Journal of Information Systems & InformationTechnology(JISIT)
ISSN:2478-0677; Vol. 6 No.1 2021; [Pages 28- 42]

Simulation of Network Layer-Based Security Attacks in a Mobile Ad-hoc Network

Uthumansa Ahamed[1], Shantha Fernando[2]

[1] Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, University Park, Oluvil, Sri Lanka.

[2] Department of Computer Science & Engineering, Faculty of Engineering, University of Moratuwa, Moratuwa, Sri Lanka.
urmail2ahamed@gmail.com, shantha@cse.mrt.ac.lk

Abstract. The opportunistic nature of the Mobile Ad-hoc Network (MANET) helps to deploy instantly where it is needed. MANET is the best solution as a network where infrastructure networks are unavailable. The fundamental characters of these networks are the reason for the vast variety of security attacks on them. Simulators provide a better platform to conduct research, though faulty designs of simulations provide incorrect results. Therefore, the issue remains available for a valid solution. We designed the study to investigate the network layer-based security attacks. The study included a detailed information of different attack simulations. Network Simulator 2 (NS2) was used. Ad-hoc On-demand Vector (AODV) routing protocol was used for the study. The Blackhole, Grayhole, and Wormhole attacks were simulated. The impacts of these attacks on the network performance were evaluated with Packet Delivery Ratio (PDR), Average End-to-End Delay (AEED), Throughput, and Simulation Processing Time of an Intermediate node (SPTIN). The active attacks caused more damages to the network performance than passive attacks do. Moreover, the results proved that the impacts of an attack depend on the design of the attack. The incorrect design provides faulty results which lead to ill decisions. We are expecting to extend the simulation of different security attacks based on different simulators.

Keywords: Blackhole, Grayhole, Security, Simulation, Wormhole

1 Introduction

MANET is a type of Ad-hoc network [1] which is created by a set of wireless devices. These devices are called nodes which are configured themselves to form a MANET. These nodes use a limited range of wireless adapters to establish communication with one another. MANET is an outcome of the 4th generation (4G) communication standards [2]. Node mobility [1] [3] is the basic character to separate MANET from other types of Ad-hoc Networks. Infrastructure-less network nature, open network boundary, limited resources

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

are few fundamental features of a MANET [4]-[6]. These features provide some advantages and disadvantages to the network. Lower initiation cost and quick deployment help to use MANET on battlefields [7]. Moreover, MANET is easy to configure. Therefore, it is used in hostile conditions where infrastructure network services are unavailable. Usually, MANET is vulnerable to affect from different types of security threats [1] than wired networks do. Past centuries are the great evidence for the researches regarding data security in MANET, though still there is a demand for more researches on data security. Therefore, in this research study, we aim to investigate the implementation of the network layer-based security attacks into the simulator. AODV is suitable for MANET [4]. Therefore, AODV is used for the study. Blackhole and Grayhole attacks are used as the Active attack. A wormhole attack is used as a Passive attack [8].The rest of the paper is organized as follows. Section 2 discusses the related works done by the researchers. Section 3 provides a brief introduction to the network layer-based security attacks. Section 4 shows the detailed description of the simulation of the security attacks. The performances of the simulated attacks are illustrated in section 5. Finally, the conclusion and the future works are suggested in section 6.

2 Literature Review

Konate and Abdourahime [9] proposed analytical modeling to model to simulate a few security attacks including Blackhole in DSDV routing protocols. Their simulation results and the theory contradict each other. They simulated Blackhole attacks with more data packet delivery. Therefore, the Blackhole attack simulation is not accurate. Ghonge and Nimbhorkar [10] claimed that they presented the simulation of the Blackhole attack in the AODV routing protocol. The given information on their work is incomplete. Moreover, we proved in our previous work that the network performance varies based on the node mobility [5] model. Therefore, their work is incomplete. Ahmed et al, [11]investigated the performance of the AODV under Blackhole attacks. The experimental configuration is led to unclear about the influence of the single Blackhole attack. Moreover, a contradiction between figures 5 and 7 is the evidence for the poor experimental setup. Ibrahim *et al,* [12] proposed a technique to detect and remove Blackhole, Grayhole, and Cooperative Blackhole attacks. They explained the use of control packets periodically among the cluster and a bait detection mechanism in their technique, though they claimed nearly equal network overhead of the proposed technique compared to the pure AODV. Jhaveri and Patel [13] proposed a bait detection scheme to detect a Grayhole attack. The definition of the Grayhole attack was the same as the definition of the Blackhole attack [14].

Therefore, it is a solution for the Blackhole attack, not Grayhole.Panos*et al,* [15] proposed a mechanism to detect a Blackhole attacker in a MANET. The proposed solution was based on the AODV. The initial

COPYRIGHT © 2021 FACULTY OF MANAGEMENT AND COMMERCE, SOUTH EASTERN UNIVERSITY OF SRI LANKA (SEUSL), UNIVERSITY PARK, OLUVIL 32360. SRI LANKA [RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

definition of the Blackhole attack in their study has contradicted the results mentioned in figure 10. The results show 80% of PDR amount in the presence of a Blackhole attack, though they are defined as Blackhole node deny to forward data packets. Moudni*et al,* [16] presented the simulation of security attacks in AODV including the Blackhole attack. The researchers did the same mistake as others that are mentioned previously. The definition of the Blackhole attack and the results contradict. They claimed that the Blackhole node discarded all data packets that it received, though figure 6.a shows the 25% of PDR value in the presence of the Blackhole attack. Li *et al,* [17] conducted a simulation study only about the Blackhole attack. During the study, they maintained 1 to 5 connections. Therefore, the impact of a single Blackhole attack could not discover, though they claimed that they identified the impacts of a single Blackhole attack. Saad [18] proposed a simulation study to evaluate the performance in a VANET. The use of the Random Waypoint Mobility (RWMM) model in his study is proven the ill on the simulation setup. In our recent study [5], we proved that RWMM is not realistic. Moreover, RWMM is not a suitable mobility model for VANET. Yasin and Zant [19] proposed a technique to enhance AODV protocol to detect single and Cooperative Blackhole attacks. They claimed that the solution was a lightweight, though the lightweight nature did not prove. Moreover, the experimental setup was not realistic because the highest PDR value of the network in the absence of the Blackhole attack was around 18%. The packets that were reached by the destination node were 18 out of 100. The results showed a maximum of 4 packets reached by the destination out of 100 sent by the source node. The simulation time was 200 seconds. Furthermore, they failed to explain the cooperative Blackhole attack in their study. Though they claimed that the proposed solution is suitable for cooperative Blackhole attacks, it is suitable for multiple Blackhole attacks. Meddeb*et al,* [6] proposed an anomaly-based Intruder Detection System (IDS) only to detect Blackhole, Grayhole, Wormhole, and Flooding attacks. Proposed IDS was dependent on the behavioral database which was created by collecting necessary data. Moreover, the operations of the IDS were not evaluated against the network performance matrices. Furthermore, they expected to carry out further analysis in future works.

As explained above, none of the researchers are explained how they simulated the security attacks. Moreover, most results of the researches are contradicted with the theories that were defined in their works.

3 Security Attacks

Security attacks are common threats that are in different forms. These attacks are categorized mainly based on a different perspective. Common categorization was based on the vigorousness (or damage) of the attack. Mainly attacks can categorize into two: Active attacks and Passive Attacks. Active attacks directly influence the network to reduce its performance of the

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

network. Finally, in most cases network will collapse. Passive attacks show the opposite action that active attacks do. In some cases, these attacks help to enhance the quality of the network or act as normal. The attacker nodes collect information to form an active attack in the future. The main examples of active attacks were Blackhole and Grayhole attacks. A Wormhole attack is an example of a passive attack [8]. Moreover, these three attacks can be categorized as network layer-based attacks.

3.1 Blackhole Attack

Blackhole is a common attack in MANET. Mainly, it intentionally performs malicious activity. It pretended as a legitimate node and took the control of the network by providing false information [20]. Therefore, Blackhole nodes allow routing packets which are used to find a route to the destination node. Moreover, it did not allow any data packets through it. Finally, the network will collapse [17] because of the influence of the Blackhole node. Another way, these types of attacks was identified as Denial-of-Service attacks.

3.2 Grayhole Attack

Grayhole attack is an extension of the Blackhole attack. These types of attacks are not inserting false information in route discovery, though it acts gently. If a route was established through the Grayhole node then it drops the data packets. Grayhole node shows two types [14] of behaviours. Either it drops all the data packets that it receives sometimes or it drops all the data packets from a specific node in the network.

3.3 Wormhole Attack

Two nodes are involved to perform a Wormhole attack. These nodes are connected with more high-performance connection than usual connections. This connection may be either wirelessly or wired. This connection is called a Wormhole Tunnel [6] which helps to connect themselves even they are apart from each other than usual. Special hardware or software configurations are used to build and maintain the tunnel. These nodes communicate with themselves during the route selection process. Therefore, they can pretend to have a shorter path to the destination node. Then they become part of the route [3]. Being a part, they collect information needed to form an active attack [20] in the future. Wormhole attacks are difficult to detect [6].

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

4 Attacks Simulation

Three different attacks which are discussed in section III are used to simulate in this study. AODV protocol is used as the routing protocol.

4.1 Blackhole Attack

Two different functions are identified in a Blackhole attack. These functions are operating in sequence manner. Functions are,

- Replies for a Route Request (RREQ) packet with maximum sequence number
- Drops all data packet what it received

The functions of the AODV protocol are defined in the aodv.cc file. This file imports a few library files including the adov.h file [21].

Step I:

Defining a Boolean type protected variable in the class AODV in the region of ”protected:” in the aodv.h file as follows. Then save the changes in the aodv.h file

```
class AODV: public Agent {
//some codes
protected:
//other variable definitions
        bool blHoleNode;
//other variable definitions
```

Step II:

Obtain the input at the runtime regarding the Blackhole node. Therefore, the aodv.cc file should alter as follows.Then save the changes in the aodv.cc file. Assign a default value for the declared Boolean variable as follows.

```
AODV::AODV(nsaddr_t id) : Agent(PT_AODV),
                 btimer(this), htimer(this),
ntimer(this),
                 rtimer(this), lrtimer(this), rqueue()
{
  //some codes
blHoleNode =false; //by default a node is gentle
  //some codes
}
```

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

Obtain the run time command to define a Blackhole node. The second argument in the command at the runtime is used. “BlackholeNode” argument value is used to identify the requirement of the blackhole node definition.

```
int
AODV::command(int argc, const char*const* argv) {
if(argc == 2) {
  //some codes
    if(strcmp(argv[1], " BlackholeNode") == 0) {
blHoleNode=true;
    return TCL_OK;
    }
//some codes
```

The false information is inserted from the following function. This will be executed when a Blackhole node is defined and an RREQ packet being received by a Blackhole node.

```
void
AODV::recvRequest(Packet *p) {
//some codes
// following codes are after the code that used to
execute when source node receive the same request
packets
if (index == indexOfBlackholeNode)
sendReply(rq->rq_src, 1, rq->rq_dst, falseSequenceNo,
MY_ROUTE_TIMEOUT, rq->rq_timestamp);
//falseSequenceNo is the higher positive integer
value which a Blachole node used to insert in RREP
//some codes
```

Finally, the following function helps to define the action that needed to be carried on after a node defined as a Blackhole node. These codes help to define the action which is to drop packets that it received.

```
void
AODV::rt_resolve(Packet *p) {
//some codes
if(blHoleNode ==true)
{
drop(p,DROP_RTR_ROUTE_LOOP); // drop packets
return;
}
//some codes
```

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

The Blackhole attack is ready after rebuilding the NS2. Blackhole attack was used by inserting the following command in the .tclfile after the code to start the simulation.

```
#$ns at 0.0 "[$n10 set ragent_] BlackholeNode"
```

We can configure a Blackhole node which index is n10 to act as a Blackhole node at the 0.0 second at the simulation.

4.2 Grayhole Attack

Program Grayhole attacks are two types: drop packets after some time, and drop packets from a specific node.

4.2.1 Drop Packets after Some Time

This type of Grayhole attack can be performed by executing the same code that was used in the Blackhole attack formation. The operation can be customized by changing the time as follows. If the Grayhole attack is needed to perform by the 10th node at the 5th second then the following code should be inserted into the .tcl file after the code used to start the simulation.

```
#$ns at 5.0 "[$n10 set ragent_] BlackholeNode"
```

4.2.2 Drop All Packets from a Specific Node

Some codes for this type of Grayhole attack require same as previous attack type. Moreover, additional few codes are required as follows in aodv.cc file.

```
void
AODV::rt_resolve(Packet *p) {
//some codes
if(blHoleNode ==true)
{
if((ih->saddr() == targetNodeaddress) || (ih->daddr()
== targetNodeaddress) || (hdr_cmn->prev_hop_() ==
targetNodeaddress)) {
drop(p, DROP_RTR_ROUTE_LOOP);
   return;
}}
```

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

4.3 Wormhole Attack

The main character of a Wormhole attack is the wormhole tunnel. The tunnel is the results of the configurations of the nodes. Therefore following code is used in the .tcl file.

```
# The wormhole nodes are define initially before
initialize other nodes or initialize at last
# code for normal node initialization
Phy/WirelessPhy set CPThresh_ 10.0
Phy/WirelessPhy set CSThresh_ 8.15781e-13#1150m
Phy/WirelessPhy set RXThresh_ 1.55924e-11#550m
Phy/WirelessPhy set bandwidth_ 2e6
Phy/WirelessPhy set Pt_ 0.28183815
Phy/WirelessPhy set freq_ 914e+6
Phy/WirelessPhy set L_ 1.0
Antenna/OmniAntenna set X_ 0
Antenna/OmniAntenna set Y_ 0
Antenna/OmniAntenna set Z_ 1.5
Antenna/OmniAntenna set Gt_ 1.0
Antenna/OmniAntenna set Gr_ 1.0
$ns node-config -adhocRouting  $val(rp) \
                -llType        $val(ll) \
                -macType       $val(mac) \
                -ifqType       $val(ifq) \
                -ifqLen        $val(ifqlen) \
                -antType       $val(ant) \
                -propType      $val(prop) \
                -phyType       $val(netif) \
                -channel       $chan \
                -topoInstance  $topo \
                -agentTrace    ON \
                -routerTrace   ON \
                -macTrace      ON \
                -movementTrace ON
#initailization of the wormhole nodes. n(8) & n(9)
are wormhole node.
set n(8) [$ns node]
$n(8) set X_ 750
$n(8) set Y_ 0
$n(8) set Z_ 0.0
$ns initial_node_pos $n(8) 20
set n(9) [$ns node]
$n(9) set X_ 250
```

COPYRIGHT © 2021 FACULTY OF MANAGEMENT AND COMMERCE, SOUTH EASTERN UNIVERSITY OF SRI LANKA (SEUSL), UNIVERSITY PARK, OLUVIL 32360. SRI LANKA [RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

```
$n(9) set Y_ 0
$n(9) set Z_ 0.0
$ns initial_node_pos $n(9) 20
#default transmission range of a normal node is 250m.
#If node mobility needed to be apply on the wormhole
nodes, then the same speed and the direction should
be maintained for wormhole nodes.
```

After altering the necessary files, save the changes. NS2 is needed to recompile. Therefore, available object files are needed to be deleted. Then NS2 should be recompiled. Finally, install the object as required by the simulator. Following codes will help to perform all three functions.

```
make clean
make
make install
```

5 Methodology

Computer simulators can be used to perform experiments virtually same as real experiments do [23]. NS2 [24] is an event-driven network simulator that was used to experiment. AODV is a routing protocol that is also known as a reactive routing protocol [7].

Table 1: Simulator parameters

Parameter	Value
Frequency	9.14 x 10^8 Hz
Bandwidth	2.0 x 10^6 bps
Antenna/OmniAntennaX,Y, and Z	0, 0, 1.5 m
Radio Propogation Model	TwoRayGround
Network Interface Type	Phy/WirelessPhy
Traffic Type	Constant Bit Rate (CBR)
Max Packetsin Interface Queue	50
Nodes Transmission Range	250 m
Number of Nodes	10
Simulation Time	5 s

Moreover, AODV is more suitable for MANETs [5]. Table 1 shows the parameters that are maintained during the simulation. For more accuracy, the experiment was repeated one hundred times and obtained an average value. The network performance was affected by node mobility [5]. Moreover, this affection is very based on the mobility pattern. Therefore, node mobility was maintained as zero ms^{-1} during the experiment to identify the actual impact of the attacks. The network topology was 1000 m x 1000 m. The influence of the attacks on the network was evaluated through four different performance matrices. Those were PDR, AEED, Throughput, and SPTIN. The PDR is a ratio between the number of packets received by the destination node and the number of packets sent by the source node. The AEED value is the total time taken by a packet to reach from the source node to the destination node. The Throughput value is a ratio between the total packet reached by the destination node and the total time is taken. All types of packets are considered to calculate PDR and Throughput value, though only data packets are considered to calculate the AEED value.

6 Results and Discussion

Figure 1 is the graph of the PDR values of the different networks. The controller network was shown 72% of PDR. The networks that were affected by Blackhole and Grayhole Type II attacks were showed the lowest PDR value. It was 0.28%. Only 0.28% of packets that were sent by the source node were received by the destination node. The highest PDR value was shown by the network which was affected by a wormhole attack. The higher PDR value is the result of the high-speed data transaction of the wormhole tunnel. The network which was affected by a Grayhole Type I attack was shown an intermediate PDR value compared to the controller and Blackhole affected network. During the simulation, we observed that the effect of the attacks of Blackhole and Grayhole Type II were similar. Because, same as the Blackhole attack, Grayhole Type II attack did not allow any packets from a specific node. If the targeted node is in the route and connected to the network before the attacker then all the packets of the node will be dropped by the attacker. The targeted node can be the source node or the destination node or a node in the network.

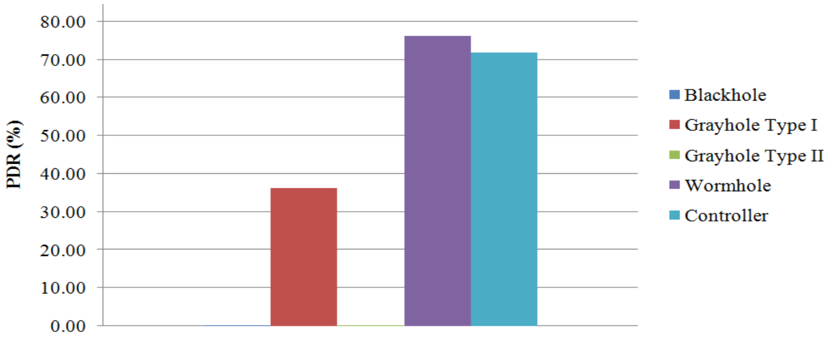

Fig. 1. PDR values of different networks

Figure 2 is the graph of the AEED values of the different networks. Because of the effects of the Blackhole and Grayhole Type II attacks, the destination nodes in the networks could not receive any data packets. Therefore, AEED values were infinity. Averagely 0.235 seconds were taken by

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

a data packet to reach the destination node from the source node in the controller network. Averagely, 0.185 seconds was taken by a data packet to reach the destination node in the network which was affected by a Grayhole Type II attack.

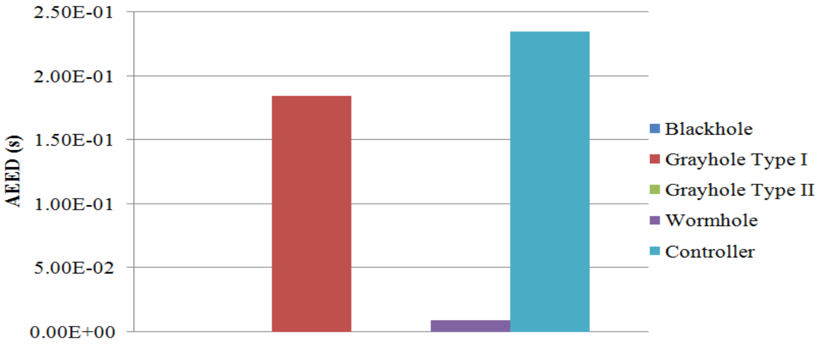

Fig. 2.AEED values of different networks

This is a slightly lower amount of AEED value than the controller network. Because during this type of attack, lower number of data packets reached by the destination node. The lowest amount of AEED value was observed during the Wormhole attack. The reason was the higher transaction rate of the wormhole tunnel. The data transfer rate through the wormhole tunnel was 26 times faster than the controller network.

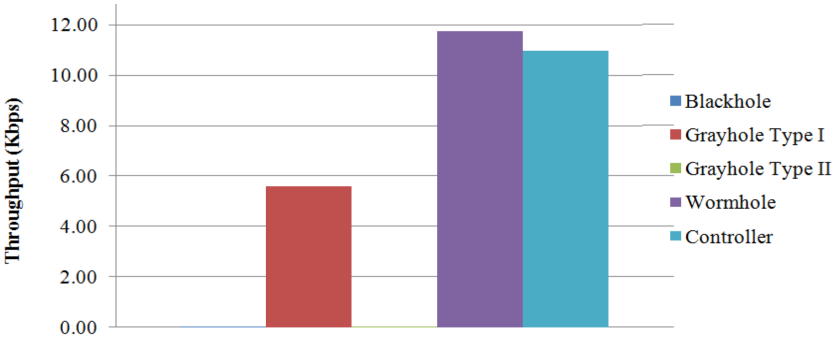

Fig. 3. Throughput values of different networks

Figure 3 is the graph of the Throughput values of different networks. 11.0 Kbps of throughput was shown by the controller network. The lowest Throughput value was the results of Blackhole and Grayhole Type I attacks. It was 0.04 Kbps. This was the throughput value of the routing packets but not data packets reached by the destination node. The highest value was the result due to the wormhole tunnel. It was 11.76 Kbps. It was 1.07 times higher than the value of the controller network. The network affected by a grayhole Type II attack showed an intermediate throughput value. It was 5.59 Kbps.

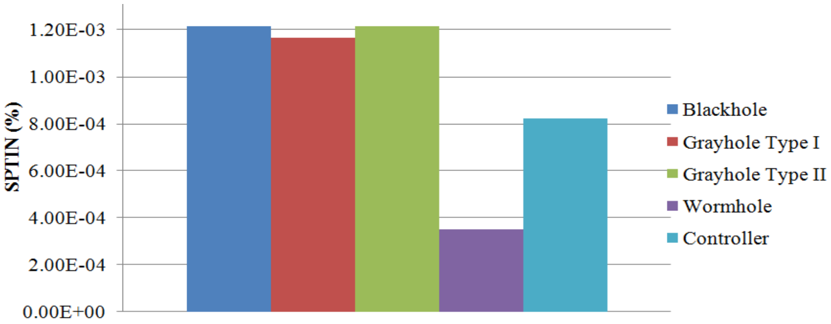

Fig. 4. SPTIN values of different networks

Figure 4 is the graph of SPTIN values of different networks. 0.0082 seconds was taken by a node in the controller network. An approximately equal amount of SPTIN value was shown by all active attacks. It was 0.0012 seconds, though a lower amount of SPTIN value was shown in the presence of a Wormhole attack. It was 0.0008 seconds.

The summary of the results was presented in Table 02. The values were calculated and compared to the values of the controller network. According to the results in the table, it is clear that the Blackhole, Grayhole Type I, and Grayhole Type II attacks are active attacks because these attacks degrade the network performance badly. The Wormhole attacks are passive attacks.

Table 2 Results Summary

Attack	PDR	AEED	Throughput	SPTIN
Blackhole	0.0040	∞	0.0040	1.4766
Grayhole Type I	0.5046	0.7858	0.5088	1.4213
Grayhole Type II	0.0040	∞	0.0040	1.4766
Wormhole	1.0608	0.0384	1.0692	0.4261

6 Conclusion and Future Works

Active attacks cause serious damage to the network performance, though passive attacks enhance the network performance or cause the least damage. The results proved that the network performance depends on the configuration of the attacks that were simulated by altering the AODV protocol functions. Moreover, the network performance is changed based on the mobility model [5] which was applied during the simulation. Therefore, the actual impact of an attack could not be identified. It is mandatory to check the behavior without applying a mobility model. If actual impacts of security attacks were identified then the researchers are able to discover necessary security mechanisms to secure the data in a MANET. We are expecting to explore more about the different security attacks on MANET. Simulating these attacks on different simulators will open the opportunity to conduct different researches.

References

1. P.G. Teodoro, L.S. Casado, and G.M. Fernández, "Taxonomy and Holistic Detection of Security Attacks in MANETs" in *Securityfor Multihop Wireless Networks*, Khan, S. and mauri, J.L. Eds., 1st edn, 2014, Taylor & Francis Group:CRC Press. pp. 3-18.

2. S. Adibi, "Application-Layer Cross-Layer Design with Simultaneous Quality of Service and Security Support" in *Securityfor Multihop Wireless Networks*, Khan, S. and mauri, J.L. Eds., 1st edn, 2014, Taylor & Francis Group:CRC Press. pp. 447-476.

3. A. Dorri, S.R. Kamal, and E. Kheyrkhah, "Security Challenges in Mobile Ad Hoc Networks: A Survey" in *International Journal of Computer Science & Engineering Survey (IJCSES)*, 6(1), 2015.

4. U. Ahamed, and S. Fernando, "Identifying the Impacts of Active and Passive Attacks on Network Layer in A Mobile Ad-hoc Network: A Simulation Perspective", in *International Journal of Advanced Computer Science and Applications*, 11(11), 2020.

5. U. Ahamed, and S. Fernando, "Identifying the Impacts of Node Mobility on Network Layer Based Active and Passive Attacks in Mobile Ad Hoc Networks: A Simulation Perspective" in *Computing Science, Communication and Security. COMS2 2021. Communications in Computer and Information Science,* N. Chaubey, S. Parikh, K. Amin, K, Eds.,Springer, Singapore, 2021, pp. 117-133.

6. R. Meddeb, F. Jemili, B. Triki, and O. Korbaa, "Anomaly based Behavioral Detection in Mobile Ad-Hoc Networks" in *23rd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems*, Elsevier, 159, 2019, pp. 77–86.

7. C.E. Perkins, E.M.B. Royer, and S.R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing". *Experimental*, RFC 3561, July 2003

8. R. Mehta, and M. Parmar," Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole &Grayhole Attacks" in *2018 3rd International Conference for Convergence in Technology (I2CT) Pune*, India: IEEE, 2018, pp. 1-6.

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

9. K. Konate, and G. Abdourahime, "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation" in *2011 Second International Conference on Intelligent Systems, Modelling and Simulation,* IEEE, 2011, pp. 367-372*.*

10. M. Ghonge, and S.U. Nimbhorkar, "Simulation of AODV under Blackhole Attack in MANET" in *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(2),Feb 2012,

11. A. Ahmed, K.A. Bakar, and M.I. Channa, "Performance Analysis of AdhocOn Demand Distance Vector Protocol with Blackhole Attack in WSN" in *Journal of Computer Science,* 10 (8), 2014.

12. H.M. Ibrahim, N.M. Omar, and E.K. William, "Detection and Removal of Gray, Black and Cooperative Black Hole Attacks in AODV Technique", in *International Journal of Advanced Computer Science and Applications*, 6(5), 2015.

13. R.H. Jhaveri, and N.M. Patel, "A sequence number-based bait detection scheme to thwart grayhole attack in mobile ad hoc networks" *Wireless Network*21, 2015, pp. 2781–2798.

14. M. Tripathi, M.S. Gaur, and L. Laxmi, "Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN" in: *The 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN),* Elsevier, 2013.

15. C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, Quantifying, and Detecting the Blackhole attack in Infrastructure-less Networks", in *Computer Networks,* 2016.

16. H. Moudni, M. Er-rouidi, H. Mouncif, and B.E. Hadadi, "Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks" in *2nd International Conference on Electrical and Information Technologies*, IEEE, 2016, pp. 1-7

17. G. Li, Z. Yan, and Y. Fu, "A study and simulation research of blackhole attack on mobile adhoc network" in *2018 IEEE Conference on Communications and Network Security (CNS)*, Beijing, China; IEEE, 2018. pp. 1-6.

18. T. Saad, "Performance Evaluation of Blackhole Attack on AODV in VANET" in *American Journal of Applied Sciences*, Science publication, 15(2), 2017.

19. A. Yasin, M.A.andZant, "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique" in *Wireless Communications and Mobile Computing,*Hindawi, 2018.

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]

20. S. Kukliński, and G. Wolny, “CARAVAN: Context-AwaRe Architecture for VANET” in: X. Wang, (ed), *Mobile Ad-Hoc Networks: Applications*, InTech, Croatia, 2011 pp. 125-148.

21. ns2cbe,*How to configure MALICIOUS nodes in NS2* (Nov 26, 2014). Accessed: April. 01 2021. [Online Video]. Available: https://www.youtube.com/watch?v=AVTcgEkSZLE

22. R. Sosa, “Computational Modelling of Teamwork in Design.” in *Experimental Design Research*. P. Cash, T. Stanković, and M. Štorga, Ed., Springer, Cham, 2016.

23. *The ns Manual* (2011). Accessed: March. 01 2021 [Online]. Available at: http://www.isi.edu/nsnam/ns/ns-documentation.html

24. T.D.S. Keerthi, and P. Venkatarm, “Confirmation of wormhole attack in MANETs using honeypot” in *Computers & Security*, 2018

Uthumansa Ahamed, Completed a basic B.Sc. (Hons) degree at the Rajarata University of SL. Seven-year experience in freelancing service in Software Engineering. Currently, reading M.Phil. research degree in the same university. Research interest areas are Software Reverse Engineering, MANET, Security of Routing Protocol, and Machine Learning. Recently, joined to the academic position in the Dept. of ICT, Faculty of Technology, South Eastern University of SL.

Dr. Shantha D. Fernando, Ph.D., M.Phil., B.Sc. Eng. (Hons), IET(UK), MIE(SL), CEng, Senior Lecturer G-1 in Department of Computer Science and Engineering, Faculty of Engineering, University of Moratuwa, co-founder of TechCERT. Research interest are e-Learning and learning management systems, adaptive course development and learning objects, information systems development philosophies and life-cycles, blended university education, m-learning, socio-technical aspects of information systems, information systems security, ICT infrastructure security, and digital forensics.

[RECEIVED: 4TH JUNE, 2021; REVISED AND ACCEPTED: 10TH JULY, 2021]