Whirlwind: A New Method to Attack Routing Protocol in Mobile Ad Hoc Network

Luong Thai Ngoc[1,2], Vo Thanh Tu[1]
(Corresponding author: Luong Thai Ngoc)
Faculty of Information and Technology, Hue University of Sciences, Hue University, Viet Nam[1]
77 Nguyen Hue street, Hue city, Vietnam
Faculty of Mathematics and Informatics Teacher Education, Dong Thap University, Viet Nam[2]
783 Pham Huu Lau street, Ward 6, Cao Lanh city, Dong Thap, Viet Nam
(Email: ltngoc@dthu.edu.vn)
(Received June 28, 2016; revised and accepted Nov. 15, 2016 & Jan. 11, 2017)

Abstract

Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes that dynamically create a network without a fixed infrastructure. However, all the characters make the security problem more serious, denial-of-Service attack is the main challenge in the security of MANET. In this article, we review some routing protocol attacks on Mobile Ad hoc Network. Specially, we propose a new attack method is called Whirlwind which originates one data Whirlwind on network that contain malicious node once the source node discovers a new route. And all data packets are resulted in drop due to over time-life without reaching the desired destination. We have, using the simulation system NS2, evaluated the harms of such attack on AODV protocol.

Keywords: AODV; MANET; Network Security; Routing Attacks

1 Introduction

Mobile Ad hoc Network is a special wireless, the advantages such as flexibility, mobility, resilience and independence of fixed infrastructure, nodes of the MANET network are coordinated with each other to communicate, data transfer among nodes is achieved by means of multiple hops. Hence, every mobile node acts both as a host and as a router [7].

Routing is the main service provided in network layer, the source node using the route to the destination is discovered and maintained. Routing protocols used in infrastructure networks cannot be applied in infrastructureless networks like MANETs. Hence, many routing protocols are recommended to adapt to MANET, they are classified into proactive, reactive, and hybrid routing [1]. Proactive routing protocol is suitable with stable network topology because routes of network nodes must be established to connect with other nodes before routing, typically DSDV [14], and OLSR [6]. In contrary, if network structure is regularly changed, then reactive routing is more suitable because nodes only discover routes in case of necessity by sending packet for route request and receiving packet for route answer, typically DSR [9], and AODV [15]. In the complex network topology, then typical routing protocols such as ZRP [5], and ZHLS [8] under the hybrid routing is more suitable to select.

Denial of service (DoS) attacks aim to deny a user of a service or a resource he would normally expect to have. Routing service at network layer is the target of many DoS [16], in which a malicious node will try to keep their resource but occupy other node's resource, for example, Blackhole [12], Sinkhole [3], Grayhole [4], and Flooding [17] under DoS attacks. Another way to interrupt routing service is to use a private tunnel connected between two malicious nodes. The result is that normal nodes will transfer data via this tunnel that appears the destination route with low cost. This type of attack is often called Wormhole [2, 10].

Ad hoc On-demand Distance Vector (AODV) is one of the most popular reactive routing protocol used for Ad hoc Networks. If source node N_S wants to communicate with destination node N_D without available route to destination, then N_S starts route discovery process by broadcasting the route request packet (RREQ) to destination. Destination node will answer to source about route by sending reply packet (RREP), maintain the route through HELLO and RERR packets. This is typical protocol under on-demand routing protocol, hence, hackers are easy to perform attacks on this protocol.

1.1 Blackhole/Sinkhole Attacks

Blackhole attack [12] is done by a malicious node or collaboration of harmful nodes. In the attack, a malicious node replies to source's RREQ packet by fake RREP (FR-

REP) packet with the best route to destination. By doing that, the Blackhole node successfully gains traffic flow from source transfer to destination. As result, the sources node sends all of data packets to the attack node which can drop or modify the packets. Another attack resemble Blackhole, called Sinkhole, was introduced in [3].

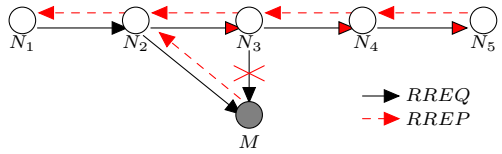


Figure 1: Description of blackhole attacks

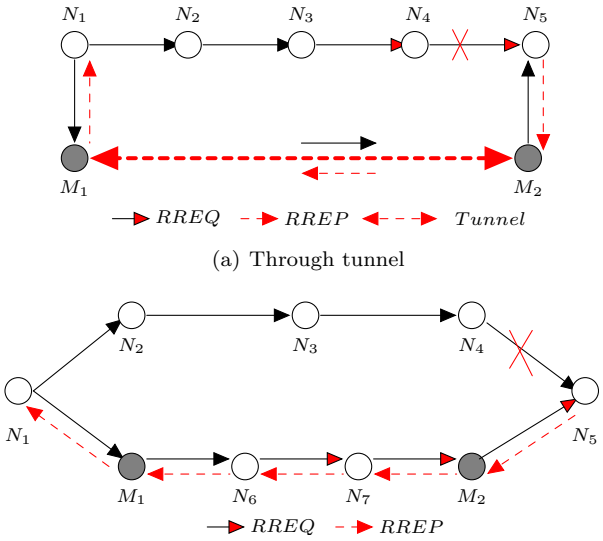
In Figure 1, source node (N_1) discovers a new route to destination node (N_5) by broadcasting RREQ packet and then receive RREP packet. The best route from N_1 to N_5 on direction $\{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_4 \rightarrow N_5\}$ is established. However, the existing of a malicious node in the network N_2 establishes route to destination through malicious node M because M pretends it having the best route to N_5 by replying FRREP packet.

1.2 Grayhole Attacks

Grayhole attack [4] is similar to Blackhole attacks type, the destruction level is however less than, it also passes through 2 phases: *Phase 1,* malicious code shall self-advertise the source node that malicious node itself has route to destination with the lowest cost, it therefore can cheat the source node to change direction to destination through it. *Phase 2,* malicious node receives all packets from source and then drops the packet in different frequency, the malicious code sometime represents as normal node to prevent any detection. In order to advertise that it has route to destination with the lowest cost, the malicious node also uses FRREP packet as Blackhole attack.

1.3 Wormhole Attacks

They have described several types of Wormhole based on the techniques used to tunnel the packets between the colluding nodes, such as: Wormhole through the tunnel (called out-of-band channel - OB), Wormhole using encapsulation, Wormhole using packet relay, Wormhole with high power transmission [11]. Especially, authors [10] described that all of them may be operated for two modes of attacks: Hidden Mode (HM) and Participation Mode (PM). In HM, malicious nodes are hidden from normal nodes, when receive packets and simply forwards them to each other without process packet, thus, they never appear in routing tables of neighbors. In contrast, PM malicious nodes are visible during the routing process because they processes packets as normal nodes. Note that the malicious node appears in routing tables of neighbors and the HC increase when packet is forwarded.



(a) Through tunnel

(b) Through packet encapsulation

Figure 2: Description of wormhole attacks types

Out-of-band channel: Attacker using 2 malicious nodes connect to each other and create a private channel called "tunnel" aiming to minimize hop count (HC) when source node discovers route by RREQ packet. In Figure 2(a), source node N_1 requests the route to destination N_5 by broadcasting RREQ via 2 routes $\{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_4 \rightarrow N_5\}$ and $\{N_1 \rightarrow M_1 \rightarrow M_2 \rightarrow N_5\}$. Finally the second route through M_1, M_2 was established because it has the best traffic cost.

Encapsulation: To attack, malicious nodes (M_1, M_2) appear in the network similar to normal nodes. When M_1 received the RREQ packet, which encapsulates it and forwards it to M_2 via normal nodes. Node M_2 is responsible for decapsulation the packet before send it to destination. Because of the packets encapsulation, the routing cost not increase during the traversal through the normal nodes. As a result, source node discovers a new route which contains malicious node. In Figure 2(b), source node broadcasts RREQ packet to destination node N_5 following to 2 routes $\{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_4 \rightarrow N_5\}$ and $\{N_1 \rightarrow M_1 \rightarrow N_6 \rightarrow N_7 \rightarrow M_2 \rightarrow N_5\}$. When M_1 received the RREQ packet, it encapsulates the packet then forward RREQ into current route. M_2 node is responsible for decapsulation the packet before broadcast it to N_5. The same process also happens when RREP generated by N_5 forwarding back to N_1 through M_2 and M_1. The purpose is keeping HC not increase while the packets travel from M_1 to M_2 and vice versa. As a result, the RREP from N_5 follow the second route is better than others, hence N_1 obviously chooses the route to N_5 through two malicious nodes.

Using packet relay: The main idea is a malicious node relays fake packets between two non-neighbor nodes creating an illusion that they are neighbors, the purpose is insert itself into route.

Wormhole with high power transmission: Malicious node has a high power antenna, thus distant nodes receive the RREQ packet faster from the malicious node. The result discovered route may contain malicious node because its routing cost is cheaper normal route.

1.4 Flooding Attacks

Flooding attack [17] is one of the main challenges in the security of MANETs. It is implemented by overwhelmingly sending control packets or useless data packets from malicious nodes to unavailable destinations. The result is a broadcasting storm of packets and increasing communication overhead, which reduce the responsiveness at each node because of its unnecessary processing of the flooded packets. For AODV, Flooding attacks try to send HELLO, RREQ and DATA packets at a high frequency.

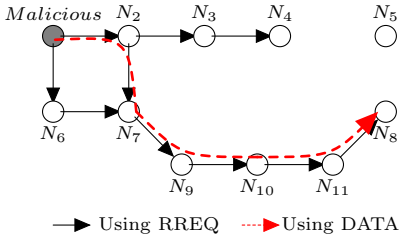


Figure 3: Description of flooding attacks

HELLO packet flooding: In MANETs, nodes periodically broadcast HELLO packets to notice their existence with their neighbors. A malicious node abuses this feature to broadcast HELLO packets at a high frequency that force its neighbor nodes to spend their resources on processing unnecessary packets. This HELLO packet flooding is only detrimental to the neighbors of a malicious node. See in Figure 3, both nodes N_2 and N_6 are affected by malicious node N_1.

RREQ packet flooding: In AODV protocol, nodes broadcast RREQ packet to discover routes. To attack, a malicious node continuously and excessively broadcasts RREQ packets, which causes a broadcast storm in the network and floods with unnecessary packets being forwarded. The RREQ flooding attack is seen as the most harmful because it has a great impact on the route discovery in the network. It also causes high resource consumption at affected nodes and increases the communication overhead. See in Figure 3, all nodes in topology are affected by malicious node N_1.

DATA packet flooding: A malicious node can excessively broadcast data packets to any nodes in the network. This can waste other nodes' resources and bandwidth. It can create congestions in the network. This kind of attack has more impact on the nodes participating in the data routing to the destinations. Figure 3, DATA packet flooding attacks effects all node in route $\{N_2 \rightarrow N_7 \rightarrow N_9 \rightarrow N_{10} \rightarrow N_{11} \rightarrow N_8\}$.

2 Proposing Whirlwind Attack in Mobile Ad Hoc Network

2.1 Main Idea

Routing protocol is responsible for exploring the route to destination when source node wants to communicate. A good protocol is not a quick gather, low routing explore cost only, but being able to prevent routing loop is also an extremely important factor. Whirlwind attacks target is to make routing loop which is done with two phases:

Phase 1: Malicious node try to set up a routing loop path in the route from source to destination node when receiving RREQ packet from any source node N_S by using the FRREP packet. The detail process is showed in Algorithm 1.

Phase 2: If attacking is successful, all data packets from source N_S to destination node are taken into data whirlwind and automatically dropped due to over time-life. We have, basing on this feature, named this attack method as Whirlwind attacks.

2.2 Description of Whirlwind Attacks in AODV Protocol

AODV protocol uses the route exploration mechanism if it is necessary. If source node N_S wants to communicate with destination node N_D however route to destination is unavailable, N_S starts the route exploration process by broadcasting RREQ packet to destination node. Destination node replies route to source by sending unicast RREP packet. In AODV, all nodes remain route by using HELLO packet and update route by using RERR packet.

In normal network topology (Figure 4(a)), source node N_1 discovers route to destination node N_5 by broadcasting of RREQ to its neighbor nodes named N_2. Intermediate node N_2 is not destination node, it therefore continue broadcasts RREQ packet to its neighbors named N_3 and save reserve route to source N_1, this process repeats at N_3 and N_4 until node N_5 receives the route request packet.

When receiving RREQ packet from node N_4, destination node N_5 sends unicast of RREP packet to source on route $\{N_5 \rightarrow N_4 \rightarrow N_3 \rightarrow N_2 \rightarrow N_1\}$. As a result, source node N_1 discovers route to destination in following direction $\{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_4 \rightarrow N_5\}$. The detail

Algorithm 1 Description of the process to set up a routing loop path in Whirlwind attacks

1: Begin
2: *Step 1:* Malicious node M wait until receiving the RREQ packet from source node N_S;
3: *Step 2:* When receiving the first RREQ packet from node N_i, node M adds route to destination N_D via N_i into its routing table (RT); and waiting to receive the second RREQ packet;
4: *Step 3:* When receiving the second RREQ of N_S from node N_j, malicious node M adds route to source N_S via N_j into its RT; and sends FRREP packet to source node via next hop (NH) N_j to inform N_j about M with route to destination N_D with lowest cost and "fresh" enough;
5: *Step 4:* If M does not receive the second RREQ packet from N_S then this process is fail and the end;
6: *Step 5:* When receiving FRREP packet, N_j adds route to destination N_D through next hop M because it assumes that M has route to destination with minimum cost;
7: *Step 6:* The FRREP packet is forwarded by N_j to source node through revert route (recorded in broadcast RREQ process) until source node receives FRREP packet;
8: *Step 7:* Destination node N_5 also replies to source node of RREP packet. Thus, source node receives two routing replies packet. However, the FRREP packet from malicious node is accepted due to it has lower cost and more "fresh". The result is the route from source N_S to destination N_D has circle consisting of nodes named N_i, N_j and M;
9: End

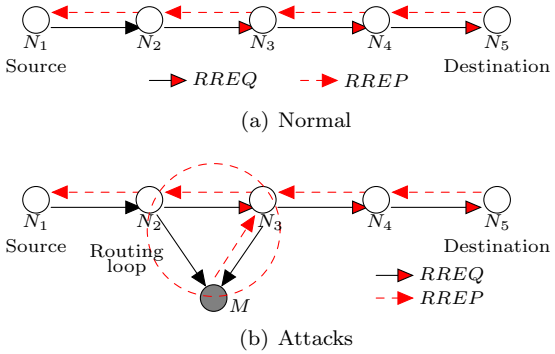


Figure 4: Description of route discovery in AODV

information of RREQ, RREP packets and routing table of each node are detailed in Table 1.

Figure 4(b) shows that malicious node M appears in network topology and conducting Whirlwind attack, M is neighbor of both nodes N_2 and N_3. When receiving the first RREQ packet from node N_2, malicious node M saves route to destination into its RT with minimum cost

Table 1: Results of discovery route in normal topology; Des: Destination address; Src: Source address

Steps	Nodes	RREQ/RREP (Src, Des, HC)	Routing Table		
			Des	NH	HC
RREQ	N_1	$N_1, N_5, 0$	NULL		
	N_2	$N_1, N_5, 1$	N_1	N_1	1
	N_3	$N_1, N_5, 2$	N_1	N_2	2
	N_4	$N_1, N_5, 3$	N_1	N_3	3
	N_5	$N_1, N_5, 4$	N_1	N_4	4
RREP	N_5	Creates RREP packet $[N_5, N_1, 0]$			
	N_4	$N_5, N_1, 1$	N_5	N_5	1
	N_3	$N_5, N_1, 2$	N_5	N_4	2
	N_2	$N_5, N_1, 3$	N_5	N_3	3
	N_1	$N_5, N_1, 4$	N_5	N_2	4

$[Des = N_5, NH = N_2, HC = 1]$. When receiving the second RREQ packet from node N_3, malicious node saves the reserve route to source N_1 into its RT with lowest cost $[Des = N_1, NH = N_3, HC = 1]$, concurrently sends unicast of FRREP to source N_1 in direction $\{M \rightarrow N_3 \rightarrow N_2 \rightarrow N_1\}$. As a result, routing table of node N_3 has route information to destination N_5 via NH is M with the cost of 1.

Destination node N_5 also replies to source node of RREP packet in direction $\{N_5 \rightarrow N_4 \rightarrow N_3 \rightarrow N_2 \rightarrow N_1\}$. When receiving the RREP packet from node N_4, node N_3 see that the cost to destination N_5 is not cheaper than the existing route, the RREP packet is therefore dropped. Table 2 shows that exist routing loop on route from N_1 to N_5 in RT of nodes named N_2, N_3, and M. Therefore, malicious node M has successfully attacked.

Table 2: Results of discovery route in attacks topology

Steps	Nodes	RREQ/RREP (Src, Des, HC)	Routing Table		
			Des	NH	HC
RREQ	N_1	$N_1, N_5, 0$	NULL		
	N_2	$N_1, N_5, 1$	N_1	N_1	1
	M	$N_1, N_5, 2$	N_5	N_2	1 *
	N_3	$N_1, N_5, 2$	N_1	N_2	2
	M	$N_1, N_5, 3$	N_1	N_3	1 *
	N_4	$N_1, N_5, 3$	N_1	N_3	3
	N_5	$N_1, N_5, 4$	N_1	N_4	4
FRREP	M	Creates RREP packet $[N_5, N_1, 0]$			
	N_3	$N_5, N_1, 1$	N_5	M	1
	N_2	$N_5, N_1, 2$	N_5	N_3	2
	N_1	$N_5, N_1, 3$	N_5	N_2	3
RREP	N_5	Creates RREP packet $[N_5, N_1, 0]$			
	N_4	$N_5, N_1, 1$	N_5	N_5	1
	N_3	Drops RREP packet			

(*) Entry is added by malicious node

However, algorithm 1 shows that Whirlwind attack is done successful if malicious nodes receive full two RREQ packets from neighbors. In Figure 5 shows that Whirlwind attack is fail due to malicious node receive only one RREQ packet from N_2.

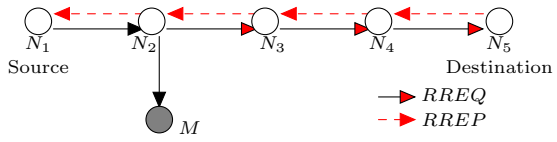


Figure 5: Whirlwind attacks is fail

2.3 Comparison of Whirlwind and Other Attacks

The recent studies show that hacker can perform many network attacks in MANET [16]. They can classify under some criteria named purpose, location, form, and lost packet cause. Attack purpose contain attack for dropping data and eavesdropping; and attack position convey external and internal; and attack forms consist of active and passive. Whirlwind attack also aims at dropping data, however data is dropped at normal node due to over time-life, this is differ from Blackhole and Grayhole attacks that packet is dropped by malicious node. Whirlwind is active attacks form, it is performed from internal location of network. Table 3 shows comparison of Whirlwind and other attacks.

Table 3: Summarized attack methods

Features		Attack types				
		BH	GH	WH	FD	WW
Purpose	Dropping	●	●	○	●	●
	Eavesdropping			●		
Localtion	External	●	●	●	●	
	Internal					●
Form	Active	●	●	●	●	●
	Passive		○			
Lost packets	Malicious nodes	●	●	●	●	
	Over time-life					●

(●) Implement; (○) Optional; BH: Blackhole; GH: Grayhole; WH: Wormhole; FD: Flooding; WW: Whirlwind;

3 Result Evaluation by Simulation

We evaluate the impact of Whirlwind attack on simulation system is NS2 [13] (version 2.35) on AODV protocol.

3.1 Simulation Settings

At the physical and data link layer IEEE 802.11 is used, the traffic pattern was generated using CBR as the data source and UDP protocol is used for transporting the data and the packet size is of 512 bytes, 200s of simulation; the transmission range of a node is 250m, FIFO queue (See more in Table 4).

Table 4: Simulation parameters

Parameters	Setting
Simulation time (s)	200
Wireless standard	IEEE 802.11
Ratio range (m)	250
Traffic type	CBR
Packet size	512 bytes
Queue type	FIFO (DropTail)

We used two network topology, *(a) Topology 1* is available with 5 normal nodes, using one CBR as the data source for transporting the data, 1 malicious node is immobile at the position as Figure 4. *(b) Topology 2* is available with 100 normal nodes and 1 malicious node, and operated in the area of 2000m x 2000m, malicious node is immobile at the central position, all nodes stay in Grid network topology as Figure 6, 10 data source CBR, the first CBR source is started at second of 0, the following CBR is 5 seconds apart from each source.

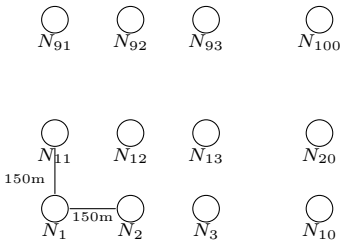


Figure 6: Grid network topology

3.2 Simulation Results

To evaluate the impact of Whirlwind attack, we use two criterion: *Packet delivery ratio and Network throughput.*

1) Packet delivery ratio (PDR): It can be measured as the ratio of the received packets by the destination nodes to the packets sent by the source node. PDR = (number of received packets/number of sent packets) * 100;

2) Network throughput: is the parameter of measuring information transported which is calculated by (total packet sent successfully * size of packet)/simulation time.

Packet delivery ratio: Figure 7 shown that Whirlwind attack had caused impact on route discovery ability of source node, hence the ratio of sending packet successfully has much been reduced. After finishing 200s simulation in the first network topology, the packet delivery ratio of AODV is 98.04% under normal network topology and there are nothing any

packet is sent to destination under Whirlwind attack. In Gird network topology, the packet delivery ratio of AODV is 97.47% under normal network topology and 31.97% under Whirlwind attack, 65.5% reduced.

Network throughput: Figure 8 shown that Whirlwind attack has reduced network throughput. After finishing 200s simulation, if one malicious node attacks, the network throughput of AODV is 0 bps in the first network topology. In Gird topology, throughput is 33,157.12 bps without attacks and 10,874.88 bps under Whirlwind attack.

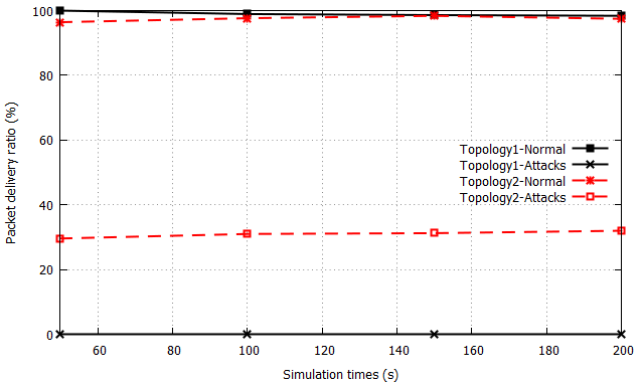


Figure 7: Packet delivery ratio

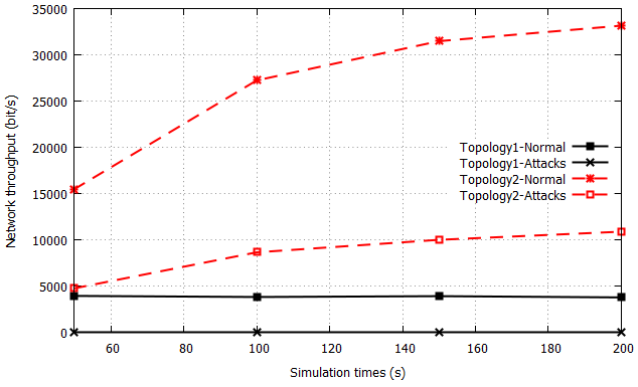


Figure 8: Network throughput

4 Conclusion

This article proposes a new attack method named Whirlwind that cause harm to performance of Mobile Ad hoc Network. Simulation results on AODV protocol show that the malicious node has successfully created data packet whirl-wind on network that cause loss packet, this decreases the packet delivery ratio, and network throughput. In Gird network topology, the packet delivery ratio of AODV 65.5% reduced under Whirlwind attack.

In the future, we shall continue installing the malicious assessment compared to other attacks on some routing protocols named DSR to evaluate harms.

References

[1] E. Alotaibi and B. Mukherjee, "A survey on routing algorithms for Wireless Ad-hoc and Mesh networks," *Computer Networks*, vol. 56, no. 2, pp. 940–965, 2012.

[2] A. P. Asad, C. McDonald, "Detecting and evading wormholes in mobile ad-hoc wireless networks," *International Journal of Network Security*, vol. 3, no. 2, pp. 191–202, 2006.

[3] L. S. Casado, G. M. Fernndez, P. Garca-Teodoro, and N. Aschenbruck, "Identification of contamination zones for sinkhole detection in MANETs," *Journal of Network and Computer Applications*, vol. 54, pp. 62–77, 2015.

[4] X. Gao and W. Chen, "A novel gray hole attack detection scheme for mobile ad-hoc networks," *IFIP International Conference on Network and Parallel Computing Workshops*, pp. 209–214, 2007.

[5] Z. J. Haas, M. Pearlman, *The Zone Routing Protocol (ZRP) for Ad-Hoc Networks*, IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, 2002.

[6] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *IEEE International Multi Topic Conference*, pp. 62–68, 2001.

[7] H. Jeroen, M. Ingrid, D. Bart, and D. Piet, "An overview of Mobile Ad hoc Networks: Applications and challenges," *Journal of the Communications Network*, vol. 3, no. 3, pp. 60–66, 2004.

[8] M. Joa-Ng and I. T. Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1415–1425, 1999.

[9] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, vol. 353, pp. 153–181, 1996.

[10] J. Karlsson, L. S. Dooley, G. Pulkkis, "A new MANET wormhole detection algorithm based on traversal time and hop count analysis," *Sensors*, vol. 11, pp. 11122–11140, 2011.

[11] M. Kumar, K. Dutta, I. Chopra, "Impact of wormhole attack on data aggregation in hieracrchical WSN," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 70–77, 2014.

[12] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method," *International Journal of Network Security,* vol. 5, no. 3, pp. 338–346, 2007.

[13] S. McCanne, S. Floyd, *The Network Simulator NS2*, Mar. 28, 2017. (`http://www.isi.edu/nsnam/ns/`)

[14] C. E. Perkins, P. Bhagwat, "Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers," *ACM SIGCOMM Computer Communication Review*, vol. 24, no. 4, pp. 234–244, 1994.

[15] C. E. Perkins, M. Park, and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99)*, pp. 90–100, 1999.

[16] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks - A survey," *Computer Communications*, vol. 51, pp. 1–20, 2014.

[17] Y. Ping, D. Zhoulin, Y. Zhong, and Z. Shiyong, "Resisting flooding attacks in ad hoc networks," in *International Conference on Information Technology: Coding and Computing (ITCC'05)*, vol. 2, pp. 657–662, 2005.

Biography

Luong Thai Ngoc is working in the Faculty of Mathematics and Informatics Teacher Education, Dong Thap University. He received B.E. degree in Computer Science from Dong Thap University in 2007 and M.A. degree in Computer Science from Hue University of Sciences in 2014. He is a PhD student in Hue University of Sciences now. His fields of interesting are network routing, analysis and evaluation of network performance, security wireless ad hoc network.

Vo Thanh Tu is an associate professor in the Faculty of Information Technology, Hue University of Sciences, Hue University. He received B.E. degree in Physics from Hue University in 1987 and PhD degree in computer science from Institute of Information Technology, Vietnam Academy of Science and Technology in 2005. His fields of interesting are network routing, analysis and evaluation of network performance, security wireless ad hoc network.