contains the IP address of the source node, current sequence number, the IP address of the destination node, and the sequence number known last.

Sinkhole Attack in AODV

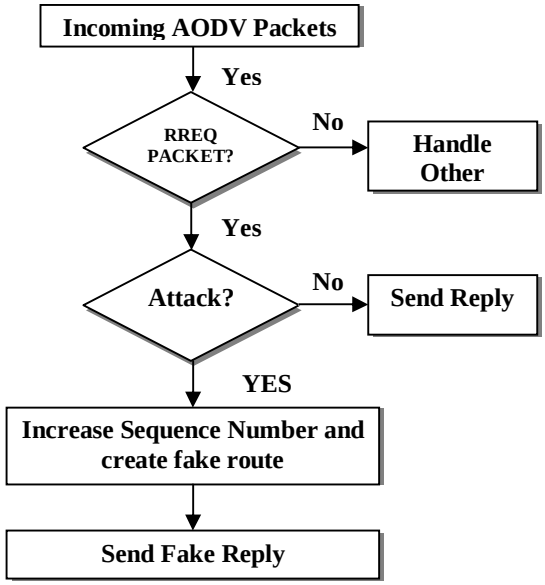

Figure 1: Framework for Sinkhole Attack

Every time a node generates route request packet (RREQ packet), it increase its sequence number by one and the sequence no. is included in the route request packet. A sequence number is used to avoid multiple transmissions of the same RREQ. Higher the sequence number indicates fresh message.

The malicious node overhears the communication channel as a part and observes the sequence number of all nodes. An attacker modifies the sequence no and source route in route request packet to launch the sinkhole attack. By modifying the sequence no, an attacker node generates bogus route request packet. An attacker node carefully observe the sequence no of the target node and send the bogus route request packet whose source node is the target node with a higher sequence no. than the sequence no of the target node.

Any node receiving this fake route request, see the higher sequence number and believe that it is the recent fresh route request. The node updates its cache, delete route from the target node and store the new fake route in the cache and will ignore all route request packets from the target node because the sequence number is less than the previous route request message. All the traffics are diverted to the sinkhole node.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

IV. ANALYSIS OF SINKHOLE PROBLEM

In a sinkhole attack, the adversary's aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As an example, a laptop-class adversary has a strong power radio transmitter that allows it to provide a high-quality route by transmitting with enough power to reach a wide area of the network.

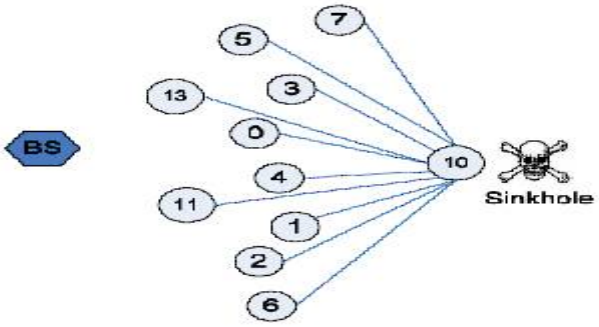

Figure 2: Demonstration of a sinkhole attack

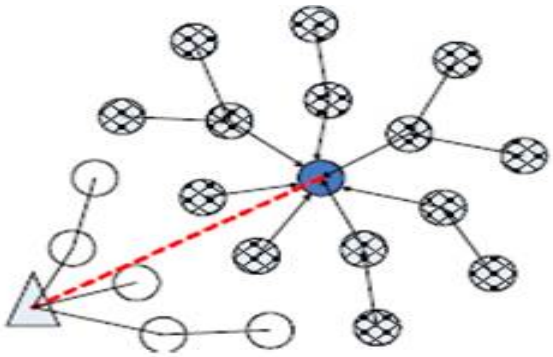

Figure 3: Sinkhole using an artificial high quality route

This type of attack occurs at network layer, in which an adversary attempts to attract all the network traffic from a particular area and preventing the base station from receiving the data from other nodes [6]. Moreover, by including false routing information into compromised node an attacker launch other attacks such as Sybil attack [7]. Subsequently the compromised sensor node rejects to forward messages and drops them. The WSN network supports multiple communication patterns, where numbers of nodes send data at a time to one base station, this type of situation is favorable for sinkhole attacks [8]. Furthermore, sinkhole attack does not attack on all sensor nodes; it only attacks on that node which is near with base station. The Figure 4 shows the WSN network before or after sinkhole attacks, where node 3 can communicate with base station through node 2 and considered as a shortest route in network. On the other hand, in Figure 4 shows the sinkhole attack, where node 1 compromised and broadcast false information. The false

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

information is about wrong shortest route to base station and other sensor nodes. In addition, the sensor node 3 is communicating by node 1 and leads to false route propagation.

As shown in figure 3, a compromised node attracts all the traffic from its neighbors by telling its neighbor that it has shortest route to reach to the base station. This route is artificial high quality route.

V. PROPOSED ALGORITHM

OUR PROPOSED ALGORITHM CONSISTS OF TWO STEPS:

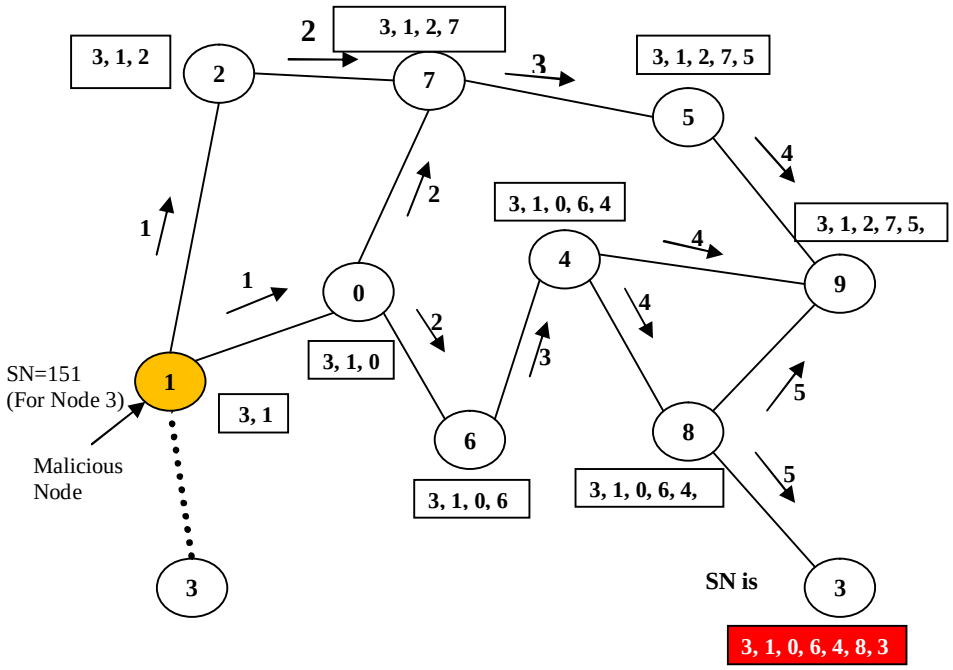

FIGURE 4: PROPAGATION OF A RREQ (ROUTE REQUEST MESSAGE)

(1) IDENTIFY THE SINKHOLE CANDIDATE NODES.

If a node receives route request packet whose source id is equal to the id of the receiving node, it checks the sequence number. If the sequence number of the route request packet is greater than the current sequence number of the node, then the node identifies that this route request packet is from the malicious node and it indicates the presence of the sinkhole. It is sure that the malicious node is on the route request path and all the nodes in the route path are sinkhole candidates.

Show in Fig.4 when node 3 receives the RREQ, it finds its own source id and checks the sequence number. Node 3 has actual sequence no. 20, while it finds the sequence no. 151 in the received RREQ. It indicates that malicious node is on the route request path and all the nodes {1, 0, 6, 4, 8} are sinkhole candidates.

(2) DETECTING THE SINKHOLE NODE.

The node (whose source id is equal to the id of the receiving node) broadcast the packet to the network. This packet contain fake route, sequence number of the fake route request packet and current sequence number of itself. Any node receives this packet first modify the stored sequence number. Both the routes are compared to find the common part between them. The node who has the shortest common path can broadcast its sinkhole detection packet.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Show in Fig. 4. Node 3 broadcast the packet to the network. This packet contains fake route <3, 1, 0, 6, 4, 8, 3>, sequence no. of fake route (151), and current sequence no. of itself (20). Every node on the path compares both the routes and finds the common path. Node 2 has shortest common path <3, 1>. So node 2 identify that node 1 is a malicious node and broadcast the message to all the nodes in the network.

VI. IMPLEMENTATION & RESULTS

For simulation we have used NS-2.34. The simulation parameters are as follow:

Sr.No.	Parameter	Value
1	Simulator	NS2.34
2	Routing Protocol	AODV
3	No. of Nodes	10-50
4	Area	700 *700
5	Simulation Time	500s

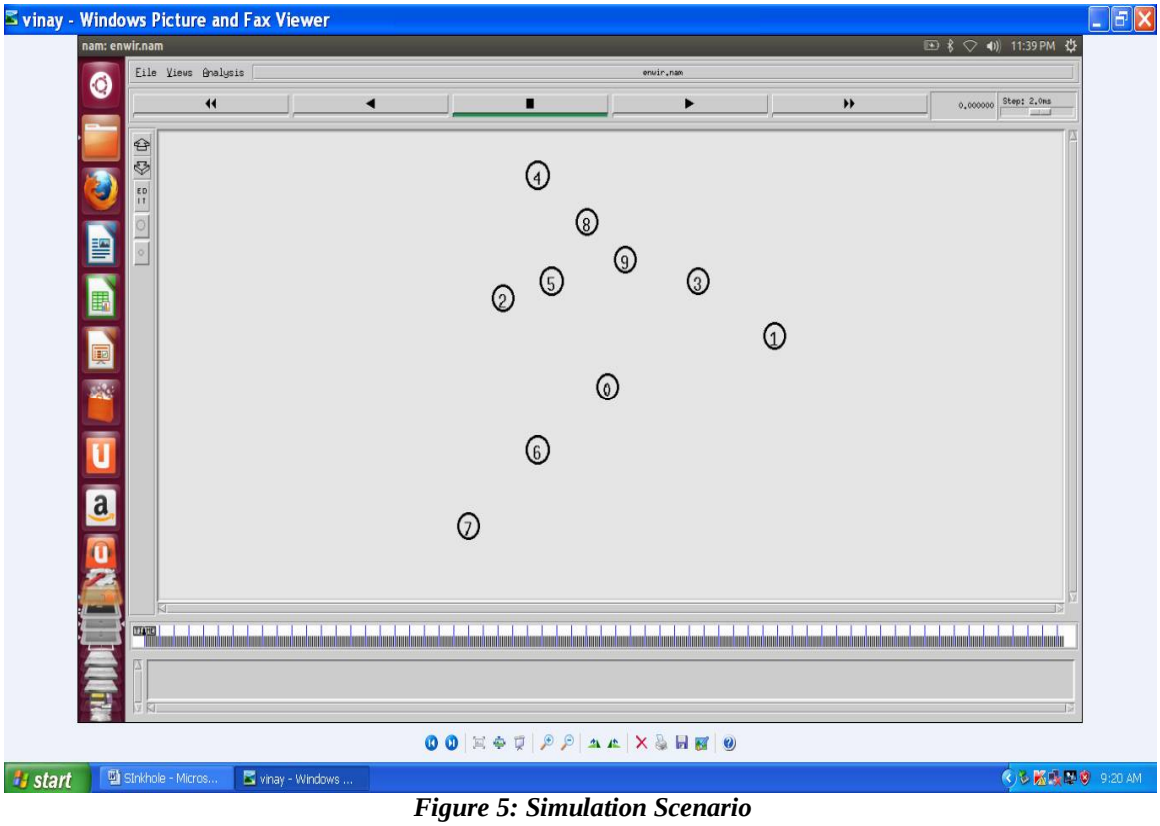

Figure 5: Simulation Scenario

We have measure packet delivery count and throughput.

(1) Packet delivery count is used to measure the no. of packets delivered to the destination node to that of the packets delivered from the source node [9].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Normal Scenario

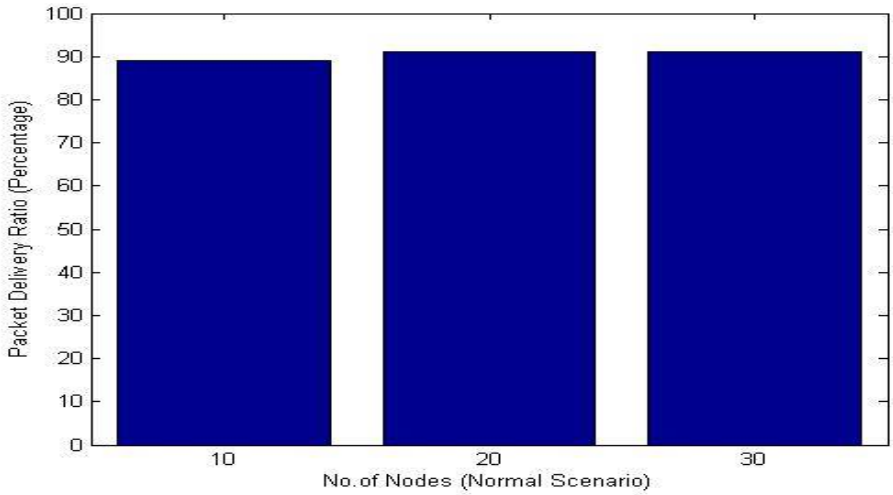

Figure 6: Packet Delivery Ratio in Normal Scenario

After the Sinkhole attack

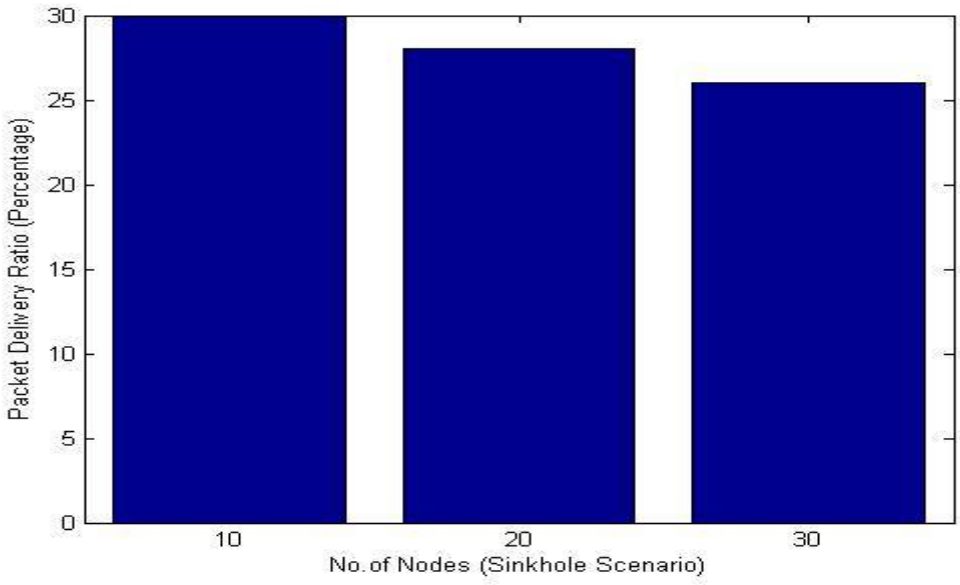

Figure 7: Packet Delivery Ratio after Sinkhole Attack Scenario

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

After Detection Algorithm Scenario

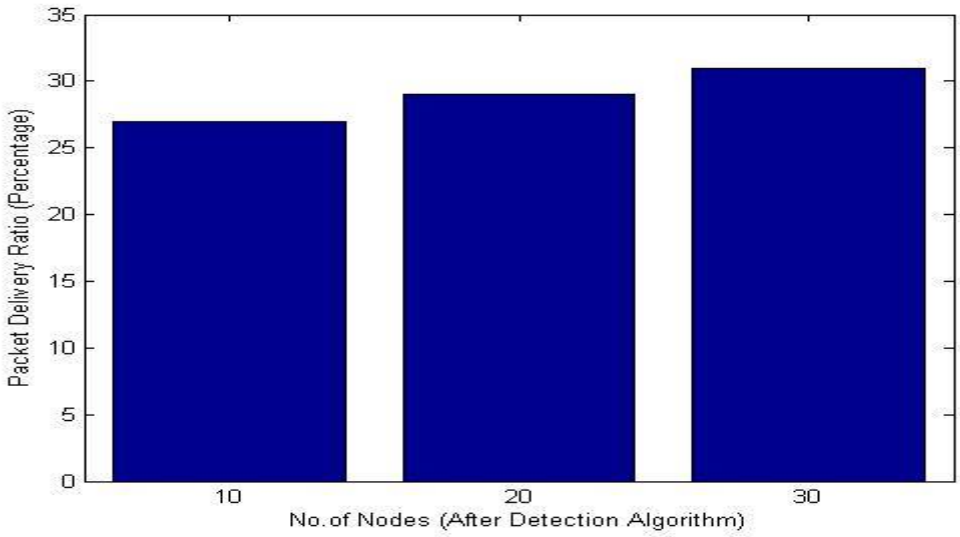

Figure 8: Packet Delivery Ratio after Detection Algorithm

(2) Throughput is the no. of data packets delivered from source to the destination per unit of time [10].

Normal Scenario

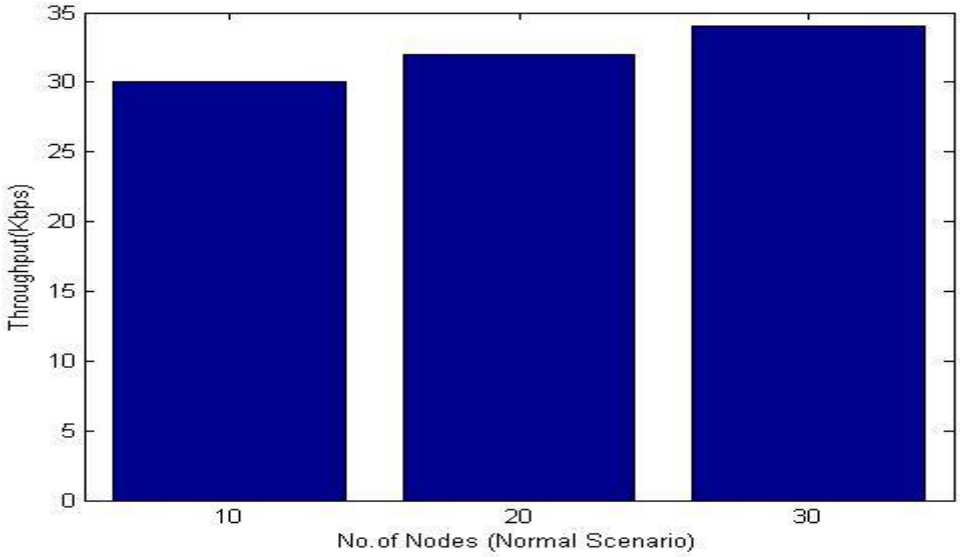

Figure 9: Throughput in Normal Scenario

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

AFTER THE SINKHOLE ATTACK

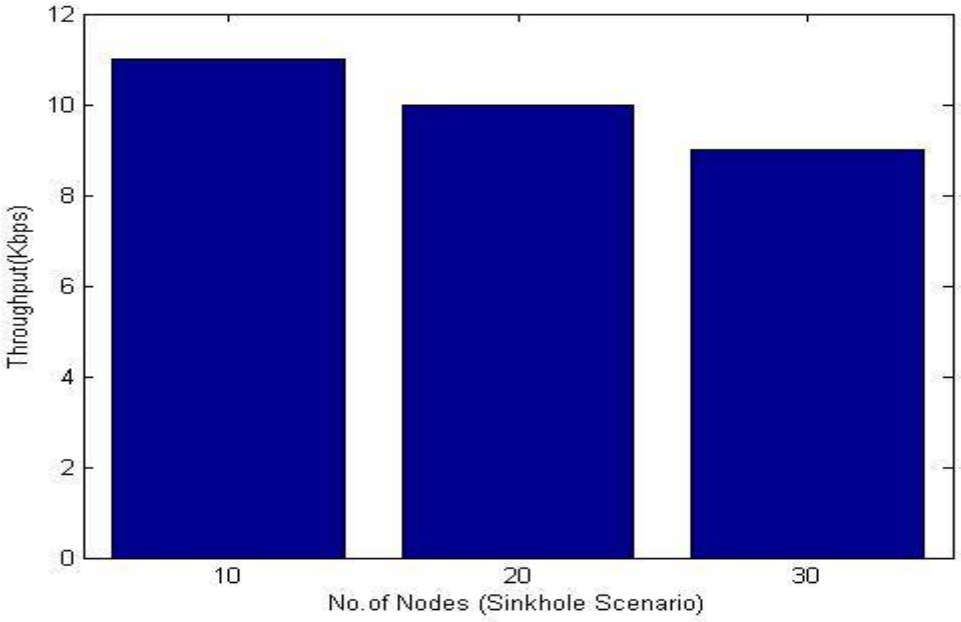

Figure 10: Throughput after Sinkhole Attack Scenario

AFTER DETECTION ALGORITHM SCENARIO

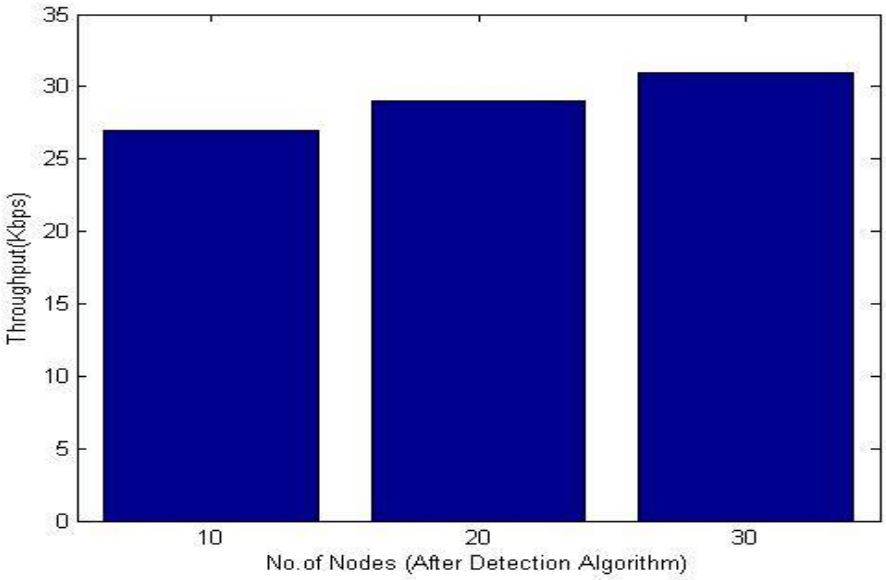

Figure 11: Throughput after Detection Algorithm

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

VII. CONCLUSION AND FUTURE WORK

In contrast to traditional networks, Wireless Sensor networks (WSN) are more vulnerable to attacks. We have identified some vulnerabilities of AODV routing protocol and shows how they can be exploited by an attacker to launch a sinkhole. Our proposed method can effectively identify the malicious node. Simulation results show that after applying detection algorithm, we have achieved throughput and packet delivery ratio that is nearer to normal AODV. Our future work will mainly focus on to analyze & study sinkhole problem on the context of other routing protocols and to evaluate variation in its performance after applying our detection & prevention mechanism by considering other performance metrics also.

REFERENCES

1. Vivek Tank, Prof. Amit Lathigara, "A Survey on Sinkhole Attack Techniques in Mobile Ad hoc Networks", International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 1, January 2015.
2. George W. Kibirige, Camilius Sanga, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network", http://www.researchgate.net/publication/276149286. MAY 2015.
3. Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal, "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method", Hindawi Publishing Corporation Scientific World Journal Volume 2015, Article ID 841267, 7 pages.
4. Md. Ibrahim Abdullah, Mohammad Muntasir Rahman et. al., "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count", I. J. Computer Network and Information Security, 2015, 3, 50-56.
5. Nisarg Gandhewar, Rahila Patel, "Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", 978-0-7695-4850-0/12 $26.00 © 2012 IEEE.
6. S.Sharmila, Dr. G. Uma Maheswari, "Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms", 978-1-61284-764-1/11/$26.00 ©2011 IEEE.
7. Fang-Jiao Zhang, Li-Dong Zhai et al., "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks", © 2014 Published by Elsevier B.V. Open access under CC BY-NC-ND license.
8. Resmi R , Lima Johnson et al., "Sinkhole attack in Mint Route and Multi hop LQI: Launching, Detection- A Survey", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)Vol. II, Special Issue X, March 2015.
9. Junaid Ahsenali Chaudhry, Usman Tariq et al., "Sinkhole Vulnerabilities in Wireless Sensor Networks", International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.401-410.
10. Savitha Devi. M, Dr. P. Thanga Raj, "A Proportional Learning on Sink, Warm Hole Attacks with Prevention Algorithms in Wireless Sensor Networks PLSWHA-W", International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2014.