VRA-AODV: Routing Protocol Detects Blackhole and Grayhole Attacks in Mobile Ad hoc Network

Thanh-Tu Vo[1], Thai-Ngoc Luong[1,2*]

[1] Faculty of Information and Technology, Hue University of Sciences, Hue University, Viet Nam.
[2] Faculty of Mathematics and Informatics Teacher Education, Dong Thap University, Viet Nam.

* Corresponding author. Tel.: +84 0917 415 995; email: ltngoc@dthu.edu.vn
Manuscript submitted January 20, 2017; accepted April 20, 2017.
doi: 10.17706/jcp.13.2.222-235

Abstract: Mobile Ad hoc Network is a collection of wireless mobile nodes that dynamically creates network without a fixed infrastructure. However, all the characters make the security problems, such as Blackhole, Grayhole attacks. In this article, we propose Valid Route Authentication mechanism (VRA) for security, and integrating VRA into the discovery route process of AODV protocol. Improved protocol named VRA-AODV which can detect Black and Grayhole attacks. Using NS2, we compare the performance of AODV and improved protocols in the mobility nodes topology under attacks. Simulation results show that improved protocol has better performance AODV based on packet delivery ratio, network throughput and routing load metrics.

Key words: AODV, MANET, VRA-AODV, network attacks, protocol, security.

1. Introduction

Mobile Ad hoc Network (MANET [1], [2]) is a wireless network connecting mobile devices, which is low cost, easy setup, infrastructure, and independent. In MANET, nodes are able to move freely to any direction and cooperate to forward packets to each other to reach destination beyond source node's transmission range. MANET is a peer–to–peer network, in which every node plays the same role as a host and also a router. The network topology changes frequently because of nodes exiting or joining. Thus, MANET is sufficient deploy in places with no infrastructure exist, in instable environment or in emergency situations such as: disaster rescue, urgent conference and communication in military mission.

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 network cannot be applied in infrastructure-less network like MANETs. Hence, many routing protocols are recommended to adapt to MANET, they are classified into proactive, reactive, and hybrid routing [3]. Proactive routing protocol is suitable with stable network topology because routes of network nodes must be established to connect with other nodes before routing. 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. In mixed network topology, hybrid routing protocols are highly sufficient. 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, in which a malicious node will try to keep their resource but occupy other node's resource, for example, Blackhole [4], Grayhole [5] under DoS. Ad hoc On-demand Distance Vector (AODV [6]) routing protocol is one of the most popular reactive routing

protocol used for Ad hoc Networks. This is typical protocol under on-demand routing protocol, hence, hackers are easy to perform Blackhole and Grayhole attacks (or called B&G attacks).

The next section, we review some studies relating to detection and prevention attacks in AODV. Section 3 describes the discovery route process and detail to setup B&G attacks in AODV. Section 4 shows the detail authentication mechanism VRA for security, and integration VRA into AODV protocol to form VRA-AODV protocol that can detect malicious nodes. Section 5 shows the damage evaluation results of B&G attacks to routing capacity of AODV protocol and performance of VRA-AODV protocol in under B&G attacks and the final section is conclusion and future works.

2. Related Works

During the last time, some research works published related to prevention of B&G attacks, solutions given mainly focus on *detection* and *prevention.* The advantages of detection solution are low cost, but they mainly base on characteristics of attacks 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.

2.1. Detection Solution

In [7], Kurosawa and his associates have introduced solutions to detect Blackhole attacks via automatic algloryghm. After the training process is done to determine the detection threshold (*th*) of Blackhole attacks, trained data contain no information of Blackhole node. In [8], Raj and his associates describe PDRAODV protocol that allow *detecting*, *preventing* and *reacting* in case of Blackhole attacks. His idea is to build-up procedures to allow check and determine "trust" of RREP packet basing on two thresholds named th_1 and th_2. Algorithm bases on checking sequence number (*SN*) number in RREP received in comparison to *SN* value in its routing table (RT), RREP is accepted if *SN* number belongs to two thresholds named th_1 and th_2. Abnormally detected nodes are noted into blacklist, RREP packets sent from malicious node are removed, node broadcasts ALARM packets containing the malicious node information to neighbor. In [9], Weerasinghe and his associates have proposed the anti-cooperation solution to attack Blackhole by using the DRI table information and cross-check. Structure of DRI table includes 2 bit: the first bit named "From" shall identify where routing information comes from, the second bit named "Through" show which node the routing information comes through, check process shall base on "trusted nodes" to transfer the packet. In [10], Patcha and his associates have introduced a cooperation solution to prevent the Blackhole attacks. Watchdog solution is recommended to handle collusion of nodes. In this algorithm, network's nodes are classified as trusted node, watchdog node and ordinary node. Each established watchdog shall monitor its normal neighbor nodes and determine whether they are trusted or malicious. In [11], Shila and his co-workers have represented a solution to detect the selective transfer attack (Grayhole attacks) in WMN network. The first phase of algorithm is Counter-Threshold, using the detection thresholds and packets counter to determine the attacks. The second phase is Query-Based, using confirmation from intermediate nodes to determine the location of attackers. In the first phase, controlling packet and ACK packet are both used to expose attacker. Moreover, this solution determines the suitable threshold values basing on data in routing number ETX [12] to improve performance according to different network topology.

2.2. Prevention Solution

In [13], 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't 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 [14] 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 key distribution mechanism for nodes. 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 [15], 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 (ID) of each node is encoded with SN and HC values; hence, it prevents iterative route attacks. Similarly, Mohammadizadeh from AODV develops SEAODV [16] 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.

3. Background

3.1. Overview on AODV Routing Protocol

AODV routing protocol uses the route discovery mechanism if it is necessary and suitable with MANET. When node N_S wants to send data to destination node N_D however there is not route in its RT, N_S discovers route by broadcasting route request packet (RREQ) to their neighbor nodes, this process is continued at intermediate nodes until destination node N_D receives the RREQ packet. When receiving RREQ packet, node N_D replies RREP containing route information to source N_S, and saves route to destination N_D into its RT, the intermediate nodes also reply RREP if there are enough "fresh" route to destination node N_D. This is a protocol belongs to routing group basing on distance vector, the routing cost is therefore calculated basing on nodes from source N_S to destination N_D, this is hop count (HC) value in RREQ request packet and RREP reply packet. HC value increases 1 when packet is forwarded by nodes. Moreover, each node remains S_N value to determine "fresh" of recently explored route. Basing on HC value and destination sequence number (DSN) value of node N_D in RREP, source node N_S updates new route provided that newly explored route is "fresh" enough and cheapest to reach destination.

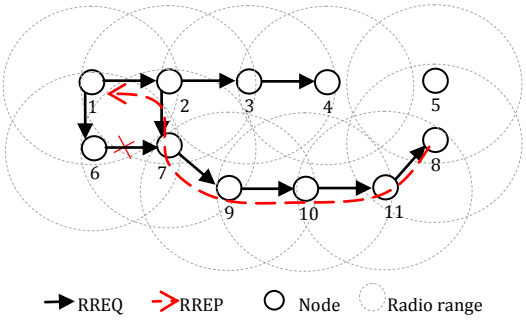

Fig. 1. Discovery route of AODV protocol.

Fig. 1 describes source node N_1 discovering route to destination N_8 by broadcasting RREQ packet to neighbors {N_2, N_6}. N_2 is not a destination node, it therefore continues broadcasting to all its neighbors named {N_3, N_7}, this processing loops in N_6 and other intermediate nodes until node N_8 receives the route requesting packet. Each node only handle RREQ packet on time, the node N_7 therefore drops RREQ packet sent by N_6 because N_2 has sent before. When receiving RREQ packet, destination node replies RREP packet to back source on route {$N_8 \rightarrow N_{11} \rightarrow N_{10} \rightarrow N_9 \rightarrow N_7 \rightarrow N_2 \rightarrow N_1$}. The result is if source node N_1 wants to route data to destination N_8, the data must be transferred via next hop intermediate node named N_2 with routing cost to

destination is 6 hops.

3.2. Description of Blackhole (Sink Hole) Attacks

Blackhole attacks [17] may be performed by one or more malicious nodes, if two connected malicious nodes are used, this form is called cooperative Blackhole attack [18]. In order to perform Blackhole attacks, malicious attack in two 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 sent from source and drops all, so this may be deemed as the destruction attack form. In Blackhole attack cooperation, data packet is transferred to the second malicious node, and data are dropped in this node to prevent any detection. It results in the drop of the data packets of UDP flow accordingly, TCP flow is interrupted because it has not received ACK signal from destination node. Author's simulation results [19] show that when data packet suffers from Blackhole attack, AODV's data packet is destroyed at the ratio of more than 90%. The similar attack method but other name called Sinkhole attacks is discussed in [20].

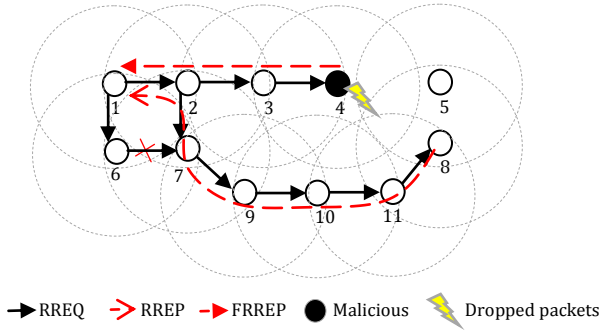

Fig. 2. Network topology under Blackhole attacks.

Fig. 2 describes source node N_1 discovering route to destination node where there is malicious node N_4 conducting Blackhole attacks. When receiving the route requesting packet, malicious node N_4 replies source node N_1 the Fake Route Reply Packet (FRREP) with the lowest cost (HC=1) and SN is big enough to ensure that route is "Fresh" enough. In this case, source node N_1 shall receive two route reply packets in directions $\{N_4 \rightarrow N_3 \rightarrow N_2 \rightarrow N_1\}$, and $\{N_8 \rightarrow N_{11} \rightarrow N_{10} \rightarrow N_9 \rightarrow N_7 \rightarrow N_2 \rightarrow N_1\}$. The route in FRREP packet has cost to destination of 3, and cost for route receiving RREP packet from source is 6. Accordingly, RREP packet is dropped, source node accepts FRREP packet to establish route to destination in direction because of low-cost. The result is if source node N_1 wants to route data to destination N_8, the data must be transferred via next hop intermediate node named N_2 with routing cost to destination is 3 hops.

3.3. Description of Grayhole Attacks

Grayhole attacks [5] is similar to Blackhole attack 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 sent from source and then drops packets 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 attacks. Simulation results of Grayhole attacks in NS2 with AODV protocol of author [21] show that drop ratio is about 80%.

4. Proposing Security Protocol VRA-AODV

B&G attacks have a common feature that malicious nodes self-advertises that it has route to destination with the lowest cost and fresh enough. In order to perform attacks, malicious node changes *HC* value in FRREP packet lower than actual route, and *DSN* value of FRREP must be big enough to ensure that the fake route must be "fresh" enough. Using this features, VRA mechanism can detect B&G attacks.

4.1. Authentication Mechanism VRA

Authentication mechanism VRA allows the source node to check safety of recently discovered route by using *HC* and *DSN* values in RREP packet. The route is defined valid if it suitable three conditions: actual neighbor nodes, normal route, and *DNS* value is valid.

- **Actual neighbor nodes:** Two nodes N_i and N_j are actual neighbors if they are under their respective coverage, it means $d(N_i, N_j) < \min(RN_i, RN_j)$. In which, d is Euclidean distance from N_i to N_j, according to formula 1.

$$d(N_i, N_j) = \sqrt{(x_{Ni} - x_{Nj})^2 + (y_{Ni} - y_{Nj})^2} \quad (1)$$

Example 1: In network topology in Fig. 3, nodes N_1 and N_2 are actual neighbors because distances between nodes is less than (or equal to) transmission radius of two nodes.

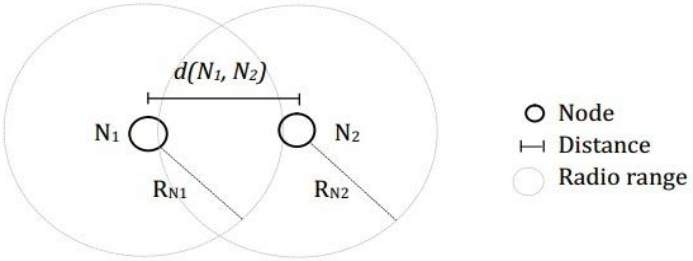

Fig. 3. N_1 and N_2 are actual neighbors.

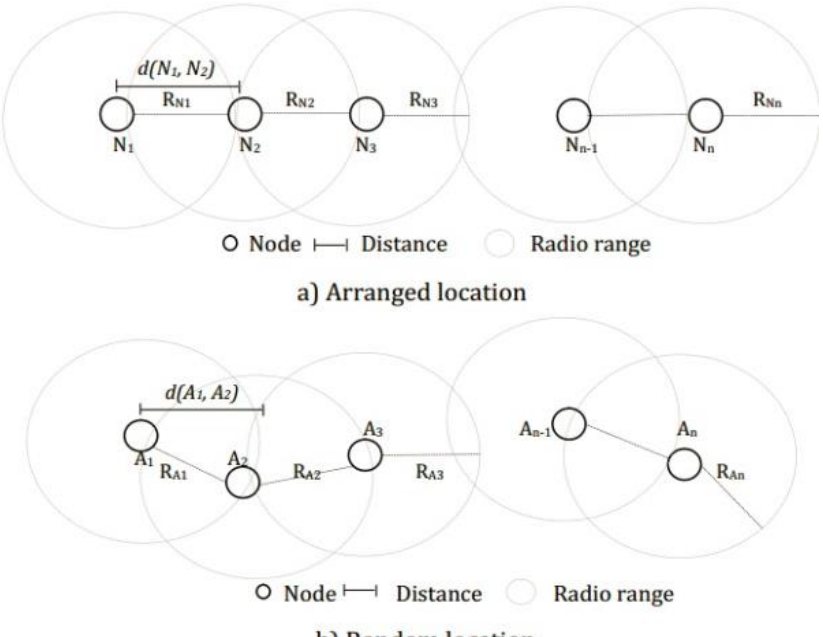

Fig. 4. Description of normal route.

- **Normal route:** It is assumed that source code N_1 discovers route to destination N_n in direction $N_1 \rightarrow N_2 ... \rightarrow N_i \rightarrow N_{i+1} ... \rightarrow N_{n-1} \rightarrow N_n$. This route is deemed as normal if with any two nodes N_i and N_{i+1}, they must be the actual neighbors.

Example 2: Route in network topology (Fig. 4) is normal route because with any two nodes (N_i, N_{i+1}), they are actual neighbors.

In order to detect any abnormality in recently discovered route, we shall analyze relation between *th* value and broadcasting radius (*R*) of each node. In which *th* is calculated basing on Euclidean distance (*d*) from source N_S to destination N_D and routing cost *HC* as formula 2, *x* and *y* values are node's location in network topology provided in LL layer in OSI model. In practice, we can use geographic coordinates information GPS [22] to determine the node's location.

$$th = \frac{d(N_S, N_D)}{HC} \tag{2}$$

In consideration of network in Fig. 4a, it is assumed that route from source node N_1 to destination node N_n is normal route, the routing cost therefore is $n - 1$. Applying respectively formula (1) and (2), we obtain the *th* value follow:

$$th = \frac{d(N_1, N_n)}{HC} = \frac{d(N_1, N_n)}{n-1} \leq \frac{(n-1)*R}{n-1} = R \tag{3}$$

In consideration of network topologies that have random nodes (Fig. 4b), route from source node A_1 to destination node A_n is normal route, the routing cost (*HC*) is $n - 1$. Because network's nodes locate randomly, the distance from A_1 to A_n is therefore less than distance from N_1 to N_n. Respectively applying the formula (1) and (2), we obtain the *th* value follows:

$$th = \frac{d(A_1, A_n)}{HC} = \frac{d(A_1, A_n)}{n-1} < \frac{(n-1)*R}{n-1} = R \tag{4}$$

From (3) and (4), we can conclude that if value *th* is less than (or equal to) maximum radio range (*R*) of node, the recently discovered route is therefore normal. In contrast there are no actual neighbor nodes on route (out of their respective coverage) due to malicious node intervention to reduce *HC*, thus, discovered route is therefore abnormal.

- **DNS value:** In AODV protocol, each node remains allowed *SN* value to determine freshness of recently discovered route. By misusing this feature, malicious node shall establish *DSN* value of FRREP packet to be big enough to ensure the fake route is "fresh" enough to perform B&G attacks. Thus, *DNS* value is valid if it is less than ($sn_{max} + \mu$) , in which sn_{max} is the maximum *SN* value of all entries in RT calculated under formula 5, μ is number of data flows, *n* is number of entries.

$$sn_{max} = Max(\text{Sequence Number}_i^{\text{Entry}}); \forall i = \overline{1..n} \tag{5}$$

Thus, the route is valid if *DSN* value is less than ($sn_{max} + \mu$) value, and *th* is less than (or equal to) maximum radio range (R); else the recently discovered route is therefore invalid, N_j is malicious node. Fig. 5 shows authentication mechanism VRA which allows the source node to check safety of recently discovered route when receiving RREP packet.

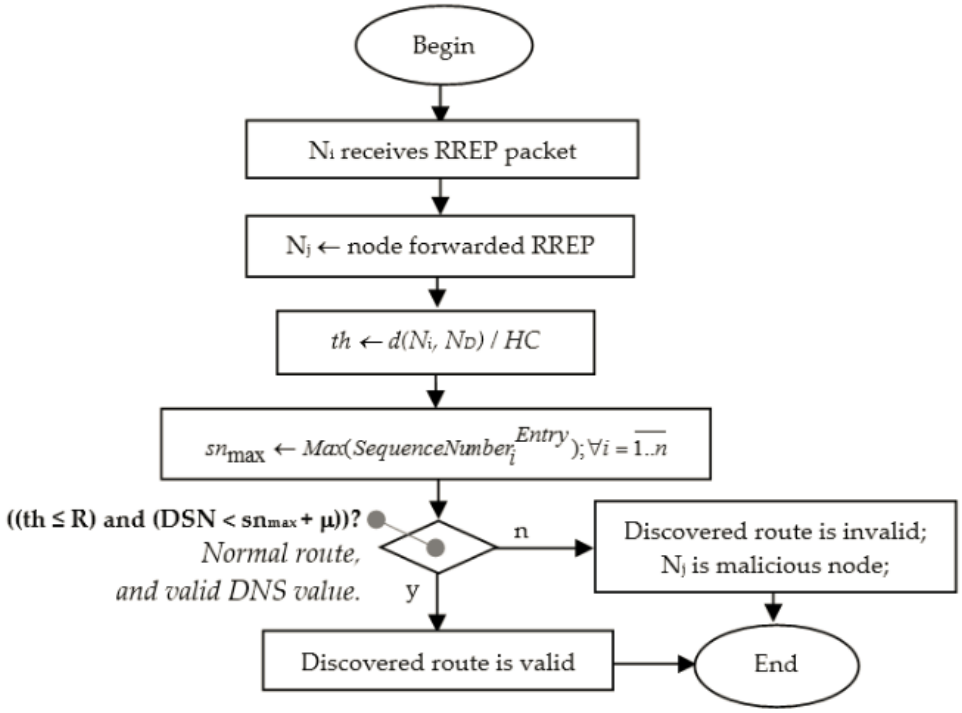

Fig. 5. Authentication mechanism VRA.

Fig. 6 (top) describes security check process by VRA for normal network topology as example at Fig. 1. Destination node replies RREP packet to back source on route {$N_8 \rightarrow N_{11} \rightarrow N_{10} \rightarrow N_9 \rightarrow N_7 \rightarrow N_2 \rightarrow N_1$} when it receive request route packet. At immediate node N_{11} uses authentication mechanism VRA to checks security, RREP is forwarded to N_{10} because the route from N_{11} to N_8 is valid ($d(N_{11}, N_8)/HC < R$ and DSN is valid). Similarly, node N_{10} also forward RREP packet to node N_9 because the route from N_{10} to N_8 is valid ($d(N_{10}, N_8)/HC < R$ and DSN is valid), processing check security is also performed at N_9, N_7, N_2 and N_1. The result is source node N_1 accepts RREP packet to setup a new route to destination node N_8, this route is valid.

However, in network topology under attacks as example at Fig. 2. FRREP packet is replied by malicious on direction {$N_4 \rightarrow N_3 \rightarrow N_2 \rightarrow N_1$}. Immediate node N_3 uses VRA to check security, FRREP packet is dropped because the route from N_3 to N_8 is invalid ($d(N_3, N_8)/HC > R$ and DSN is invalid), the detail of security check process in described in Fig. 6 (bottom).

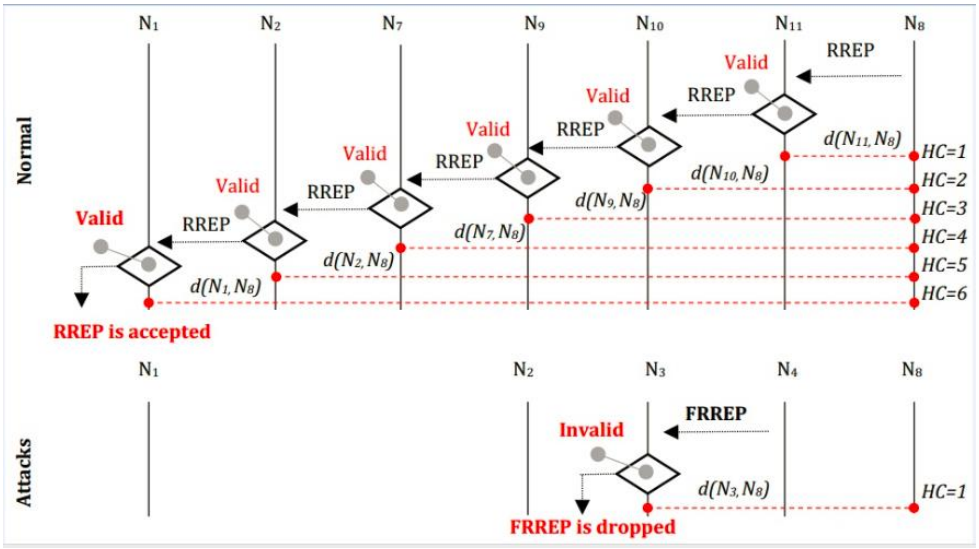

Fig. 6. Description security check process with VRA.

4.2. Integration of VRA into AODV Protocol

In route discover process of AODV protocol, when receiving RREQ packet, destination node replies RREP containing route information to source node. Intermediate node accepts all RREP packets received and forwarded to source, this is security weakness that is exploited by hacker to perform B&G attacks. Our solution is to add the authentication mechanism VRA into algorithm reply route of AODV in order to make security improved protocol named VRA-AODV that can detect B&G attacks, VRA performs in network layer as mobile agent for security checking and collects node location information by using the GPSP packet.

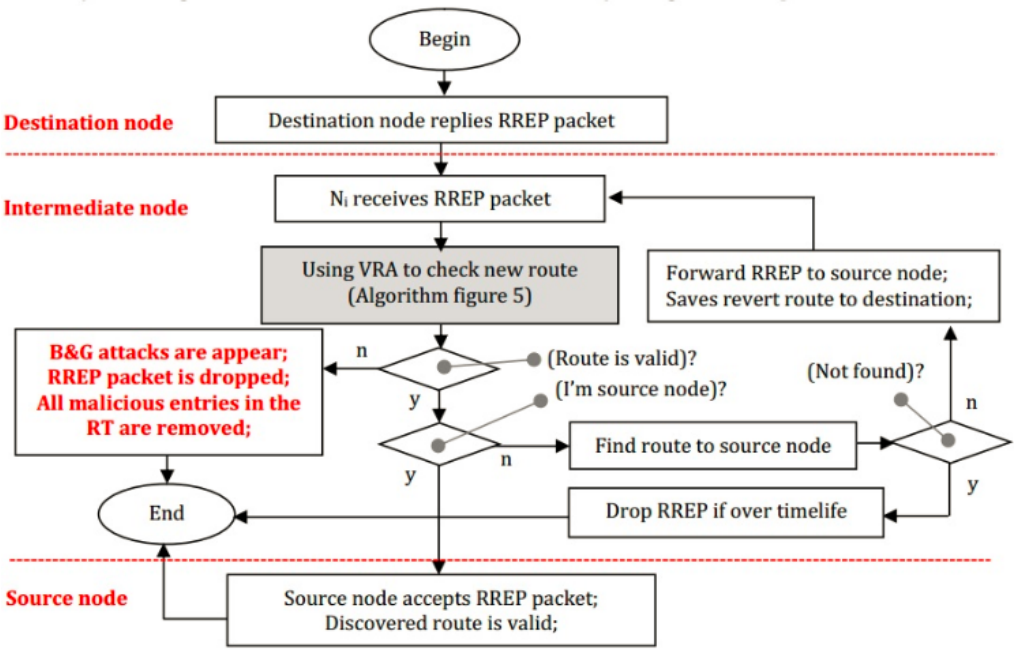

Fig. 7. Improved algorithm to reply RREP packet for security.

Improved algorithm (Fig. 7) shows that when receiving RREP packet forwarded from neighbor node N_j, node N_i checks security of recently discovered route by calling VRA mechanism. If the discovered route is valid, node shall continue forwarding RREP to source; else B&G attacks are appear, RREP packet is dropped, N_j is the malicious node, all malicious entries in node's RT are removed.

4.3. Collecting Location

Node location is ground to detect any abnormalities in discovering route, thus, we uses one-dimension vector (Table 1) to store the location status of all nodes. To collect node location, our solution is to use the mobile agent (MA [23]), they cooperates to collect locations of all nodes in network by using the GPSP packet, see algorithm in Fig. 8.

Table 1. Vector Stores Node Location

Nodes	[x, y]	[x, y]	[x, y]	[x, y]	[x, y]	[x, y]		[x, y]
	1	2	3	4	5	6	…	MAX_NODES

The communication overhead increase if nodes location are updated regularly. Thus, MA only broadcast GPSP packet to update nodes location if there are any location change with distance of GPS_D_MAX compared to former location, this reduce the communication overhead.

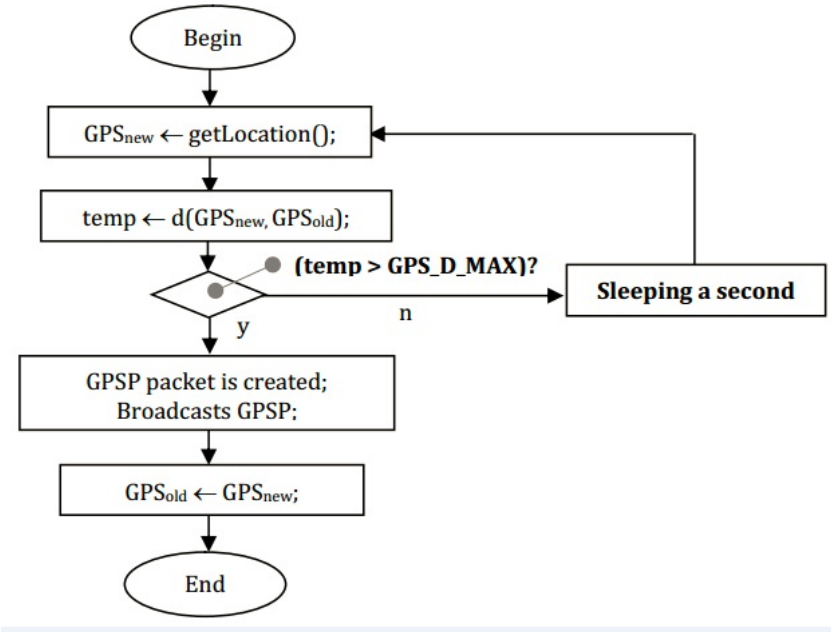

Fig. 8. Collection nodes location algorithm.

5. Performance Evaluation

In this section, we evaluate the impact of B&G attacks on AODV protocol and security efficiency of VRA-AODV protocol on simulation system is NS2 [24] – version 2.35, Fig. 9 shows NS2 simulation screen.

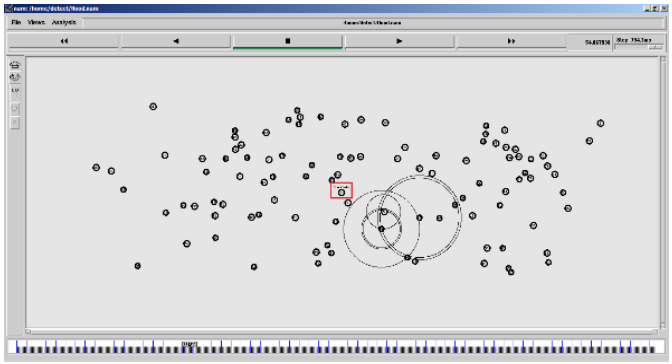

Fig. 9. NS2 simulation screen.

5.1. Simulation Settings and Evaluation Metrics

Simulation scenario is available with 100 normal nodes and 1 malicious node, and operated in the area of 3200m *x* 1000m, mobility nodes under Random Waypoint [25], created by ./setdest tool. Routing protocols are AODV and VRA-AODV, during 200s of simulation; node transmission range was 250m, FIFO queue, 10 UDP connects, CBR traffic type, two packets/ second, packet capacity of 512 bytes; malicious node is immobile at the central position (1600m, 500m) and perform B&G attacks at second of 50; the first UDP is started at second of 0, the following UDP is 5 seconds apart from each node; the detail of simulation parameters are listed in the following Table 2.

In order to evaluate the damages of B&G attacks, we use the simulation parameters as in Table 1 and add 1 malicious node that attacks from the 50th seconds, malicious node is fixed in center (1600m, 500m) as in Fig. 9, malicious node in Grayhole attacks changes from attack to normal status and normal to attack status after 5 seconds. Parameter used for evaluation is: Number of detected fake routes, packet delivery ratio, network

throughput, and routing load. [14]

Table 2. Simulation Parameters

Parameters	Setting
Simulation area (m)	3200 x 1000
Attack types	Blackhole, Grayhole
Node transmission range (m)	250
Simulation time (s)	200
Number of nodes	101 (1 malicious nodes)
Traffic type	UDP-CBR
Number of connection	10 pair (20 nodes)
Packet size (bytes)	512
Queue type	FIFO (DropTail)
Routing protocols	AODV, VRA-AODV
Mobility model	Random Waypoint
Speed (m/s)	1..10
GPS_D_MAX (m)	50

- *Number of fake routes are detected:* Parameter evaluates the numbers of fake routes that are detected by our security solution.
- *Packet Delivery Ratio (PDR):* Parameter evaluates trust of routing protocol that is calculated basing on total packets successfully sent to destination/total number of sent packets. The PDR decreases when there is a malicious node in the network because some of the packets are dropped by malicious nodes.
- *Throughput network:* Parameter evaluates the amount of data transferred from source to destination in a given amount of time that is calculated by (The number of packets delivered successfully * Packet size) / Simulation times.
- *Routing load (RL):* Parameter evaluates damage of B&G attacks, it is the ratio of the number of control packets overhead to the total number of the received data packets.

5.2. Simulation Results Analysis

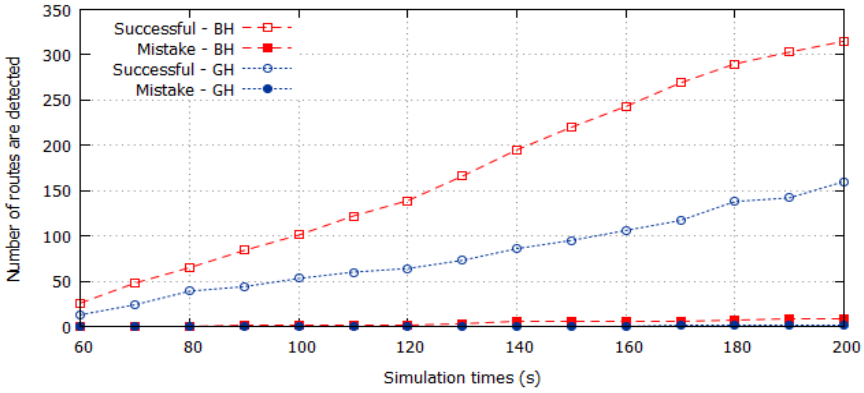

Fig. 10. Number of fake routes are detected; GH: Grayhole, BH: Blackhole.

Number of fake routes are detected: Number of detected fake routes chart (Fig. 9) shows that VRA-AODV protocol operates effectively when suffers from B&G attacks. However, detection efficiency of fake routes depends on node's location update that is regulated basing on constant GPS_D_MAX. In order to minimize communication overhead, node's location is only updated if its location changes 50m to former location, this leads to some mistakes in algorithm detecting fake route. After 200s simulation in Blackhole attacks topology,

there are 329 fake route is detected with 8 mistake route (the mistake ratio is 2.43%), and Grayhole attacks topology then there are 159 fake route is detected with 3 route is mistake (the mistake ratio is 1.88%).

Packet delivery ratio: Packet delivery ratio (PDR) chart (Fig. 11) shows that B&G attacks causes major damage to packing routing performance of AODV protocol. After 200s simulation, PDR only obtains 33.96% in case of Grayhole attacks and 16.36% upon suffering from Blackhole attacks, respectively reduce 52.93% and 70.53% in comparison to normal network topology. The same simulation, it gives out good result when integrating VRA into AODV protocol, packet delivery ratio of VRA-AODV protocol are 81.71% and 80.23% respectively when operating in B&G attacks network topology that is 5.18% and 6.66% lower respectively compared to normal network topology.

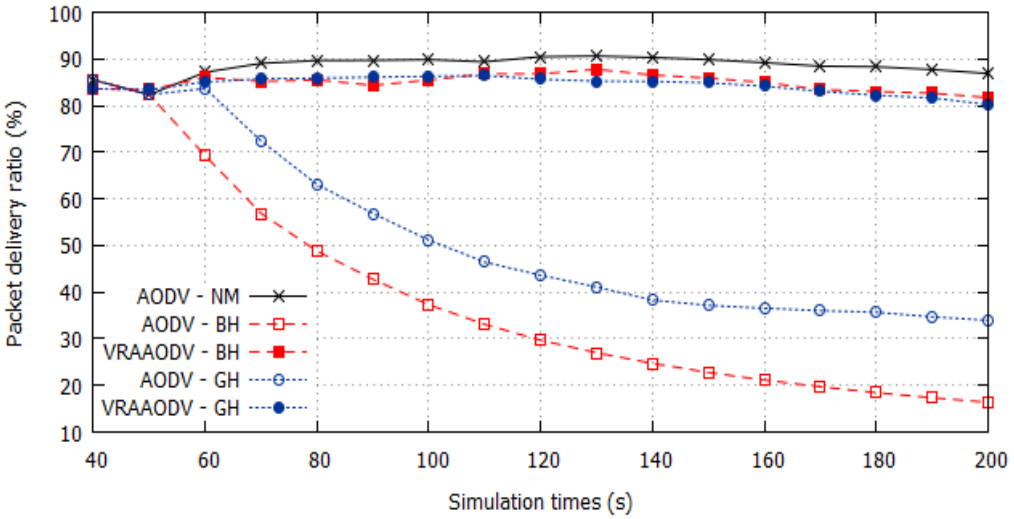

Fig. 11. Packet delivery ratio; NM: Normal, GH: Grayhole, BH: Blackhole.

Network throughput: Network throughput chart (Fig. 12) shows that B&G attacks cause serious damages the network throughput of AODV protocol reduces vastly. After 200s simulation, AODV's network throughput only obtains 11898.88 bit/s in network topology suffering from Blackhole attack and 24739.8 bit/s in case of Grayhole attacks. Network throughput of VRA-AODV protocol is improved significantly, respectively 59842.6 bit/s and 58183.7 bit/s in case of B&G attacks, this shows that VRA-AODV protocol can detect B&G attacks.

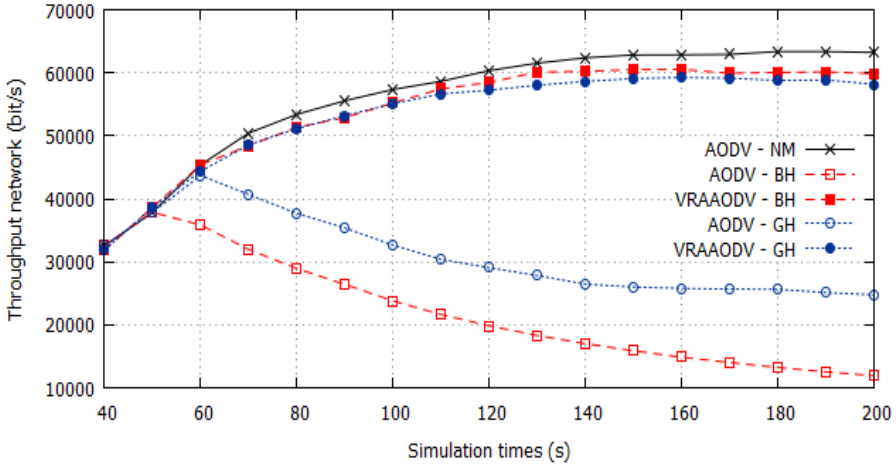

Fig. 12. Network throughput; NM: Normal, GH: Grayhole, BH: Blackhole.

Routing load: Routing load chart (Fig. 13) shows RL of VRA–AODV protocol increases higher than AODV, the reason is that VRA use the routing control packet GPSP to update node's location. After 200s simulation, RL of AODV increases by 26.79 packets when suffering from Blackhole attacks and 11.67 packets in case of Grayhole attacks, RL of VRA-AODV is 36.76 and 38.01 packets in corresponding to B&G attacks scenario.

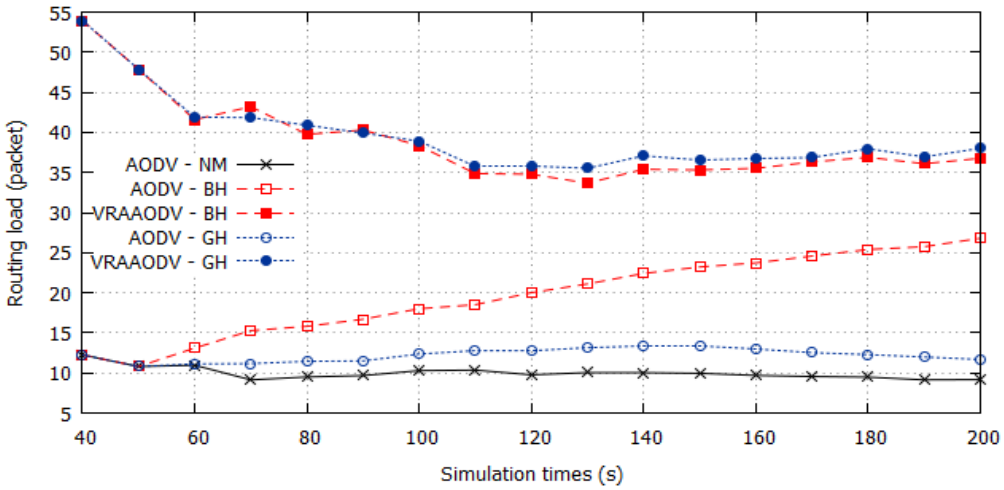

Fig. 13. Routing load; NM: Normal, GH: Grayhole, BH: Blackhole.

6. Conclusion and Future Works

B&G attacks are to destroy, it therefore reduces significantly packet delivery ratio, in which Blackhole causes more serious damages than Grayhole one. Security protocol VRA-AODV is recommended by us by improving AODV protocol that has given good detection fake route (97.56%, 98.11%) under B&G attacks, thus the PDR and throughput network are improved. Simulation result shows that in B&G attacks network topology, PDR of VRA–AODV protocol is improved significantly that is only slightly lower AODV protocol in network topology without attacks. However, the simulation results show that node has removed true routes which is not sent by malicious node, the reason is because node's location is not updated timely in mobility node network topology. Additionally, security solution of VRA-AODV protocol has used more GPSP's packets that cause communication overhead increase, moreover hacker can make use of GPSP packet to attack by faking destination nodes location.

In the future, we shall continue studying to keep security of GPSP packet as well as determining the suitable GPS_D_MAX constant value to enhance performance of detecting fake route and minimizing the communication overhead.

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] Jeroen, H., Ingrid, M., Bart, D., & Piet, D. (2004). An overview of mobile Ad hoc networks: Applications and challenges. *Journal of the Communications Network, 3,* 60–66.

[2] Al-Mistarihi, M. F., Al-Shurman, M., & Qudaimat, A. (2011). Tree based dynamic address autoconfiguration in

mobile ad hoc networks. *Computer Networks, 55(8),* 1894–1908.

[3] Alotaibi, E., & Mukherjee, B. (2012). A survey on routing algorithms for wireless Ad-hoc and mesh networks. *Computer Networks, 56(2),* 940–965.

[4] Roy, D. B., Chaki, R., & Chaki, N. (2010). BHIDS: A new, cluster based algorithm for blackhole IDS. *Security and Communication Networks, 3(2–3),* 278–288.

[5] Gao, X., & Chen, W. (2007). A novel grayhole attack detection scheme for mobile Ad-hoc networks. *Proceedings of International Conference on Network and Parallel Computing Workshops* (pp. 209–214).

[6] Perkins, C. E., Park, M., & Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)* (pp. 90–100).

[7] Kurosawa, S., Nakayama, v., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile Ad Hoc networks by dynamic learning method. *International Journal of Network Security, 5(3),* 338–346.

[8] Raj, P. N., & Swadas, P. B. (2009). DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET. *IJCSI*, *2,* 54–59.

[9] Weerasinghe, H., & Fu, H. (2007). Preventing cooperative blackhole attacks in mobile Ad Hoc networks: Simulation implementation and evaluation. *Future Generation Communication and Networking, 2,* 362–367.

[10] Patcha, A., & Mishra, A. (2003). Collaborative security architecture for blackhole attack prevention in mobile ad hoc networks. *Proceedings of 2003 IEEE Radio and Wireless Conference on RAWCON* (pp. 75–78).

[11] Shila, D. M., & Anjali, T. (2008). Defending selective forwarding attacks in WMN. *Proceedings of 2008 IEEE International Conference on Electro/Information Technology, IEEE EIT* (pp. 96–101).

[12] De Couto, D., Aguayo, D., Bicket, J., & Morris, R. (2005). A high-throughput path metric for multi-hop wireless routing. *Wireless Networks*, *11(4),* 419–434.

[13] Zapata, M. G. (2002). Secure Ad hoc on-demand distance vector routing. *Mobile Computing and Communications Review*, *6(3),* 106–107.

[14] Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2002). A secure routing protocol for Ad Hoc networks. *Icnp*, 78–89.

[15] Li, Q., Zhao, M. Y., Walker, J., Hu, Y. C., Perrig, A., & Trappe, W. (2009). SEAR: A secure efficient ad hoc on demand routing protocol for wireless networks. *Security and Communication Networks, 2(4),* 325–340.

[16] Mohammadizadeh, M., Movaghar, A., & Safi, S. (2009). SEAODV : Secure efficient AODV routing protocol for MANETs networks. *ICI, 9*, 940–944.

[17] Mohanapriya, M., & Krishnamurthi, I. (2013). Modified DSR protocol for detection and removal of selective blackhole attack in MANET. *Computer and Electrical Engineering, 40(2),* 530–538.

[18] Jaiswal, R., & Sharma, S. (2013). A novel approach for detecting and eliminating cooperative blackhole attack using advanced DRI table in Ad hoc network. *Proceedinds of IEEE 3rd International Conference on Advance Computing (IACC)* (pp. 499–504).

[19] Su, M. (2011). Prevention of selective Blackhole attacks on Mobile Ad hoc Networks through intrusion detection systems. *Computer Communications*, *34(1),* 107–117.

[20] Sánchez-Casado, L., Maciá-Fernández, G., García-Teodoro, P., & Aschenbruck, N. (2015). Identification of contamination zones for sinkhole detection in MANETs. *Journal of Network and Computer Applications*, *54,* 62–77.

[21] Sen, J., Girish Chandra, M., Harihara, S. G., & Reddy, H. (2007). A mechanism for detection of Grayhole attack in mobile ad hoc networks. *Proceedings of the 6th International Conference on Information, Communications and Signal Processing.*

[22] Chu, H. C., & Jan, R. H. (2007). A GPS-less, outdoor, self-positioning method for wireless sensor networks. *Ad Hoc Networks, 5(5),* 547–557.

[23] Cao, J., & Das, S. K. (2012). *Mobile Agents in Networking and Distributed Computing*.

[24] DARPA. (1995). The Network Simulator NS2. Retrieved from http://www.isi.edu/nsnam/ns/

[25] Yoon, J., Liu, M., & Noble, B. (2003). Random waypoint considered harmful. *IEEE INFOCOM,* 2, 1–11.

Thanh-Tu Vo 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, wireless sensor network. He has published two books and more than 40 papers in national/international conferences and journal.

Thai-Ngoc Luong 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.