DOI: http://dx.doi.org/10.26483/ijarcs.v12i5.6767

Volume 12, No. 5, September-October 2021

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

WIRELESS SENSOR NETWORK PERFORMANCE ANALYSIS UNDER SINKHOLE ATTACKS

Maghrib Abidalreda Maky Alrammahi
ITRDC, University of Kufa
Al Najaf, Iraq

Balasem A. Al-Isawi
Computer Center, University of Babylon
Babel, Iraq

Othman M.Hussein Anssari
ITRDC, University of Kufa
Al Najaf, Iraq

Abstract : WSN is one of the modern networks that use technologies and applications in public places. It consists of hundreds and thousands of tiny sensor nodes scattered in the network and has limited scope and range resources connected to the base stations. The specifications of these nodes are low cost and low energy and used for monitoring purposes. Since the sensors are small and many, it is easy to attack these networks. Therefore, there will be many potential attacks on the network of sensors, and among these attacks are jamming, sinkhole, eavesdropping, and other attacks. The sinkhole attack is the most attack that works to destroy paths by announcing the update of the fake routing related to it; the attack occurs through the compromised node (the malicious node) So that it announces a file containing the routing information and works to attract the rest of the nodes to do this routing the data towards it and then operating the sphere of influence. One of the effects of this attack is to reduce the overall network performance, and it can also be used to make another attack, such as a selective redirection attack and a spoofing attack. This paper aims to analyze and detect sinkhole attacks in wireless sensor networks.

Keywords: Wireless Sensor Network (WSNs), Security Attack, Sinkhole Attack, Malicious nodes, Omnet+4.

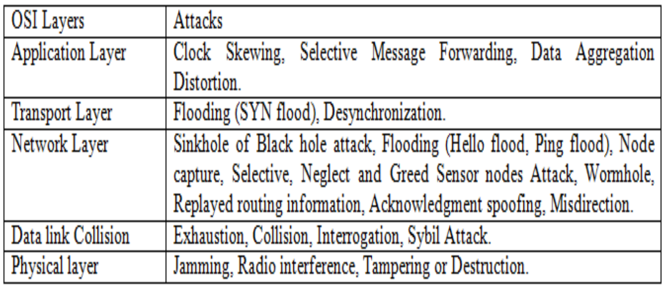
I. INTRODUCTION

WSNs are used in most applications in indoor or outdoor locations [4]. Through the transmission of data and information in the network and most importantly, providing security for it. [6] Security is one of the most difficult things in WSN as it is always difficult to monitor the sensor nodes/network every time. However, the protection must be increased to prevent an intruder from tampering with the data transmission.

There are a lot of complex sensor limitations, especially for its size and cost, which must be at least one. These restrictions lead to a very small memory size, a relatively limited power source, and a limited transmission area as well. In the end, there will be difficulty in non-encryption, decryption, and the authentication process through which it is possible to the sensor nodes. So that the most common terms used in the attacker and the attack, as the attacker is the person who is not allowed to gain access to network sources and data, or is the person who is trying to manipulate information and while an attack is considered when the attacker accesses network resources[25].

There are layers designed in WSN networks that help protect the sensor from multiple attacks. Figure 1 shows the model of the protection layers in wireless sensor networks.

Table I: WSN attacks on OSI layers



OSI Layers	Attacks
Application Layer	Clock Skewing, Selective Message Forwarding, Data Aggregation Distortion.
Transport Layer	Flooding (SYN flood), Desynchronization.
Network Layer	Sinkhole of Black hole attack, Flooding (Hello flood, Ping flood), Node capture, Selective, Neglect and Greed Sensor nodes Attack, Wormhole, Replayed routing information, Acknowledgment spoofing, Misdirection.
Data link Collision	Exhaustion, Collision, Interrogation, Sybil Attack.
Physical layer	Jamming, Radio interference, Tampering or Destruction.

WSN networks are considered more Impact of security attacks depending on the type of transmission in the transmission medium in wireless networks, so that often there are dangerous environments in which the contract is made, so that there is no physical protection, and therefore this will lead to its risk and reduce its security. Many types of attacks have been documented, and there are two main types of attacks: active attack and passive attack. Figure 1 shows the main classifications of these attacks.

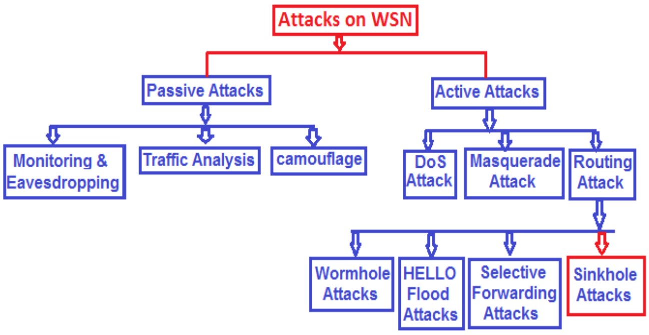


Figure 1: classifications of attacks

Based on the above types of attacks, there will be many attacks. One of these attacks is known as the sinkhole attack, this attack works to penetrate nodes and manipulate network traffic by announcing updates to special fake directives. The most important risk of this attack is that it can be used to launch attacks of other types, such as a selective redirect attack or another type, which is a spoofing attack, so that these attacks work by sending incorrect information to the base stations in the network.

II. Objective of Research

Most of the time, wireless sensors are installed in open places, and thus these networks are more vulnerable to danger, attacks, and easy to intrusive. It is considered a wide-ranging network, and it is difficult to follow and monitor each node and protect it. When this network's response security has been stopped immediately again With a message, the sensor node may generate fake or surprising response messages and may be manipulated and thus lead to undesirable actions permanently. There are different types of security levels for the wireless sensor device in the network, which are described below:

- Privacy (Confidentiality): data transmission must be maintained confidential and cannot be accessed by an unauthorized user to login.
- Data-authentication: undesirable effects can be isolated after confirming that she represents the approach and identity of the nodes in which the communication is located
- probity (Integrity): Include that information and data are correct The intruder does not change it.
- Availability: The service must be available at all times.
- Freshness: it is better than the data always be new and not old It must be returned.
- Non- rejection (Non-repudiation): It means that the node cannot refuse to send a file The message you sent earlier.
- Authorization: They are a group of authorized persons only have access to data and network resources.

III. Preview of AODV protocol

The AODV protocol is present in all nodes in the WSN networks so that it works to broadcast or flooding in network. Where this protocol works in the nodes so that node A works by broadcasting by sending packets which is a message and is called route request (RREQ) and send it to the neighbors for the rest of the nodes. A packet called route replay (RREP) contains all the information and nodes that were during the transmission path from beginning to end, starting from the last node and back to the same path sent until it reaches the nodes A. Therefore, this protocol is very important in the process of sending and receiving between nodes in WSN networks.

IV. Design and Implementation

A. *Attack of Sinkhole*

This type of attack is attack that is used from the inside and not from outside, meaning inside the network, so that an intruder penetrates And the nodes that are inside the network and makes an attack and then tries to penetrate this node by attracting manipulation in the traffic in its neighboring nodes depending on the routing scale that is used in the routing protocol And when this thing is achieved, the attacker will depend on the communication pattern adopted in the wireless sensor networks, which consists of a group of communications so that each node sends data To the important devices in the network, which is the base station. The attack will penetrate the nodes in the WSN networks.

B. *Simulation Sinkhole Attack*

An Omnet+4 simulation will be used in the scenario of a sinkhole attack, through which an attack will be identified and detected. Sinkhole attack Malicious nodes send incorrect routing information meaning fake and claim to have the correct next path. Other nodes will route data packets through themselves and the attacker works by forging and altering routing responses to attract tracers. An important set of Hungarian attack parameters consists of:

- (sinkhole Attack Probability-double) The probability of answering the message (RREQ) with the answer to a dummy or imaginary route reply(RREP), the action is specified between 0 and 1 and is set to a value of zero by default which demonstrates the normal behavior of the protocol AODV.
- (sink Only When Route In Table-bool): If set to true, the attacker will send dummy requests RREP only which contain the correct path the attacker is holding and therefore will contain the routes in their own routing table and vice versa (false values), nodes send dummy requests RREP to any message Reach RREQ even if she doesn't know the right paths.
- (seqno Added-double): Fake serial numbers will be generated by the attacker node and will be added to the serial numbers depending on the requests and not on the condition that the numbers are always the same every time and these numbers are determined based on the statistical distribution by default and this distribution follows a uniform value between 20 and 30.

- (num Hops-int): It represents the imaginary numbers of hops by default that the attacker has returned, a representation of the value 1, and this represents that the attacker will reach the end of the connection in only one hop and also at the end where the statistical distribution can be adopted in a certain way.

C. Sinkhole Attack Scenarios

This report demonstrates the sinkhole attack with a scenario of one attacker having a fake hop count to the destination node (node D). In the scenario of the sinkhole attack, Serial numbers will be added to the fake nodes and these values are between 50 and 60 and the number of fake hops is 1.

D. Methodology

Through the flowchart below, an explanation of the steps and mechanism of the Sinkhole attack scenario and how to hack the message, update it and resend it to other nodes will be clarified.

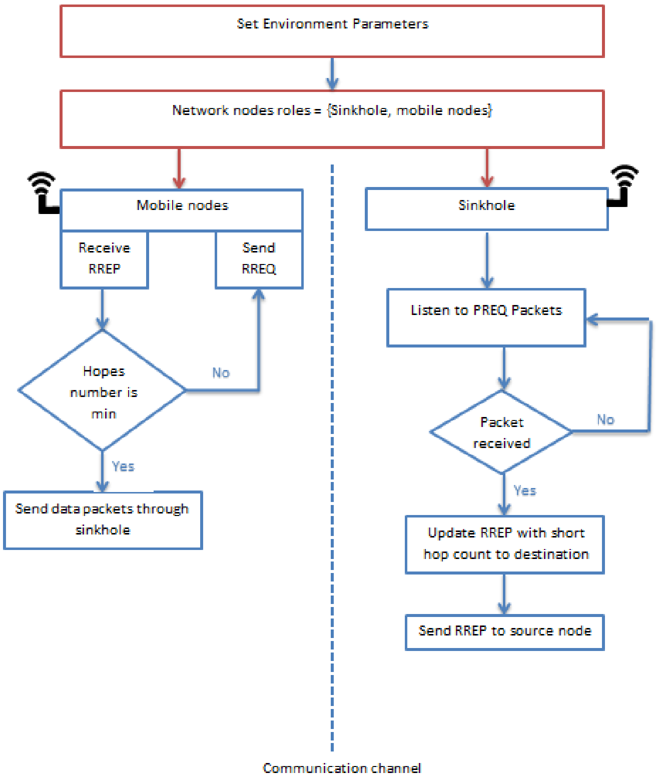
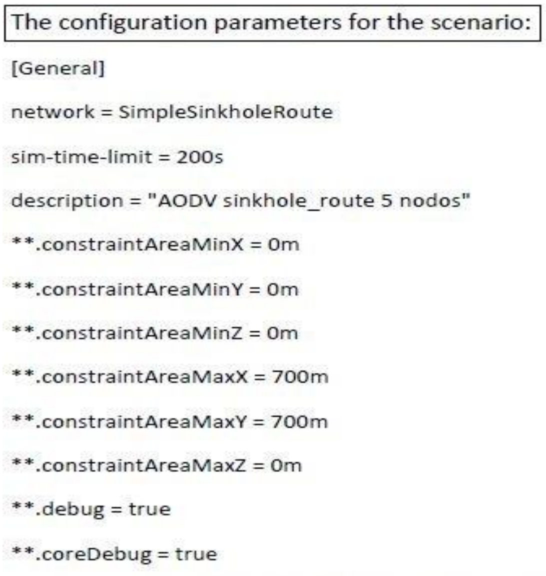

Set Environment Parameters
Network nodes roles = {Sinkhole, mobile nodes}
Mobile nodes
Receive RREP
Send RREQ
Hopes number is min
No
Yes
Send data packets through sinkhole
Sinkhole
Listen to PREQ Packets
Packet received
No
Yes
Update RREP with short hop count to destination
Send RREP to source node
Communication channel

Figure 2. Sinkhole attack scenario

E. Configuration

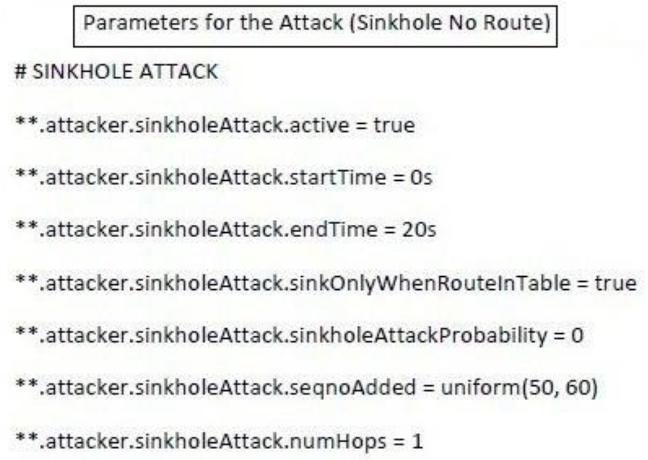
The following listing (Listing 1), illustrates the parameters adaptations for the environment and various node types (mobile nodes as well as attacker nodes). In the beginning, the settings include global environment physical settings, like area, also simulation parameters, like simulation time.

The settings part that follows concerns the sinkhole attack parameters. The rest of the headings include various nodes configurations with different architectural levels for each and every node.



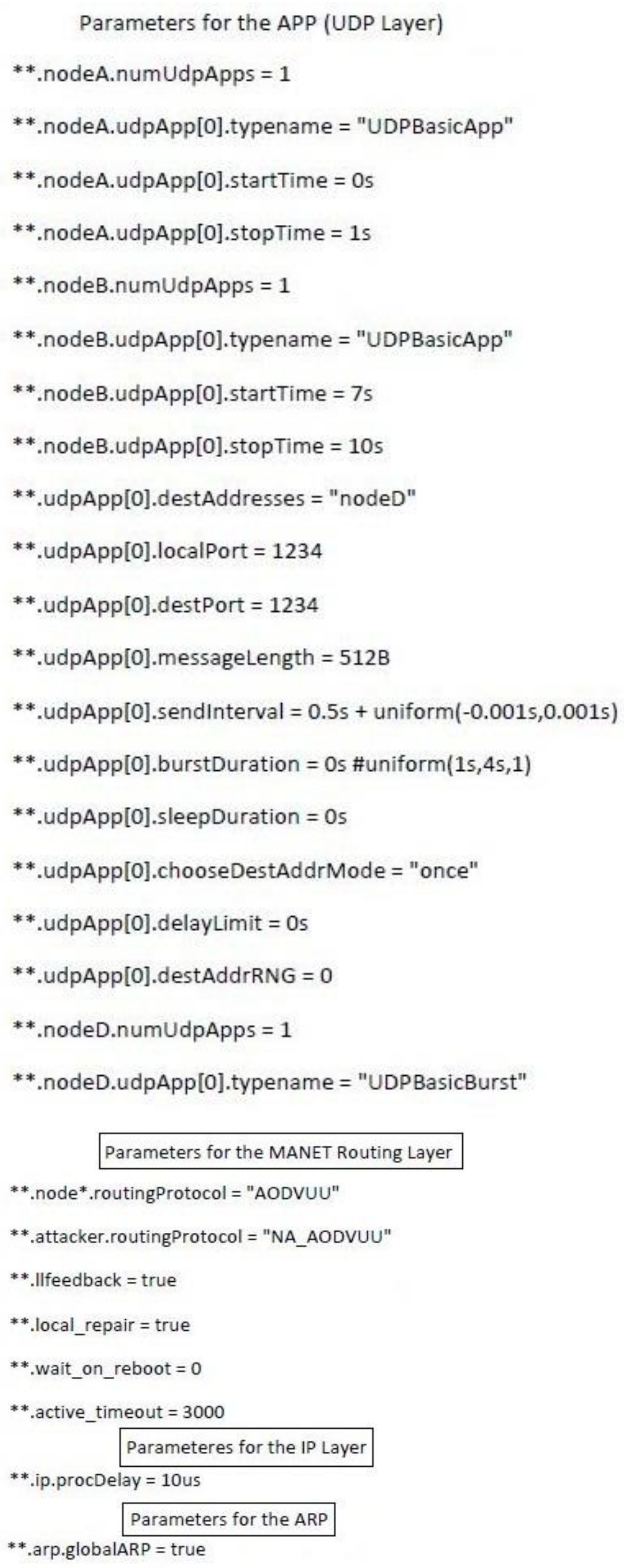
The configuration parameters for the scenario:

```
[General]

network = SimpleSinkholeRoute

sim-time-limit = 200s

description = "AODV sinkhole_route 5 nodos"

**.constraintAreaMinX = 0m

**.constraintAreaMinY = 0m

**.constraintAreaMinZ = 0m

**.constraintAreaMaxX = 700m

**.constraintAreaMaxY = 700m

**.constraintAreaMaxZ = 0m

**.debug = true

**.coreDebug = true
```

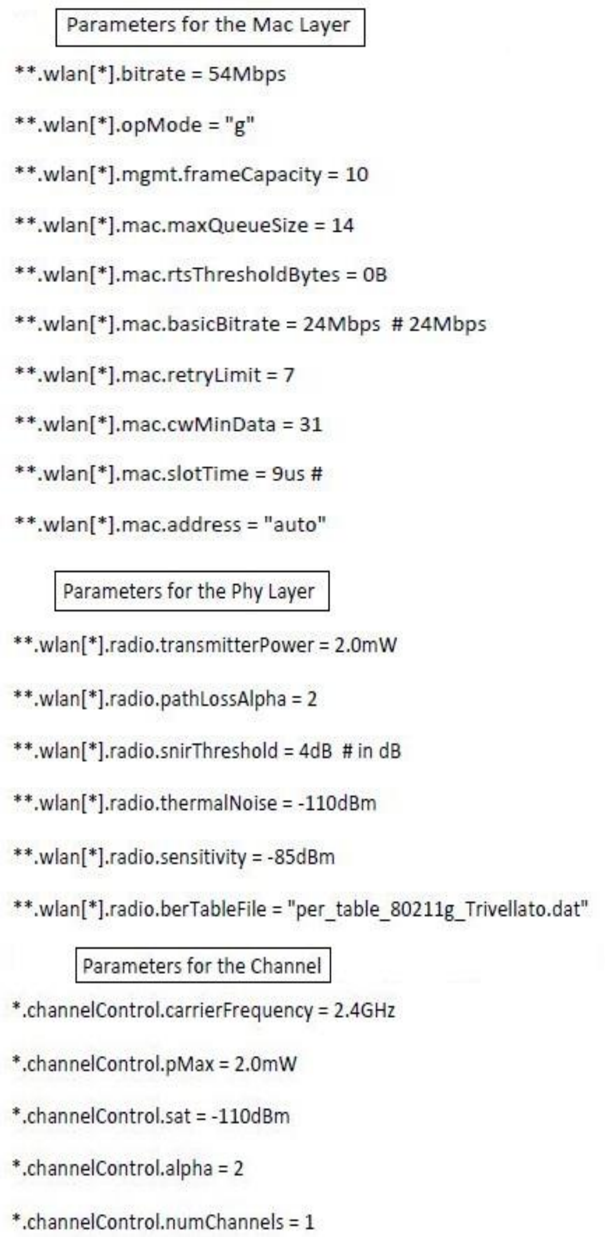


Parameters for the Attack (Sinkhole No Route)

```
# SINKHOLE ATTACK

**.attacker.sinkholeAttack.active = true

**.attacker.sinkholeAttack.startTime = 0s

**.attacker.sinkholeAttack.endTime = 20s

**.attacker.sinkholeAttack.sinkOnlyWhenRouteInTable = true

**.attacker.sinkholeAttack.sinkholeAttackProbability = 0

**.attacker.sinkholeAttack.seqnoAdded = uniform(50, 60)

**.attacker.sinkholeAttack.numHops = 1
```



```
Parameters for the APP (UDP Layer)

**.nodeA.numUdpApps = 1
**.nodeA.udpApp[0].typename = "UDPBasicApp"
**.nodeA.udpApp[0].startTime = 0s
**.nodeA.udpApp[0].stopTime = 1s
**.nodeB.numUdpApps = 1
**.nodeB.udpApp[0].typename = "UDPBasicApp"
**.nodeB.udpApp[0].startTime = 7s
**.nodeB.udpApp[0].stopTime = 10s
**.udpApp[0].destAddresses = "nodeD"
**.udpApp[0].localPort = 1234
**.udpApp[0].destPort = 1234
**.udpApp[0].messageLength = 512B
**.udpApp[0].sendInterval = 0.5s + uniform(-0.001s,0.001s)
**.udpApp[0].burstDuration = 0s #uniform(1s,4s,1)
**.udpApp[0].sleepDuration = 0s
**.udpApp[0].chooseDestAddrMode = "once"
**.udpApp[0].delayLimit = 0s
**.udpApp[0].destAddrRNG = 0
**.nodeD.numUdpApps = 1
**.nodeD.udpApp[0].typename = "UDPBasicBurst"

Parameters for the MANET Routing Layer

**.node*.routingProtocol = "AODVUU"
**.attacker.routingProtocol = "NA_AODVUU"
**.llfeedback = true
**.local_repair = true
**.wait_on_reboot = 0
**.active_timeout = 3000

Parameteres for the IP Layer

**.ip.procDelay = 10us

Parameters for the ARP

**.arp.globalARP = true
```



```
Parameters for the Mac Layer

**.wlan[*].bitrate = 54Mbps
**.wlan[*].opMode = "g"
**.wlan[*].mgmt.frameCapacity = 10
**.wlan[*].mac.maxQueueSize = 14
**.wlan[*].mac.rtsThresholdBytes = 0B
**.wlan[*].mac.basicBitrate = 24Mbps  # 24Mbps
**.wlan[*].mac.retryLimit = 7
**.wlan[*].mac.cwMinData = 31
**.wlan[*].mac.slotTime = 9us #
**.wlan[*].mac.address = "auto"

Parameters for the Phy Layer

**.wlan[*].radio.transmitterPower = 2.0mW
**.wlan[*].radio.pathLossAlpha = 2
**.wlan[*].radio.snirThreshold = 4dB  # in dB
**.wlan[*].radio.thermalNoise = -110dBm
**.wlan[*].radio.sensitivity = -85dBm
**.wlan[*].radio.berTableFile = "per_table_80211g_Trivellato.dat"

Parameters for the Channel

*.channelControl.carrierFrequency = 2.4GHz
*.channelControl.pMax = 2.0mW
*.channelControl.sat = -110dBm
*.channelControl.alpha = 2
*.channelControl.numChannels = 1
```

Listing 1: Simulation configurations.

V. EXPERIMENTAL RESULT

A. Result

In the simulation environment, 5 nodes will be created as in Figure 3 and in this scenario, the attacking node knows the route to the destination node. The nodes placement is shown in Figure 3, we have a total of five nodes, four natural nodes (NA_AdhocHost) and one hacked node(NA_ AttackerAdhocHost). In the scenario, a message will be sent from node A to this node D, within a certain time between zero and one, and the attacker performs a successful penetration. The attacker will know the path to nodes D, knowing that nodes C is learning the path previously, which is a single hop to nodes D, so node B will be chosen by the attacker as the next step because of its fake response.

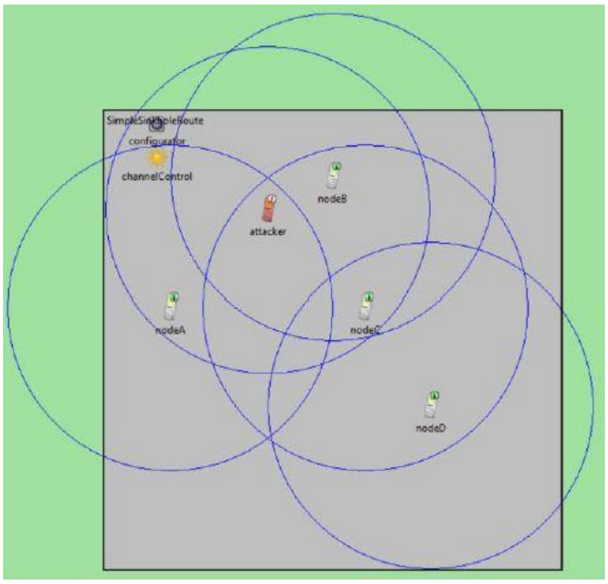


Figure 3: Nodes Placement for Simple Sinkhole Route

We can see in Table 2 the numbers of sent and receive packets that will be sent by the nodes, it can be seen that the attacker node does not participate in the network data payload.

Table II. Network Data Payload

Packets	Attacker	Node A	Node B	Node C	Node D
Sent	0	2	6	0	0
Received	0	0	0	0	8

During the simulation, the communicated AODV negotiations counts are listed in Table 3, which indicate that when node A request the rout for node D it takes the shortest hop count (=1) from the attacker (a fake hop count) and hence all the subsequent routing was made through the Attacker node. When the attacker node gets the desired traffic, it can initiate another attack type.

Table III. number of iteration effect on network performance

AODV	Attacker	NodeA	NodeB	NodeC	NodeD
Rreq sent	1	5	0	0	0
Rreq received	5	6	0	0	0
Rrep sent	3	4	0	0	0
Rrep received	1	6	0	0	0
Rreq ack sent	0	2	0	0	0
Rreq ack received	1	1	0	0	0
Rerr sent	2	3	0	0	0
Rerr received	1	6	0	0	0
Total sent	6	14	0	0	0

B. Detecting and Identifying Attack

- Basic rule:

Depending on the behavior and techniques used, the rules of the sinkhole attack construction and when applying these rules in the simulation are designed to detect intrusion that occurs on sensor nodes and apply them to packets sent through network nodes, in the event of a violation of the rules for any node then it is considered hostile and has been hacked and then isolated from the network.

- Detection based on document anomalies:

Works to detect the document to the deviation. The normal user's behavior is determined by detecting abnormal intrusion in the network. Thus, a state of abnormal parasitism and abnormal activity will appear compared to normal behavior. Finally, foundation-based and statistical approaches that rely on anomaly-based detection approaches will be installed.

- Statistical methods:

Specific activities of the nodes are determined, and then the data associated with the nodes in the network are studied and recorded by researchers. For example, monitoring regular messages or packets carried between nodes or keeping track of the exhaustion of major nodes resources such as the CPU. When the contract is breached, the state of the resources or data will be compared by using the threshold value used as a reference. In the event that any node exceeds this value, it will be considered intrusive and an attack on the contract has occurred.

- Identification and detection of hybrid intrusion :

This approach uses a combination of anomalies and signature misuse of spelling. By using the two methods, the positive error rate resulting from anomalies will be reduced, and any suspicious node will be detected through capture. Which does not contain the signature in the detection database

- Key management

The use of keys in the process of sending and receiving packets and messages is very important so that through them we can verify the authenticity of the message or the presence of tampering with it, using the key is used in the process of encryption and decryption and the key is added to the packets during their transmission between nodes to ensure and verify that packets are not breached during the path.

V. Conclusion and Future Works

The sinkhole attack It is one of the important types that can occurs inside and is called(insider attack), so the attack by itself is unpredictable. The severity of this attack is that the attacker can initiate another type of attack in parallel with its operation. These attacks include Sending false data to the base station, changing routing paths, or using a spoofing attack.

Therefore, in future work and increase protection from the above attack, it is preferable to use public symmetric keys, the difficulty of penetrating these keys and their difficulty for the attacker, and also it is preferable to increase protection to use or combine two algorithms between them to obtain a strong and hybrid algorithm to prevent or increase the prevention of intrusion on the nodes

VI. REFERENCES

[1] Kaur, M., & Singh, A. (2016, September). Detection and mitigation of sinkhole attack in wireless sensor network. In 2016 International conference on micro-electronics and telecommunication engineering (ICMETE) (pp. 217-221). IEEE.

[2] Hao, B., Chang, D., Zhang, Z., & Ji, H. (2019, March). Performance Analysis of Routing for Wireless Sensor Network. In 3rd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2019) (pp. 328-334). Atlantis Press.

[3] Qi, J., Hong, T., Xiaohui, K., & Qiang, L. (2012, November). Detection and defence of Sinkhole attack in Wireless Sensor Network. In 2012 IEEE 14th International Conference on Communication Technology (pp. 809-813). IEEE.

[4] Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.

[5] Modares, H., Salleh, R., & Moravejosharieh, A. (2011, September). Overview of security issues in wireless sensor networks. In 2011 third international conference on computational intelligence, modelling & simulation (pp. 308-311). IEEE.

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

[7] Gandhewar, N., & Patel, R. (2012, November). Detection and Prevention of sinkhole attack on AODV Protocol in Mobile Adhoc Network. In 2012 Fourth International Conference on Computational Intelligence and Communication Networks (pp. 714-718). IEEE.

[8] Zhou, Y., Fang, Y., & Zhang, Y. (2008). Securing wireless sensor networks: a survey. IEEE Communications Surveys & Tutorials, 10(3), 6-28.

[9] young Kim, J., Caytiles, R. D., & Kim, K. J. (2014). A review of the vulnerabilities and attacks for wireless sensor networks. 9(3), 241-250.

[10] Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In 2006 8th International Conference Advanced Communication Technology (Vol. 2, pp. 6-pp). IEEE.

[11] Ngai, E. C., Liu, J., & Lyu, M. R. (2006, June). On the intruder detection for sinkhole attack in wireless sensor networks. In 2006 IEEE International Conference on Communications (Vol. 8, pp. 3383-3389). IEEE.

[12] Salehi, S. A., Razzaque, M. A., Naraei, P., & Farrokhtala, A. (2013, July). Detection of sinkhole attack in wireless sensor networks. In 2013 IEEE international conference on space science and communication (IconSpace) (pp. 361-365). IEEE.

[13] Stafrace, S.K. and Antonopoulos, N. (2009) Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks. Comput. Commun., 38, 619–638.

[14] Sheela, D., Kumar, C.N. and Mahadevan, G. (2011) A non Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks. Proc. IEEE Int. Conf. Recent Trends in Information Technology (ICRTIT), Chennai, Tamil Nadu, pp. 527–532.

[15] Sutagundar, A.V. and Manvi, S.S. (2013) Location aware event driven multipath routing in wireless sensor networks: agent based approach. Egypt. Inf. J., 14, 55–65.

[16] Karlof, C. and Wagner, D. (2003) Secure routing in wireless sensor networks: attacks and countermeasures. Ad hoc Netw., 1, 293–315.

[17] Ren, F., Zhang, J., He, T. and Das, S.K. (2011) EBRP: energy-balanced routing protocol for data gathing in wireless sensor networks. TEEE Trans. Parallel Distrib. Syst., 22, 2108–2125.

[18] Perkins, C.E., Das, S.R. and Royer, E. (2000)Ad-Hoc on Demand DistanceVector routing (AODV). Mobile Computing Systems and Applications, New Orleans, LA, pp. 90–100.

[19] Chen, L. and Leneutre, J. (2009)Onmultipath routing in multihop wireless networks: security performance and their tradeoff. EURASIP J. Wirel. Commun. Netw., 2009, 1–13.

[20] Zhou, J., Peng, L., Deng, Y. and Lu, J. (2012) An ondemand routing protocol for improving channel use efficiency in multichannel ad hoc networks. J. Netw. Comput. Appl., 35, 1606–1614.

[21] Mohammadi, S. and Jadidoleslamy, H. (2011) A comparison of link layer attacks on wireless sensor networks. Int. J. Appl. Graph TheoryWirel. Ad Hoc Netw. Sensor Netw. (GRAPH-HOC), 3, 1–22.

[22] Challal, Y., Ouadjaout, A., Lasla, N., Bagaa, M. and Hadjidj, A. (2011) Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks. J. Netw. Comput. Appl., 34, 1380–1397.

[23] Yu, W. and Ray Liu, K.J. (2005) Attack-resistant cooperation stimulation in autonomous ad hoc networks. IEEE J. Sel. Areas Commun., 23, 2260–2271.

[24] Ding, M., Chen, D., Xing, K. and Cheng, X. (2005) Localized fault-tolerant event boundary detection in sensor networks. Proc. INFOCOM, 2, 902–913.

[25] Alrammahi, M. A. M. (2017). Increase life of Cluster Head in Wireless Sensor Network by using LEACH Protocol. International Journal of Advanced Research in Computer Science, 8(1).