ISSN 2354-0575

IMPLEMENTATION OF BLACK HOLE ATTACK ON AODV ROUTING PROTOCOLS IN MANET USING NS2

Nguyen Duy Tan, Le Trung Hieu, Luu Van Tan
Hung Yen University of Technology and Education

Received: 01/12/2019
Revised: 11/3/2020
Accepted for publication: 22/3/2020

Abstract:

One of the major challenges of Mobile Ad hoc Network (MANETs) is how to implement and avoid of different kind of security attack such as Denial of service (DoS), wormhole, replay, masquerade, black hole etc. MANETs use routing protocol to communicate the data packet from one node to another and each node acts as a host or router, which can choose suitable paths for transmission of packet. AODV is one of the most popular used routing protocols in ad-hoc networks, but it also has a lot of potential lack of security. The goal of attacks is usually to disrupt the operation of the network or to affect the network performance. In this paper, we implement and analyses performance of multiple black hole attack nodes simultaneously in AODV routing protocol in terms of throughput, energy efficiency and data packet delivery. Our simulation results show that the more attackable nodes in network simultaneously, the lower the energy efficiency and network performance.

Keywords: *Security threats, Routing Protocols, AODV, MANET, Black hole attack, Network Simulator.*

I. Introduction

Mobile Ad hoc Networks (MANETs) consist of several nodes that can organize by themselves without infrastructure (access point, etc.) networks. In MANETs, the nodes work as a router to forward data in the network and communicate each other by propagating radio waves in individual nodes. Hence, MANET vulnerable to many attacks such as Grey hole attack, Black hole attack, Sybil attack, Daniel of services etc [1]. Black hole attack is one of the most dangerous in network layer attack, which attracts traffic towards it and drops all the packets. This problem makes performance degradation of the network to greater or the energy of node is exhausted quickly. The most decreasing of performance of network is many attackable nodes simultaneously, which is called as collaborative attack. Many routing protocols in MANET are used to select best path for data transmission and maintain working in MANET, but most of it is lack of security. Therefore, it makes MANET vulnerable to black hole and collaborative black hole attacks. There are many researchers have also assessed the impact of attacks that reduce performance of working in MANET network throughout routing protocols such as Garima Neekhra et al [2] is introduced some of the comparison between gray hole attack with performance decreases from 30 to 40% in AODV routing protocol. K.Madhuri et al [3] analyze the effect of black hole attack for various network parameters like packet delivery ratio, dropped packets or throughput using AODV to find path for data packets. Kriti Chadha and Sushma Jain [4] show the effects of black hole attack on using AODV protocol based on various performance metrics such as throughput, packet drop ratio, normalized routing load and number of dropped packets and pause time with changing the number of nodes. However, none of the above improvements consider using the energy efficiency of nodes in MANET. This is an important problem because in many cases, devices in MANET must use batteries in turning on for disaster area, where is not electric resource to support for rescuing of the aftermath.

In this paper, we focus on the implementing and performance evaluation of the AODV routing protocols to help the development of security schemes in MANET. Our simulation results show that the energy consumption of AODV with black hole attack network consumes energy less and the more black hole attack nodes in MANET, the lower the energy efficiency in case of large network (50 nodes deployed in 1000 m × 1000 m area). Besides the energy consumption of nodes, throughput, packet drop ratio is also presented in comparison with our results in AODV protocol.

II. Protocols Description

In this section, we briefly describe the AODV protocols, black hole attack, and implementing solution for the black hole attack in AODV protocol, which are used in our analysis.

A. AODV Routing Protocol

Ad Hoc On-Demand Distance Vector (AODV) is an on demand routing protocol which is used to discovery and store route between the source and destination node and consist of two stages:

Route discovery stage:

At the source node S (as shown in Figure 1), when it needs a route to send data to destination D, first it finds this in the routing table, if there is a good enough, it will use this route, otherwise, it will broadcast of RREQ to its neighbors (A and B) specified for certain destination D. An intermediate node receives RREQ message, it will check its routing table for route to destination. If it found, it will send RREP message through the reverse route path, which is established by RREQ, towards the source and it ignores this RREQ message if it is processed already. Otherwise, the intermediate node will update its routing table for a fresh route toward source node and send RREQ message to these neighbors, this process is repeated until the RREQ message is received by the destination node D [5].

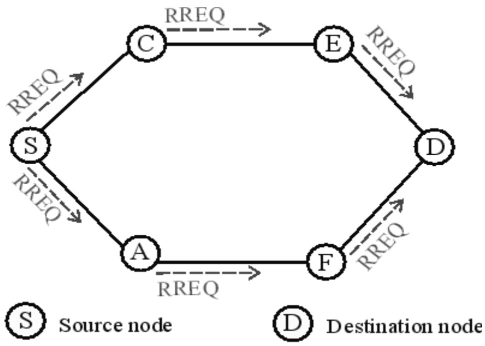


Figure 1: Broadcasting of RREQ message

At destination D, after receiving RREQ message, it will send RREP message to source D by unicast the single reverse path as shown in Fingure 2. When the source S received several RREP, it will choose the best path that whose destination's sequence number is the highest, but if there are several RREP in which destination's sequence numbers of are equal, that of which the smallest counter will be selected.

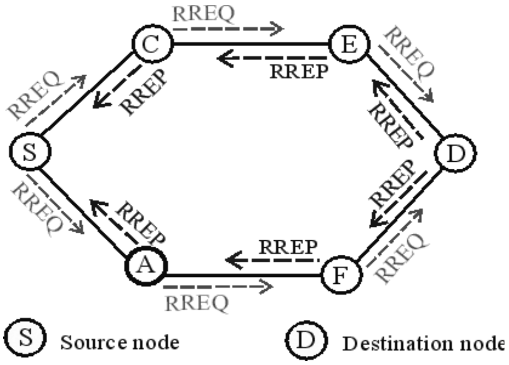


Figure 2: Sending of RRER message

Route Maintenance Stage:

In this stage, all nodes in network will broadcast a HELLO message periodically to inform its working state and receive it from all active neighbors. If node does not receive HELLO message from a neighbor, then it will notify the source with an RERR packet and entire routes based on the node is invalidated. Sources can recovery a new route by performing route discovery stage or drop node in its routing table.

Messages in AODV:

There are four control messages which are used by AODV described as below:

Routing Request (RREQ): This message is used whenever the source node need discovery the better route to the destination for data transmission.

Src_ address	Src_ sequence	Broad_ cast_ID	Dest_ address	Dest_ sequence	Hop count

Figure 3: Format of RREQ message

Routing Reply (RREP): used by node, if it is the destination, or has a fresh route enough to the destination, at that time it will unicast route reply message (RREP) back to the source, which has following format.

Src_ address	Src_ sequence	Broad_ cast_ID	Dest_ address	Dest_ sequence	Hop count

Figure 4: Format of RREP message

Route Error Message (RERR): All nodes monitor their own neighborhood and broadcast this message whenever it detects a broken link with adjacent neighbor due to out of network or mobility. RERR has format as shown in Figure 3.

Unreachable Dest_address	Unreachable Dest_seq_number	Dest_ count

Figure 5: Format of RERR message

HELLO Messages: All nodes keep on the connectivity between their own neighborhoods by broadcasting HELLO messages, which indicate the working of node in network.

B. Black Hole Attack

A black hole attack in which a black hole node will refuse to forward data packets to the following node in the route connected between source and destination. In order to process its attacks, the black hole node fakes that it has fresh enough routes for data transmission to all destinations requested by all the source nodes and absorbs the network traffic. In Figure 6, by using the routing AODV protocol, when the source node S broadcasts the RREQ message for finding any paths to the destination D, the black hole node immediately responds with an RREP message that it includes path with the highest sequence number. This message is seen as if it is sending from the destination or a node which has a fresh enough route to the destination. After black hole node assumes that the destination is behind it by sending RREP with a single path, it discards the other RREP packets coming from other nodes.

When the source received the RREP, which is transmitted by black hole node, it starts to send out its data packets to the black hole with trusting that these packets can reach the destination D but black hole node will discard all data packet here. In Figure 6, node B is a black hole node and as a result, all the data packets through node B are simply consumed or lost and this process make the performance will be decreased or lack of energy. Node B could be said that it is a form of destruction in the network, and we call it as the black hole attack node [6, 7].

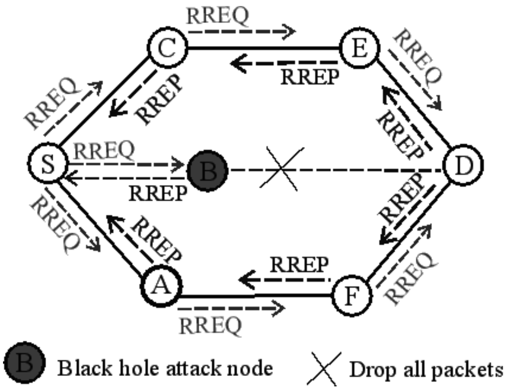


Figure 6: A single black hole attack in MANET

C. Implementing code for Black Hole Attack in AODV Protocol

To implement code for black hole attack in AODV routing protocol, we use NS2 (Network Simulator) version 2.35 with steps bellow:

Step 1: Create "blackholeAODV" base on AODV routing protocol in "ns-allinone-2.35/ns-2.35" directory as shown in Figure 7, we change all file in "aodv" directory by "blackholeaodv" such as "aodv.cc" by "blackholeaodv.cc", "aodv.h" by "blackholeaodv", etc.

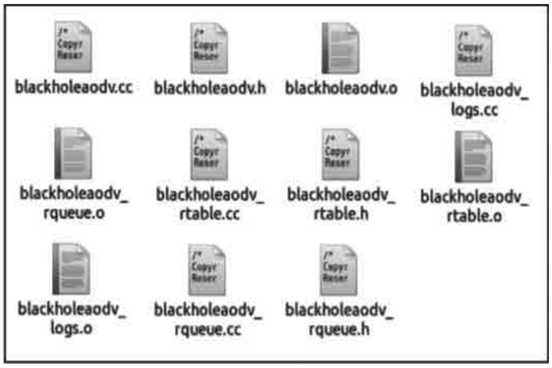
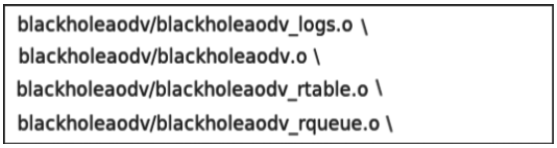


Figure 7: Creating the "blackholeAODV" base on AODV routing protocol.

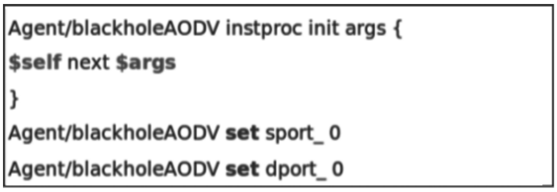
Step 2: Change in the "\makefile", which is in ns-2.35 with the lines as shown in Figure 8.



```
blackholeaodv/blackholeaodv_logs.o \
blackholeaodv/blackholeaodv.o \
blackholeaodv/blackholeaodv_rtable.o \
blackholeaodv/blackholeaodv_rqueue.o \
```

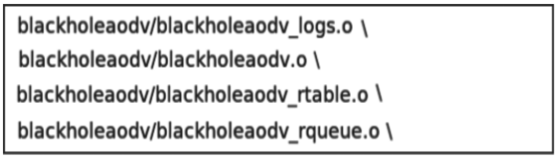
Figure 8. Adding in the "\makefile" at the "ns2.35" directory.

Step 3: Initialize in the “ns-agent.tcl” and “ns-mobilenode.tcl” file, which is in ns-2.35/tcl/lib with the lines as shown in Figure 9 and Figure 10.



```
Agent/blackholeAODV instproc init args {
$self next $args
}
Agent/blackholeAODV set sport_ 0
Agent/blackholeAODV set dport_ 0
```

Figure 9. Adding in the agent for “blackholeAODV” agent



```
blackholeaodv/blackholeaodv_logs.o \
blackholeaodv/blackholeaodv.o \
blackholeaodv/blackholeaodv_rtable.o \
blackholeaodv/blackholeaodv_rqueue.o \
```

Figure 10. Adding “blackholeAODV” for processing at nodes

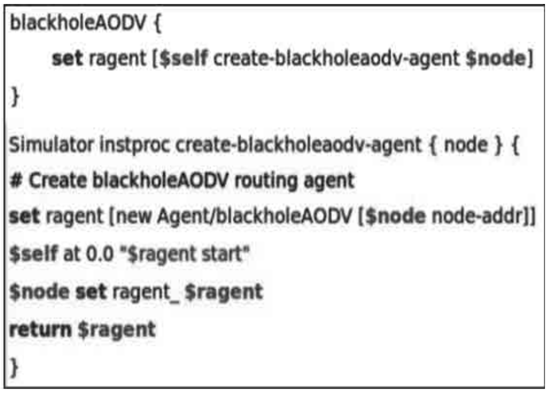
Step 4: Add “blackholeAODV” routing agent in “tcl\lib\ns-lib.tcl” file with some lines where protocol agents are coded that is presented in Figure 11.

Step 5: In “blackholeAODV.cc” file, we added “recvReply()” function with the lines to receive all the first RREQ message to set a black hole attack that is in Figure 12.

Step 6: Run the command to compile in the terminal window of linux.

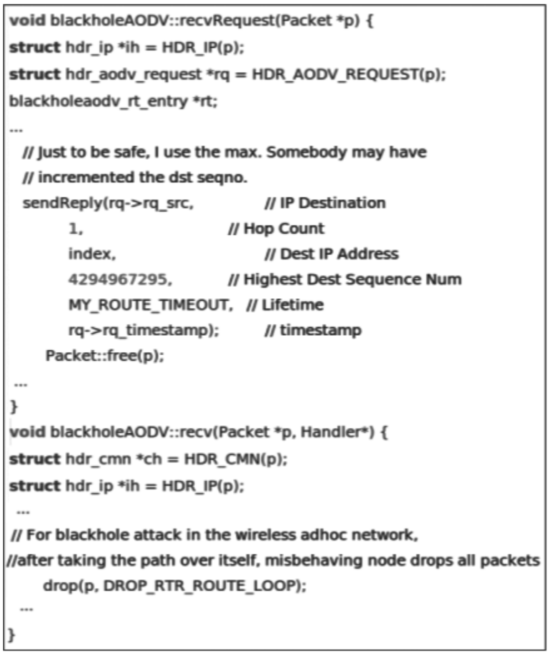
```
make clean
make
```

Step 7: The end.



```
blackholeAODV {
      set ragent [$self create-blackholeaodv-agent $node]
}
Simulator instproc create-blackholeaodv-agent { node } {
# Create blackholeAODV routing agent
set ragent [new Agent/blackholeAODV [$node node-addr]]
$self at 0.0 "$ragent start"
$node set ragent_ $ragent
return $ragent
}
```

Figure 11. Adding “blackholeAODV” protocol agen in the “tcl\lib\ns-tcl.tcl” file.



```
void blackholeAODV::recvRequest(Packet *p) {
struct hdr_ip *ih = HDR_IP(p);
struct hdr_aodv_request *rq = HDR_AODV_REQUEST(p);
blackholeaodv_rt_entry *rt;
...
  // Just to be safe, I use the max. Somebody may have
  // incremented the dst seqno.
  sendReply(rq->rq_src,            // IP Destination
        1,                     // Hop Count
        index,                     // Dest IP Address
        4294967295,            // Highest Dest Sequence Num
        MY_ROUTE_TIMEOUT,  // Lifetime
        rq->rq_timestamp);         // timestamp
     Packet::free(p);
...
}
void blackholeAODV::recv(Packet *p, Handler*) {
struct hdr_cmn *ch = HDR_CMN(p);
struct hdr_ip *ih = HDR_IP(p);
 ...
// For blackhole attack in the wireless adhoc network,
//after taking the path over itself, misbehaving node drops all packets
     drop(p, DROP_RTR_ROUTE_LOOP);
 ...
}
```

Figure 12. Adding RREP replying and install black hole attack mechanism in “blackholeAODV” protocol.

D. Simulation Parameters

To evaluate the performance of routing protocols affect of multiply black hole attacks, we use the network simulator ns-2 (v.2.35) [8, 9] to simulate the network coverage is about 1000 square meters with the parameters in the scenarios that are described in Table I, [10].

Table I: The Arrangement of Channels

Parameters	Values
Topology area	1000 m × 1000 m
Numbers of nodes	10, 20, 30, 40, 50
Antenna type	Omni Antenna
Routing protocol	AODV, blackholeAODV
Packet size	512 bytes
Simulation time	500 seconds
Transmission range (m)	250
Traffic type	CBR, TCP
Data rate	10 (kbps)
Initial energy	5 (Joules)
Idle power	712e-6 (Watt)
Receiving power	0.3 (Watt)
Transmission power	0.6 (Watt)
Sleep power	144e-9 (Watt)

E. Performance Metrics

1) Throughput:

Throughput express the total count of data packets transported to destination nodes of one flow (connection) in network during the simulation time [8, 9].

The average throughput of the entire network expresses the average throughput of each connection. The average throughput of each connection is calculated by the total size of received packets at destination node per the time, which takes for traffic to flow through the connection.

$$\text{Throughput\_of\_ flow}_{\text{j}} = \frac{\sum_{i=1}^{m} Ps_i * 8}{t_2 - t_1} \quad (bps) \qquad (3)$$

$$\text{Throughput\_of\_ network} = \sum_{\text{j}=1}^{\text{k}} (\text{Throughput\_of\_ flow})_j \qquad (4)$$

where Ps_{i} is the size of length of the i^{th} packet reaching the destination, t_1 and t_2 are the time when first packet sent by source node and the time when last packets received by destination node, respectively.

2) Energy Efficiency:

Energy efficiency is defined as the throughput achieved per unit of energy consumed, where the throughput represents the number of successfully delivered packets.

$$Energy\_efficiency = \frac{Throughput(packets)}{Energy\_consumption(Joules)} \qquad (5)$$

3) Packet Delivery Ratio (PDR):

PDR represents the ratio of data packets successfully received from all the sent data packets, which is computed as below:

$$PDR = \frac{Nr}{Ns} \qquad (6)$$

Where Nr and Ns are the number of data packets received by destination node and the number of data packet sent by source node, respectively.

4) Packet Loss Ratio (PLR):

This measure represents the ratio of number packets dropped by nodes due to various reasons, the lower value of the packet lost means that the better performance of the protocol. PLR is computed as below:

$$PLR = \frac{Ns - Nr}{Ns} \qquad (6)$$

III. Results and Analysis

As illustrated in Figure 13 and 14, the average throughput of AODV routing protocols is analyzed in two scenarios with multiply black hole attack nodes. We can see that if there are many black hole attack nodes in network, the average throughput will decrease quickly.

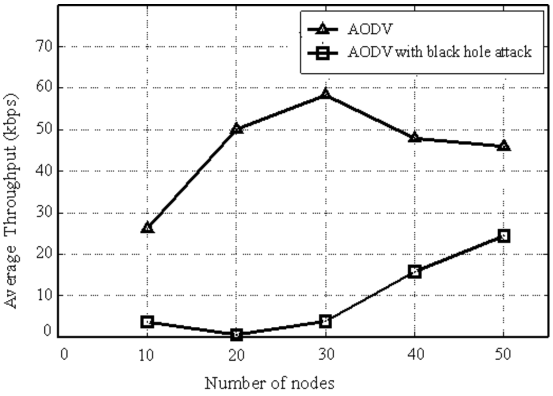


Figure. 13. The average throughput

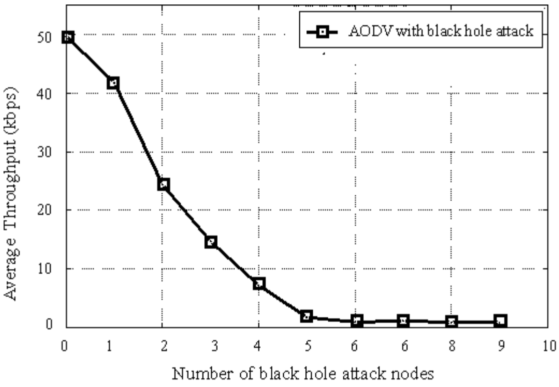


Figure. 14. The average throughput

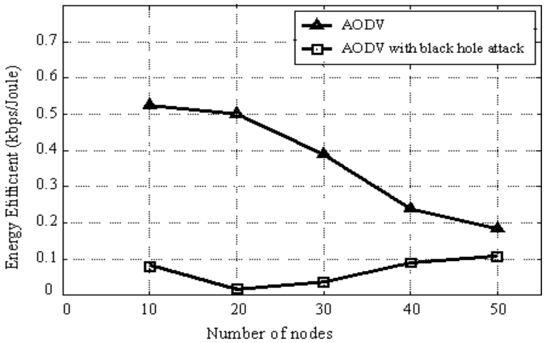


Figure. 15. Energy efficiency

As illustrated in Figure 15 and 16, the energy efficiency of AODV protocol is analyzed in two scenarios with increased number of nodes. We can see that the energy efficiency of network with impact of black hole attack nodes in dropping the packets to reduce the received packets is obvious. In addition, in network with the more black hole attack nodes, the worse energy efficiency achieve.

In Figure 17 and 18, we illustrate the packet delivery ratio for AODV routing protocols in the number of black hole attack nodes. Based on results shown in Figure 17 and 18, we can obviously observe that if there is not black hole attack in the network, the packet delivery ratio is higher than about 40% compared to the same protocols.

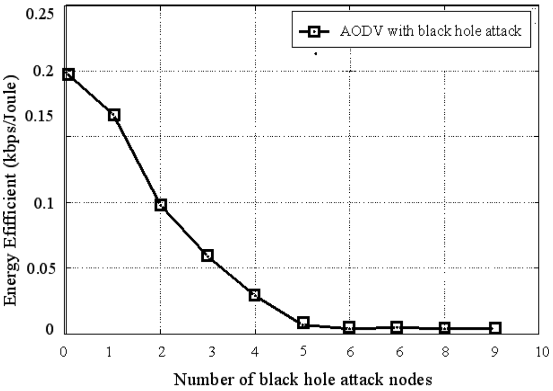


Figure. 16. Energy efficiency

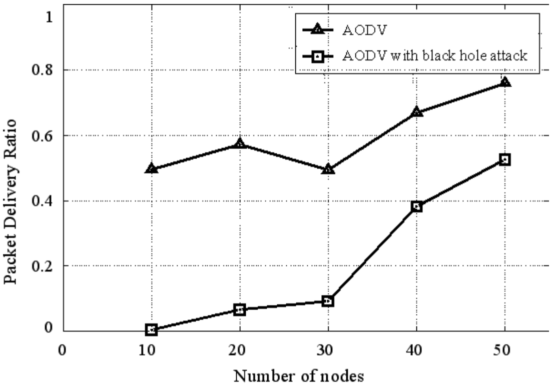


Figure. 17. Packet delivery ratio

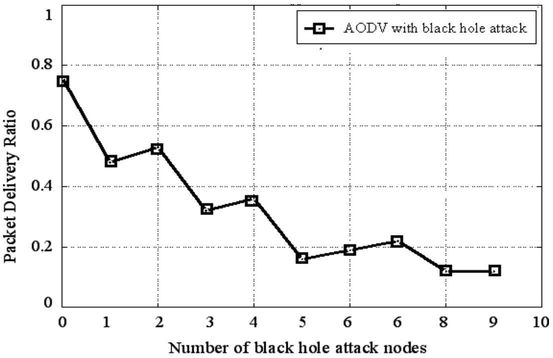


Figure. 18. Packet delivery ratio

The percentage of packet loss in different two scenarios are illustrated in Figures 19 and 20 in which in network with black hole attack nodes have packet loss ratio more than original AODV protocol and the more black hole attack nodes, the more packet loss ratio in the same protocol.

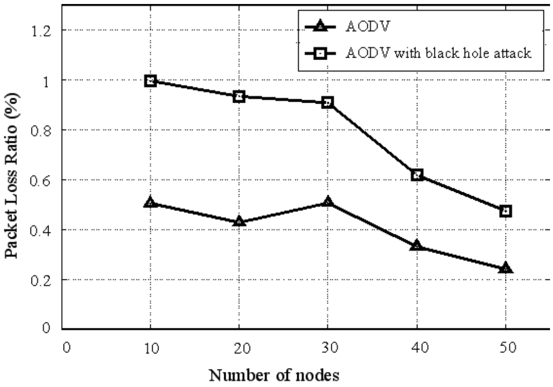


Figure. 19. Energy consumption in several states with IEEE 802.11 MAC

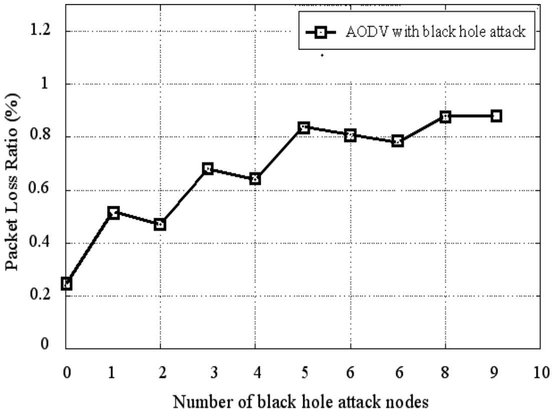


Figure. 20. Energy consumption in several states with S-MAC

IV. Conclusion

In this paper, we analyzed the energy consumption of nodes in MANET with implementing black hole attack with AODV routing protocols. Our goal is to implement and evaluate impact of black hole attack to performance in AODV routing protocol, which helps the development of security schemes in MANET. Our simulation results show that the more black hole attack nodes in network, the lower performance in case of large network (50 nodes deployed in 1000 m × 1000 m area).

References

[1]. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", *Human-centric Computing and Information Sciences*, **vol 1,** pp. 1-16, 2011.

[2]. Garima Neekhra, Sharda Patel, Ashok Verma, Ashish Chaurasia, "Effect Of Grayhole Attack With Ids Technique For Aodv Routing Protocol Using Network Simulator", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, **vol 3**, pp. 4184- 4190, December 2014.

[3]. K.Madhuri, N.Kasi Viswanath, P.Usha Gayatri, "Performance Evaluation of AODV under Black Hole Attack in MANET using NS2", *International Conference on ICT in Business Industry Government (ICTBIG)*, pp. 1-3, November 2016.

[4]. Kriti Chadha and Sushma Jain, "Impact Of Black Hole And Gray Hole Attack In AODV Protocol", *IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, pp. 1-7, May 2014.

[5]. Mehdi Medadian, M.H. Yektaie, A.M Rahmani, "Combat with Black Hole Attack in AODV routing protocol in MANET", *First Asian Himalayas International Conference on Internet*, pp. 1-5, November 2009.

[6]. Padmalaya Nayak, V. Bhavani and B. Lavanya, "Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN", *International Journal of Computer Applications*, **vol 116**, pp. 42-46, April 2015.

[7]. Semih Dokurer, Y. M. Erten and Can Erkin Acar, "Performance analysis of ad-hoc networks under black hole attacks", *IEEE SoutheastCon Proceedings*, pp. 148-153, March, 2007.

[8]. T.Sairam Vamsi, E.R. Praveen Kumar, T.Sruthi, "Performance Analysis of Aodv Routing Protocol in Manet under Blackhole Attack", *International Journal of Engineering Research and Applications*, **vol. 9**, pp. 58-63, May 2019.

[9]. Yatin Chauhan, Jaikaran Singh, Mukesh Tiwari, Anubhuti Khare, "Performance Evaluation of AODV based on black hole attack in ad hoc network", *Global Journal of researches in engineering Electrical and electronics engineering*, **Vol. 12**, pp. 43-47, February 2012.

[10]. VINT Project, "The network simulator - NS2," http://www.isi.edu/nsnam/ns (accessed: Sep 5, 2019), 1997.

TRIỂN KHAI TẤN CÔNG HỐ ĐEN TRÊN GIAO THỨC ĐỊNH TUYẾN AODV TRONG MẠNG MANET SỬ DỤNG NS2

Tóm tắt:

Một trong những thách thức lớn của mạng di động tùy biến (MANETs) là làm sao triển khai hệ thống an ninh tránh các loại tấn công khác nhau như tấn công từ chối dịch vụ, tấn công lỗ sâu, phát lại, tấn công lỗ xám, lỗ đen, v.v ... Mạng MANET sử dụng giao thức định tuyến để truyền thông gói dữ liệu từ nút nguồn đến nút đích và mỗi nút đóng vai trò như là máy chủ hoặc bộ định tuyến, chúng có thể chọn các tuyến đường phù hợp để truyền gói tin đến đích. AODV là một trong các giao thức định tuyến được sử dụng phổ biến nhất trong các mạng di động tùy biến, nhưng nó cũng tiềm ẩn nhiều cuộc tấn công mạng. Mục tiêu của cuộc tấn công mạng thường làm gián đoạn hoạt động của mạng hoặc ảnh hưởng đến hiệu suất mạng. Trong bài báo này, chúng tôi thực hiện triển khai và phân tích hiệu suất của nhiều nút tấn công lỗ đen đồng thời trong giao thức định tuyến AODV. Các tham số như thông lượng, hiệu quả sử dụng năng lượng và hiệu suất phân phối gói dữ liệu được phân tích và so sánh. Kết quả mô phỏng của chúng tôi cho thấy trong mạng có càng nhiều nút tấn công đồng thời, hiệu suất mạng và hiệu quả năng lượng càng thấp.

Từ khóa: *Security threats, Routing Protocols, AODV, MANET, Black hole attack, Network Simulator.*