Effect of the Black-Hole Attack in Vehicular Ad-Hoc Networks

Mohamed Anis Mastouri
Communication systems – Sys'Com Laboratory
National school of engineers of Tunis – ENIT
Tunis, Tunisia

Salem Hasnaoui
Communication systems – Sys'Com Laboratory
National school of engineers of Tunis – ENIT
Tunis, Tunisia

Abstract
VANETs have become one of the most attractive research areas in the world of wireless networks in recent years. Indeed, vehicular networks have become capable of optimizing road traffic, which significantly reduces the number of accidents through notifications exchanged between nearby vehicles. The routing function based on the opportunistic algorithm is a critical part of the vehicle's communication system and will therefore be an ideal target for attacks that could aim to prevent alert messages from reaching their destination, and thus endanger human lives. The black hole attack is a major threat to the security of VANETs. The main idea of this paper focuses on the analysis of this type of attack in VANETs using Discrete-Time Markov Chains (DTMC). and deduce at the end the effect of the number of malicious nodes on the delivery rate in the network.

Keywords:
VANET, opportunistic, routing, security, DTMC, Black-hole.

I. MOTIVATION

Vehicle Area Networks (VANETs) are a special case of Disconnected MANETs which are characterized by the high mobility of its nodes as well as a direction of the vehicular nodes. provide efficient and cost-effective solutions for various applications such as: road safety, traffic management and multimedia applications using multi-hop wireless communications between communicating vehicles. However, the implementation and maintenance of reliable multi-hop links in VANET environments pose real challenges mainly due to rapid changes in topology and frequent disconnections of links, leading to the failure and inefficiency of traditional ad hoc routing protocols. This work proposes a new secured routing protocol adapted to the intrinsic characteristics of VANET networks.

Vehicular networks with its two types Vehicle-to-Vehicle (V2V) and Vehicle-to-Road Side Units (V2R) disseminates information to specific geographical areas using a content-based opportunistic routing. So, the big idea is to design intelligent algorithms based on security and opportunistic routing to improve safety on the roads.
In this network, communicating can converge to the fragmented mobile networks that are always changing organization and topologies due to their high mobility. Vehicles are characterized by a variety of speeds Vehicles are characterized by a variety of speeds which cause the network topology to change quickly and frequently. Communication mechanisms must therefore be adapted to this particular context.
Under such conditions, traditional routing protocols are not adapted to such high mobility conditions. This has led researchers in recent years to propose new routing approaches such as epidemic and social approaches.
Indeed, the designed communication model must be able to tolerate intermittent connectivity, as well as latency in transmissions thanks to its temporal decoupling and asynchronism.

The features of this network require more advanced communication techniques that suit these properties. These techniques must on the one hand satisfy the needs of the applications using the publish-subscribe model. On the other hand, they must constantly and securely determine the routes between any producer of information and its consumers since these routes may become unusable because of their high mobility.
Opportunistic routing is based on the Store-Carry-Forward technique where the packet is routed through a set of neighboring nodes that will act as message carriers from one node to another. [1]

Sometimes, some nodes in the network act maliciously and behave unpredictably. Indeed, the algorithm assumes that these carrier nodes are cooperative nodes, which is not always true in reality. Nodes may act in a malicious way in order to degrade the network performance. In this context, the attack of the black hole is an example of that. It is a Denial-of-Service type attack. Instead of routing the packet the malicious node acting as a carrier tries to absorb it by removing it, which influences the normal functioning of the network. Another version of the black hole attack is designed in such a way that the malicious node behaves more efficiently by assuming that the packet it has received is already being transported to its recipient, which also causes a network dysfunction.

Manuscript received August 5, 2024
Manuscript revised August 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.8.14

1. PROBLEMATIC

The objective of wireless vehicle networks is to improve road traffic and preserve the safety of drivers and passengers. It is by warning drivers of neighboring vehicles early enough in case of accident risks.
Given the importance of the information exchanged between vehicles and the Openness of the VANET environment, an attacker can issue w arning messages with falsified content or prevent the delivery of a valid message in order to cause accidents. For these reasons, security in these networks represent a very important challenge to researchers. There is a lot of research work being done on the subject of network security wireless vehicles to fight and protect these networks from threats and attacks. For the same purpose, our study focuses on the security of the VANET network

II. ATTACKS IN VANET

A. Denial of Service

Denial of Service is an attack that occurs when the attacker takes control of a vehicle's resources and blocks the communication channel used by the Network of different vehicles, preventing important and urgent information from reaching its destination. This attack amplifies the risk if the driver has to depend on the information.

B. Attack on information consistency

In the attack on information consistency, the malicious entity aims to inject and disseminate erroneous information about the state of road traffic in the network, in order to modify the behavior of other entities, such as causing other vehicles to change their route or guiding them into congestion.

C. Deleting messages

An attacker can delete packets from the network. These packets may contain information important for the receiver. The attacker deletes these packets and can use them again in a new one. time. The purpose of such an attacker is to prevent the registration and insurance authorities from knowing the vehicle collisions or to avoid submitting collision reports to access points by roadside. For example, an attacker can remove a congestion warning and use it to at another time, so that other vehicles do not receive the warning and find themselves obliged to to wait in traffic.

D. Deleting messages

An attacker can delete packets from the network. These packets may contain important information for the receiver. The attacker deletes these packets and can use them again at another time. For example, an attacker may remove a congestion warning and use it at another time, so that other vehicles do not receive the warning and are forced to wait in traffic.

E. Message alteration

Message alteration is an attack that occurs when an attacker alters one of the existing data, or changes the actual input of the transmitted data.

F. Sybil Attack

Sybil attack is an attack that occurs when an attacker creates a large number of pseudonyms, and acts by pretending that there are more vehicles on the road in order to inform other vehicles about a false congestion and force them to change their route.

G. Identity theft

In identity theft, the malicious entity uses the identity of another entity to be legitimate in the network and therefore have the attributions of the latter.

III. TYPES OF DOS ATTACK

The DOS attack is the result of any action that prevents all or part of the network from functioning properly. There are two types of attackers: the first type is the "Insider" attacker, which is an authenticated user in the network with detailed knowledge of the network. The second type is the "Outsider" attacker, it is considered an intruder with limited attack capacity, and it has no details about the architecture or operation of the network because it is not authenticated. Regardless of the type of attacker, the damage is the same and can be severe.
DOS attacks are classified according to the source of the attack, we have:

- Attacks that do not require to penetrate the network, in this case, the attacker can launch a remote attack on the network;
- Attacks where the attacker exploits a certain known vulnerability to penetrate the network then runs resource consumption attacks;
- Distributed DOS attack (DDOS) where DDOS attackers penetrate or compromise many nodes, called zombies, and use them to launch a DOS attack against the target network. In many cases, owners are unaware that their machines are being used to carry out attacks.

In this type of attacks in VANET network, attackers can launch an attack directly on other vehicles or on the RSU. The services of traffic-related information can be disrupted and busy during such an attack. This produces serious damage to human users, preventing them from accessing resources of the network in real time.
Among the most common attacks in the VANETs is the “black hole” attack. It is due to a malicious node that claims that have an optimal route to the destination that indicates that the packet should be routed by it by transmitting false

routing information. The impact of this attack is that the malicious node can either destroy or misuse the packets intercepted without transmitting them. The following Figure illustrates a Black Hole attack where a “Black Hole" region is created by a number of malicious vehicles that refuse to broadcast messages received from legitimate vehicles to other vehicles legitimate behind them. The following figure depicts an example of the black-hole attack

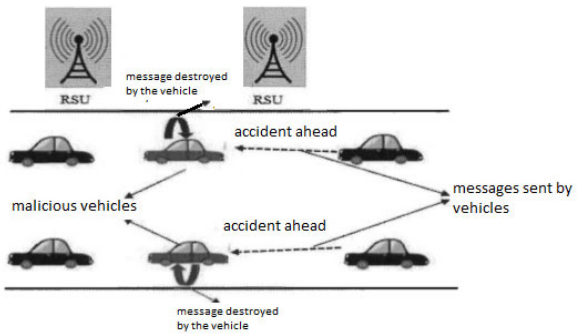

Fig. 1. Example of Black-hole Attack in VANET

Fig. 2.

IV. OPPORTUNISTIC ROUTING IN VANET

Vehicle networks are highly mobile. The density of the network is related to the traffic density, which is affected by location and time. For example, the density traffic is low in rural areas and at night, but is very high in the rural areas. large populated areas and during rush hours. In addition, a vehicle in movement can carry the package and pass it on to the next vehicle. Thanks to the “store-carry and Forward” algorithm, the message can be forwarded to the destination without a multi-step communication.

After studying a few routing protocols dedicated to vehicular wireless networks in order to find a protocol that guarantees the transmission of packets using the best route with the least delay. We noticed that the opportunistic routing protocol responds quite well to these constraints.[3] It is designed to manage the problems of frequent disconnections and extreme vehicle network mobility. It implements the "store and forward" strategy, while a node is on the move, it stores packets until a new node arrives in its region and then transmits the stored packets to that node.

This protocol provides the mobility of nodes based on two factors: network traffic and the type of route, allowing a node to discover the next transmission node. It usually sends the packet according to three main principles:
- Continue to use the available wireless channel;
- Send the packet to the carrier node by using the store-carry-and-forward algorithm
- use the publish-subscribe middleware to transmit the packet to the interested node.

In opportunistic routing, when a packet is sent, all of the neighbor nodes receive a copy. These neighbors are acting as potential next-hop forwarders. Which are called candidate-set. The nodes in this candidate-set will be responsible for cooperating with each other after a candidate coordination method. One of the selected nodes will act as the carrier of the message to a next encountered node until the node arrives at the destination which is the subscriber node. In each time a copy of the packet is received by the candidate-set nodes or by the interested node, the receiving node sends an acknowledgement. Otherwise, the sender retransmits the packet.

The opportunistic routing protocols operate under the assumption that all nodes in the network will be cooperative. This assumption may be flawed in the reality where nodes may act maliciously for several reasons which results in decreasing the performance of the network.

V. THE "BLACK HOLE" ATTACK ON THE OPPORTUNISTIC ROUTING PROTOCOL

The Black Hole attack was briefly explained in the section on attacks in the VANETs network in a previous paragraph. In this section, we will explain it in more detail with relation to the opportunistic protocol.

In a black hole attacks, a malicious node refuses to transmit data packets to the next node in a route between a source and a destination.
To carry out its attack, the malicious node must first be a network member on the data transmission route, and then takes the action of destroying all data passing through it.
Two types of black hole attacks can be described in order to distinguish them:

The attack of the internal black hole:
For this type of attack, an internal malicious vehicle integrates itself into the route from the source to the destination. As soon as it has the chance, this malicious node becomes an active part of the data route. At this stage, it now becomes capable of starting the attack as soon as data transmission begins.

The attack of the external black hole
For the external black hole attack, the attacker remains physically outside the region. of the vehicle network to be attacked. The external "Black Hole" attack can become a kind of "black hole". internal attack when it takes control of a malicious vehicle on the road between source and

interested node and control it to attack the other nodes in the network. This type of attack can block access to network traffic, create congestion or disrupt the entire network.

Scenario of the «Black Hole» attack:
The scenario of the integration of the Black Hole attack goes through the following steps:
1. A malicious Black Hole node detects that an active vehicle carrying the packet is looking for a neighbor to transmit the packet.
2. The malicious node sends a signal that shows that it is the direct neighbor.
3. Once the vehicle carrying the packet receives this message from the malicious node, it sends the packet to the malicious node.
4. As soon as the malicious node receives the packet then it can destroy it and never retransmit it.

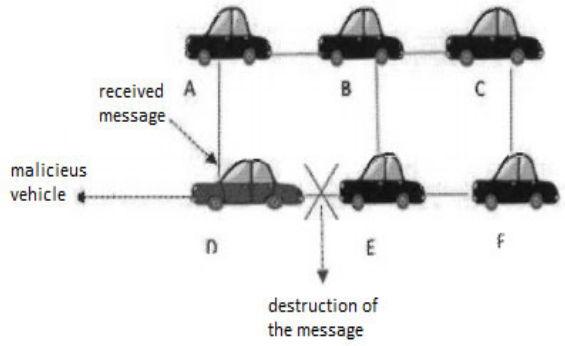

Fig. 3. Scenario of the "Black Hole" attack

Figure 2 illustrates an example where node A wants to send data packets to a node interested in the same topic F. A looks for the first neighbor to transfer the packet. As a malicious node, D acts as a direct neighbor node, so a route through the Black Hole node would be formed.
Once node D has taken control of the route to F, it can delete the data packets it receives.

VI. PERFORMANCE EVALUATION OF THE OPPORTUNISTIC ROUTING IN PRESENCE OF THE BALCK-HOLE ATTACK

In order to evaluate the opportunistic routing in the context of vanet, we analytically model it in presence of malicious nodes using Discrete-Time Markov Chains (DTMC). In OR, the packet is transmitted according to a predetermined link probability between each node and its candidates,
A coordination between the candidates is considered perfect if only one routes the packet and the others reject it, until the packet reaches its destination.

A DTMC using two absorption states can be imagined as an opportunistic routing protocol with two states as well: forwarding the packet to its destination (Success state), and abounding or not receiving the packet (Fail state) after K retransmissions. Additionally, another common point between the DTMC and the opportunistic routing process is that the arrival at a state at time t is independent of past states. we defined (ID,R) to indicate a state where ID is the node identifier and R represents the number of retransmissions of a packet until the acknowledgement is received. if R exceeds k, the node changes to the state (Fail state).

Since the assumption in opportunistic routing, that the forwarding node is positively involved in the routing of the packet, is not always true in reality, wireless nodes can act maliciously.
To do this we will model the influence of malicious nodes on opportunistic routing in vanet network.
We assume that the system is composed of N nodes in total and M black-hole nodes.
Since M is the number of malicious nodes then M absorption states will be associated to these nodes. Hence, the number of transient states will be ((N - M - 1) × (K + 1)).
The number of states in the final DTMC is equal to
n_states = (N - B - 1) × (K + 1) + M + 2 (1)
Once we have determined the DTMC states, we can create a stochastic matrix representing the probability of transition from one node to another and analyze the probability matrix later to extract network parameters such as the end-to-end packet delivery rate. The following figure depicts a DTMC for a linear topology in presence of two black-hole node (M = 2) and the total number of nodes is equal to 6.

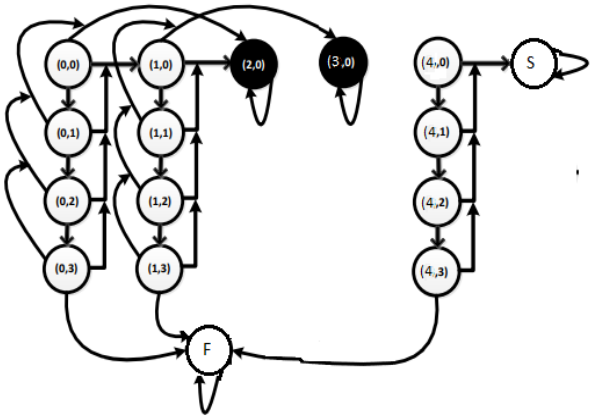

Fig 3. A DTMC for a linear topology with M=2

In this scenario, all of the selected candidates for the node 1 act as malicious nodes (node 2 and 3). In this case all of packets will not be received by the destination. So, in this situation the probability to reach the success state is 0.

The transition probability matrix P can be divided into four matrices.

$$P = \begin{bmatrix} P1 & P2 \\ P3 & P4 \end{bmatrix}$$

P1: (N - M - 1, K + 1) × (N -M -1, K + 1) indicating the transition probability between transient states.

$$P1 = \begin{bmatrix} p_{(0,0)}^{(0,0)} & p_{(1,0)}^{(0,0)} & \cdots & p_{(N-M-1,K)}^{(0,0)} \\ p_{(0,0)}^{(1,0)} & p_{(1,0)}^{(1,0)} & \cdots & p_{(N-M-1,K)}^{(1,0)} \\ \vdots & \vdots & \ddots & \vdots \\ p_{(0,0)}^{(N-M-1,K)} & p^{(N-M-1,K)} & \cdots & p_{(N-M-1,K)}^{(N-M-1,K)} \end{bmatrix}$$

P2: (N -M -1, K +1)×(M +2) indicating the transition probability between transient and absorbing states

$$P2 = \begin{bmatrix} p_{BH_1}^{(0,0)} & \cdots & p_{BH_M}^{(0,0)} & p_{Fail}^{(0,0)} & p_{Dest}^{(0,0)} \\ p_{BH_1}^{(1,0)} & \cdots & p_{BH_M}^{(1,0)} & p_{Fail}^{(1,0)} & p_{Dest}^{(1,0)} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ p_{BH_1}^{(N-M-1,K)} & \cdots & p_{BH_M}^{(N-M-1,K)} & p_{Fail}^{(N-M-1,K)} & p_{Dest}^{(N-M-1,K)} \end{bmatrix}$$

P3, which is logically filled with zero elements, shows the probability of transition from an absorbing state to a transient state.
Finally, P4 is an identical matrix (M+2)×(M+2). This matrix represents the transition probability to one of the black-hole state, the success-state or the Fail-state. In fact, given that (i,j) is an absorbing state:

$$P_{i,j}^{i,j} = 1$$

P3=0 et P4=I.

$$P3 = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix} \quad P4 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

We note that the coordination between the members of the candidate-set is considered perfect if the packet is transmitted by a higher priority candidate all others will be notified not to transmit it.the probability to reach the state corresponding to the highest priority candidate is equal to the probability of link delivery between node i and its corresponding highest priority candidate c1.

$$P_{c1,0}^{i,j} = proba\_link(i, c1) \quad (2)$$

The current node retransmits the packet each time it has not been received and the node goes to the fail state if the number of retransmissions exceeds k.Therefore, the probability of changing the current state to a state corresponding to the non-receipt of the packet that can lead to a retransmission or the transition to the fail state is equal to:

$$P_{i',j'}^{i,j} = 1 - \sum_{t=1}^{NC} P_{ct,0}^{i,j} \quad (3)$$

the delivery ratio of packets to the destination node is obtained by calculating the probability of reaching the destination state (success-state) from the initial state (Source); [5]

To reach the destination, we go through h steps or transitions. So the probability of reaching the destination in h steps is equal to P^h where P represents the transition matrix, which contains the probability for each transition between a pair of states.

$$P^h = \begin{bmatrix} P1^h & (I + P1 + \cdots + P1^{h-1}) * P2 \\ 0 & I \end{bmatrix} \quad (4)$$

The fundamental matrix of the Markov process N = (I + P1 + $P1^2$ ... + $P1^{h-1}$) = $(I - P1)^{-1}$ may be reconstructed.
Through N, the probability of reaching the absorbing state from any other transient state is equal to N × P2.

Therefore, the probability of attaining any other transient state of the source after h steps is bounded by v × P^h, which involves the first line of P^h, given that v = [1 0 ... 0]
Through the DTMC model, we measured the effect of the number of malicious nodes on the delivery of packets to their destination. The number of nodes in this scenario was set to 40 nodes, and the maximum number of attempts was set to 3. As can be seen in Figure 3, by increasing the number of malicious nodes in the wireless network, the delivery rate decreases significantly.

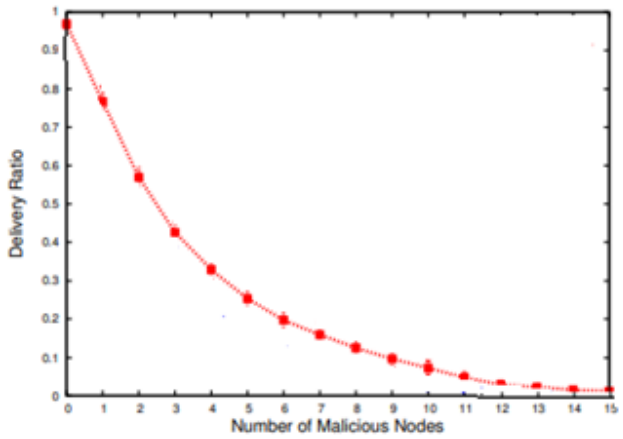

Fig3. Variation of the delivery ratio according to the number of malicious nodes

VII. CONCLUSION

Opportunistic routing protocols aim to increase the reliability of communications in VANETs. However, black holes are a well-known routing attack in which malicious nodes attempt to degrade network performance. This affects the normal performance of the network. Indeed, as shown in the previous paragraph, by increasing the number of malicious nodes in the wireless network, the delivery rate decreases significantly. For these reasons, we must combat and protect these networks from threats and attacks.

REFERENCES

[1] M. A. Mastouri and S. Hasnaoui, "Opportunistic routing in the context of publishsubscribe model for VANET," 2020 4th International Conference on Advanced Systems and Emergent Technologies (IC_ASET), Hammamet, Tunisia, 2020, pp. 181-186, doi: 10.1109/IC_ASET49463.2020.9318259.

[2] Al-kahtani, M.S, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs) ", in Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on, pp. 1-9, December 2012, Gold Coast, Australia. Print ISBN: 978-1-4673-2392-5.

[3] M. N. Lima, H. W. da Silva, A. L. dos Santos, and G. Pujolle, "A Security Management Architecture for Supporting Routing Services on WANETs," Federal University of Parana, Curitiba, Parana, Brazil, Technical Report, 2010.

[4] M. A. Mastouri and S. Hasnaoui, "Opportunistic routing in the context of publishsubscribe model for VANET," 2020 4th International Conference on Advanced Systems and Emergent Technologies (IC_ASET), Hammamet, Tunisia, 2020, pp. 181-186, doi: 10.1109/IC_ASET49463.2020.9318259.

[5] A. Darehshoorzadeh and L. Cerdà-Alabern, "Distance Progress Based Opportunistic Routing for wireless mesh networks," 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, Cyprus, 2012, pp. 179-184, doi: 10.1109/IWCMC.2012.6314199.

[6] John Tobin, Christina Thorpe, Damien Magoni, Liam Murphy. An Approach to Mitigate Multiple Malicious Node Black Hole Attacks on VANETs. 16th European Conference on Cyber Warfare and Security, Jun 2017, Dublin, Ireland. ffhal-01577471f

[7] Manish Kumar, Vanita Jain, Achin Jain, Uttam Singh Bisht & Neha Gupta (2019) Evaluation of black hole attack with avoidance scheme using AODV protocol in VANET, Journal of Discrete Mathematical Sciences and Cryptography, 22:2, 277-291, DOI: 10.1080/09720529.2019.1585635

[8] H. Hasrouny, A.Samhat, C.Bassil, A.Laouiti, VANET security challenges and solutions: A survey, Vehicular Communications, Volume 7, January 2017, Pages 7-20. http://dx.doi.org/10.1016/j.vehcom.2017.01.002

[9] K.S. Praveen, H.L. Gururaj, B. Ramesh, Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols, Procedia Computer Science, Volume 85, 2016, Pages 325-330. http://dx.doi.org/10.1016/j.procs.2016.05.240