SMA_2AODV: Routing Protocol Reduces the Harm of Flooding Attacks in Mobile Ad Hoc Network

Vo Thanh Tu[1] and Luong Thai Ngoc[1,2]
[1] Faculty of Information Technology, Hue University of Sciences, Hue University, Vietnam
[2] Faculty of Mathematics and Informatics Teacher Education, Dong Thap University, Vietnam
Email: vttu@hueuni.edu.vn, ltngoc@dthu.edu.vn

Abstract—Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes that dynamically create a network without a fixed infrastructure. All the characters of MANET make the security problem more serious. The Flooding attacks in the MANET prevents the discovery route process, reduces network througth and increases routing load. In this article, we describe a solution to build Security Mobile Agent (SMA), and integrating SMA into the discovery route process of AODV protocol, improved protocol is called SMA_2AODV. Using NS_2, we compare the performance of both protocols in the random waypoint and grid network topology under Flooding attacks. Simulation results show that the detection ratio Flooding attacks successfully over 98%, and improved protocol has very reduced the harm of Flooding attacks based on the packet delivery ratio, network throughput and routing load metrics.

Index Terms—AODV, SMA_2AODV, MANET, fooding attacks, routing protocol

I. 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. [1]

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 infrastructure-less networks like MANETs. Hence, many routing protocols are recommended to adapt to MANET, they are classified into proactive, reactive, and hybrid routing protocol [2]. 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 destination of many DoS [3], in which a malicious node will try to keep their resource but occupy other node's resource, for example, Blackhole [4], [5], Sinkhole [6], Grayhole [7], Wormhole [8], [9], Whirlwind [10] and Flooding attacks [11] under DoS. Flooding attacks is implemented by sending flood of controsl packets from malicious nodes to nodes that are not available in the network or transfer a larger number of useless data packets to block network. The result is to create broadcast storm of packets and to increase routing load, reduce the responsive ability at each node because of unnecessary processing of message packets. This type of attacks is easy to perform with on-demand routing protocol, typically AODV.

Ad hoc On-demand Distance Vector (AODV [12]) 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 RREQ packet to destination. Destination node will answer to source about route by sending answer packet of RREP, maintain the route through HELLO and RERR packets. This is typical protocol under on-demand routing protocol, hence, hackers are easy to perform flooding attacks on this protocol, typically HELLO, RREQ and DATA flooding attacks. [13], [14]

A. 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. In Fig. 1, all the nodes $\{N_5, N_9, N_{12}\}$ are affected by the malicious node N_8.

B. RREQ Packet Flooding

In AODV protocol, nodes send route request packets (RREQ) to discover routes. To attack, a malicious node continuously and excessively broadcasts fake RREQ packets, which causes a broadcast storm in the network and floods with unnecessary packets being forwarded . The RREQ flooding attacks 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. In Fig. 1, all nodes $\{N_1$ to N_7, and N_9 to $N_{12}\}$ are affected by the malicous node N_8 with RREQ Flooding attacks.

C. DATA Packet Flooding

A malicious node can excessively broadcast data packets to any nodes in the network. This can waste other

Manuscript received March 12, 2017; revised July 19, 2017.
doi:10.12720/jcm.12.7.371-378

nodes' resources and bandwidth. It can create congestions in the network. This attack type has more impact on the nodes participating in the data routing to the destinations. In Fig. 1 show that DATA Flooding attack effects all the node in the route $\{N_8 \rightarrow N_{12} \rightarrow N_{11} \rightarrow N_{10} \rightarrow N_7 \rightarrow N_2 \rightarrow N_1\}$.

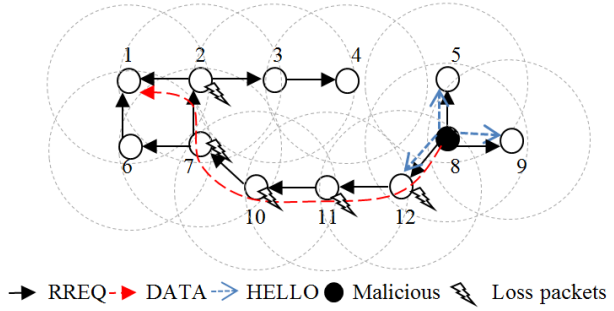


Fig. 1. Description of flooding attacks

The next section, the article presents the research works related to detection and prevention of flooding attacks. Section 3 presents in detail solutions to build SMA agent for security, and integrate SMA into the route discovery mechanism of AODV routing protocol. A new routing protocol is called SMA_2AODV that can detect flooding attacks of RREQ packet. Section 4 presents the simulation scenarios to evaluate the damage, and the efficiency of improved solutions, and finally conclusion.

II. Related Works

During the last time, some research works published related to prevention of flooding attacks, solutions given mainly focus on *detection* and *prevention*. The advantages of detection solution are low cost, but they mainly base on characteristics of attack form to detect, hence, it only brings about efficiency to some independent attacks. In contrary, prevention solutions apply mechanism of authentication, integrity, and non-repudiation based on digital signature or one-way hash. Its advantages are high security, many of attacks prevented.

A. Detection Solution

In [11], Ping has presented a security solution that prevents DATA and RREQ packet flooding attacks in the variable network. One priority method that is based on RREQ processing procedure called FIFO (First-In-First-Out) is recommended and supplemented into processing of AODV protocol. The authors argued that the priority of one node is adversely proportional to its broadcast frequency of RREQ. Hence, nodes used to do lots of route requests will have lower priority and removed out of the routing process. To detect DATA flooding attack, the solution is to remove suspected routes with useless data packet routed. Hence, victim nodes can send RERR packet to remove route related to flooding attack. However, the detail of selecting threshold value of priority to detect RREQ flooding attacks is not presented specifically. This issue is solved in [15], authors has also included solutions to detect RREQ and DATA packet flooding attacks. To detect RREQ flooding, one threshold value is established basing on data of all neighbors. In addition, detection of DATA flooding attack is also presented basing on data received at the application layer.

In [14], Jiang proposed a double defense wall system (DDWS) basing on energy-saving technology to reduce impact of flooding attacks in the AODV routing protocol. Basing on RREQ RATELIMIT parameter defined in the RFC standard, priority of one network node creating RREQ is based on flow rate with 3 levels: legal, moderate and stronger. Then, RREQ packets received from one node with leading priority (equivalent third priority) are forwarded (or removed if contrary). For nodes with moderate priority, upgrading and downgrading policies will be applied according to changes in flow rate of RREQ of nodes.

In [16], Desilva presented about RREQ flooding attack and its impact on network throughput basing on the numbers of malicious nodes. To reduce impacts of flooding attacks, they recommended an adaptive statistical packet dropping mechanism. This method is based on random delay assessment technique to follow redundant message packets received during a certain time. Finally, profile of one node is created and threshold value is calculated into each period of sampling. This threshold value is used to realize RREQ flooding attacks or moderate.

Similarly, in [17] Balakrishnan also shown a solution of adding more new component into each node which is tasked to follow the limited threshold of route request message of all neighbors. This solution has resolved detection of RREQ flooding attacks but DATA packet.

B. Prevention Solution

In [18], SAODV is improved from AODV by Zapata to prevent dummy attacks by changing HC and SN values of route discovery packet. However, the existence of SAODV only supports certification from end-to-end without certifying hop-by-hop, hence, intermediate node can not certify message packet from the preceding node. In addition, because SAODV is not available with key distribution mechanism for node, malicious can pass over security by using fake keys

Sanzgiri also recommended ARAN protocol [19] as well as prevention solutions apply mechanism of authentication, integrity, and non-repudiation based on digital signature. Different from SAODV, route discovery packet RDP in ARAN is signed and certified at all hop-by-hop nodes and end-to-end. Furthermore, ARAN has supplemented the testing member node mechanism, thus, malicious can not pass over security by using fake keys. Structure of RDP and REP of ARAN is not available with HC to identify routing cost; this means ARAN is unable to recognize transmission expenses to the destination, ARAN argued that the first REP received is the route packet with the best expenses.

In [20], SEAR protocol is designed by Li basing on the ideal of AODV which use a one-way hash function to build up a hash set of value attached with each node and is used to certify route discovery packages. In SEAR, Identification of each node is encoded with SN and HC values; hence, it prevents iterative route attacks. Similarly, Mohammadizadeh from AODV develops SEAODV [21] by using certification scheme HEAP with symmetric key and one-way hash function to protect route discovery packet. By simulation, the author has shown that SEAODV is more security with lower communication overhead.

III. Our Solution

RREQ flooding attack, one out of three kinds of flooding attacks, is the most hazardous because it is easy to create broadcast storm. This article focuses on solutions applied to detect flooding attacks of RREQ by recommending a new mobile agent SMA. During building up a security solution to detect RREQ flooding attacks in the AODV protocol, we use some related definitions following:

- **Definition 1:** Route discovery time is the duration from the start of discovery to receiving route responses which is calculated by formula 1 in which *s* is the time-point route discovery is performed, *e* is the time-point of receiving route response.

$$t = e - s \quad (1)$$

- **Definition 2:** Route discovery time-slot (RDTS) is the duration between two discoveries calculated by formula 2 in which e_i is the time-point of receiving route of i, s_{i+1} is the time-point of following route discovery is started.

$$T = s_{i+1} - e_i \quad (2)$$

- **Definition 3:** Minimal route discovery time-slot of one node is the minimal duration of route discoveries, is calculated by formula 3, where *m* is the number of time-slot.

$$T_{\min} = Min(T_i); \forall i = \overline{1..m} \quad (3)$$

- **Definition 4:** Minimal route discovery time-slot of one system is the minimal duration between route discoveries in the entire system which is calculated by formula 4 in which *n* is the number of network node.

$$TS_{\min} = Min(T^j_{\min}); \forall j = \overline{1..n} \quad (4)$$

- **Definition 5:** Diagram of route discovery time-slot of the system (DRDTS) is built up basing on time-slot diagram of each node as Fig. 2. It is assumed that N_i receives 5 route discovery requests of N_1, then route discovery time-slot diagram of node N_1 at node N_i is described in Fig. 2a.

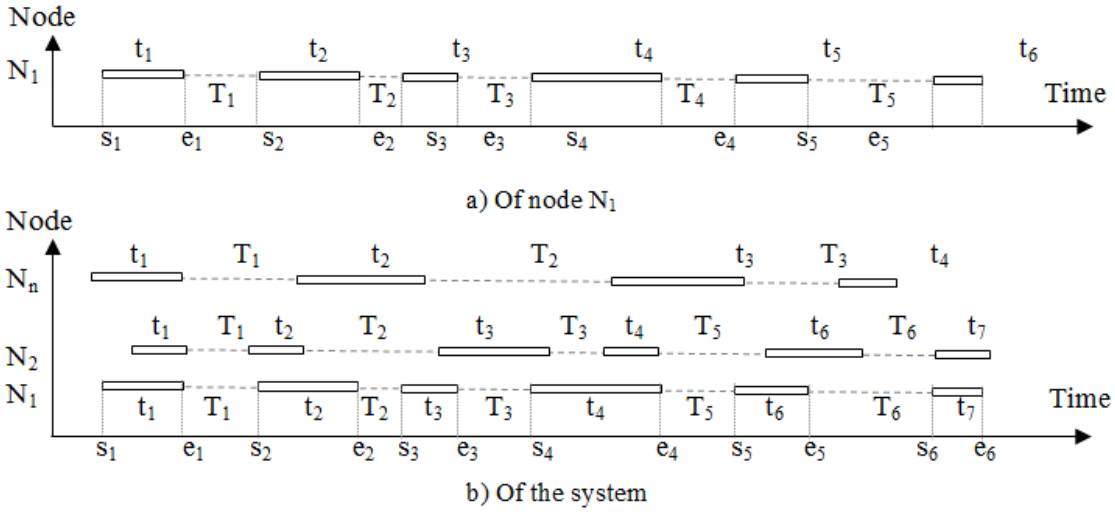


Fig. 2. Diagram of route discovery time-slot

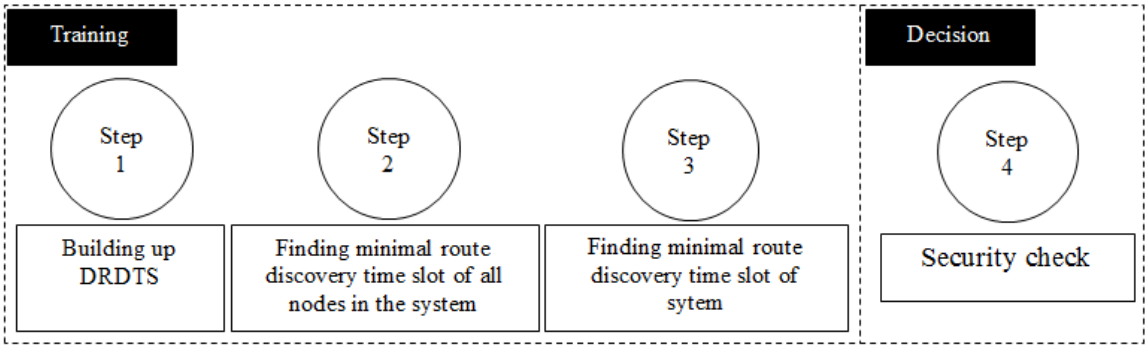


Fig. 3. SMA diagram to detect RREQ flooding attacks

A. Proposing Security Mobile Agent (SMA)

The frequency of route discovery depends on the demand of routing at each node in the normal network condition with low route discovery frequency. However, when it appears malicious nodes to attack Flooding using RREQ packet, then frequency of route discovery becomes regular, this is the characteristic is used by us to build up SMA which allows to detect malicious nodes as shown in Fig. 3.

SMA includes two basic stages, training and checking. Where, checking is only performed after finishing training. The detail of each stage is as follows:

a) Step 1: Building up diagram of a system time-slot

In the stage of training, all nodes collect route discovery information of other nodes in the system when receiving request package of RREQ to build up diagram of system time-slot.

b) Step 2: Finding minimal route discovery time-slot of each node

Using input data it is route discovery time-slot diagram of the system build up in step 1 and applying formula 3 to calculate minimal time-slot (T_{min}) of all nodes.

c) Step 3: Finding route discovery time-slot of the system

Basing on data collected at step 1 and step 2, applying formula 4 to calculate minimal time-slot (TS_{min}) of the system. This is the threshold value to check security at step 4.

d) Step 4: Security check

If the training stage is completed, each node will check security when receiving route request from any source node N_i. If route discovery time-slot of node N_i is smaller than minimal route discovery time-slot of the system ($T < TS_{min}$), then RREQ Flooding attacks appear, RREQ packet is dropped and N_i is added Black List (BL).

B. Improved Protocol SMA$_2$AODV

Original AODV protocol accepts all RREQ route discovery packets from any source nodes, this is the weak point utilized by Hackers to perform RREQ Flooding attacks. Our solution is to integrate the SMA into the broadcast RREQ packet process to discovery route of AODV protocol, new protocol named SMA$_2$AODV.

See in Fig. 4, in the stage of training (curent time < TRAIN_TIME), SMA$_2$AODV operates under mechanism of AODV protocol, all RREQ packets received are all accepted and continued to broadcast to all neighbors. Compared with AODV, SMA agent is used to collect information for calculation of minimal time-slot of the system (TS_{min}), makes it different. This value is used by current node to detect RREQ Flooding attacks; hence, requirement in tranning phase is the removal of malicious nodes.

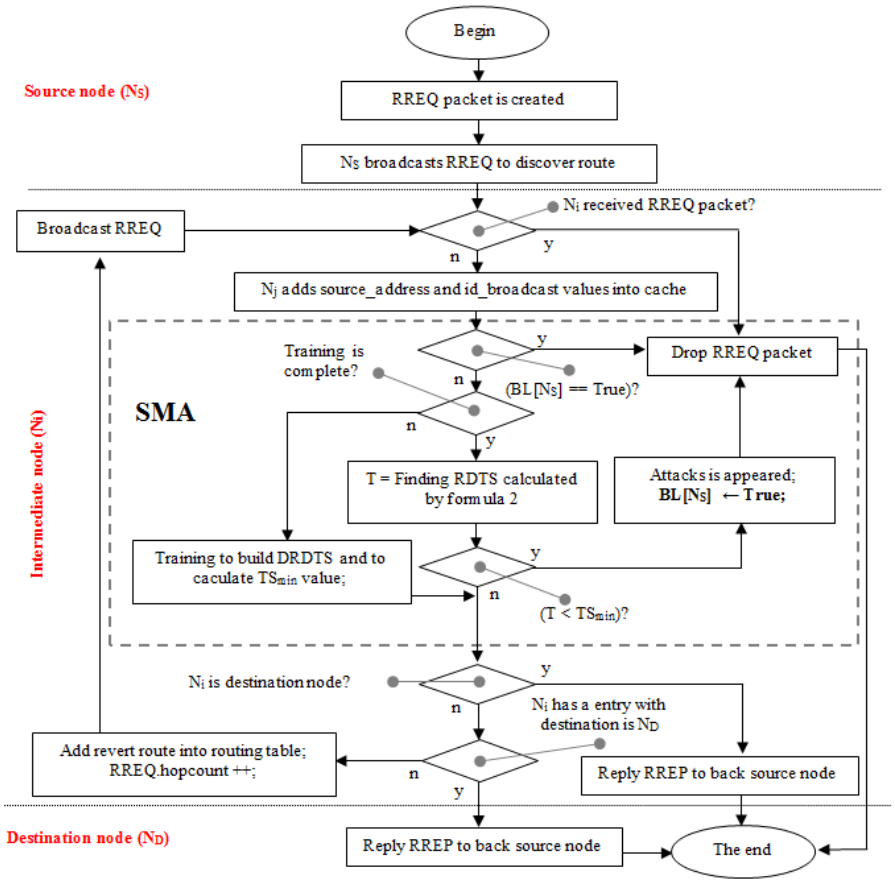


Fig. 4. Improved algorithm to broadcast RREQ packet in SMA$_2$AODV protocol

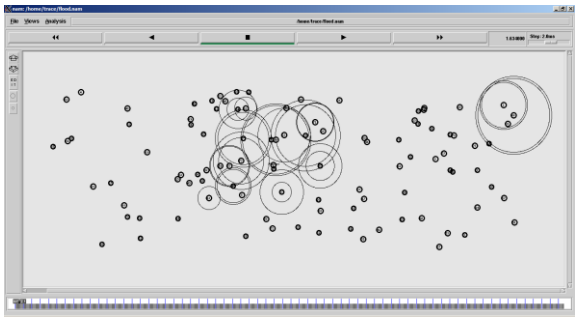
After training phase, all node (N_i) checks security of RREQ packet received from source node N_j before broadcasting to its neighbors. If route discovery time-slot is smaller than minimal time-slot of the system ($T < TS_{min}$), then Flooding attacks are appeared, N_i adds N_j into Black List. All RREQ packets of nodes in Black List will be dropped without security check needed to increase processing efficiency.

IV. Performance Evaluation by Simulation

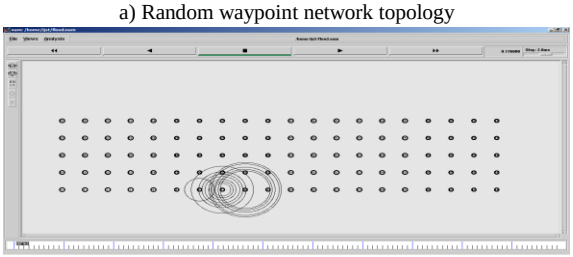
We evaluate the impact of flooding attack on AODV protocol and security efficiency of SMA_2AODV protocol on two network topologies with mobile node or immobile nodes, simulation system is NS2 [22] –version 2.35.

A. Simulation Settings

Both simulation topologies are available with 100 normal nodes and 1 malicious node, and operated in the scope of 3200m x 1000m. Mobility node topology including mobility nodes (Fig. 5a) under Random Waypoint (RWP [23]), created by *./setdest* tool. Grid network topology (GRID) including nodes arranged in the shape of grid (Fig. 5b), each node is 150m far from each other.



a) Random waypoint network topology



b) Grid network topology

Fig. 5. Simulation screen on NS2

Simulation protocols are AODV and SMA_2AODV, during 200s of simulation; node transmission range was 250m, FIFO queue, 10 UDP connects, CBR Traffic type, packet capacity of 512bytes; malicious nodes are immobile at the central position (1600, 500) and perform flooding attack behavior of RREQ started at second of 50; the first UDP is started at second of 0, the following UDP is 5 seconds apart from each node, nodes participating into data flow (source and destination node) include {(0, 19); (3, 56); (6, 93); (21, 77); (41, 59); (62, 91); (65, 73); (80, 12); (84, 32); (99, 40)}; the detail of simulation parameters are collected in the following Table I.

TABLE I: SIMULATION PARAMETERS

Parameters	**Setting**
Simulation area	3200 x 1000 (m)
Node transmission range	250 (m)
Simulation time	200 (s)
Number of nodes	101
Number of malicious nodes	1
Traffic type	CBR
Number of connection	10 UDP
Packet size	512 (bytes)
Queue type	FIFO (DropTail)
Routing protocols	AODV, MSA_2AODV
TRAIN_TIME	50 (s)
Mobility speed	1..10 (m/s)

To evaluate the impact of RREQ Flooding attack and advanced solutions of AODV protocol to detect attack, we use some criterion: *The detection ratio of fake RREQ, Packet Delivery Ratio, Network throughput, Packet overhead, and Routing load.* [19], [24]

- *Detection ratio of fake RREQ packets (DRFP):* Parameter evaluates the dectection ratio of fake RREQ packets that are detected by our security solution.
- *Packet delivery ratio (DPR):* 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;
- *Network throughput (NT):* The parameter is amount of data transferred from source to destination in a given amount of time which is calculated by (total packet sent successfully * size of packet) / simulation times.
- *Routing load (RL):* This is the ratio of overhead control packets to delivered data packets.

B. Simulation Results

Fig. 6 shows that MSA_2AODV protocol operates effectively when suffers from RREQ Flooding attacks. After 200s simulation, the detection ratio successfully of fake RREQ packets is 98.79% in GRID network topology and 98.14 % in Random waypoint network topology.

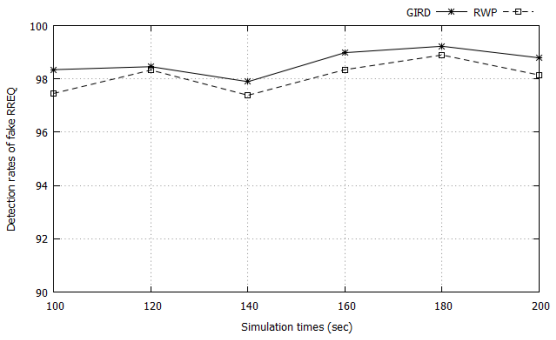
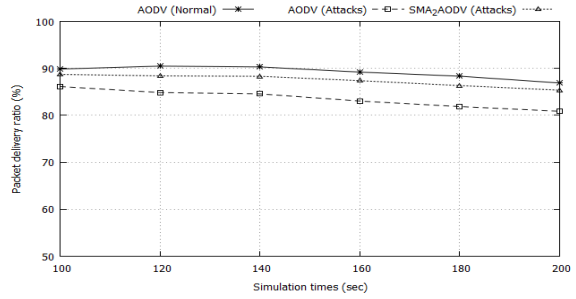


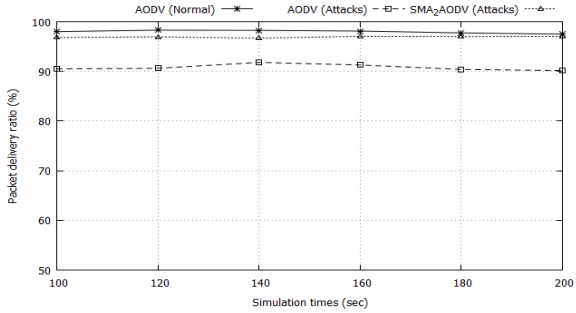
Fig. 6. Detection rates of fake RREQ packets

Fig. 7a shown that RREQ Flooding 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 RWP network topology, the PDR of AODV is 86.89% in normal network topology and 80.88% under RREQ Flooding attacks, 6.01% reduced. With the same simulation scenario of getting RREQ Flooding attacks, then PDR of SMA_2AODV protocol is 85.35%, 4.47% improved. In GRID network topology, Fig. 7b shown that the PDR of AODV is 97.5% under normal network topology and 90.17% under attacks, 7.33% reduced. Using SMA_2AODV protocol then PDR is 97.06%, 6.89% improved.



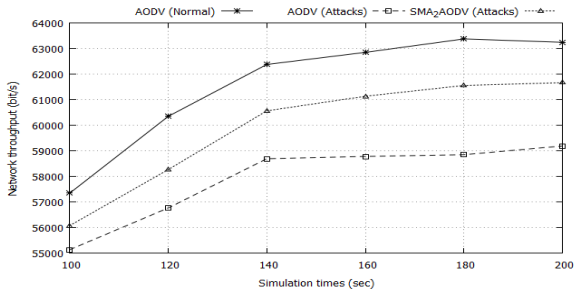
a) RWP



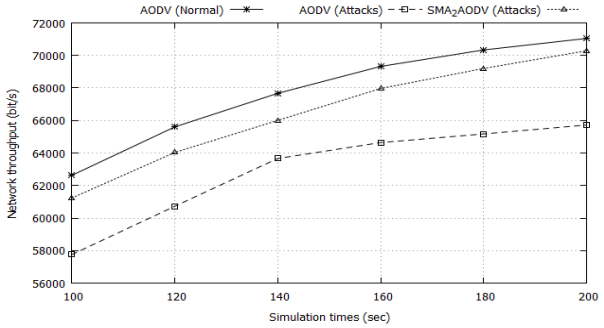
b) GRID

Fig. 7. Packet delivery ratio

Fig. 8a shown that RREQ Flooding attacks has reduced network throughput. After finishing 200s simulation in RWP network topology, the NT of AODV is 63,242.2 bit/s in normal network topology and 59,187.2 bit/s under RREQ Flooding attacks, 6.01% reduced. Network throughput of SMA_2AODV protocol has been improved to 61,665.3 bit/s, 2,478.1 bit/s improved. Fig. 8b shown that the NT of AODV protocol is 71,045.1 bit/s in normal network topology, and 65,720.3 bit/s under attacks network topology, 7.5% reduced. The NT of SMA_2AODV is 70287.4 bit/s under attacks, 4,567.1 bit/s improved.



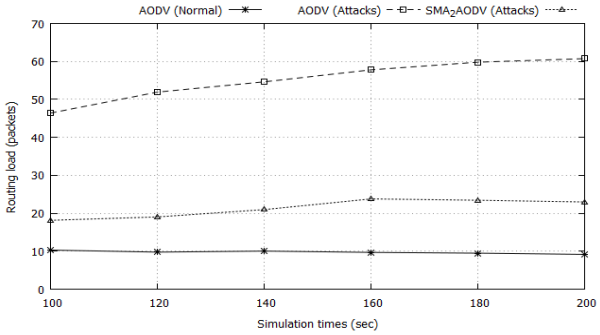
a) RWP



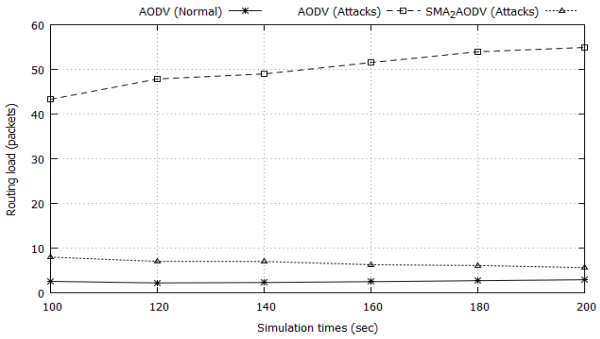
b) GRID

Fig. 8. Network throughput

Fig. 9a shown that routing load is increased in attacks network topology, after 200s of simulation in normal network topology, then RL is 9.16 packets, increasing to 60.74 packets (663.19%). With the same simulation scenario in the attacked network topology, then RL of SMA_2AODV protocol is 22.97 packets, reducing to 37.77 packets compared with AODV protocol. Fig. 9b shown that the RL of AODV increase suddenly to 54.90 packets, compared with 2.91 packets when operating in normal network topology (1,889.81%). However, because SMA_2AODV protocol is effectively operated, RL is only 6.64 packets, reducing to 48.26 packets compared with AODV.



a) RWP



b) GRID

Fig. 9. Routing load

V. Conclusion and Future Works

We recommended a security routing protocol SMA_2AODV by integrating SMA into the discovery route process of AODV protocol. The simulation result shown that our solution is effectively operated in the

attacked network topology, the detection ratio successfully of fake RREQ packets is over 98% in GRID and RWP network topology. Addition, the packet delivery ratio, network throughput and routing load of SMA_2AODV become better when operating under RREQ Flooding attacks network toology. In the future, we will continuously improve SMA so that Flooding attacks in HELLO and DATA packets can be detected.

ACKNOWLEDGMENT

The article is supported with financial of Scientific and Technological Project no B2016-DHH-21, Ministry of Education and Training, Viet Nam.

REFERENCES

[1] 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, pp. 60–66, 2004.

[2] 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.

[3] T. Cholez, C. Henard, I. Chrisment, O. Festor, G. Doyen, and R. Khatoun, "A first approach to detect suspicious peers in the KAD P2P network," in *Proc. Conference on Network and Information Systems Security*, 2011, pp. 1–8.

[4] K. Yaser, B. Abdulraheem, M. Wail, and B. Muneer, "A new protocol for detecting black hole nodes in ad hoc networks," *International Journal of Communication Networks and Information Security*, vol. 3, no. 1, 2011.

[5] D. B. Roy, R. Chaki, and N. Chaki, "BHIDS: A new, cluster based algorithm for black hole IDS," *Security and Communication Networks*, vol. 3, no. 2–3, pp. 278–288, 2010.

[6] L. Sánchez-Casado, G. Maciá-Fernández, P. García-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.

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

[8] I. Khalil, S. Bagchi, and N. B. Shroff, "MobiWorp: Mitigation of the wormhole attack in mobile multihop wireless networks," *Ad Hoc Networks*, vol. 6, no. 3, pp. 344–362, 2008.

[9] S. Khurana and N. Gupta, "End-to-end protocol to secure ad hoc networks against wormhole attacks," *Security and Communication Networks*, vol. 4, no. 9, pp. 994–1002, 2011.

[10] L. Thai-Ngoc and V. Thanh-Tu, "Whirlwind: A new metho d to attack routing protocol in mobile ad hoc network," *International Journal of Network Security*, vol. 19, no. 5, pp. 832–838, 2017.

[11] Y. Ping, D. Zhoulin, Y. Zhong, and Z. Shiyong, "Resisting flooding attacks in ad hoc networks," in *Proc. International Conference on Information Technology: Coding and Computing- Volume II*, vol. 2, pp. 657–662, 2005.

[12] C. E. Perkins, M. Park, and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. Second IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 90–100.

[13] H. Ehsan and F. A. Khan, "Malicious AODV: Implementation and analysis of routing attacks in MANETs," in *Proc. Conference on Ubiquitous Computing and Communications*, 2012, pp. 1181–1187.

[14] F. C. Jiang, C. H. Lin, and H. W. Wu, "Lifetime elongation of ad hoc networks under flooding attack using power-saving technique," *Ad Hoc Networks*, vol. 21, pp. 84–96, 2014.

[15] P. Yi, Y. Hou, Y. Bong, S. Zhang, and Z. Dui, "Flooding attacks and defence in ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 17, no. 2, pp. 410–416, 2006.

[16] S. Desilva and R. V. Boppana, "Mitigating malicious control packet floods in ad hoc networks," in *Proc. IEEE Wireless Communications and Networking Conference, WCNC*, 2005, vol. 4, pp. 2112–2117.

[17] V. Balakrishnan, V. Varadharajan, and I. Group, "Mitigating flooding attacks in mobile ad-hoc networks supporting anonymous communications," in *Proc. 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, 2007, p. 29.

[18] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106–107, 2002.

[19] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proc. ICNP*, 2002, pp. 78–89.

[20] Q. Li, M. Y. Zhao, J. Walker, Y. C. Hu, A. Perrig, and W. Trappe, "SEAR: A secure efficient ad hoc on demand routing protocol for wireless networks," *Security and Communication Networks*, vol. 2, no. 4, pp. 325–340, 2009.

[21] M. Mohammadizadeh, A. Movaghar, and S. Safi, "SEAODV : Secure efficient AODV routing protocol for MANETs networks," in *Proc. ICIS '09*, 2009, pp. 940–944.

[22] DARPA. (1995). The network simulator NS2. [Online]. Available: http://www.isi.edu/nsnam/ns/

[23] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful," in *Proc. IEEE INFOCOM 2003*, vol. 2, 2003, pp. 1–11.

[24] C. Joseph, P. C. Kishoreraja, R. Baskar, and M. Reji, "Performance evaluation of MANETS under black hole attack for different network scenarios," *Indian Journal of Science and Technology*, vol. 8, no. 29, pp. 1–10, 2015.

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 routing protocol, wireless ad hoc network.

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 security routing protocol, analysis and evaluation of network performance.