

A new Secure Routing Algorithms in VANETs with ability to discover DoS Attacks

Reza Behrouzi

M.S. Student, Department of Computer Engineering, East Azarbaijan Science and Research Branch, Islamic Azad University, Tabriz, Iran
rezabehrouzi.ir@gmail.com

Mohammad Ali JabraeilJamali

Assistant Professor, Department of Computer Engineering, Shabestar Branch, Islamic Azad University, Shabestar, Iran
m_jamali@itrc.ac.ir

Abstract

Mobile ad hoc networks are networks that are created by moving parts and are capable of communicating with each other, there are two important features the first is the lack of static and the second is relationship between temporal components.

Including the type of network traffic can be cited between networks. Due to the lack of clear direction in the network may cause interference or manipulation of these networks is that these protocols against these threats must be retrofitted. Here is the precise definition of the function in terms of demand distance vector routing protocol to the protocol of immunization against Denial of Service attacks that black holes are made. Then The protocol to the protocol primitives obtained by simulation tool NS2 to simulate the different scenarios we have to compare the obtained according to the outputs of the software NS2 have been 19.6 percent and 9.5 percent respectively compared to existing protocols logical addressing method, to avoid the black hole attack.

Keywords:

Inter-vehicle networks, denial of service, node, ad hoc network, and security black hole attack.

1- Introduction

Mobile ad hoc wireless networks of independent components, each of which is managed by Themselves - they are in no particular shape is formed. Therefore, this type of network topology is dynamic and nodes - a moment that can be joined or separated. These networks in military, rescue, and research, to create a network where there is no fixed structure has many applications. The network has two important characteristics: the first is the lack of communication between components is proved to be temporary and the latter. In addition, each component of the network to send and receive information to other members of the current network plays an important role in conveying information from one source of each other as a destination have a role in the origin of the information or destinations into routers network be able to run. Among these networks can include networking between vehicles. In this network , the access to their propagation and interference or manipulation of these networks there. The Mechanism of this network is

that each node after getting the package, it is control that what kind of is it or sent to its destination node or it is for another node [4].

If the destination is a node, it retrieves the data analysis and will take the necessary action This action may be due to the higher layer data network (application layer) or a change in your schedule and variable node And if he is not close to the destination, if it knows the destination of the packet and sends the packet otherwise it will be deleted.

2- review existing concepts and protocols

Ad hoc On-Demand Distance Vector (AODV) protocol is one of the most suitable protocols for mobile ad hoc networks. because It consumes very little bandwidth and performance is simple. In this protocol, if a node wants to send data to another node requests a serial number beginning with Public release a specified node which produces And they say that the release identifier of the access route to the destination network is offered. Each node of the current node receives a request, if the destination node is not the first as well as the access route to the destination node does not have a route back to the previous node that was request it creates and then again at the request of the public are published [11].

The way to reach the destination node and the destination node is a node that has a route optimization continues. Destination node and or nodal which have the access route destination node is after receiving action appeal to It would also accountability and a response to the previous node that was request it sends out. Since each node in the optimal path of the request and issued a temporary path to the node before it has created However, the response of the establishment of origin to the destination in its routing table and the answer to the previous node that receives the request it sends. This process continues until the answers to the origins and causes a communication path from the source to the destination. After the establishment of the source node has data to send. We know how important it is, if a node with a route request is received if received before a certain serial re-route requests to remove it, In other cases, if the application is not determined until the last node is removed from the network and in the end, the entire route is small fraction of the seconds moment in and to stop the displacement nodes made Enough time to provide data transmission between nodes. Networks, mobile ad hoc networks, as well as other information that may be of service attack denial of such attacks can:

- Gray Hole Attack (Routing Misbehavior)
- Black Hole Attack

Cited . Like other protocols based on demand distance vector routing protocol for mobile ad hoc network can deal with acts of sabotage and malicious node detection and correction is the way that the network performance will be impaired. Several measures taken in this regard by the experts in this field have gained relative success of each and perfect agreement has been obtained. In this article we will explain the black hole attack and One of the methods to secure distance vector routing protocols in terms of demand in the face of attacks and the simulation results of its performance with NS2 We'll see [5].

3- The work done in this field

Many groups have been working in this field, which a few are mentioned. Denial of service attack, according to "M- RAYA" is as a nightmare for network security experts. Since they are not installed with any rational purpose, hence it is very difficult to stop them, especially in the wireless media. To mitigate these attacks he proposed switching between different channels or even communication technologies. To avoid the problems of rejection episodes advanced networking features, until the network is restored, it will

automatically turn off and the driver information. This is possible when the number of vehicles is limited [3].

To prevent security threats in the network, “Karan verma et al” Much research has been done on the issue of denial of service attack in such networks, and methods of this study was to prevent it recently presented. Using the Internet Protocol address to disrupt the performance of data transfer between moving vehicles, the matter was investigated [1].

That defense of denial of service attacks, fake identities of malicious vehicles with information to help them analyze the logical address. Data packets periodically by all the vehicles to announce their presence and thus exchanged will be notified of the location of the next node. Each node periodically exchanges data with the environment; your database will be stored. In the meantime, if some nodes have the same logical address of previous data stored in the database, the rejection of the attack are identified. Model to deal with the attack called Chock logical address that the simulation results indicate a detection rate of attack was increased .

4- Attack type black hole

As the name has become a black hole to swallow the attacks and disruption of failures and network level information to be. The mechanism for distance vector routing protocol performance in terms of attack change request is made such a network node that wants to attack almost in the center of the network to route all requests to receive. And when the node receives route requests without having to control the access route to the route table exists or not reply with access to the best source of content and sends its best route to reach the destination. The highest sequence number of the destination (4294967295) to the target access path is updated to indicate that the lowest step to the destination (one-step) and a written response will be sent to the source; Upon receiving the response and compare it with the source sequence number in the routing table, due to the larger sequence numbers replace the previous track will reply Or if it is the first time that this route will bring it to your table. Since a number of other routes were likely to receive less than the amount received from the new node, so the matter will be aggressive. Thus, the source node to the destination node must send all the information that will be sent to the attacker node, the node will remove all of them get too aggressive [7].

Nodes, an attacker can make all the nodes so as to mislead or vortex of a black hole and its surrounding information nodes spread and destroy it. It is a black hole attack in Transmission Control Protocol (TCP), which requires proper acknowledgment packet (ACK) from the destination is received, because it is not received by the destination is identified, but initially, will be routed incorrectly. But this problem is not recognized protocol data without the user data without the user protocol (UDP) because, as you know, lighter mobile networks using the more general case. Such as messaging, news, image, video and audio.

5- Activity

5-1- Study

To study the behavior of black hole attacks in wireless networks using vector routing protocol Distance according to the demand of a simulation environment for this purpose was created in NS2 software through Statistics obtained the proposed solutions to deal with that action was appropriate. 3 different scenarios were designed so that the behavior of the distance vector routing protocol with node number 8 in terms of demand ,1 node with a black hole in an area the size of 500×500 m and 5 min were simulated in NS2 (Fig. 1).All nodes are moving and in different situations. In this scenario, nodes with even number of nodes associated with subsequent odd-numbered (for example node 2 to node 3) and constant bit rate (CBR) Traffic is established between them.

After running the simulation data were extracted from Table 1.

	The total number of packets sent	The number of packets received by the destination node	The total number of packets dropped	The number of packets dropped by the black hole	Percentage of packets dropped by the black hole
Scenario 1	2599	253	2346	1058	40.7
Scenario 2	2633	238	2359	1256	47.6
Scenario 3	2621	35	2585	1009	38.5
Total	7853	526	7326	3323	42.3

Table 1: Statistics obtained from simulations based on demand distance vector routing protocol

As you can see, on average, about 42.3 percent packet losses due right around the black hole can be seen that the amount is substantial.

5-2- Proposed actions

Upon receiving the request, since the black hole node, the attacker sends a response so the answer is likely to be much faster than the sending node will be as valid as the analysis of simulation output files as this seems obvious. So if these issues are the most balanced coverage of 50% of the time this happens in 50% of cases the responses were can be stored in the central memory in the routing table recorded answers reputable presumed decided. For this purpose, we established a new protocol based on demand distance vector routing protocol, which was modified in terms of the proposed measures.

The same scenarios A and the distance vector routing protocols in terms of demand nodes to the proposed protocol, we repeated the simulations (Fig. 2), and the results are listed in Table 2.

	The total number of packets sent	The number of packets received by the destination node	The total number of packets dropped	The number of packets dropped by the black hole	Percentage of packets dropped by the black hole
Scenario 1	2588	926	1661	575	22.2
Scenario 2	2540	501	2139	611	23.1
Scenario 3	2631	652	1979	604	22.9
Total	7859	2079	5779	1790	22.7

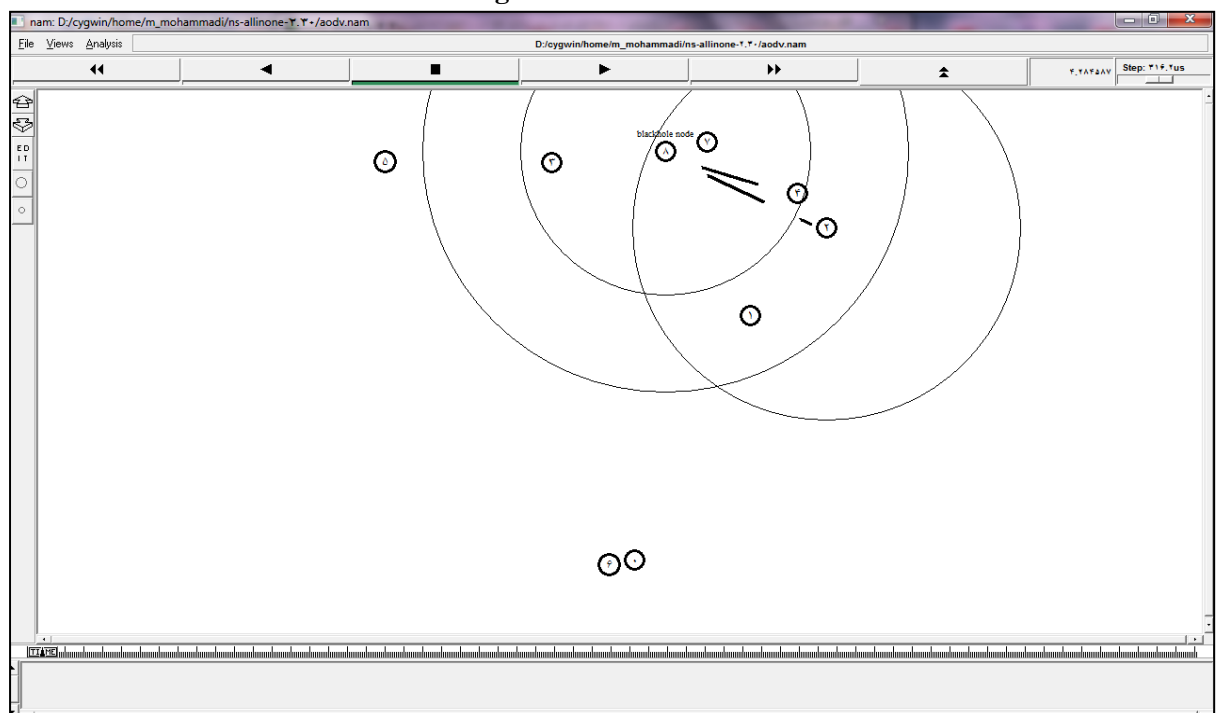
Table 2: Statistics obtained from simulations of the proposed protocol

6- Conclusion

Our next step in this direction is to implement the proposed protocol can improve the identification performance.

	The total number of packets sent	The number of packets received by the destination node	The total number of packets dropped	The number of packets dropped by the black hole	Percentage of packets dropped by the black hole
AODV	7853	526	7326	3323	42.3
The proposed protocol	7859	2079	5779	1790	22.7

Figures and charts



557

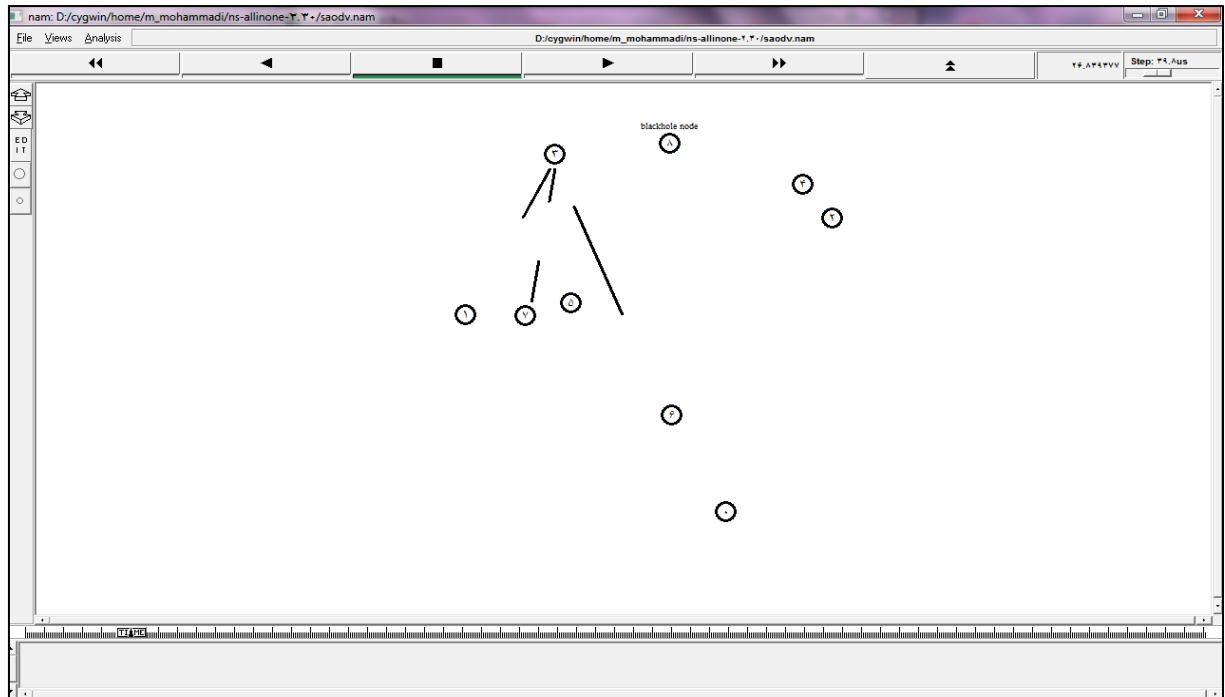


Image -2 nodes to simulate the proposed protocol

References

- [1] Verma, K., Halabi H., Kumar, A., (2013). Prevention of DoS Attacks in VANET. Springer Science+Business Media New York 2013, DOI 10.1007/s11277-013-1161-5.
- [2] Alsharif, N., Wasef, A., Shen, X., (2011). Mitigating the Effects of Position-Based Routing Attacks in Vehicular Ad Hoc Networks. IEEE ICC 2011 proceedings. 978-1-61284-233-2/11.
- [3] EAli, M., Reda, O. M., ElOuahidi, B., (2011). A Contribution to Secure The Routing Protocol “Greedy Perimeter Stateless Routing” Using A Symmetric Signature Based AES And MD5 Hash. International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.5.
- [4] Zhang, J., (2011). A Survey on Trust Management for VANETs. 2011 International Conference on Advanced Information Networking and Applications, DOI 10.1109/AINA.86.
- [5] Halabi, H., Irshad, A. S., Manan, J. A., (2010). Denial of Service (DoS) Attack and Its Possible Solutions in VANET. World Academy of Science, Engineering & Technology; May 2010, Issue 41, p411.
- [6] Zeadally, Sh., Hunt, R., Chen, Y., Irwin, A., Hassan, A., (2010). Vehicular ad hoc networks (VANETS): status, results, and challenges. Springer Science+Business Media, LLC. DOI 10.1007/s11235-010-9400-5.
- [7] María de Fuentes, J., Isabel González-Tablas, A., Ribagorda, A., (2010). Overview of security issues in Vehicular Ad-hoc Networks. Handbook of Research on Mobility and Computing, Copyright 2010, IGI Global.
- [8] Yan, G., Olariu, S., Weigle, M.C., (2008). Providing VANET security through active position detection. DOI:10.1016/j.comcom.2008.01.009.
- [9] Samara, Gh., Al-Salihy, W. A. H., Sures, R., (2010). Security Analysis of Vehicular Ad Hoc Networks (VANET). 2010 Second International Conference on Network Applications, Protocols and Services. DOI:10.1109/NETAPPS.17.

- [10]Naumov, V., Gross, Thomas R., (2007). Connectivity-Aware Routing (CAR) in Vehicular AdHoc Networks. a research program of the Swiss National Science Foundation. 0743-166X/07. IEEE.
- [11]Raya, M., Pierre, J., Hubaux, (2007). Securing vehicular ad hoc Networks. Journal of Computer Security, Vol.15, Issue 1, January, pp. 39-68.
- [12]Vigna, G., Gwalani, S., and Srinivasan, K., (2004). An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks Proc. of the 20th Annual Computer Security Applications Conference (ACSAC'04).
- [12]Ning, P., Sun, K., (2003). How to Misuse AODV: A Case Study of Insider AttacksAgainst Mobile Ad-Hoc Routing Protocols. Proc.of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY. This work is supported by the Army Research Office (ARO) under grant DAAD19-02-1-0219. pages 60–67, June 18-20, 2003.
- [14]Syed, A., Khayam., Radha, H., (2003). Analyzing the Spread of Active Worms over VANET. Department of Electrical & Computer Engineering / 2120 Engineering Building.
- [15]Taleb, T., Sakhaee, E., Jamalipour, A., Hashimoto, K., Kato, N., Nemoto, Y., (2007). A Stable RoutingProtocol to Support ITS Services in VANET Networks. IEEE Transactionson Vehicular Technology. VOL. 56, NO. 6. IEEE.
- [16]Mustafa, B., Waqas Raja, U., (2010). Issues of Routing in VANET. Master thesis. Blekinge Institute of Technology, Sweden. Computer Science, Thesis no: MCS-2010-20.