International Journal of Engineering & Technology, 7 (2.4) (2018) 153-156

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Analysis of AODV Routing Protocol under Sinkhole Attack in Wireless Sensor Network

Harkesh Sehrawat [1], Yudhvir Singh [1], Vikas Siwach* [1]

[1] Department of CSE, UIET, MDU, Rohtak
**Corresponding author E-mail: singhvikashuiet@gmail.com*

Abstract

A Wireless Sensor Network (WSNs) is a collection of number of sensor nodes which are left open in an unsecured environment. Sensor nodes work and communicate together to attain the desired goals. They are placed at the locations where monitoring is otherwise impossible. Wireless Sensor Networks are resource constrained which may be computational power, memory capacity, battery power etc. As Wireless Sensor Networks are implemented in the unattended environment, they are prone to discrete type of security attacks. Because of their limitations these networks are easily targeted by intruders. Sinkhole attack is one of the security attacks which try to disturb the ongoing communication in wireless sensor network. In sinkhole attack, the intruder or the malicious node try to attract the network traffic towards itself, that sensor nodes will pass data packets through this compromised node thereby manipulating messages which sensor nodes are transferring to the base station. In this paper we analyze the impact of Sinkhole attack on AODV protocol under various conditions. We analyzed the impact of Sinkhole attack on AODV protocol with varying number of attacker nodes.

Keywords: *Sinkhole Attack; Wireless Sensor Network; AODV.*

1. Introduction

Wireless sensor network: WSNs [1] [2] is a collection of hundreds of tiny nodes known as sensor nodes which works together to achieve some predefined goals. The function of sensor nodes is to send messages (data) or information to the base station which is the destination node. Fig 1 below shows the component of a sensor node. Analog and digital converters and sensors constitutes sensing unit. A small memory unit called the processing unit manages the task of communication amid sensor nodes. Nodes communicate through transceiver unit and power unit is the most important part of sensor node which provides the network with needed power.

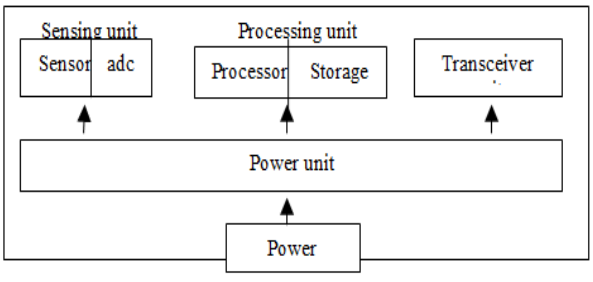

Fig.1: Components of Sensor Unit.

a) Applications of wireless sensor network[3]
- Intrusion detection
- Monitoring weather
- Security and tactical surveillance
- Disaster management
- Inventory control
- Medical diagnostics
- Military surveillance
- Environment surveillance

b) Features

Nodes can function as a router and for forwarding with several hopes. Nodes can make an individual network on an acknowledged protocol automatically. The wireless sensor network has a dynamic topology.

2. Attacks on wireless sensor network (WSNs)

In WSN's the sensor nodes are placed in an unattended, unprotected environment, because of which WSN is likely to be attacked by intruders. There are different types of security attacks [4] [5] [6] [18] [19] [22] [23] such as:

a) Tampering: It is the consequence of physical access by an attacker in the node; the intention is to retrieve cryptographic details like the keys used for encryption and decryption.
b) Selective forwarding: In this attack, compromised nodes may refuse to pass on some messages and subsequently drop them [7].
c) Sybil attack: Intruder can make use of identities of others nodes in order to capture necessary information [8].
d) Sinkhole attack: In sinkhole attack, compromised node tries to attract data packets so that any packet transmitted shall pass through it [9].
e) Wormhole attack: Intruders here are tactically placed at ends of the network. They receive information and sends back information to different nodes via a tunnel [10].
f) Black hole attack: Its only goal is to pass nothing thereby fashioning a black hole in the network[11].

3. Sinkhole attack

Wireless sensor network is unprotected from different type of attacks, an example of this is sinkhole attack[9]. This attack is caused by luring the maximum traffic possible towards itself. Based on routing protocols, the attacker node tries to attract traffic from the neighboring nodes. Mischievous node takes over control in regulating the traffic, throws the attack in the network. Because of the many to one pattern in WSN where each and every node sends data to BS, Wireless sensor network are more susceptible to sinkhole attack. Fig 2 below is an example of sinkhole attack where the sinkhole node tries to attain network traffic by sending incorrectdata to the nearby node, then changes the content of the information and finally passes it to the base station. Sinkhole node prevents base station from getting access to entire information.

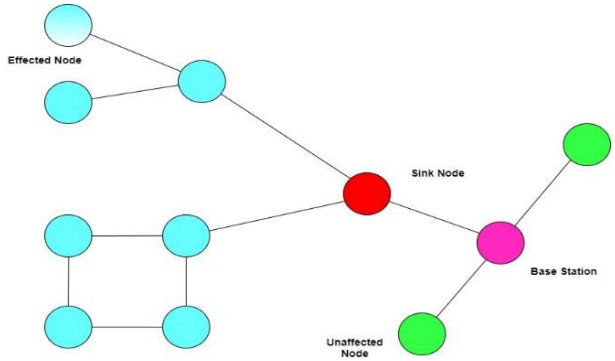

Fig.2: Sinkhole Attack in WSN.

4. Sinkhole attack in AODV (ad-hoc on demand distance vector routing protocol)

AODV [12] performs routing by sending route request messages to sensor nodes and by receiving route reply messages from the sensor node. Route request are sent as broadcast message and route reply is done by sending a unicast message back to the sender node. A sender can receive many reply i.e. a RREQ can get many RREP message. A RREP with highest sequence number is accepted by the source node. A high sequence number means the freshness of the route. Higher the sequence number, newer is the route. Source and destination address and sequence number are contained in the RREQ and RREP packets. Route is created when one sensor node sends an RREQ message to another sensor node and the other sensor node reply with an RREP message [20][21].

A sinkhole node or a malicious node is a node which represents itself as the most promising node of the network. It tries to attract the traffic towards itself by representing itself as a node with highest sequence number.The goal of the attacker is to modify these sequence number.Route request packet is generated when a node sequence no is augmented by 1. Greater the sequence number, more will be the freshness of message. The malicious node insert a fake sequence number in its RREP message and thus shows itself as best node for forwarding the data. The attacker node also generates a fake route request data packet with highest sequence number. After noticing this highest false sequence number of this malicious node, all other nodes starts transmitting message towards this malicious node. Thus malicious node attracts traffic towards itself and can initiate other attacks thereby ultimately damaging the whole network. Fig. 4 below shows sinkhole attack in AODV.

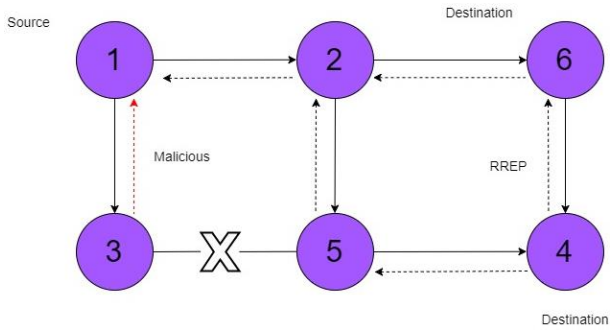

Fig.4: Sinkhole Attack in AODV.

5. Related works

Chen et al. [13] presented a method for detecting sinkhole attack. The scheme is applicable only to large scale wireless sensor networks. This method observes CPU usage as well as records regularity of CPU usage. This method is capable of differentiating amid compromised node and original node. For checking the goodness of the algorithm extensive simulations are used. The paper surveyed different features and challenges of WSNs in building up the detection procedure based algorithm here, base station computes the remainder of CPU usage by observing the CPU utility of nodes within definite time periods. Base station is able to sense compromised node by equating the difference with given threshold value. Simulations and network analyses are used to check algorithm. Performance of algorithm states that compromised node can be detected in less time with lesser rate of false positive.

Rassam et al. [14] discuss the powerlessness of MintRoute routing protocol and the principles for regulating as well as detecting attacks using different structures. The experimental result exhibit the potential of the protocol in detecting the sinkhole attack for small scale wireless network. Media of broadcasting in WSNs is radio communication which makes them unsafe to security attacks. Several sort of protocols are suggested for WSN but no protocol guarantees protection from attacks. Wormhole attack and black hole attack are introduced by sinkhole attack in the network. Future work will be to apply the principles for large scale WSNs and a new detection scheme based on fuzzy logic.

Chaudhry et al. [15] discussed problems in finding sinkhole attack. They have considered two scenarios for sinkhole detection. They considered that intruder nodes are more powerful than other nodes in the network in the first scenario. For the second scenario, they considered all nodes including the intruder nodes having equal power. They classified various existing tactics into anomaly-centric, statistical, rule-centric, crypto-graphic as well as hybrid tactics.

Kibirige and Sanga [16] emphasized on earlier solutions which are used to prevent sinkhole attack. Proposed solution is build up based upon the investigation of merits and demerits of existing solution. Different researcher gives different solutions to find sinkhole attack in WSNs. Some uses rule based approach, some uses key management, while some other uses IDS (intrusion detection scheme). A lower number of researchersmanage to apply their security system for their real WSNs. Future of this approach will aim on reducing computational power and network overhead.

Dallas et al. [17] inspect the challenges of preventing WSN against attacks which disturb dynamic directing conventions. They proposed an interruption identification framework which distinguishes the nearness of a sinkhole attack that deludes movement by downplaying the cost of an assault course. Their investigation demonstrates that conventions intended to choose the shortest way amid two hubs will handpick a progression of means whose length will show a log-ordinary conveyance through time. They had created an inconsistency discovery plot which will recognize sinkhole assaults in a computationally productive way via attainment of resistance limits from the “log-normal dispersion” of way lengths in normal settings. They had demonstrated that assaults can be

identified with 96% accuracy whereby no-false cautions are generated by utilizing a solitary discovery framework in a mimicked organize.

6. Proposed work

In this paper,AODV protocol is analyzed under the influence of sinkhole attack. The main aim of sinkhole attack is to lure the traffic towards itself. The AODV protocol works on the basis of route request and route reply mechanism. Each node maintain a sequence number and this sequence number is sent with every message. A higher sequence number in the message means freshness of the path. A malicious node takes advantage of this and reply each route request message with a very high false sequence number. Various number of malicious node are taken here which ranges from 2 to 12. The behavior of AODV protocol is inspected on varying number of malicious or attacker nodes on different parameters.

7. Results and discussion

We have implemented our scenario in Qualnet 7.3.1. A total number of 50 nodes were taken in an area of 1500m X 1500 m with no mobility i.e the nodes are stable at their positions.

Parameters	Values
Simulator	Qualnet 7.3.1
Area	1500X1500 m
No. of node	50
Network Layer Protocol	AODV
MAC layer Protocol	IEEE 802.15.4
No. of Applications	15-20
Application Used	Zigbee
Item Size	50
Simulation Time	1000 s
Items to Send	1000
Start Time	1
Interval	1
Mobility Model	Static
Number of sinkhole attackers	2-12
Parameters compared	Throughput, End to end delay, packet dropped, route request initiated

Mal 0 shows that there is no attacker in the network and simply AODV is running in normal environment. The sinkhole attack is initiated by generating the highest false sequence number of RREP messages. The fig. 5 shows the number of RREP packets generated in the network. As the number of malicious nodes are increasing, the number of RREP messages increasing sharply.

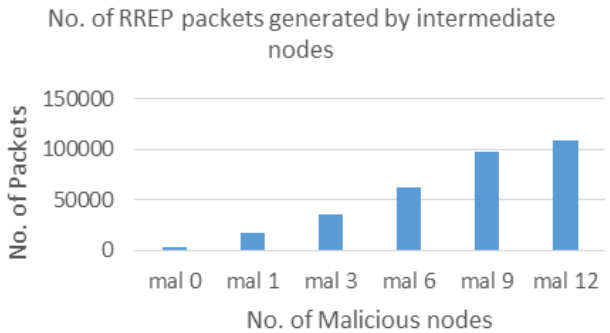

Fig. 5: Number of Route Request Generated.

Fig. 6 shows the number of packets dropped due to non-availability of the valid routes. Attacker node attracts the traffic towards them but sends them nowhere, so ultimately they are dropped. As number of malicious nodes is increasing, the number of packet dropped also increases.

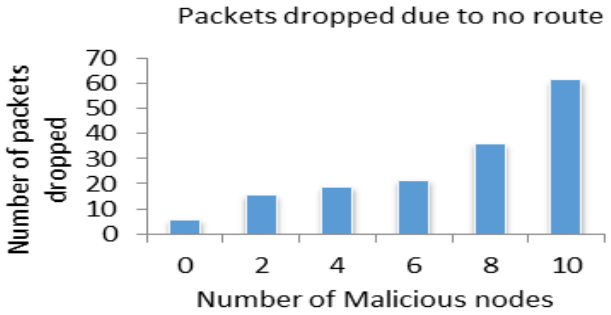

Fig. 6: Number of Packets Dropped.

Fig. 7 below describes the impact of attacker nodes on the throughput of the network. It can be clearly seen that the throughput of network decreases with increase in number of attacker nodes.

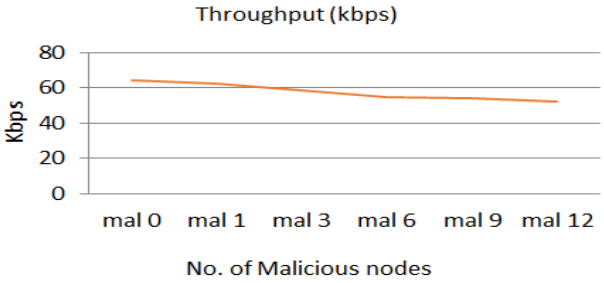

Fig. 7: Throughput.

Fig. 8 below shows the impact of number of attacker on the end to end delay which measures the delay in data transmission between source and destination and it increases with increase in number of malicious node.

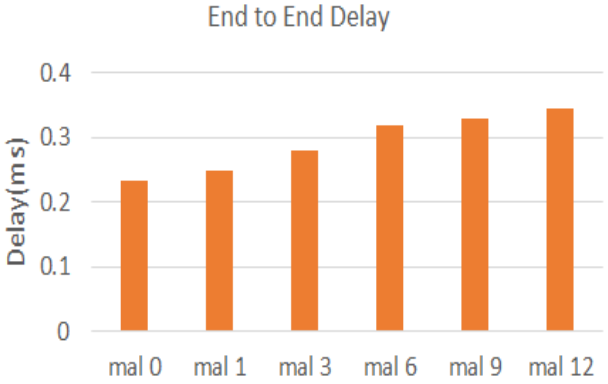

Fig. 8: End-To-End Delay.

8. Conclusion and future work

Wireless sensor networks have many features which make them susceptible to critical attacks in an open and unprotected environment. A wireless channel is normally open to everyone with a radio interface configured at the same frequency, thus anyone can participate in communication. Various kinds of attacks either insider or outsider can harm the network. This paper provides the details about the impact of sinkhole attack on wireless senor networks using AODV routing protocol. In future, we will introduce the concept of how sinkhole attacks can be detected as well as controlled.

References

[1] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," Int. J. Comput. Sci. Inf. Secur., vol. 4, no. 1, pp. 1–9, 2009.

[2] T. Kavitha and D. Sridharan, "Security Vulnerabilities in Wireless Sensor Networks : A Survey," J. Inf. Assur. Secure. vol. 5, pp. 31–44, 2010.

[3] T. Singh, "Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool," Int. J. Adv. Comput. Sci. Appl., vol. 4, no. 2, pp. 32–35, 2013.

[4] A. Tayebi, S. Berber, and A. Swain, "Wireless Sensor Network Attacks:An Overview and Critical Analysis," in Seventh International Conference on Sensing Technology Wireless, 2013, pp. 97–102

[5] K. Xing, R. S. S. Srinivasan, M. Rivera, J. Li, and X. Cheng, "Attacks and Countermeasures in Sensor Networks : A Survey," in Network Security, S. C.-H. Huang, D. MacCallum, and D.-Z. Du, Eds. Boston, MA: Springer US, 2005, pp. 251–272.

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

[7] H. M. Sun, C. M. Chen, and Y. C. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in IEEE Region 10 Annual International Conference, TENCON 2007, 2007, pp. 4–7.

[8] S. Chen, G. Yang, and S. Chen, "A security routing mechanism against Sybil attack for wireless sensor networks," in 2010 International Conference on Communications and Mobile Computing (CMC 2010), 2010, pp. 142–146.

[9] K. Tunwal, R. Khandelwal, D. Acharya, and P. S. Dabi, "A Survey of Sinkhole-Based Attack and Detection Techniques in WSN," Int. J. Enhanc. Res. Sci. Technol. Eng., vol. 3, no. 6, pp. 377–380, 2010.

[10] A. Gupta and A. K. Gupta, "A Survey: Detection and Prevention of Wormhole Attack in Wireless Sensor Networks," vol. 14, no. 1, 2014.

[11] S. D. Roy, S. A. Singh, S. Choudhury, and N. C. Debnath, "Countering sinkhole and black hole attacks on sensor networks using dynamic trust management," in Proceedings -of IEEE Symposium on Computers and Communications, 2008, pp. 537–542.

[12] C. Lin, "AODV Routing Implementation for Scalable Wireless Ad-Hoc Network Simulation (SWANS)."

[13] C. Chen, M. Song, and G. Hsieh, "Intrusion detection of sinkhole attacks in large-scale wireless sensor networks," in IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010, pp. 711–716.

[14] M. A. Rassam, A. Zainal, and M. Al-shaboti, "A Sinkhole Attack Detection Scheme in Mintroute Wireless Sensor Networks," in 1st IEEE International Symposium on Telecommunication Technologies, 2012, pp. 71–75.

[15] J. A. Chaudhry, U. Tariq, M. A. Amin, and R. G. Rittenhouse, "Dealing with Sinkhole Attacks in Wireless Sensor Networks," Adv. Sci. Technol. Lett., vol. 29, no. 2, pp. 7–12, 2013.

[16] G. Kibirige and C. Sanga, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network," Int. J. Comput. Sci. Inf. Secur., vol. 13, no. 5, pp. 1–9, 2015.

[17] D. Dallas, C. Leckie, and K. Ramamohanarao, "Hop-count monitoring: Detecting sinkhole attacks in wireless sensor networks," in Proceedings of the15th IEEE International Conference on Networks, 2007.

[18] Preeti, Yogesh Chaba, Yudhvir Singh; Review of Detection and Prevention Policies for DDoS attacks in MANETs; In Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008) RIMT-IET, Mandi Gobindgarh; March 29, 2008; pp 56-59.

[19] Neeraj Sharma, B.L. Raina, Prabha Rani, Yogesh Chaba, Yudhvir Singh,"Attack Prevention Methods for DDoS Attacks in MANETs", Asian Journal Of Computer Science And Information Technology, ISSN – 2249-5126,Vol 1, Issue 1, pp. 18 – 21 (2011).

[20] Yogesh Chaba, Yudhvir Singh, Aarti, "Performance Analysis of Scalability and Mobility on Routing Protocols in MANETs" International Journal of IT & Knowledge Management (ISSN: 0973-4414) Vol. 1, No. 2, pp. 327-336 (July-Dec, 2008).

[21] VikashSiwach,Yudhvir Singh, Seema,DheerDhwaj Barak, "An approach to optimize QoS routing protocol using genetic algorithm in MANET", IJCSMS, ISSN: 2231-5268, Vol 12, Issue 3, pp 149-53, (Sept 2012).

[22] RenuDalal, Manju Khari, Yudhvir Singh, "Survey of Trust Schemes on Ad-hoc Network", Springer - Lecture Notes of the Institute for Computer Sciences, Social Informatics & Telecommunications Engineering (LNICST) Series 84, Springer, NETCOM-3, CCSIT-2012,pp 170-180,(2012).

[23] Pooja, Manisha, Yudhvir Singh, "Security Issues and Sybil Attack inWireless Sensor Networks", International Journal of P2P Network Trends and Technology,ISSN: 2249-2615, Volume3, Issue1, pp7-13, 2013