A Study of Blackhole and Wormhole Attacks in Mobile Adhoc Networks

Tran Hoang Hai*, Nguyen Dang Toi

Hanoi University of Science and Technology, No. 1, Dai Co Viet, Hai Ba Trung, Ha Noi, Viet Nam

Received: February 24, 2020; Accepted: June 22, 2020

Abstract

In the Mobile Ad-hoc Network (MANET), there are several ways of attacking network operation bypassing fault routing information between malicious and normal nodes. It will degrade efficiency of the network so we cannot archive the purposes of the designed MANET. Since it is deployed in an open network environment with characteristics of high mobility, lack of physical security and independent management, the network is vulnerable to attacks. In related works, we have seen a lot of works focusing on single type of attacks but in our paper, we study how routing attacks work and study how we can simulate combination of blackhole and wormhole attacks. Our code will be open to community so others can use to test with its security mechanism or secure routing protocols.

Keywords: MANET, routing attacks, simulation

1. Introduction

Mobile Ad Hoc Networks (MANET) or Wireless Sensor Networks (WSNs) is a type of wireless network made up of countless mobile nodes that can communicate with each other without specialized routers like TCP/IP networks in which the nodes are both able to act as terminals or acting as routers for data communication and information transmission [1]. Due to the unique characteristics of the MANET network, there are now many routing protocols designed and dedicated to this network such as the AODV [2] (Ad-hoc On-demand Distance Vector), DSR [3] (Dynamic Source Routing), OLSR [4] (Optimized Link State Routing Protocol), etc. MANET has the ability to automatically self-configure which use a peer-to-peer connection or does not need centralized administrator to manage or control. Therefore, it is understandable that MANET is more vulnerable than other networks. There are many types of routing attacks in the MANET network, such as blackholes, wormholes, link spoofing, gray holes, link spoofing, etc. Each attack has different modes of operation and level of influence which leads to increased complexity in prevention and detection. Therefore, understanding how the network operation works and analyzes the system's performance against attacks is always the first task in the mission to protect MANET network. This article focuses on simulating combination of routing attacks that can occur on MANET or WSNs. We will show how the attack patterns are simulated and executed by modifying the AODV and AOMDV protocols in network emulator tool ns2.35. The tool is being used widely for both MANET and WSNs simulation. The methods can be re-used by the community in other routing protocols to simulate the performance of other routing protocols.

2. Related works

In MANET, an attacker can re-route network traffic, or inject itself into the path between the source and destination and thus control the network traffic flow so that the networ providers cannot receive data sensing. A number of attacks on routing of MANET have been identified and studied in security research [5-15]. One of the most common routing attacks in MANET is the blackhole attack [5-7]. In this attack, a “black” node within the network displays itself as having the shortest path to the destination node. Once the packets are drawn to the attacker, they are then dropped instead of relayed, and the communication of the MANET will be disrupted [5-6]. Performance of AODV and OLSR protocols under blackhole attack is comparative analysis in [7] but with single static blackhole. In [8], the authors propose a global reputation system that helps AODV protocol in selecting the best path to destination and also consider the situation when blackhole continuously moves.

In wormhole attacks, the attacker receives packets at one point in the network and tunnels them to another part of the network for malicious purposes. In MANET with AODV routing protocol, this attack can be done by tunneling every REQUEST to the target destination node directly. When the destination's neighboring nodes hear this REQUEST packet, they will rebroadcast that REQUEST packet in a normal operation and then discard any other REQUESTS for the same route discovery [12]. There

[*] Corresponding author: Tel.: (+84) 983020981
Email: hai.tranhoang@hust.edu.vn

is a huge work on the study of how blackhole and wormhole can manipulate the network traffic in MANET but mostly the authors focus on separate, single and static routing attack. In [13], the authors analyzed the performance of Mobile Ad-hoc Networks (MANET) under blackhole and wormhole attack separately for AODV protocol. In [14], AODV and DSDV protocols are analyzed in terms of routing overhead, packet delivery ratio, throughput and end to end delay under blackhole attacks. The authors investigated the performance of the network with single blackhole attack and collaborative blackhole attacks which assume that blackhole nodes can work in collaboration. In general, it concludes that AODV performs better than DSDV in packet delivery ratio, throughput and routing overhead but the delay of AODV is higher than DSDV.

3. Implementation of collaborative blackhole and wormhole attacks on AODV and AOMDV

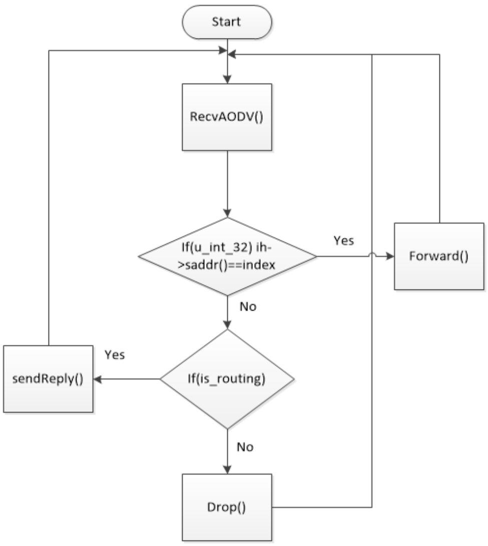

Fig. 1. Flow activity of blachole node.

The environment we illustrate using ns-2.35, a discrete event network simulator, which is very popular to simulate MANET networks [15]. AODV.h and AODV.cc is library in ns-2.35 to simulate AODV routing protocol, therefore some updates need to be modified to inject malicious nodes in the environment. We need to define a Boolean MALICIOS variable that determines whether a node is malicious or normal. Some library in ns-2 have to be modified in order to simlate blackhole attack, as we illustrate in Table 1-2. In both AODV and AOMDV routing protocols, were defined the *sendReply function* of the blackhole node. If the blackhole node calls *sendReply*, we set hop count equal to one and highest dest sequence num = 4294967295. For AOMDV, the destination node and source node will be assigned to last host and next hop. The blackhole node behavior is illustrated in Table 3-4 for AODV and AOMDV respectively.

It is difficult for us to simulate wormhole behavior, we need to update two libraries such as ll.h; ll.cc in Table 5-6 respectively. Wormhole_peer is a struct data type with 3 parameters which are ll point to a link layer; ID and the next pointer points to the second worm node in wormhole pair. We define the main attacking node in wormhole pair is *wormhole_peer_head*. *Wormhole_peer_head* is the first wormhole node received messages from the normal node and processing the packet. If the routing packet forwarded via the wormhole link are data packets, there probably more behaviors such as dropping data packets; forwarding the data packet to the destination or forwarding data packet to the destination and replicating another copy to the external nodes as malicious behavior.

Table 1. Update on AODV.cc library

- index = id;
- seqno = 2;
- bid = 1;
- LIST_INIT(&nbhead);
- LIST_INIT(&bihead);
- MALICIOUS=false;
- logtarget = 0;
- ifqueue = 0;

Table 2. Setting blackhole value for a node in AODV

```
if(strcmp(argv[1], "blackhole") == 0)
{
 Blackhole=True;
 return TCL_OK;
                  }
```

Table 3. Example of blackhole node in AODV

```
if(BLACKHOLE) seqno=rq-
>rq_src=4294967295;


   sendReply(rq->rq_src,
// IP Destination
             1,
// Hop Count
             index,
// Dest IP Address
             seqno,
// Dest Sequence Num
             MY_ROUTE_TIMEOUT,     //
Lifetime
             rq->rq_timestamp);
// timestamp

    Packet::free(p);
  }
```

Table 4. Example of blackhole node in AOMDV

```
if(BLACKHOLE) seqno=rq-> if
(BLACKHOLE) seqno=rq-
>rq_src=4294967295;


sendReply(
             rq->rq_src,
// IP Destination
             1,
// Hop Count
             index,
// (RREQ) Dest IP Address
             seqno,
// Dest Sequence Num
             MY_ROUTE_TIMEOUT,
// Lifetime
       rq->rq_timestamp,        //
timestamp
                     ih->saddr(),
// nexthop
              rq->rq_bcast_id,
// broadcast id to identify this
route discovery
                      ih->saddr());

Packet::free(p);
}
```

Table 5. Update on ll.h library

```
if(class LL;
typedef struct wormhole_peer_struct {
       LL* ll;
       int id;
       struct wormhole_peer_struct*
next;
} wormhole_peer;
```

Table 6. Update on ll.cc library

```
wormhole_head.ll = NULL;
wormhole_head.id = -1;
wormhole_head.next = NULL;;
```

Table 7. Example of establishing Wormhole link

```
else if( strcmp( argv[1], "wormhole-
peer" ) == 0 ) {
       wormhole_peer* wp =
(wormhole_peer*) malloc( sizeof(
wormhole_peer ) );
       if( !wp ) {
                          fprintf(
stderr, "(%03d) - LL::command - error
allocating memory for new wormhole
peer!" );
exit(-1);
             }
       // init fields
       wp->ll = (LL *)
TclObject::lookup( argv[2] );
       wp->id = wp->ll->mac_->addr();

       // insert at head of list
       wp->next = wormhole_head.next;
       wormhole_head.next = wp;
printf( "(%03d) - LL::command - added
%d to wormhole peer list\n", mac_-
>addr(), wp->id );
       return TCL_OK;
       }
```

Table 8. Example of wormhole behavior

```
//from here for Wormhole attack
             Scheduler& s =
Scheduler::instance();
// wormhole decision point (decide if
this packet is going throught the
wormhole or not)
             if( wormhole_head.next
) {
             if( is_broadcast ) {
             // send a copy to each
wormhole peer
             wormhole_peer *wp =
&wormhole_head;
             while( wp->next ) {
             wp = wp->next;
             Packet *p_copy = p-
>copy();
       hdr_cmn::access(p_copy)-
>direction() = hdr_cmn::UP;
       s.schedule( wp->ll, p_copy,
delay_ );
             }
;
```

4. Results

Using our proposed flow activity for blackhole attack in Figure 1, and wormhole attack in Figure 1-2, and by modifying the libraries in ns2.35, we can simulate different types of collaborative blackhole and wormhole attacks in different ways to see the impact of these attacks. In general, all properties of network operation, such as throughput, delay, packet delivery ratio etc. are much worsen by collaborative routing attacks than single type of blackhole or wormhole attack. The results in Figure 3 are network performance we collected during implementing collaborative attacks to evaluate performance of AODV and AOMDV routing protocols. More details of the performance of AODV and AOMDV routing protocols under collaborative routing attacks can be found in [16]. We also found that the location of malicious nodes is very important to the impact of these attacks. When nodes are randomly distributed, malicious nodes seem to appear in the network center which result in malicious nodes can control more incoming packets and decreasing transfer rates. Moreover, when the malicious nodes appear in the network, the number of neighbor nodes increasing leading to malicious nodes penetrating more deeply into the network. Therefore, the performance decreases significantly.

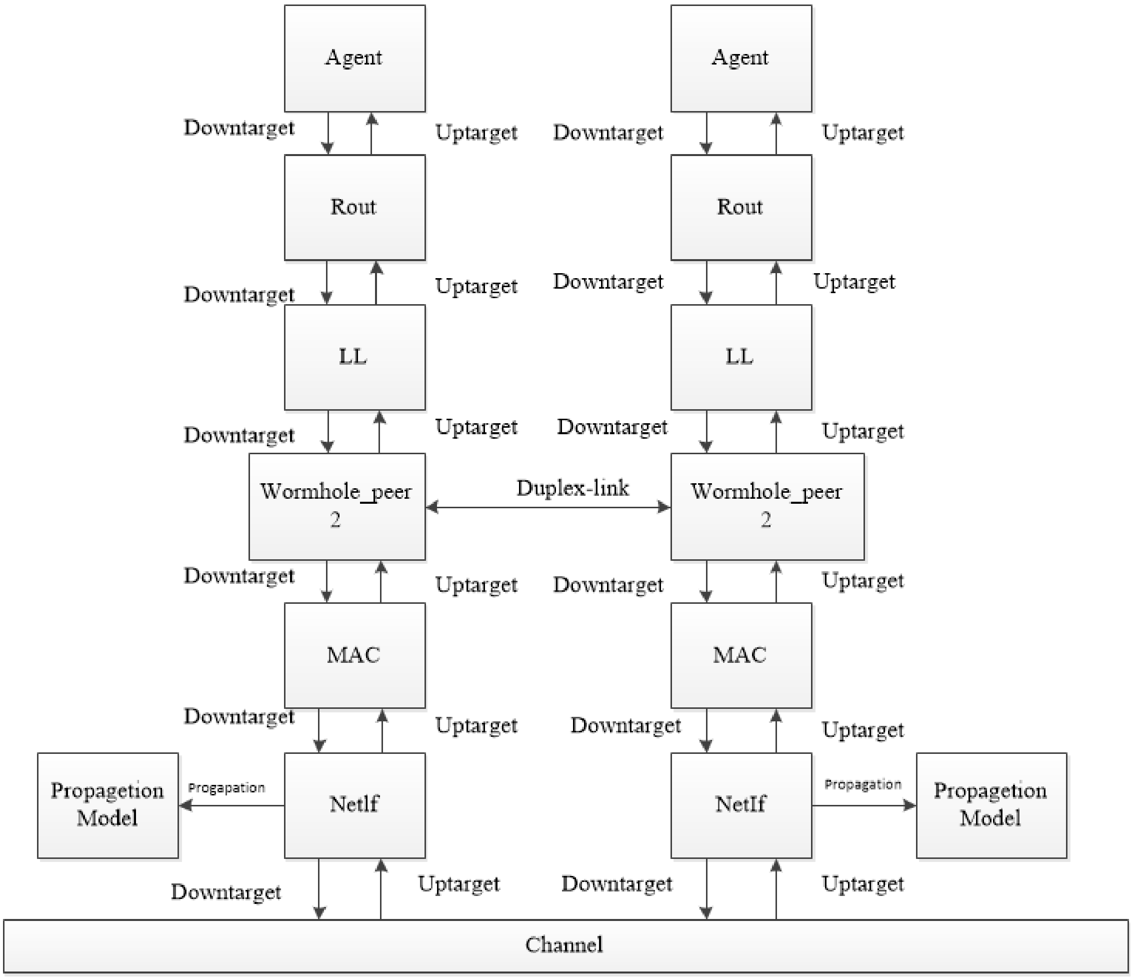

Fig. 2. Flow activity of wormhole nodes.

Protocol	NN	nonattack			2blackhole			2blackhole+1wormhole		
		raito	e2e	t_put	raito	e2e	t_put	raito	e2e	t_put
AODV	50	30.047	264.96	153.926	15.7	271.3	80.42	16.4	179.318	83.973
	80	41.921	610.27	184.834	17.783	106.45	91.345	10.738	150.13	59.958
	100	30.88	899.7	158.383	12.585	364.5	64.535	13.832	211.7	56.614
	120	34.54	645.136	177.432	37.136	688.96	180.282	14.866	245.706	76.179
AOMDV	50	34.023	1101.23	174.304	21.556	725.9	110.86	14.959	446.8	91.45
	80	27.766	1954.098	176.579	27.51	532.4	140.965	13.251	68.229	694.27
	100	46.694	1299.886	213.996	19.644	760.43	101.312	16.376	317.55	78.18
	120	41.058	1491.32	227.875	16.741	1102.426	85.78	13.321	361.429	69.099

Fig. 3. Results of collaborative attacks on AODV and AOMDV of 50-80-100-120 nodes respectively.

5. Conclusion

In this paper, we study how to simulate blackhole and wormhole attacks in collaborative ways. This methodology is very important and the first work to illustrate those attacks in algorithmic design so others can re-use easily which is very important to evluate the performance and security of MANET. Moreover, we also found that the collaborative attacks are more vulnerable than single-type of attack in simulation results with different network scenarios.

Acknowledgments

This research is funded by Hanoi University of Science and Technology (HUST) under grant number T2017-PC-079.

References

[1] Raja, M.L. and Baboo, C.D.S.S. (2014) An Overview of MANET: Applications, Attacks and Challenge.

[2] Jhaveri, R.H.; Patel, N.M. (2015). Mobile Ad-hoc Networking with AODV: A Review. International Journal of Next-Generation Computing. 6 (3): 165–191.

[3] Johnson, David B.; Maltz, David A. (1996). Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing. The Kluwer International Series in Engineering and Computer Science. 353. pp. 153–181.

[4] Extensions to OSPF to Support Mobile Ad Hoc Networking, Madhavi Chandra, Abhay Roy, Mar-10. Computer Science, Volume 3, 2011.

[5] Gurung, S. & Chauhan, A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability, S. Wireless Netw (2019).

[6] Elahe Fazeldehkordi, Iraj Sadegh Amiri, Oluwatobi Ayodeji Akanbi, Chapter 2 - Literature Review, Editor(s): Elahe Fazeldehkordi, Iraj Sadegh Amiri, Oluwatobi Ayodeji Akanbi, A Study of Blackhole Attack Solutions, Syngress, 2016, Pages 7-57, ISBN 9780128053676.

[7] K.S. Praveen, H.L. Gururaj, B. Ramesh, Comparative Analysis of Blackhole Attack in Ad Hoc Network Using AODV and OLSR Protocols, Procedia Computer Science, Volume 85, 2016.

[8] Qussai M. Yaseen, Monther Aldwairi, An Enhanced AODV Protocol for Avoiding Blackholes in MANET, Procedia Computer Science, Volume 134, 2018, Pages 371-376.

[9] P. Nagrath and B. Gupta, Wormhole attacks in wireless adhoc networks and their counter measurements: A survey, 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, 2011, pp. 245-250.

[10] Farjamnia, G., Gasimov, Y. & Kazimov, Review of the Techniques Against the Wormhole Attacks on Wireless Sensor Networks, C. Wireless Pers Commun (2019) 105: 1561.

[11] Dutta N., Singh M.M. (2019) Wormhole Attack in Wireless Sensor Networks: A Critical Review. In: Mandal J., Bhattacharyya D., Auluck N. (eds) Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing, vol 702. Springer, Singapore.

[12] Raja Datta, Ningrinla Marchang, Chapter 7 - Security for Mobile Ad Hoc Networks, Editor(s): Sajal K. Das, Krishna Kant, Nan Zhang, Handbook on Securing Cyber-Physical Critical Infrastructure, Morgan Kaufmann, 2012.

[13] Kumar, Dr Mukesh. (2013). Analysis of Blackhole and Wormhole Attack using AODV Protocol. International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264) Vol.1; No. 1, June 2013 www.ijrmst.org. 44-28.

[14] A.A. Chavan, D.S. Kurule, P.U. Dere, Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Blackhole Attack, Procedia Computer Science, Volume 79, 2016.

[15] Henderson, Tom (2012-06-09), Upcoming ns-2.35 release (Mailing list). ns-235 GSoC 2015 students. Archived from the original on 2012-03-27. Retrieved 2013-05-31.

[16] Tran Hoang Hai, Nguyen Dang Toi, Eui-nam Huh (2019) Performance Evaluation of AODV and AOMDV Routing Protocols Under Collaborative Blackhole and Wormhole Attacks, Advances in Computer Science and Ubiquitous Computing. CUTE 2019, CSA 2019.