RESEARCH ARTICLE OPEN ACCESS

Limited Computation Decentralized Mobile Networks Efficiency Penetrated by a Black hole.

Maghrib Abidalreda Maky Alrammahi*, Ahmed Ibrahim Turki **, Othman M.Hussein Anssari***

*, ***(ITRDC, University of Kufa, Al Najaf, Iraq)

maghrib.alramahi@uokufa.edu.iq

othman.alansari@uokufa.edu.iq

**(Department of Physics, University of Samarra, Samarra, Iraq)

ahmed.ibrahim@uosamarra.edu.iq

Abstract:

One of the most important modern wireless technology is Mobile Ad hoc Network (MANET) and this network works by linking a group of non-fixed (mobile) nodes and its design is decentralized but rather dynamic, it does not need central devices or base stations or central control so that each node is considered to be operating as a router for data and messages between nodes.

The general design of the topology in MANET networks is always changing and it is free to move randomly, one of the characteristics of the network is that it can work independently or it can be linked with external networks according to its general design. One of its most important features is that the mobile nodes in the network have low memory and energy, as well as weight, and are involved in many important industries. Because it is an open network and free to move around, this is considered one of the important negatives and suffers from serious security problems. In this paper, we will focus on the attacks and security breaches that occur in one of these important attacks is the packet drop attack that occurs on the routing protocol and we work by creating a virtual environment for the purpose of work Analyze and detect this attack for the purpose of improving the network environment.

Keywords — **MANETs, OMNeT++, Blackhole Attacks, Packet Dropping attack.**

I. INTRODUCTION

In MANET networks, the transmission and receiving operations Relies on the devices in the network are the nodes. Therefore, in the case of the two-node were inside the specified range of transmission with some of them, it is possible to communicate directly through the wireless channel, another case is that if the two nodes are not within the specified range of communication, then the neighbouring nodes and it is necessary that there will be help from the rest of the nodes to ensure communication and interconnection between these two nodes.

The concept of routing is very important in this type of network, and it is considered a mechanism that allows packets to be correctly forwarded from the nodes available in the network within the specified range of transmission. The main job of routing protocols is to direct packets to the appropriate nodes, and through the attacker, the attacker takes advantage of the packet transmission period and starts the attack process using a packet drop attack.

Routing consists of three stages, starting with path discovery, then rerouting, and finally updating the path.

1) Path discovery (Route Discovery):

Path determination is very important in the process of routing packets and maintaining data to redirect packets efficiently between the sending to receiving. The purpose of discovering the way is to determine everything the correct possibilities of the neighbouring nodes in the network and through it to create the main routing tables which are the network topology (the network topology) and

through which we can finally determine the hops from the source to the destination during the transmission of packets and determine and know the minimum packets, transport cost and power consumption from Beginning of sending to the end of receiving

2) Redirect of data (Data Forwarding):

After the first stage of the route, discovery is completed, depending on the neighboring and intermediate nodes, messages will be forwarded from sender (source) to recipient (destination) depending on the built-in paths that are in the routing tables that were previously created in the above stage.

3) Path update(Route Update):

There are cases where link paths may stop or fail. When nodes detect a link failure, they will send update packets to all nodes in notifies the other nodes in the network that there is a failure.

Finally, when the other nodes receive the notification, they will update their routing table.

Through these stages above, an attacker can exploit any of these stages and start the attack process and then penetrate the nodes. Table 1 below shows the types of attack, packet-dropping vs. routing protocols.

TABLE I

PACKET DROPPING ATTACK TYPES AGAINST ROUTING TABLE

Packet Dropping Attack Types	Route Discovery	Data Forwarding	Route Update
Back hole	×	✓	✓
Message Selective Forwarding	×	✓	×
Node Selective Forwarding	✓	✓	✓

II. OBJECTIVE OF RESEARCH

The concept of routing is considered a very important topic for sending packets and between src (source) and desc (destination) nodes in MANET networks. Due to the lack of a certain centralization and prior infrastructure of this type, the principle of operation of MANET networks is to rely on the node participant among themselves to send packets to the last destination.

The routing protocol determines the way between the two directions depending on the intermediate nodes and therefore in the event that the intermediate nodes fail due to the attack, it means the communication failure in the path and losing important information, when the connection fails, the routing will affect all other programs that are running and depending on the routing protocols that supplies services to the applications. The goal of the paper is to ensure the reliability and security of the connection and the availability of data by detecting the attack that causes connection failure and packet loss. The opponent has various objectives to launch the attack, for example launching an attack to congest the intermediate nodes, which causes the packets passing through the nodes to be dropped, Which leads to the imbalance of the entire network structure and its impact on the packet rate delivery. We need to understand the attack and the opponent's goals so that we can increase appropriate security and reduce packet loss in secure routing protocols through methods of identifying and detecting the attack and increasing network performance.

III. PACKET DROPPING ATTACK

Sometimes, the first step that begins in a packet-dropping attack is through the interference of malicious nodes during the creation of the path. The attacker exploits weaknesses in the routing protocols used in MANET networks, which depend on trust between nodes in the network. Once the path between the sender and recipient is established, malicious nodes can maliciously drop packets, causing communication to be suspended or generating false packets. There is more than one type of packet drop attack and the most important type is the black hole attack**.**

IV. DESIGN AND IMPLEMENTATION

A. Black hole attack

This type of attack works by dropping all or some of the packets that pass through the intermediate nodes through the malicious nodes. One of the types of attack that is used is the black hole attack, in which an opponent trying to take advantage of vulnerabilities in routing protocols

when it is elected by choosing the least distance path is towards the node from which you wish to penetrate the packets. Thus, the attacker can receive packets that have a direct link to their victims and use attack to bring them down. Figure 1 shows the attack of the black hole.

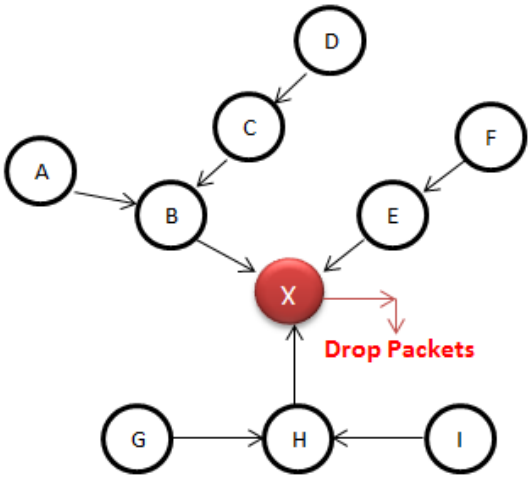

Fig. 1 Attack of blackhole

B. Simulation of Black-hole Attack Scenario

Through the use of the OMNeT++ simulation program, we find the scenario below that offers how the attack of a black hole occurs. The scenario consists of three nodes, two are normal (NA Ad hoc Mobile) and one is used to attack (NA Attacker Ad hoc Mobile) and is in the middle. The parameters of the attack are to drop packets on IP at a value of zero seconds and stop dropping when reaching 20 seconds, that is, the attacker works to drop half of the packets that pass through the malicious node. The attack can be understood seen through the simulation in Figure 2.

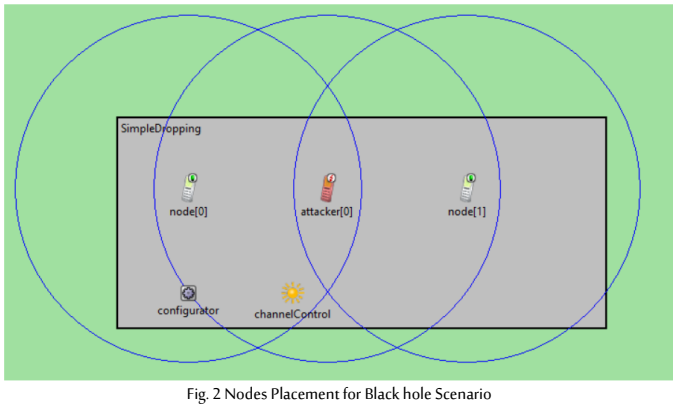

Fig. 2 Nodes Placement for Black hole Scenario

C. Methodology

To clarify the work and steps of the scenario of attack of a black hole through the flowchart below shows the complete steps from the beginning of sending packets from the source to the end of the penetration and the occurrence of packets being dropped.

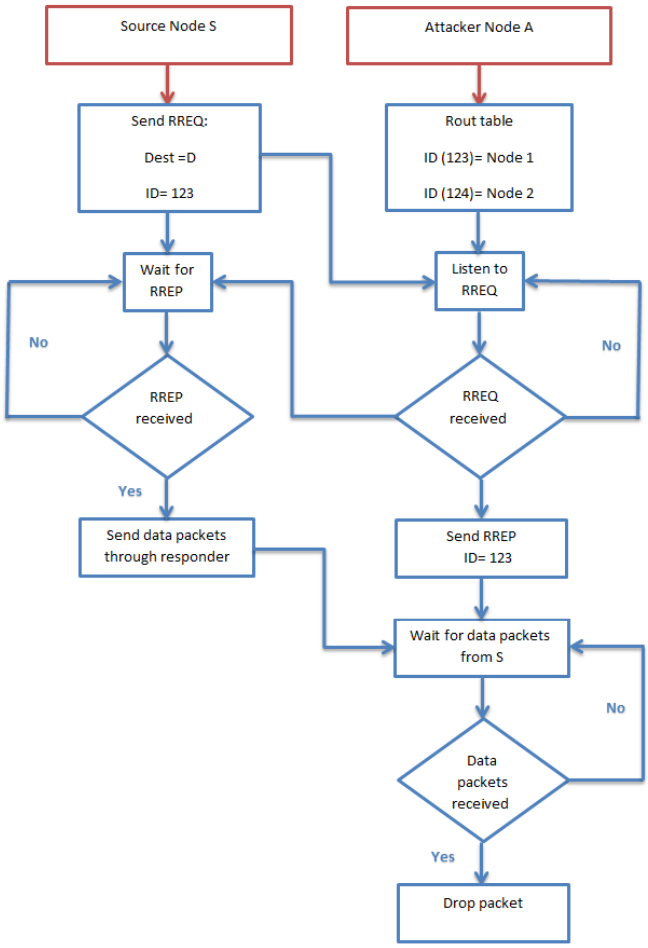

Fig 3. Black hole Attack Scenario

D. Configuration

The following index (Index 1) shows all the special settings for the simulation and all the parameters used as well as all the values and their intervals, the different types of nodes (attack nodes and mobile nodes that are represented on a mobile). In addition to the settings related to the simulation parameters, such as simulation time, and the most important thing is to determine the number of important packets that penetrate and the preparation of messages that are dropped from the attacker's pocket, which is half the number.

Configuration file

```
network = SimpleDropping
sim-time-limit = 200s
description = "Simple IPv4 dropping"
**.constraintAreaMinX = 0m
**.constraintAreaMinY = 0m
**.constraintAreaMinZ = 0m
**.constraintAreaMaxX = 700m
**.constraintAreaMaxY = 700m
**.constraintAreaMaxZ = 0m
**.debug = true
**.coreDebug = true
*.numHosts = 2
*.numDroppers = 1

Parameters for the Attack (IPv4 Dropping)
IPv4 DROPPING ATTACK
**.attacker*.droppingAttack.active = true
**.attacker*.droppingAttack.startTime = 0s
**.attacker*.droppingAttack.endTime = 200s
**.attacker*.droppingAttack.droppingAttackProbability = 0.5

Parameters for the APP (UDP Layer)
**.node[0].numUdpApps = 1
**.node[0].udpApp[0].typename = "UDPBasicApp"
**.udpApp[0].startTime = 1s
**.udpApp[0].stopTime = 200s
**.udpApp[0].destAddresses = "node[1]"
**.udpApp[0].localPort = 1234
**.udpApp[0].destPort = 1234
**.udpApp[0].messageLength = 512B
**.udpApp[0].sendInterval = 0.5s + uniform(-0.001s,0.001s)
**.node[1].numUdpApps = 1
**.node[1].udpApp[0].typename = "UDPSink"

Parameters for the MANET Routing Layer
**.routingProtocol = "AODVUU"
**.llfeedback = true        **.local_repair = true
**.wait_on_reboot = 0

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
```

Parameters for the Mobility

**.mobilityType = "StationaryMobility"

**.mobility.initFromDisplayString = false

**.node[0].mobility.initialX = 100m

**.node[0].mobility.initialY = 100m

**.attacker*.mobility.initialX = 300m

**.attacker*.mobility.initialY = 100m

**.node[1].mobility.initialX = 500m

**.node[1].mobility.initialY = 100m

Index 1: Simulation configurations.

V. EXPERIMENTAL RESULT

By applying all the presets in the simulation, implementing parameters, and completing the design of the network, which consists of three main nodes, two normal nodes (NA Ad hoc Mobile) and one malicious node (NA Attacker Ad hoc Mobile). The scenario is that half of the packets will be dropped through the malicious middle nodes through which they will pass., after implementing it in the simulation, we will get the final results shown in Table 2.

TABLE II

NUMBER OF DROPS PACKETS ON NETWORK PERFORMANCE

	Attacker	Node[0]	Node[1]
Sent Packets	**187**	**398**	**0**
Received Packets	**398**	**1**	**186**
Dropped Packets	**212**	**0**	**0**

VI. CONCLUSION AND FUTURE WORKS

Depending on the weaknesses in the routing protocols and the attack method, in addition to the type of network environment (fixed or mobile) and knowing the final preparation for the sum of the nodes in the MANET networks, we note that there are different types of attack that can be applied to the MANET networks and the work of penetration on the nodes and through the use of simulation on a small network and analysis for the network, it is now possible to identify one of the types of attack, which is an attack of a black hole.

Future proposals are increasing the protection of the routing protocols through the use of more complex encryption keys to increase the degree of difficulty for the attacker to penetrate. It is possible to improve the proprietary protocols in the MANET networks to reduce or prevent the penetration of nodes.

REFERENCES

[1] Abdel-Fattah, F., Farhan, K. A., Al-Tarawneh, F. H., & AlTamimi, F. (2019, April). Security challenges and attacks in dynamic mobile ad hoc networks MANETs. In 2019 IEEE jordan international joint conference on electrical engineering and information technology (JEEIT) (pp. 28-33). IEEE.

[2] 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).

[3] Poongodi, T., Khan, M. S., Patan, R., Gandomi, A. H., & Balusamy, B. (2019). Robust defense scheme against selective drop attack in wireless ad hoc networks. IEEE access, 7, 18409-18419.

[4] Boulaiche, M. (2020). Survey of secure routing protocols for wireless ad hoc networks. Wireless Personal Communications, 114(1), 483-517.

[5] Liu, G., Yan, Z., & Pedrycz, W. (2018). Data collection for attack detection and security measurement in mobile ad hoc networks: A survey. Journal of Network and Computer Applications, 105, 105-122.

[6] Karthigha, M., Latha, L., & Sripriyan, K. (2020, February). A comprehensive survey of routing attacks in wireless mobile ad hoc networks. In 2020 International Conference on Inventive Computation Technologies (ICICT) (pp. 396-402). IEEE.

[7] Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K. (2020). A survey on intrusion detection and prevention in

wireless ad-hoc networks. Journal of Systems Architecture, 105, 101701.

[8] Thamilarasu, G., & Sridhar, R. (2012). A cross-layer game for energy-efficient jamming detection in ad hoc networks. Security and Communication Networks, 5(4), 364-373.

[9] Poongothai, T., & Jayarajan, K. (2008, December). A noncooperative game approach for intrusion detection in mobile adhoc networks. In 2008 International Conference on Computing, Communication and Networking (pp. 1-4). IEEE.

[10] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. IEEE Communications magazine, 40(10), 70-75.

[11] Balakrishnan, V., & Varadharajan, V. (2005, April). Packet drop attack: A serious threat to operational mobile ad hoc networks. In Proceedings of the international conference on networks and communication systems (NCS 2005), Krabi (pp. 89-95).

[12] Peng, M., Shi, W., Corriveau, J. P., Pazzi, R., & Wang, Y. (2016). Black hole search in computer networks: State-of-the-art, challenges and future directions. Journal of Parallel and Distributed Computing, 88, 1-15.

[13] Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2014). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE systems journal, 9(1), 65-75.

[14] Fahad, A. M., Ahmed, A. A., Alghushami, A. H., & Alani, S. (2018, October). Detection of black hole attacks in mobile ad hoc networks via hsa-cbds method. In International conference on intelligent computing & optimization (pp. 46-55). Springer, Cham.

[15] Razzak, F. (2012). Spamming the Internet of Things: A Possibility and its probable Solution. Procedia computer science, 10, 658-665.

[16] Xia, H., Jia, Z., Li, X., Ju, L., & Sha, E. H. M. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Networks, 11(7), 2096-2114.

[17] Yu, Y., Guo, L., Wang, X., & Liu, C. (2010). Routing security scheme based on reputation evaluation in hierarchical ad hoc networks. Computer Networks, 54(9), 1460-1469.

[18] Khan, A., Suzuki, T., Kobayashi, M., Takita, W., & Yamazaki, K. (2008). Packet size based routing for stable data delivery in mobile ad-hoc networks. IEICE transactions on communications, 91(7), 2244-2254.

[19] Komninos, N., Vergados, D., & Douligeris, C. (2007). Detecting unauthorized and compromised nodes in mobile ad hoc networks. Ad Hoc Networks, 5(3), 289-298.

[20] Nadeem, A., & Howarth, M. P. (2014). An intrusion detection & adaptive response mechanism for MANETs. Ad Hoc Networks, 13, 368-380.

[21] Zhong, D., Lv, H., Han, J., & Wei, Q. (2014). A practical application combining wireless sensor networks and internet of things: safety management system for tower crane groups. Sensors, 14(8), 13794-13814.

[22] Doshi, C. K., Sankaranarayanan, S., Lakshman, V. B., & Chandrasekaran, K. (2017). Game theoretic modeling of gray hole attacks in wireless ad hoc networks. In Proceedings of the International Conference on Signal, Networks, Computing, and Systems (pp. 217-226). Springer, New Delhi.

[23] Ode, R. N., Perdana, D., & Sari, R. F. (2017). Performance evaluation of aodv, aodv-uu, and aodv with malicious attack mode on vehicular ad-hoc network. Advanced Science Letters, 23(5), 3990-3994.

[24] Kebir, Z., Omari, M., & Soulimani, H. (2017). Mobile adhoc network protocols simulation: Distance vector vs source routing comparison. Wireless Netw., 6(2), 25-34.

[25] Yildiz, H. U., Bicakci, K., Tavli, B., Gultekin, H., & Incebacak, D. (2016). Maximizing Wireless Sensor Network lifetime by communication/computation energy optimization of non-repudiation security service: Node level versus network level strategies. Ad Hoc Networks, 37, 301-323.

[26] Baadache, A., & Belmehdi, A. (2012). Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. Journal of

Network and Computer Applications, 35(3), 1130-1139.
[27] Nakayama, H., Kurosawa, S., Jamalipour, A., Nemoto, Y., & Kato, N. (2008). A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. IEEE transactions on vehicular technology, 58(5), 2471-2481.
[28] Von Mulert, J., Welch, I., & Seah, W. K. (2012). Security threats and solutions in MANETs: A case study using AODV and SAODV. Journal of network and computer applications, 35(4), 1249-1259.
[29] Krco, S., & Dupcinov, M. (2003). Improved neighbor detection algorithm for AODV routing protocol. IEEE Communications Letters, 7(12), 584-586.
[30] Lacuesta, R., Lloret, J., Garcia, M., & Penalver, L. (2012). A secure protocol for spontaneous wireless ad hoc networks creation. IEEE Transactions on Parallel and Distributed Systems, 24(4), 629-641.