BDAODV: A Security Routing Protocol to detect the Black hole Attacks in Mobile Ad Hoc Networks

Le Duc Huy[1], Truong Thi Thu Ha[2], and Nguyen Van Tam[3]
[1]Faculty of Information Technology; Ha Noi University of Business and Technology, Viet Nam
[2]Faculty of Information Technology; Huu Nghi University of Management and Technology, Ha Noi, Viet Nam
[3]Graduate University of Sciences and Technology; Vietnam Academy of Science and Technology, Ha Noi, Viet Nam
Email: huyld@hubt.edu.vn, thuha.bh@gmail.com, nvtam46@gmail.com

***Abstract*—**One of the challenges of Mobile Ad Hoc Networks (MANET) is black hole attack. This is a form of destructive attack, causing very heavy damage to network performance once successfully implemented. By replying to the route with HC=1 and the largest SN, the malicious node fools the source node into thinking that it has the best and freshest cost-effective route to the destination node. As a result, all the data packets get caught in the malicious node and go missing without being able to reach the destination node. Most of the previous research was based on the characterization of black hole attacks or simple check mechanisms to detect cyberattacks. This leads to limitations that need to be overcome such as: Error rate in malicious node detection algorithm, routing waste, data routing efficiency in normal network scenario. This paper proposes a black hole attack detection algorithm (BDA) based on statistical theory. BDA collects information in real time so it can detect and prevent black hole attacks as they begin to act. The proposed solution uses a balance threshold value, calculated based on statistical theory, as the threshold for detecting black hole attack. A node that replies to the route with an SN value greater than the threshold is identified as a malicious node and isolated immediately upon attack. The article also proposes a black hole attack detection routing protocol (BDAODV) by improving the AODV protocol using BDA solution. The performance of the BDAODV protocol is evaluated and compared with related solutions on a network model with random mobile nodes. The simulation results have shown that the proposed protocol has very good performance in the network scenario under black hole attack with different number of malicious nodes.

Index Terms—AODV, Black hole attacks, BDAODV, MANET, Statistical theory.

I. Introduction

MANET is a wireless network, mobile devices connecting each other to create an independent network, regardless of the infrastructure. Node moves independently in all directions, they combine together to send data to the node to be far from the connection area, Each node works on par, with the same role as a terminal (host), it take the function of a router helps route data. Network topologies change regularly due to nodes entering or leaving networks, so that MANET is suitable for use where there is no unstable network or regional infrastructure such as rescue, disaster relief, battlefield tactics or conferences [1].

Routing is a service provided at the network layer, the source node uses the discovered route to the destination and maintained by routing protocols. The routing protocols in the network has an inappropriate structure to operate with the non-structural network, so many routing protocols are proposed to adapt to the MANET network. MANET configuration is frequently changed, so the reaction protocol is suitable for use, typically AODV [2]. The reason is that the source node only explores the route when necessary, by sending the the route request broadcast packet and receiving route reply packet. However, AODV is a target of many types of Denial of Service attack (DOS), such as Black hole attacks [3], Grayhole [4], Wormhole [5] and flooding [6].

Black hole attack is a form of DOS to undermine information on the MANET. To attack, malicious nodes advertise for the source node that itself has the route to the destination with the best cost and enough "fresh", so that the malicious node can fool the source navigation to the destination through it. As a result, the data packet of UDP streams is canceled, while the TCP channel is interrupted because it does not receive the ACK signal from the destination node. Therefore, many solutions to detect and prevent Black hole Attacks are studied. Most previous studies are based on the characteristics of Black hole Attacks or simple testing mechanisms to detect network attacks. This leads to limitations that need to be overcome such as: Error rate in malicious node detection algorithm, routing waste, data routing efficiency in normal network scenarios. This article proposes a new algorithm based on statistical theory named DBA to detect Black hole Attacks. This solution uses a balance index (BI [7]) threshold value, calculated based on statistical theory, to set the threshold of the Black hole attack. A node reply to the SN value greater than the allowed threshold will be defined as a malicious node and isolated as soon as the attack. This solution does not depend on the SN value of the reply package so the ability to detect better attacks than previous studies. In addition, the structure of route control packets is not changed, so the route exploration cost is almost

Manuscript received April 15, 2022; revised September 10, 2022.
Corresponding author email: huyld@hubt.edu.vn.
doi:10.12720/jcm.17.10.803-811

unaffected compared to the original protocol. The contribution of the article includes:

(1) Build scenarios and assessing the harmful effects of Black hole Attacks on the performance of the AODV protocol on a randomly moving scenario;
(2) Proposing a solution based on statistical theory to detect Black hole attack (DBA);
(3) Propose security protocol BDAODV by integrating BDA into route discovery mechanism of AODV protocol;
(4) Evaluation of the security effect of BDAODV protocol on topology of random mobile nodes and under Black hole attack with different number of malicious nodes.

The structure of the article includes: Section 2 presents a number of published researches related to security solutions of Black hole Attacks. Section 3 presents some related studies. Section 4 presents the results of assessing the impact of Black hole Attacks on the packet routing capabilities of the AODV protocol, and the security effectiveness of the BDAODV protocol when network is attacked. Final section is the conclusion and development direction.

II. Blackhole Attack on AODV

This section presents the AODV protocol and Black hole Attacks on this protocol.

A. AODV Protocol

The AODV protocol [2] discovers the route through a route request packet (RREQ), receives the route through an reply packet (RREP), maintains the route through a HELLO packet, and updates the route RERR. When the source node N_S wants to send a packet to the destination node N_D without a route in the routing table, the N_S discovers the route by broadcasting the RREQ request packet to its neighbors. The intermediate node Ni stores the path back to the source in the routing table (RT) and continues to broadcast the RREQ packet to all its neighbors, this process continues until the destination node N_D receives the route request packet. Upon receiving the RREQ message, the destination node N_D sends a Route Reply Packet (RREP) containing the path information back to the source N_S based on the previously stored uplink information. The intermediate node forwards the RREP packet to the source N_S, and stores the route to the destination N_D in the routing table. Route replies can also be performed at intermediate nodes if there exists a sufficiently 'fresh' path to the destination.

The routing cost of the AODV protocol is calculated based on the number of hops from the source N_S to the destination N_D, this is the HC value in the RREQ packet (or RREP packet), HC will increase by 1 each time a node forwards RREQ (or RREP). In addition, each node always maintains the SN value as a basis for determining the "freshness" of the discovered route to avoid route loop. Based on the value of HC and DSN (which is the SN value of the destination node N_D) in the RREP packet, the source node N_S updates the new route if it satisfies the condition that the newly discovered route is "fresh" enough and has the best cost. Fig. 1 shows the source node (N_1) discovering the route to the destination (N_5) by broadcasting a RREQ packet to neighbors {N_2, N_8}. N_2 is not the destination node, so it continues to broadcast to all its neighbors including {N_3, N_6}, the process continues at N_8 and other intermediate nodes until node N5 receives the RREQ packet. Each node only processes the RREQ packet once, so N_7 discards the RREQ packet received from N_9 because it was previously received from N_6. Upon receiving the RREQ packet, the destination node N_5 replies to the route by sending the RREP packet back to the source in the direction {$N_8 \rightarrow N_4 \rightarrow N_3 \rightarrow N_2 \rightarrow N_1$}. Upon receiving the RREP packet, N_1 establishes a route to N_5 through the next intermediate node (NH) of N_2 with a cost (HC) to the destination of 4 in the direction of {$N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_4 \rightarrow N_5$}.

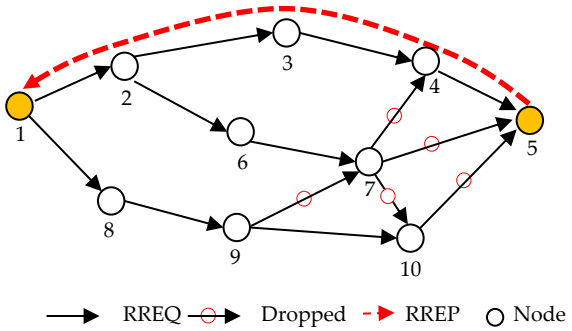

Fig. 1. AODV route discovery mechanism

B. Black Hole Attacks on AODV

Black hole attacks can be performed with one or more individual malicious nodes [8], in the case of using two malicious nodes connected together, this form is called collaborative attack [9]. To perform a Black hole attack, the malicious node goes through two stages: Stage 1, the malicious node advertises itself to the source node that it has the route to the destination at the best cost, so that the malicious can trick the source node into redirecting to the destination through it. In the second stage, the malicious node receives all packets from the source node and drops them all, so this is called a destructive attack. In a collaborative Black hole Attack, the data packet is forwarded to a second node, and dropped at this node to avoid detection. As a result, data packets of UDP streams are dropped, and TCP streams are interrupted because no ACK signal is received from the destination. A form of attack that is similar in nature to a Black hole attack is a sinkhole attack presented in [10].

Fig. 2 depicts the source node N_1 discovering the route to the destination N_5 and the malicious node N_9 performing the Black hole Attack. Upon receiving the route request packet, the malicious node N_4 replies the source node N_1 with a fake route reply packet (FRREP) with the best cost (HC=1) and a large enough SN to ensure that the route is

"fresh" enough. In this case, source node N_1 receives two route reply packets in the direction of $\{N_9 \rightarrow N_8 \rightarrow N_1\}$, and $\{N_5 \rightarrow N_4 \rightarrow N_4 \rightarrow N_2 \rightarrow N_1\}$. The route corresponding to the FRREP packet has a cost to the destination of 2, the route receiving the RREP packet from the source has a cost of 4. As a result, the RREP packet is dropped, the source node accepts the FRREP packet to establish a path to the destination in the direction $\{N_1 \rightarrow N_8 \rightarrow N_9\}$ due to its low cost. In case the FRREP packet has a higher cost than the RREP packet, the source node still establishes a route through the malicious node because the SN value of the FRREP packet is larger than the RREP packet.

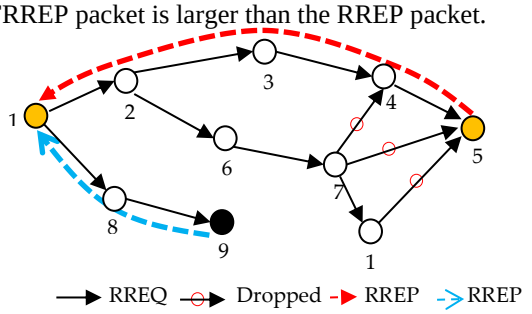

Fig. 2. Description of Blachole attacks on AODV

III. Related Researches

The essence of the Black hole Attack is that the malicious node immediately responds to the received route request (RREQ) packet. Therefore, the author [11] proposed a solution to discard the first route reply packet (RREP) received, accept the second RREP packet to establish the route. The security performance of this improved protocol (idsAODV) is increase but not much, the reason is that the first RREP packet received does not always come from the malicious node and the solution is only effective if the malicious node is near the source node.

The Black hole Attacks detection solution based on the automatic learning algorithm was proposed by Kurosawa *et al* in [12]. The result after the training process is to determine the threshold (th) to detect the Black hole Attack, the problem is that the training data does not include the information of the Black hole node. Further, to improve security, Raj *et al* improved the results of [12] and presented the DPRAODV protocol [13] that enables detection, prevention and response when a Blachole Attack occurs. The author has added a threshold value th2 which is the maximum value of the SN value in the routing table. The RREP packet is accepted if the security condition in [12] is met and the SN value in the received RREP packet is less than the threshold th2. Nodes detected anomalous are blacklisted (BL - Black List), RREP packet from malicious node is dropped, node broadcasts ALARM message packet containing malicious node information to neighbors. The limitation of the solution is that it has to go through the training process to build the threshold value th1, the training data is not general. In addition, the ALARM package can also be exploited by hackers to attack by telling nodes in the system that a normal node is a malicious node.

Authors [14] proposed "Security Agent for detect and avoid co-operative black hole node attack in MANETs". This method use SRT and RRT routing table and alarm classification and alarm generation to find out black hole node and use security agent to avoiding cooperative black hole attack in mobile Ad hoc network. This technique improve packet delivery ratio, network throughput and reduce end to end delay of data packet transmission.

Authors [15] proposed "Preventing of Black hole Attack in AODV protocol using timer based detection technique" used AODV protocol for data transmission between source node to destination node in this technique transition delay, queuing delay, propagation delay and processing delay is used to find out black hole node in network if the delay is more than threshold value then it may be possibility of black hole node present in that route of communication so avoided that route for further communication. This method improve throughput of communication.

Authors [16] proposed "Mitigating effects of black hole node attack in mobile ad-hoc Networks: Military perspective" work is based on the MANET deployment in a military battlefield scenario along the border. The proposed methodology uses the basic methodology of flooding a fake RREQ packet in MANET to identify the Black hole node (BHN). Once the node is identified then it is checked from the adjacent node that is that node identified as the BHN is forwarding any packets to the node towards the destination. If the adjacent node gives a positive response to information then the attack is identified as cooperative black hole else single Black hole attack. In both the case Black Hole List (BHL) is updated.

Authors [17] analyzed the black hole attack in wireless P2P networks using the AODV as the routing protocol. In a black hole attack, a malicious node assumes the identity of a legitimate node, by creating forged answers with a higher sequence number, and thus forces the victim node to prioritize it as a relay node. They proposed a SBAODV routing protocol, based on a modification of the AODV routing protocol, taking into account the behavior of each node participating in the network.

IV. Proposed Our Solution

This section presents the Black hole Attack detection algorithm (BDA) and improves the AODV protocol to the Black hole attack detection protocol (BDAODV).

A. BDA Solution

The AODV protocol uses two parameters SN and HC in the RREP packet to establish a route. This is the cause of the Black hole Attack. The paper proposes the BDA solution, which is calculated based on the balanced index. Algorithms 1, 2 and 3 describe the steps of a BDA solution, in which algorithm 1 allows to collect information about

the SN value of all nodes each time a RREQ packet is received, this value is used to caculate the balanced index.

Algorithm1: Algorithm to collect SN values

Input: RREQ packet
Ouput: L is the list of SN values of all the nodes in the network
Procedure getSequenceNumber(RREQ, L);
Begin
// The address of the source node
src ← getIDSourceNode();
if (L[src] < RREQ.SN) then
L[src] ← RREQ.SN;
End;

Algorithm 2 allows a balanced index (bi) value to be calculated, which is used to identify a node as malicious or normal. BI is calculated based on statistical theory as a dynamic threshold value for black hole attack detection.

Algorithm 2: Algorithm to calculate the balanced index value

Input: L is the list of SN values of all the nodes in the network
Ouput: *bi* is the balanced index
Function getIndexBalance(L);
Begin
//n is number of nodes in network and n≥1
if *n=1* then Return L[1];
$avg \leftarrow \frac{\sum_{k=1}^{n} L[i]}{n}$; //the sample mean
$sd \leftarrow \sqrt{\sum_{k=1}^{n} \frac{(L[i]-avg)^2}{n-1}}$ // standard deviation
$bi \leftarrow 2 * avg * \frac{avg}{sd+1}$ // balanced index
Return *bi*;
End;

Algorithm 3 allows a node to check for security. A node that replies to the route with an DSN value greater than the allowed threshold (bi) will be identified as a malicious node and isolated immediately upon attack. This algorithm executes every time the node receives the RREP packet for security check.

Algorithm 3: Security Checking

Input: RREP packet
Ouput: True if the destination node is normal; otherwise, return False
Function checkSecurity(RREP, L);
Begin
dst ← getIDDestinationNode();
if BDP + NQP > NPP then return True;
//Address of destination node that it sends
//RREP packet
bi ← getIndexBalance(RREP, L);
if (RREP.DSN > bi) then
Return False
Else
Return True;
End;

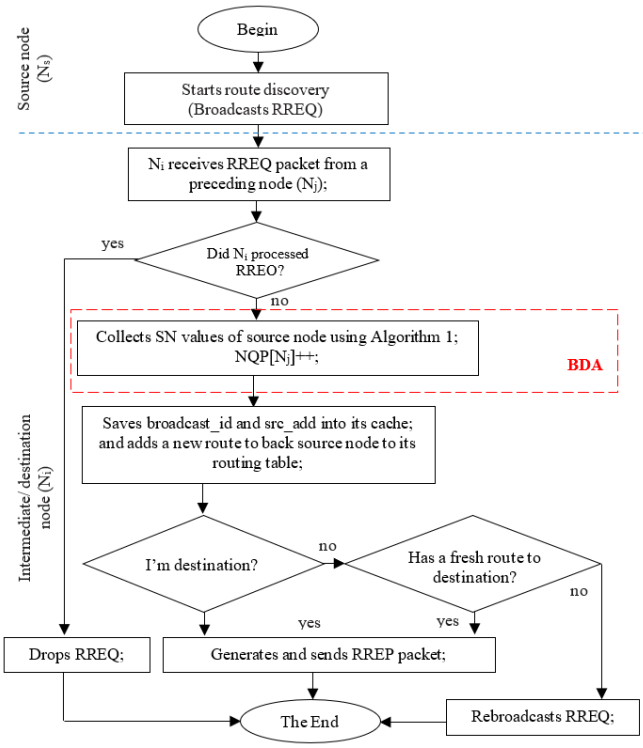

Fig. 3. Route request algorithm of BDAODV

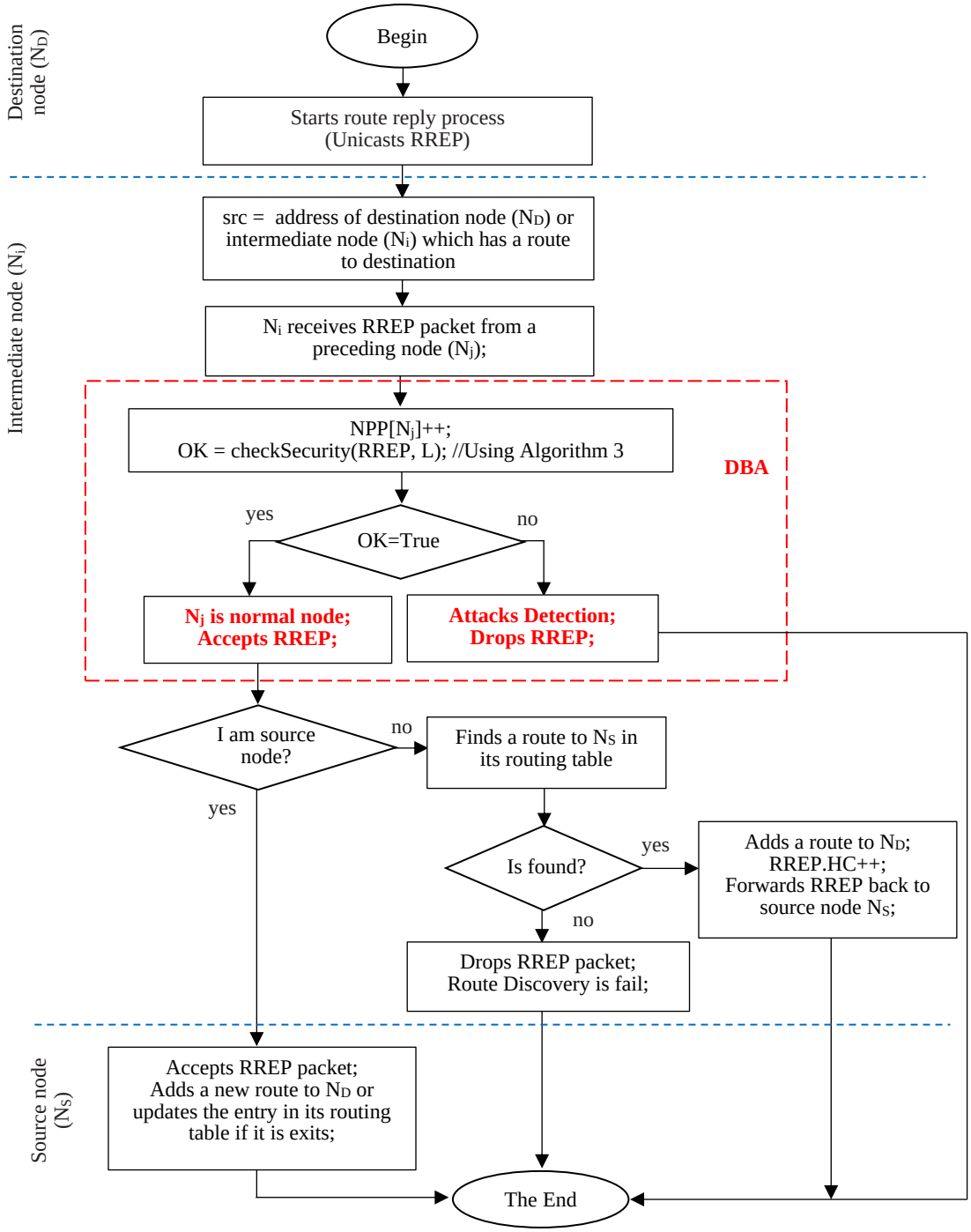

Fig. 4. Route reply algorithm of BDAODV

B. *Proposed BDAODV Protocol*

The article proposes the BDAODV protocol by improving the AODV protocol using the BDA solution. The route discovery algorithm of the BDAODV protocol is developed from AODV at the route request process as shown in Fig. 3 and route reply as shown in Fig. 4. Similar to [17], the node records the number of route request packets (NQP), the number of route reply packets (NPP), and the number of data packets (NDP), received from Nx. If BDP + NQP > NPP then N_x is a trusted node

a) Route Request algorithm: To discover the route to the destination node N_D, the source node N_S initiates the RREQ packet and broadcasts to all the neighbors of the N_S, the RREQ packet is processed at many intermediate nodes before reaching the destination. Whenever receiving a RREQ packet from the previous node (N_j), the intermediate node (N_i) processes the RREQ packet as the original AODV protocol, the difference is that every time a RREQ packet is received, node N_i collects the SN value of the source node and counts the number of route request packets (NQP), algorithm details as Fig. 3.

b) Route reply algorithm: Upon receiving the RREQ message, the destination node N_D replies to the RREP packet containing the path information back to the source

N_S based on the previously stored reverse path information (Fig. 4). RREP packet processing is performed as the original AODV protocol. The difference is that every time the RREP packet is received, the intermediate node (N_i) uses algorithm 3 to check the security before forwarding the RREP packet to the source, the checking process is as follows:

– N_i node counts the number of route reply packets (NPP) and to check security using algorithm 3;

– If OK = True, go to Step 1; otherwise to Step 2;

Step 1: The node replies that the route is normal, N_i accepts the RREP packet and forwards the RREP packet to the source N_S, and saves the route to the destination ND in the routing table.

Step 2: The node replies that the route is determined to be malicious, the RREP packet is dropped, the algorithm terminates.

V. Evaluate the Results by Simulation

Using NS-2.35 [18], we evaluate the original AODV, the SBAODV, and BDAODV and compare their performances with Black hole Attacks in terms of Packet delivery ratio, End-to-end delay, and Routing load metrics. [6], [7], [19]

a) Packet delivery ratio (PDR): The ratio of the received packets by the destination nodes to the packets sent by the source nodes (eqn 1); where *n* is number of data packets that are received by destination nodes, *m* is number of data packets that are sent by source nodes.

$$PDR = \frac{\sum_{i=1}^{n} DATA_i^{recieved}}{\sum_{j=1}^{m} DATA_j^{sent}} * 100\% \quad (1)$$

b) End-to-end delay (ETE): This is the average delay between the sending time of a data packet by the CBR source and its reception at the corresponding CBR receiver (eqn 2), where $Delay_{DATA}^{i}$ is the delay time for sending i^{th} data packet to its destination successfully, *n* is number of data packets that are received by destination nodes.

$$ETE = \frac{\sum_{i=1}^{n} Delay_{DATA}^{i}}{n} \quad (2)$$

c) Routing load (RL): This is the ratio of the overhead control packets sent (or forwarded) to successfully deliver data packets (eqn 3), where *n* is number of data packets that are received by destination nodes, *g* is number of overhead control packets that are sent or forwarded. Routing discovery packets including: legitimate RREQ, fake RREQ, RREP, HELLO and RERR packets.

$$RL = \frac{\sum_{j=1}^{g} CONTROL\_PACKET_j^{overhead}}{\sum_{i=1}^{n} DATA_i^{recieved}} \quad (3)$$

A. Simulation Parameters

The paper uses 5 network topologies, each topology includes 50 nodes, all nodes move randomly according to Random Way Point model (RWP [20]), simulation time is 500s, number of emitters CBR is 25, the first source starts at the 0th second, the next sources are 15 seconds apart, parameter details are in Table I.

Table I. Details of Simulation Paramerters

Parameters	**Value**
Simulation time	500 (s)
Number of normal nodes	50
Number of malicious nodes	1, 2, 3
Broadcasting radius	250 (m)
Mobile model	RWP
Speeds	1..10, 1..20 m/s
Transport protocol	UDP
Routing protocol	AODV, SBAODV [17], BDAODV
Number of CBRs	25
Traffic type	CBR
Packet size	512 bytes
Queue	FIFO (DropTail)

B. Simulation Results

After performing 90 simulation scenarios with 3 protocols on 5 random mobile network topologies, with different maximum speeds, different number of malicious nodes, the results are statistically in Table II including: Average and standard deviation.

Table II. Simulation Results

Average									
	PDR			**RL**			**ETE**		
MN	BDAODV	SBAODV	AODV	BDAODV	SBAODV	AODV	BDAODV	SBAODV	AODV
1	79.37	48.64	4.86	2.09	3.92	17.24	286.52	482.59	151.81
2	78.53	50.72	3.66	2.20	3.80	19.06	276.19	537.72	119.28
3	78.82	53.41	3.70	2.29	3.71	17.82	280.86	534.88	86.83
Standard deviation values									
1	8.15	3.21	0.36	0.47	0.90	2.58	21.82	159.02	52.38
2	4.82	1.52	0.14	0.48	0.76	1.87	58.66	241.13	88.80
3	10.96	1.35	0.24	0.70	0.60	1.75	68.75	96.60	48.22

a) Packet delivery ratio. The graph of packet delivery ratio in Fig. 5 shows that the Black hole Attack has affected the routing efficiency of two protocols AODV and SBAODV. After 500 seconds of simulation in the attacked network scenario using 1 malicious node, the packet delivery ratio of AODV protocol is 4.86%, SBAODV is 48.64% and BDAODV is 79.37%, standard deviation is 0.36%, 3.21% and 8.15%, respectively. Under 3 malicious nodes to attack, the packet delivery ratio of AODV protocol down to 3.7%, SBAODV is 53.41% and BDAODV is 78.82%, standard deviation is 0.36%, 3.21% and 8.15%, respectively. The security mechanism of the SBAODV solution is less reliable than BDAODV because the first route reply packet received does not always come from the malicious node, dropping the first received RREP packet will have a huge effect to the routing efficiency, on the contrary, the proposed mechanism has good efficiency, so the PDR of BDAODV is much higher than that of SBAODV.

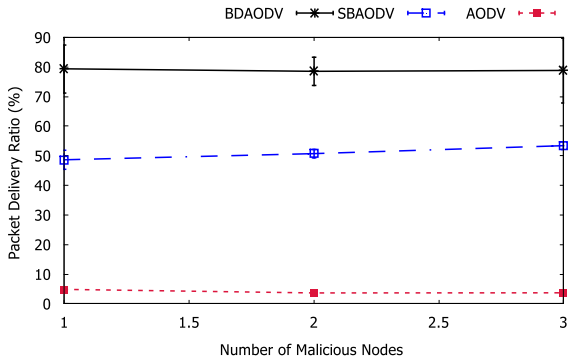

Fig. 5. Packet delivery ratio

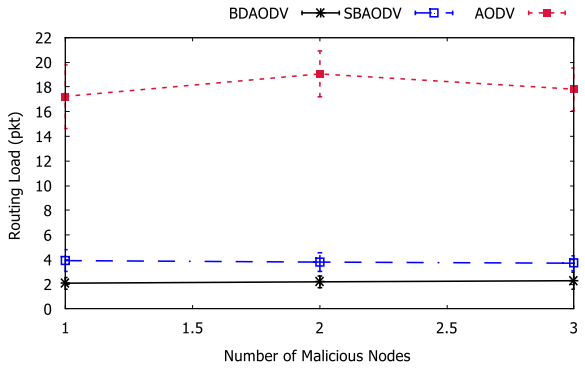

Fig. 6. Routing load

b) Routing load. The graph in Fig. 6 shows that the routing load (RL) of the BDAODV protocol is lower than the other two protocols in the Black hole Attack scenario. At the end of 500 seconds of simulation under 1 malicious node, the routing load of AODV is 17.24pkt, SBAODV is 3.92pkt and BDAODV is 2.09pkt, standard deviation is 2.58pkt, 0.9pkt and 0.47pkt, respectively. Under 3 malicious nodes to attack, the routing load of AODV protocol is 17.82pkt, SBAODV is 3.71pkt and BDAODV is 2.29pkt, standard deviation is 1.75pkt, 0.6pkt and 0.7pkt, respectively. The BDAODV protocol has good security performance, so the packet delivery ratio to the destination is high, which leads to a lower routing load than the SBAODV and AODV protocols.

c) End-to-end delay. Fig. 7 shows that in a network scenario under Black hole Attack, the end-to-end delay time to successfully route a data packet to the destination of AODV is 151.81ms, SBAODV is 482.59ms and BDAODV is 286.52ms under 1 malicious node, standard deviation is 52.38ms, 159.02ms and 21.82ms, respectively. Under 3 malicious nodes, the end-to-end delay of AODV is 86.83ms, SBAODV is 534.88ms and BDAODV is 280.86ms, standard deviation is 48.22ms, 96.6ms and 68.75ms, respectively. This result shows that the security mechanism of the BDAODV protocol has affected the EtE of the original protocol.

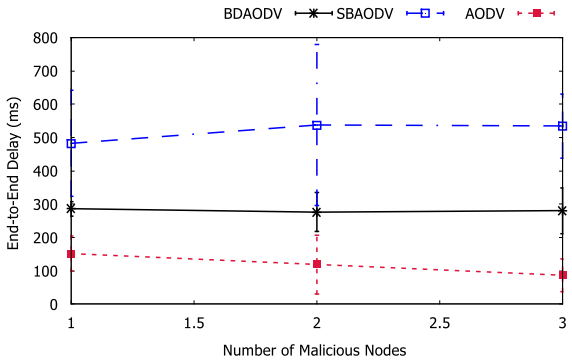

Fig. 7. End-to-End delay

VI. Conclusion

The article proposed a BDA solution based on statistical theory and security protocol BDAODV against Black hole Attack. This solution uses a balanced threshold value, calculated based on statistical theory, as the Black hole Attack detection threshold. A node that replies to the route with an SN value greater than the threshold is identified as a malicious node and isolated immediately upon attack. This solution does not depend on the SN value of the route reply packet, so the attack detection ability is better than previous studies. The simulation results show that the performance of the BDAODV protocol is very good in the Black hole Attack network scenario, much better than the SBAODV solution. In the future, we will continue to implement and evaluate the security effectiveness of the proposed solution with some similar studies on WSN, VANET and BAN network scenarios.

Conflict of Intrest

The authors declare no conflict of interest.

Author Contributions

D.H. Le proposed idea and performed the measurements, V. T. Nguyen were involved in planning and supervised the work, D. H. Le processed the experimental data, performed the analysis, drafted the manuscript and designed the figures. T. T. H. Truong aided in interpreting

the results and worked on the manuscript. All authors discussed the results and commented on the manuscript.

ACKNOWLEDGMENT

This research is supported by the project B2022.DCQ.02.TT, the Huu Nghi University of Management and Technology, Vietnam.

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, no. 3, pp. 60–66, 2004.

[2] 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 (WMCSA)*, pp. 90–100, 1999.

[3] M. Mohanapriya and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," *Computer and Electrical Engineering*, vol. 40, no. 2, pp. 530–538, 2013.

[4] 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.

[5] T. T. Vo, N. T. Luong, and D. Hoang, "MLAMAN: A novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network," *Wireless Networks*, vol. 25, no. 7, pp. 4115–4132, 2019.

[6] N. T. Luong, T. T. Vo, and D. Hoang, "FAPRP: A machine learning approach to flooding attacks prevention routing protocol in mobile ad hoc networks," *Wireless Communications and Mobile Computing*, 2019.

[7] M. J. Faghihniya, S. M. Hosseini, and M. Tahmasebi, "Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network," *Wireless Networks*, 2017.

[8] M. Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," *Computer Communications*, vol. 34, no. 1, pp. 107–117, 2011.

[9] R. Jaiswal and S. Sharma, "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in ad hoc network," in *Proc. IEEE 3rd International Advance Computing Conference (IACC)*, 2013, pp. 499–504.

[10] 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.

[11] S. Dokurer, "Simulation of black hole attack in wireless ad-hoc networks," Computer Engineering Atilim University, 2006.

[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] P. N. Raj and P. B. Swadas, "DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET," vol. 2, pp. 54–59, 2009.

[14] V. G. Mohite and L. Ragha, "Security agents for detecting and avoiding cooperative blackhole attacks in MANET," in *Proc. International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, 2015, pp. 306–311.

[15] N. Choudhary and L. Tharani, "Preventing black hole attack in AODV using timer-based detection mechanism," in *Proc. International Conference on Signal Processing and Communication Engineering Systems - Proceedings of SPACES 2015, in Association with IEEE*, 2015, pp. 1–4.

[16] B. Singh, D. Srikanth, and C. R. S. Kumar, "Mitigating effects of black hole attack in mobile Ad-Hoc NETworks: Military perspective," in *Proc. 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016*, 2016, pp. 810–814.

[17] P. Ndajah, A. O. Matine, and M. N. Hounkonnou, "Black hole attack prevention in wireless peer-to-peer networks: A new strategy," *International Journal of Wireless Information Networks*, vol. 26, no. 1, pp. 48–60, 2019.

[18] T. Issariyakul and E. Hossain, "Introduction to network simulator NS2," *Springer*, pp. 1–438, 2009.

[19] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET," *Wireless Networks*, 2017.

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

Huy D. Le was born in Bac Ninh province, Vietnam in 1990. He received B.E. degree in Information Technology from Hanoi University of Business and Technology, 2012 and M.A. degree in Computer Science from the Thai Nguyen University Of Information And Communication Technology, 2015. He is currently studying for his Ph.D. in Graduate University of Sciences and Technology; Vietnam Academy of Science and Technology. His research interests include computer network, and security mobile ad hoc network.

Ha T. T. Truong was born in Nghe an province, Vietnam in 1979. She received B.Sc. degree in Information Technology from Hanoi National University of Education, 2000; M.Sc. degree in Information Technology from University of Engineering and

Technology - Vietnam National University, Hanoi, 2007 and Ph.D degree from Military Technical Academy , 2018. Her research interests include data science and computer network.

Tam V. Nguyen was born in Vinh Phuc province, Vietnam in 1947. He graduated from CVUT University, Praha, Czechoslovakia in 1971. He successfully defended his Phd at VUMS Computer Research Institute, Praha, Czechoslovakia in 1977. He was appointed as Associate Professor of Informatics in 1996. Currently, he works Graduate University of Sciences and Technology; Vietnam Academy of Science and Technology. His research interests include: Network Technology, Network Performance and Security.