ATTACK ANALYSIS IN VEHICULAR AD HOC NETWORKS

Ömer Mintemur[1] and Sevil Sen[2]

[1]Computer Engineering, Hacettepe University, Ankara, Turkey
omermintemur@gmail.com
[2]Computer Engineering, Hacettepe University, Ankara, Turkey
ssen@hacettepe.edu.tr

ABSTRACT

One of the most promising and exciting area of communication technology is Vehicular Ad Hoc Networks (VANETs). It enables cars to communicate among and between each other and fixed infrastructures and, provides safe and enjoyable driving experience. However, VANETs are very susceptible to attacks that could easily be evasive due to its dynamic topology and, cause very dramatic results in traffic. To develop suitable security solution for VANETs, we must firstly understand how attacks could affect the network. Therefore, we analyse four different types of attacks against two popular routing protocols (AODV, GPSR) in VANETs. All attacks, blackhole, dropping, flooding, and bogus information, are implemented on two real maps having low and high density. The results clearly show how attacks could severely affect the communication and, the need of security solutions for such highly dynamic networks.

KEYWORDS

VANETs, AODV, GPSR, security, intrusion, misbehaviour, attacks, blackhole, flooding, dropping, bogus, information.

1. INTRODUCTION

Conventional communication technology is changing rapidly. Opportunity to communicate via wireless technology brings unlimited alternatives such as mobile ad hoc networks (MANETs), wireless sensor networks (WSN), and the like. In mobile ad hoc networks, mobile nodes can communicate without any fixed infrastructure. This infrastructureless characteristic of mobile ad hoc networks makes way for many different communication technologies to enlive. One of the most intriguing of them is vehicular ad hoc networks (VANETs). Basically, this new environment makes cars communicate among and between each other and fixed structures called Road Side Units (RSUs). In such networks, every car is equipped with a device called On-Board Units (OBUs) that enables cars to have communication capability [1]. Cars could send and receive any information such as traffic conditions, road conditions, and the like [2]. The main purpose of VANETs is to provide safer and efficient driving pleasure to drivers. They are expected to become widespread when some research challenges are addressed. One of these challenges is to provide security of such dynamic networks.

Although VANETs are highly desirable for a safe and comfortable driving experience, using wireless channel and having a fast changing topology make them vulnerable to new forms of attacks [3]. A malicious car could disrupt the network and, cause unwanted results such as loss of lives, money, time and the like [3], [4]. An attacker could achieve its purpose mainly by using the weakness of the routing protocols and application protocols in VANETs.

A rigorous analysis of attacks is a necessity in order to develop suitable security solutions for VANETs. It is the main aim of this study. Four types of attacks, namely blackhole, dropping, flooding, and bogus information attacks are analysed on two popular routing protocols AODV, GPSR in this study. In our study, real high/low density road maps in which vehicles moves as in a real road are simulated. Furthermore, attack scenarios are implemented on real maps having realistic conditions (network mobility and density). We believe this analysis helps researchers to create efficient and suitable security solutions for VANETs.

2. RELATED WORK

Analysis of attacks in AODV have been widely analysed in literature. However these analyses are usually carried out on mobile ad hoc networks, not highly dynamic vehicular ad hoc networks. Furthermore, there has not been a study of attacks in GPSR to the best of our knowledge.

Extensive analysis of different types of attacks against AODV on MANETs can be found in [5]. In this study, both atomic and compound misuses are introduced for AODV. In the simulations, only one attacker is assumed to be in the network. Furthermore, the simulated networks consist of only five nodes in atomic misuses, and 20 nodes in compound misuses. Even though all kinds of attacks are presented in details in this study, the simulations are limited.

One of the mostly analysed attacks in the literature is the blackhole attack due to being a specific attack to ad hoc routing protocols. Four routing protocols (AODV, DSR, OLSR and TORA) are analysed under blackhole attack in MANETs [6]. The results show that AODV has poorer performance that other protocols on simulated networks under attack. Blackhole attack is also analysed in VANETs by using AODV and OLSR [7]. The results support the study given in [6] that AODV is more susceptible to attacks than OLSR. Although the simulations are done for VANETs, the nodes in the experiments are assumed to move at constant speed (10 m/s), which is not realistic for vehicular communication.

As in MANETs, a watchdog-based detection mechanism is usually proposed for the detection of blackhole attacks in VANETs [8]. In this method, every packets sent by vehicles is being watched. Every car maintains a trust table for its neighbours, and this trust value is determined by the ratio of packets that should be transmitted over packets that are really transmitted. Any vehicle that drops below certain threshold is considered as a malicious vehicle.

Flooding attack [9] is another type of attack analysed for MANETs in the literature. The network performance is very affected by sending lots of packets [10]. This study also uses AODV as an exemplar protocol. They also proposed a detection mechanism for ad hoc flooding attack in which every vehicle watches its neighbours. If a neighbour sends RREQ packets exceeding a certain threshold, it is tagged as an attacker. A similar threshold-based approach [11] is proposed for the detection of flooding attacks on VANETs. For further information on attack detection mechanisms in VANETs, the readers could refer to the recent survey [12].

As it is shown in the literature, the analysis of attacks on VANETs is very limited. Moreover, although bogus information attack could have a disastrous effect on VANETs, the studies mainly propose a detection technique, do not analyze the attack in details as we do in this study. Furthermore, the simulation environment in these studies might not be very realistic. In our study, real high/low density road maps in which vehicles moves as in a real road are simulated. As far as we know, this is the most rigorous attack analysis in terms of the type of attacks, and the number of attackers in VANETs.

3. ROUTING PROTOCOLS: AODV AND GPSR

VANETs can inherit routing protocols that are currently used in MANETs. Extensive review of routing protocols of VANETs can be found [13]. In this study widely known AODV (Ad-Hoc on Demand Distance Vector Routing) [14] and GPSR (Greedy Perimeter Stateless Routing) [15] routing protocols are used. This section briefly explains these two routing protocols. While AODV is one of the most popular routing protocols, GPSR is one of the position-based protocols that are suited to VANETs [16].

3.1. AODV (Ad-Hoc on Demand Distance Vector Routing Protocol)

AODV routing protocol is a reactive routing protocol [14]. In this protocol, the routes are established just before any packet transmission begins. In the route discovery, two types of routing control packets are used: RREQ (route request) and RREP (route reply).

When a vehicle wants to send a data packet to another vehicle and do not know the path to this destination vehicle, a RREQ packet is generated and broadcast to the network. Vehicles that receive these RREQ packets control their routing table whether they already know a path to the destination vehicle or not. If they have a fresh route to the destination vehicle, they return a RREP packet to the source vehicle. Otherwise, the RREQ packet is rebroadcast. When a RREQ packet arrives to the destination, a unicast RREP packet is sent back to the source vehicle. As soon as the source node receives a RREP packet, it starts sending data packets. There could be more than one path between two communication endpoints, but the shortest path is built in AODV.

AODV has also a routing control packet called RERR (Route Error), that are sent by vehicles if any of their neighbours are unreachable. This packet type indicates broken links, vehicles that gone out of range, etc. The local connectivity could be maintained both at the link layer and at the routing layer. If a link breakage is detected, RERR packets are sent to the neighbours.

3.2. GPSR (Greedy Perimeter Stateless Routing Protocols)

GPSR routing protocol is a geographic-based routing protocol which transmits data packets by using vehicles' geographical positions [15]. Unlike AODV, GPSR does not establish a route in advance.

PSR uses two different forwarding mechanisms: greedy and perimeter forwarding. In GPSR, vehicles know their neighbours by sending periodic beacon packets. By sending and receiving beacons, vehicles construct their routing table. At the beginning, positions of each vehicle are saved in a look up table. When a vehicle moves, the look up table is updated with the new position of the vehicle by using LocService (LOCS) packets which are periodic packets to inform vehicles about vehicles' positions. When a vehicle wants to send a message, it originates a packet contains only the originator address and the destination address. The source vehicle transmits the packet to its neighbour that are closest to the destination according to neighbours' positions. This mechanism continues until the destination is reached (greedy forwarding). Hence, the next hop is determined by forwarding nodes during data packet transmission. When greedy forwarding fails, it means that packet transmitting vehicle cannot find any vehicle closer to the destination within its coverage area, hence GPSR turns to perimeter forwarding. In perimeter forwarding, packets are forwarded using the planar graph. Packet is traversed by the right hand rule within the network until the packet transmission turns back to greedy forwarding. As stated in [15], beacons interval could be selected optionally. Beacons interval is selected as 0.5 sn in this study to be compatible with the nature of VANETs. It is shown that the bigger the beacon interval is, the less packets are delivered successfully [15]. Hierarchical location service [17], which divides the area covered by the network into a hierarchy of regions for discovering the locations of nodes, is also employed in the simulations.

4. Implemented Attacks

In this study, the effects of four types of attacks are evaluated on both routing protocols. The implementation details of these attacks on AODV and GPSR are given in details in this section.

4.1. Blackhole Attack

The main aim of this attack is to direct data packets to the malicious vehicle by claiming it has the best route to the destination. It is mainly employed with dropping attack. After the route is established through the malicious vehicle, data packets are dropped.

In AODV, the freshness of a route is defined with sequence numbers. In the blackhole attack scenario in this study, the attacker takes advantage of this characteristic of AODV. The malicious vehicle receiving a RREQ packet replies with a RREP packet by incrementing the destination sequence number in the original RREQ packet. Even though the source node could receive more than RREP packets, it will accept the freshest one coming from the malicious vehicle. Hence the malicious vehicle puts itself in the route between the source and the destination node. He could either listen to their communication, or disrupt it. In this attack scenario, the attacker simply drops data packets passing through him.

In GPSR, the source vehicle always chooses a vehicle closest to the destination for forwarding its packet. In this attack scenario, the attacker takes control of the traffic by advertising itself as the nearest node to the destination. As in AODV, the malicious vehicle drops data packets passing through him. In order to achieve his goals, the attacker needs to be accessible from the source node, so he could get the request and send a fake reply.

4.2. Dropping Attack

In this attack type, malicious vehicle simply drops all the packets that he receives. This attack is different from blackhole attack. In the blackhole attack scenario, malicious vehicle claims itself having the shortest path and take control of the traffic, then drops data packets. However in packet dropping attack scenario, malicious vehicle could only drop data packets if a packet is transmitted through it. Even it is a simple attack, it could cause serious consequences, especially in safe-related applications. Furthermore, it is difficult to be indistinguishable from legal packet dropping on networks under high mobility.

4.3. Flooding Attack

The flooding attack is a type of DoS attack. The main aim of the attack is to exhaust network by sending lots of control packets, hence nodes in the network may not be able to process legal traffic. While malicious vehicles could bombard the network with RREQ packets in AODV, beacon messages are employed in GPSR for this purpose. This attack both exhausts network bandwidth, and nodes' packet queues, and the network becomes unavailable to legitimate users.

In the simulations, in AODV malicious vehicle broadcasts a fake RREQ packet for a non-existent vehicle in the network every 0.2 seconds. In GPSR, a malicious vehicle broadcasts lots of beacons to its neighbours to disrupt their functionalities. Beacon packets are sent at 0.2 second intervals. Fake packets keep being sent in both routing protocols until the simulation terminates.

4.4. Bogus Information Attack

In bogus information attacks, the attacker send falsified information to the network. For example, an attacker could send information about a fake accident on a road, so divert traffic to another road. It could be very effective when there is no other vehicle to verify this falsified information. It is called motorway attacker [18] if the attacker moves around quickly, and disseminate false information to a large group of nodes.

In the attack scenario, the attacker chooses a node as victim, and then prepare a RREQ or beacon packet for AODV and GPSR respectively as it is generated from this victim one. The packets are generated for a randomly selected destination node and, the attacker node broadcasts these packets on behalf of the victim node every 5 seconds. The attacker attracts traffic by being the freshest node or the closest node to the destination in AODV and GPSR respectively. Again, any packets transmitting through the attacker will be dropped. This attack could also be used to make a node to isolate from the network, and the like. However it will have little effect on the network due to fast changing topology of VANETs. Any packet that is not transmitted through the attacker will not be affected.

5. EXPERIMENTAL RESULTS

In this section, firstly the simulation environment is introduced. Then, the effects of each attack on the network is evaluated by analysing simulation results. Each attack is evaluated with well-known network performance metrics: packet delivery ratio, overhead, end-to-end (E2E) delay.

5.1. Simulation Environment

All simulations are conducted in widely used network simulator, ns-2 [19]. Each simulation is run for 200 seconds. Each attack is evaluated in networks with varying number of attackers (0%, 5%, 10%, 15%, 20%, 25%, and 30%). In each group of attackers, the position of attackers are assigned randomly ten times. 10 different connection files are established, and each connection file has 15 different connections. Hence, 700 simulations are run for an attack against a routing protocol and, their averaged results are presented in the subsequent section. In total, 5600 simulations run for a map. The simulation parameters used in the experiments are given in Table 1: Simulation Parameters

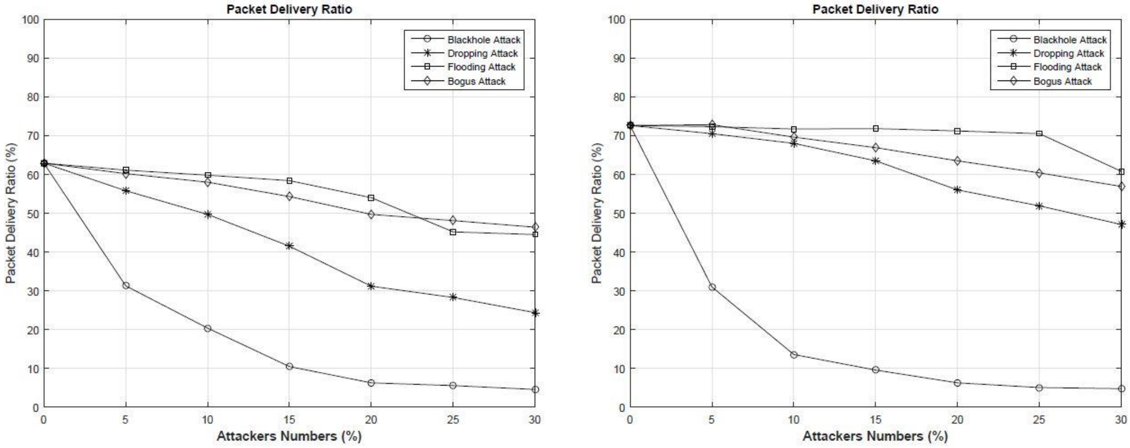
Table 1: Simulation Parameters

Simulation Parameters	**Value**
Simulation Time	200 Seconds
Network Area	Istanbul Motorway (2600m X 1340m) Munich City Center (2000m X 1380m)
Number of Vehicles	35
Data Packet Type	CBR
Packet Size	512 bytes
Vehicle Speed	0 – 70 m/sn
Propagation Model	Nakagami [20]
Communication Range	250 m
MAC Layer Protocol	802.11
Local Link Connectivity	Link Layer Notifications (MAC Control Packets)

Simulations are implemented on two real maps: Munich city center, and a part of Istanbul motorway. These roads are chosen due to their traffic densities. While Munich road has high density, Istanbul motorway has low density. These maps are generated by using SUMO [21] and OpenStreetMap [22].

5.2. Results in AODV

5.2.1. Packet Delivery Ratio – AODV



(a) Istanbul Motorway

(b) Munich City Center

Figure 1. Packet Delivery Ratio – AODV

Figure 1 shows the packet delivery ratio of AODV in Istanbul Motorway 1(a) and Munich City Center 1(b). In general, dense network has a higher packet delivery ratio than sparse network. As expected, while the attacker percentage in the network increases, packet delivery ratio decreases in both maps. Figures clearly show that Istanbul Motorway is affected more severely than Munich City Center. Because of the density, vehicles in Munich are able to find more connections than Istanbul Motorway even in the existence of attackers.

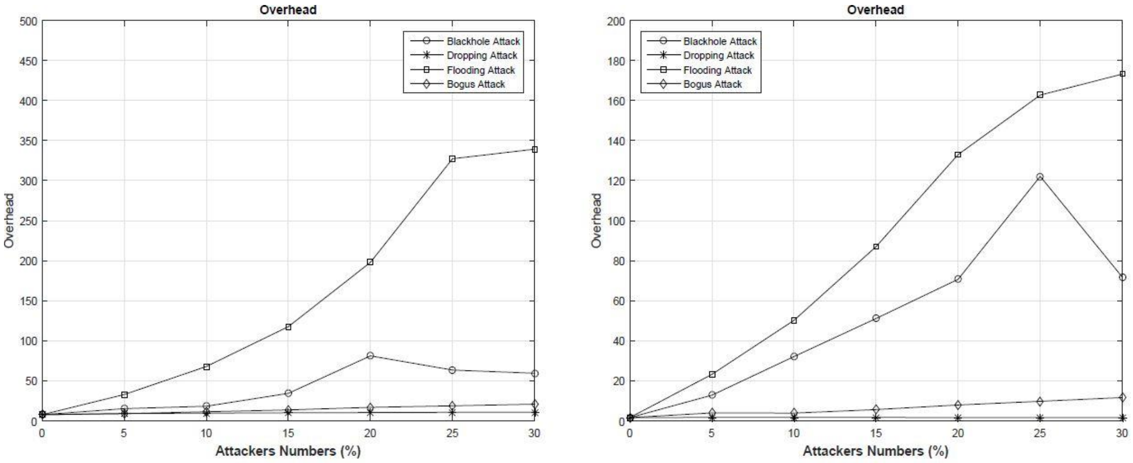
Packet dropping attack decreases the packet delivery ratio as expected, however the increase is not as much as in the blackhole attack scenario. This attack is more effective if the attacker is in a critical position such as being the only node that connect two endpoints, or two network partitions [23]. Since the attacker diverts traffic through itself in blackhole attack, it is more effective. However in a simple packet dropping attack scenario, the attacker only drops packets if they are transmitted through it. Since the attacker diverts traffic through itself in blackhole attack, it is more effective. However in a simple packet dropping attack scenario, the attacker only drop packets if they are transmitted through it.

Flooding attack does not have a severe effect as much as blackhole and dropping attacks do. As the number of fake packets broadcast to the network increases, it will cause more packets to be dropped due to heavy traffic on the network. This situation applies to the increase of the number of attackers as clearly seen in the figure.

In bogus attack scenario, by pro-actively forging fake routing control packets without receiving any packets (differently from blackhole attack), the attacker diverts and then drops data packets, and hence decreases the packet delivery ratio as shown in figure 1.

In general, sparse networks (i.e Istanbul Motorway) is affected more than dense networks (i.e Munich City Center). Moreover, when there are no malicious vehicles in the network, dense networks have higher packet delivery ratio than dense networks as expected. In such networks, vehicles could find more vehicles that could be able to continue the packet transmission.

5.2.2. Overhead – AODV

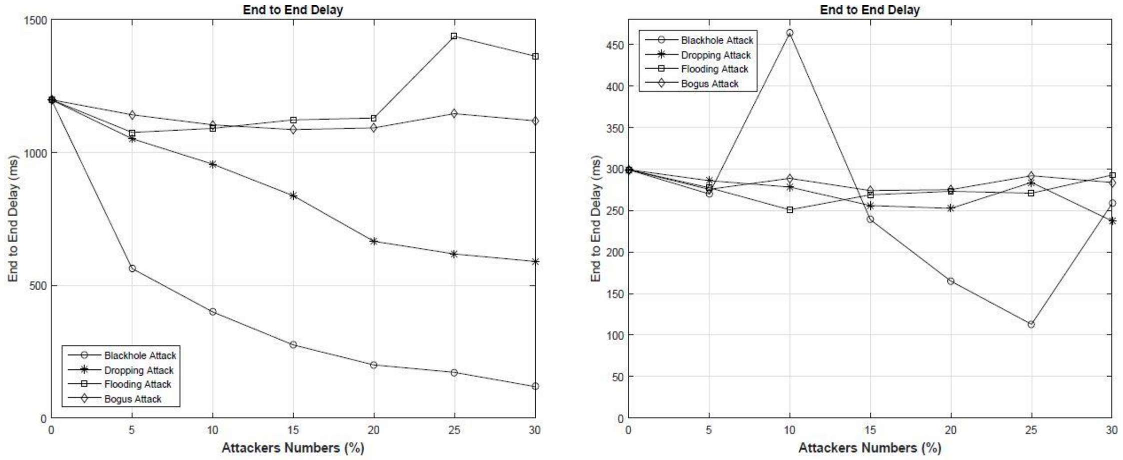


(a) Istanbul Motorway (b) Munich City Center

Figure 2. Overhead – AODV

Figure 2 shows the overhead results for the attacks in both Istanbul Motorway and Munich City Center. As the number of attacker increases, the overhead also increases due to disrupted routes. Flooding attack due to its very nature increases the overhead most. Blackhole attack also increases the overhead considerably due to disrupting effective routes. The density of maps affects the overhead results as well. Since the dense network provides more connectivity, they introduce less control packets into the network.

5.2.3. End to End Delay – AODV



(a) Istanbul Motorway (b) Munich City Center

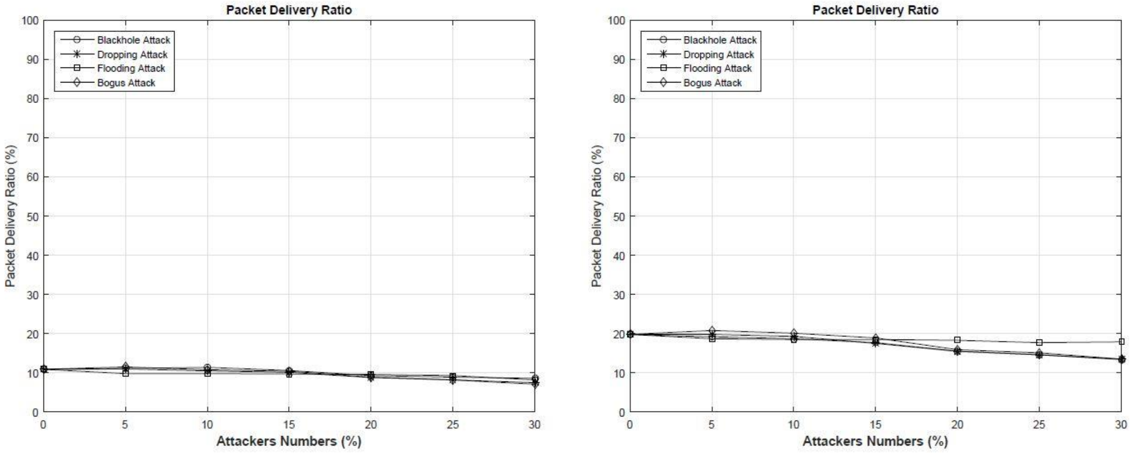
Figure 3. End - to - End Delay - AODV

Istanbul Motorway is affected much more than Munich City Center in terms of end-to-end delay as shown in figure 3. End-to-end delay remains the same or increases when the number of attackers exceed certain threshold in flooding and bogus information attacks. In the existence of blackhole or dropping attacks, since less data packets are trying to be sent, they will be able to reach their destinations without waiting due to traffic in the network. Even though the number of routing control packets increases, as shown in figure 2, this increase is not very significant. Because of dropped data packets, routes to the destination are re-built. In the simulations, it is observed that the average hop count could also decrease while the number of attackers increases and the topology changes. Due to sending data packets to closer nodes, a decrease in end-to-end delay is also occurred in the case of blackhole and dropping attacks.

There is a fluctuation in blackhole attack in Munich City map in figure 3. Selection of attackers, position of attackers, communication patterns, etc. could cause this fluctuation.

5.3. Results in GPSR

5.3.1. Packet Delivery Ratio – GPSR



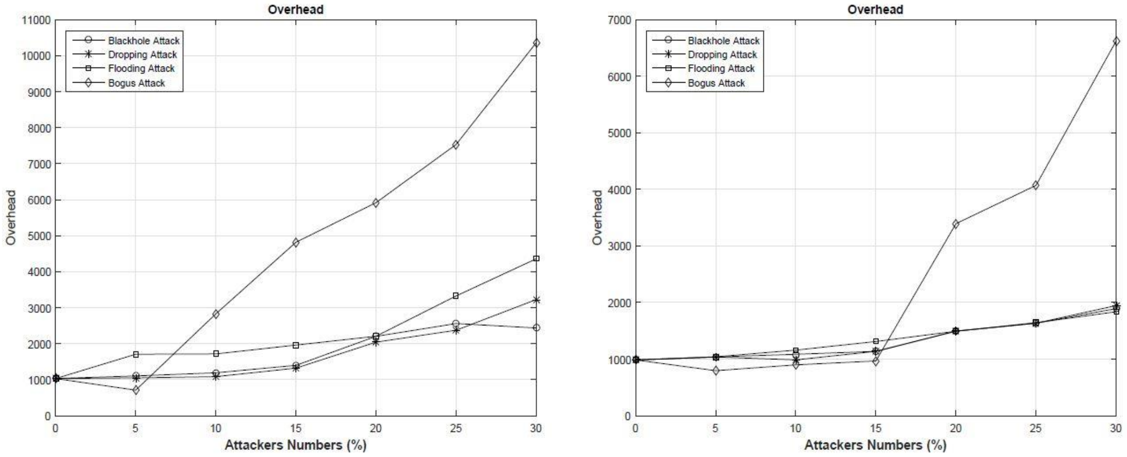
(a) Istanbul Motorway

(b) Munich City Center

Figure 4. Packet Delivery Ratio – GPSR

Figure 4 shows the packet delivery ratio of the all attacks in both maps. GPSR's instantaneous vehicle selection to transmit a packet does not always succeed. Lack of selecting the best destination for packet transmission results in poor packet delivery performance. The packet delivery ratio is higher on dense networks. Since a node could find more alternative routes to a destination node in such networks, the sustainability of a communication could be provided longer. GPSR is affected almost equally for all attacks as demonstrated in figure 4. The main difference between AODV and GPSR is that AODV has a pre-route establishment, where routes are established before packet transmission begins. That is why AODV has higher packet delivery ratio than GPSR. Also, the density of networks plays an important in packet delivery ratio. Since a node could find more alternative routes to a destination node in dense networks, the sustainability of a communication could be provided longer.

5.3.2 Overhead – GPSR



(a) Istanbul Motorway

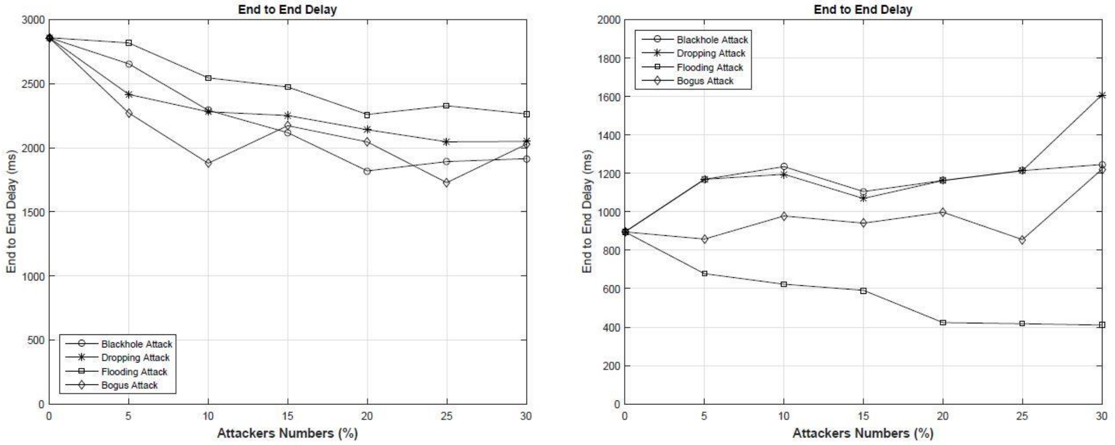
(b) Munich City Center

Figure 5. Overhead – GPSR

Overhead results are given in figure 5 for all attacks in both maps. GPSR clearly has more overhead than AODV. Due to the high number of beacon packets and having two different forwarding mechanisms [24], overhead is quite high in GPSR even under no attack. When GPSR could not find a suitable vehicle to transmit a packet, more control packets (beacons) are broadcast to the network. Besides periodic beacon packets, LOCS packets sent more frequently under high mobility is another factor affecting overhead in GPSR. As demonstrated, the overhead of GPRS under attack demonstrates a dramatic increase.

Since there are already more routing control packets in the low density networks, they are a bit more affected by flooding attacks in both routing protocols. As the attacker number increases more control packets will be burst to the network which result in more overhead. Moreover, in GPSR this attack is more damaging as the attacker sends beacon packets to his all neighbours. The increase in the routing control packets could be clearly seen in figure 5.

5.3.3 End – to – End Delay – GPSR



(a) Istanbul Motorway

(b) Munich City Center

Figure 6. End - to - End Delay – GPSR

Figure 6 shows the-end-to end delay for attacks in two different maps. In Istanbul Motorway, GPSR's end-to-end delay for all attacks are decreasing. Since less packet is transmitted in a short time to the destination point, end-to-end delay is decreasing. On the other hand, Munich City Center is not affected as much as Istanbul Motorway due to the high density of nodes in the city centre traffic and, more application of GPSR's greedy forwarding mechanism under attack. Please note that density is not the only major factor affecting end-to-end delay. There are also other parameters such the location of attackers and the network topology, traffic patterns, and the like.

To sum up, each attack negatively affects the communication in vehicular ad hoc networks. AODV is generally more severely affected by routing attacks. On the other hand, AODV has a better packet delivery ratio than GPSR in a network under no attack. This is because GPSR does not always select the best route as it decides packet transmission location instantaneously. Results showed that both protocols have better performance in dense networks under no attack as expected. Although AODV demonstrates a fairly good performance on networks under no attack, pre-establishing mechanism of AODV shows a weakness in which attackers could exploit. On the other hand, the instantaneous path selection mechanism of GPSR hardens attackers to put themselves in a path. The attacker could directly change the communication links to its neighbours only. In the results, the attack which affects AODV the most is blackhole attack. In AODV, an attacker has a high chance of diverting the packet transmission by sending fake RREP packets. GPSR are generally affected by each attack especially when the percentage of attackers in the network exceeds 20% of all nodes. More dense networks consisting of more vehicles could be more suitable for showing the reaction of GPSR against attacks.

6. CONCLUSION

Vehicular ad hoc networks is an emerging technology. It is believed to be extensively used in the near future. Security is one of the biggest issues to be handled before that. In order to be able to develop suitable prevention and detection mechanisms for VANETs, the nature of attacks and their effects on the network should be analysed carefully. It is the main aim of this study. The attacks, namely blackhole, dropping, flooding and bogus information, are implemented on AODV and GPSR routing protocols. Although there are some analysis of attacks specific to MANETs in the literature, their effects on more dynamic environments should be explored as done in this study. More popular attacks against VANETs such as bogus information attacks are also implemented and analysed. More importantly, all attacks are implemented on real maps and under realistic scenarios. Furthermore, the impacts of the number of attackers, and the density of road traffic are shown in the results. Especially GPSR is affected when the number of attackers exceeds 20% of the network. For AODV, the attack type is more influential. The subtle attacks such as blackhole attack decrease the performance of AODV dramatically. The simulation results clearly show the need of security mechanism suitable for such highly dynamic environment. We believe this analysis helps researchers working in this area. As far as we know this is one of the most extensive attack analysis for VANETs in the literature.

REFERENCES

[1] R. Engoulou Gilles, M. Bellache, S. Pierre, and A. Quintero, “Vanet Security Surveys,” *Computer Communications*, vol. 44, pp. 1 – 13, 2014.

[2] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan “Vehicular ad hoc networks (vanets): status, results, and challenges,” *Telecommunication Systems*, vol. 50, no 4, pp. 217 – 241, 2010.

[3] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, vol. 15, no. 1, pp. 39 – 68, 2007.

[4] R. D. Pietro, S. Guarino, N. Verde, and J. Domingo-Ferrer, “Security in wireless ad-hoc networks a survey,” *Computer Communications*, vol. 51, pp. 1 – 20, 2014.

[5] P. Ning and K. Sun, “How to misuse aodv, a case study of insider attacks against mobile ad hoc routing protocols,” *Ad Hoc Networks*, vol. 3, no. 6, pp. 795 – 819, 2005.

[6] E. F. Ahmed, R. A. Abouhogail, and A. Yahya, “Performance evaluation of blackhole attack on vanet’s routing protocols,” *International Journal of Software Engineering and Its Applications*, vol. 8, no. 9, pp. 39 – 54, 2014.

[7] V. Bibhu, R. Kumar, B. S. Kumar, and D. K. Singh, “Performance analysis of black hole attack in vanet,” *International Journal Of Computer Network and Information Security*, vol. 4, no. 11, pp. 47–54, 2012.

[8] J. Hortelano, J. C. Ruiz, and P. Manzoni, “Evaluating the usefulness of watchdogs for intrusion detection in vanets,” in *Proceedings of The Conference on Communications Workshops (ICC)*, IEEE. IEEE, 2010, pp. 1–5.

[9] P. Yi, Z. Dai, S. Zhang, and Y. Zhong, “A new routing attack in mobile ad hoc networks,” *International Journal of Information Technology*, vol. 11, no. 2, pp. 83–94, 2005.

[10] M. Abdelshafy and P. King, *Resisting flooding attacks on AODV*. International Academy, Research and Industry Association, IARIA, 2014, pp. 14–19.

[11] A. Sinha and S. K. Mishra, “Preventing vanet from dos & ddos attack,” *International Journal of Engineering Trends and Technology (IJETT)*, vol. 4, no. 10, pp. 4373–4376.

[12] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and iov,” *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[13] B. T. Sharef, R. A. Alsaqour, and M. Ismail, “Vehicular communication ad hoc routing protocols: A survey,” *Journal of Network and Computer Applications*, vol. 40, pp. 363 – 396, 2014.

[14] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” in *Proceedings of The 2nd International IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*. IEEE, 1999, pp. 90–100.

[15] B. Karp and H.-T. Kung, “Gpsr: Greedy Perimeter stateless routing for wireless networks,” in *Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom)*. ACM, 2000, pp. 243–254.

[16] H. Ghafoor and K. Aziz, “Position-based and geocast routing protocols in vanets,” in *Proceedings of the 7th International Conference on Emerging Technologies (ICET)*. IEEE, 2011, pp. 1–5.

[17] W. Kieß, H. F¨ußler, J. Widmer, and M. Mauve, “Hierarchical location service for mobile ad-hoc networks,” *ACM SIGMOBILE mobile computing and communications review*, vol. 8, no. 4, pp. 47–58, 2004.

[18] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J. P. Hubaux, “Fast exclusion of errant devices from vehicular networks,” in *Proceedings of the 5th International Conference of Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2008, pp. 135–143.

[19] “The Network Simulator NS-2,” http://www.isi.edu/nsnam/ns/, 2017.

[20] P. K. Singh, “Article: Influences of tworayground and nakagami propagation model for the performance of adhoc routing protocol in vanet,” *International Journal of Computer Applications*, vol. 45, no. 22, pp. 1–6, 2012.

[21] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, “Sumo–simulation of urban mobility,” in *Proceedings of The 3rd International Conference on Advances in System Simulation (SIMUL)*, 2011.

[22] M. Haklay and P. Weber, “Openstreetmap: User-generated street maps,” *Pervasive Computing*, vol. 7, no. 4, pp. 12–18, 2008.

[23] S. Sen, J. A. Clark, and J. E. Tapiador, “Security threats in mobile ad hoc networks,” S*ecurity of Self-Organizing Networks: MANET, WSN, WMN, VANET, Auerbach Publications*, pp. 127–147, 2010.

[24] M. R. Jabbarpour, A. Jalooli, E. Shaghaghi, A. Marefat, R. M. Noor, and J. J. Jung, “Analyzing the impacts of velocity and density on intelligent position-based routing protocols,” *Journal of Computational Science*, vol. 11, pp. 177 – 184, 2015.

Authors

Photo

Short Biography