ATTACK ANALYSIS IN VEHICULAR AD HOC NETWORKS

Ömer Mintemur and Sevil Sen

Computer Engineering, Hacettepe University, Ankara, Turkey

ABSTRACT

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

KEYWORDS

VANETs, security, attacks, blackhole, bogus, information.

1. INTRODUCTION

Conventional communication technology is changing rapidly. The opportunity to communicate via wireless technology brings about unlimited alternatives such as mobile ad hoc networks (MANETs), and wireless sensor networks (WSN). In mobile ad hoc networks, mobile nodes can communicate with no fixed infrastructure. This infrastructureless characteristic of mobile ad hoc networks enables the application of many different communication technologies. One of the most intriguing is vehicular ad hoc networks (VANETs). Basically, this new environment enables communication among and between vehicles and fixed structures called Road Side Units (RSUs). In such networks, each vehicle is equipped with a device called an On-Board Unit (OBUs) that enables their communication capability [1]. Vehicles can send and receive information such as traffic conditions and, road conditions [2]. The main purpose of VANETs is to provide drivers with a safer and more efficient driving experience. VANETs are expected to become widespread once certain research challenges have been successfully addressed, such as provision of security for these dynamic networks.

Although VANETs are highly desirable for a safe and comfortable driving experience, the use of wireless channels and fast changing topology make them vulnerable to new forms of attack [3]. A malicious vehicle could disrupt the network and, cause unwanted results such as loss of lifes, money, and time [3], [4]. An attacker could achieve its purpose mainly through exploitation of the weakness of the routing protocols and application protocols in VANETs.

An extensive analysis of attacks is necessary in order to develop suitable security solutions for VANETs, which is the primary aim of this study. In this study, four types of attacks, namely

Natarajan Meghanathan et al. (Eds) : ICCSEA, WiMoA, SPPR, GridCom, CSIA - 2017
pp. 35– 46, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.71103

blackhole, dropping, flooding, and bogus information attacks were analyzed on two popular routing protocols, AODV and GPSR. Real high/low density road maps were simulated in which vehicles move as on real roads. Furthermore, attack scenarios were implemented on real maps having realistic conditions (network mobility and density). The code and configuration files of attack simulations will be made publicly available. The authors believe that this analysis helps researchers to create efficient and suitable security solutions for VANETs.

2. RELATED WORK

Analysis of attacks in AODV have been widely analyzed in the literature. However, such analyses are mostly conducted out on mobile ad hoc networks, rather than, highly dynamic vehicular ad hoc networks. Furthermore, there has been little study of attacks in GPSR on VANETs.

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

One of the mostly analyzed attacks to be found 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) were analyzed under blackhole attack in MANETs [6]. The results showed that AODV performed poorer than other protocols on simulated networks under attack. Blackhole attack was also analyzed 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 were for VANETs, the nodes in the experiments were assumed to move at a constant speed (10 m/s), which is unrealistic for vehicular communication.

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

In the literature flooding attack [9] is another type of attack analyzed for MANETs, where network performance is greatly affected by the sending of numerous packets [10]. This current study also used AODV as an exemplar protocol. The current study also proposed a detection mechanism for ad hoc flooding attack in which every vehicle watches its neighbors. If a neighbor 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, see the recent surveys in this area [12],[13].

As shown in the literature, analysis of attacks on VANETs is very limited. Moreover, although a bogus information attack could have a disastrous effect on VANETs, the literature mainly proposes a detection technique, and does not analyze the attack in detail as in this current study. Furthermore, the simulation environment in some studies might be unrealistic. In this current study, real high/low density road maps are simulated in which vehicles move as on a real road. To the best of the authors knowledge, this current study is the most extensive attack analysis in terms of attacks type, and the number of attackers in VANETs.

3. ROUTING PROTOCOLS: AODV AND GPSR

VANETs can inherit routing protocols currently used in MANETs. An extensive review of routing protocols of VANETs can be found in [14]. This current study employs widely known AODV (Ad-Hoc on Demand Distance Vector Routing) [15] and GPSR (Greedy Perimeter Stateless Routing) [16] routing protocols. 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 suited to VANETs [17].

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

AODV routing protocol is a reactive routing protocol [15] in which 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 check their routing table as to whether or not they already know a path to the destination vehicle. If they locate 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 returned 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 also has a routing control packet called RERR (Route Error), which are sent by vehicles if any of their neighbors are unreachable. This packet type indicates broken links, vehicles that have 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 neighbors.

3.2. GPSR (Greedy Perimeter Stateless Routing Protocol)

GPSR routing protocol is a geographically-based routing protocol which transmits data packets by using vehicles' geographical positions [16]. Unlike AODV, GPSR does not establish a route in advance.

GPSR uses two different forwarding mechanisms: greedy and perimeter forwarding. In GPSR, vehicles know their neighbors by sending periodic beacon packets. Through the sending and receiving of beacons, vehicles each construct their own 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 informing about vehicles' positions. When a vehicle wants to send a message, it originates a packet containing only the originator address and the destination address. The source vehicle transmits the packet to its neighbor closest to the destination, according to the neighbors' 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 the 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. Packets are traversed by the right hand rule within the network until the packet transmission turns back to greedy forwarding. As stated in [16], beacon intervals could be selected optionally. In the current study, the beacon interval was selected as 0.5 s to ensure compatibility with the nature of VANETs. The literature shows that the bigger the beacon interval, the fewer packets are delivered successfully [16].

Hierarchical location service [18], 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 current study, the effects of four types of attacks were evaluated on both routing protocols. The implementation details of these attacks on AODV and GPSR are detailed 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 of the current 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 one RREP packet, it will accept the freshest one coming from the malicious vehicle. Hence the malicious vehicle place itself in the route between the source and the destination node. The malicious vehicle could either listen to or disrupt the source vehicles' communication. In this attack scenario, the attacker simply drops data packets it receives.

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 it receives. In order to achieve its goals, the attacker needs to be accessible to the source node in order to receive the request and send a fake reply.

4.2. Dropping Attack

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

4.3. Flooding Attack

The flooding attack is a type of DoS attack. The main aim of the attack is to exhaust the network by sending numerous control packets, resulting in network nodes unable to process legitimate 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 current study's simulations, in AODV a 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 neighbors in order to disrupt their functionalities. Beacon packets are sent at 0.2 second intervals. Fake packets are continually sent in both routing protocols until the simulation terminates.

4.4. Bogus Information Attack

In bogus information attacks, the attacker sends falsified information to the network. For example, an attacker could send information about a fake road accident in order to divert traffic onto another road. This scenario could be very effective when there is no other vehicle to verify this deception of the falsified information. It is termed as a motorway attacker [19] if the attacker moves around quickly, and disseminates false information to a large group of nodes.

In the attack scenario, the attacker chooses a node as its victim, and then prepares a RREQ or beacon packet for AODV and GPSR respectively as generated from the victim. The packets are generated for a randomly selected destination node, and the attacker node broadcasts these packets on behalf of the victim node every five 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 isolate a node from the network; however, it will have little effect on the network due to the fast changing topology of VANETs. Packets not transmitted through the attacker will remain unaffected.

5. EXPERIMENTAL RESULTS

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

5.1. Simulation Environment

All simulations are conducted in a widely used network simulator, ns-2 [20]. Each simulation is run for a period of 200 seconds. Each attack is evaluated in networks with varying numbers of attackers (0%, 5%, 10%, 15%, 20%, 25%, and 30%). In each group of attackers, the position of attackers is assigned randomly 10 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, 5,600 simulations are ran for a map. The simulation parameters used in the experiments are given in Table 1.

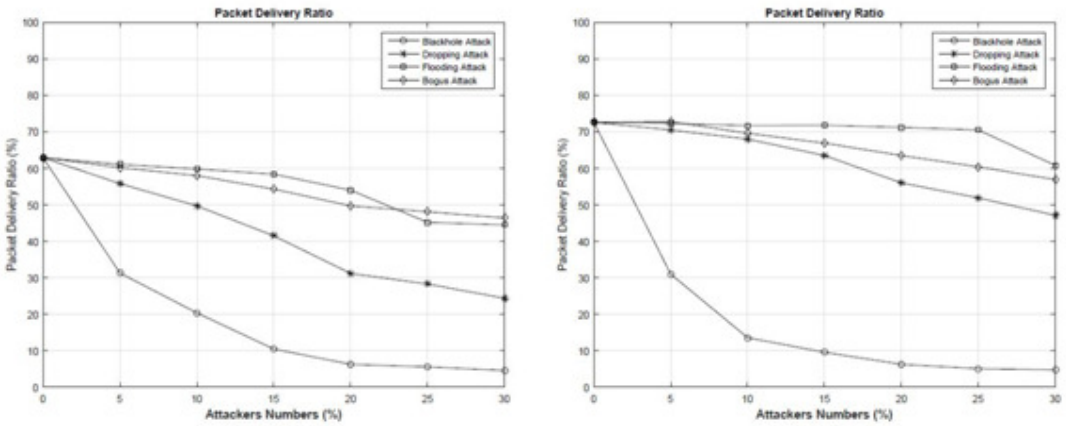
Table 1: Simulation Parameters

Simulation Parameters	**Value**
Simulation Time	200 seconds
Network Area	Istanbul Highway (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/s
Propagation Model	Nakagami [21]
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 the Istanbul Highway network. These roads were chosen due to their traffic densities. While the Munich road has high density, the Istanbul Highway has low density. These maps are generated by using SUMO [22] and OpenStreetMap [23].

5.2. Results in AODV

5.2.1. Packet Delivery Ratio – AODV



(a) Istanbul Highway (b) Munich City Center

Figure 1. Packet Delivery Ratio – AODV

Figure 1 shows the packet delivery ratio of AODV in Istanbul Highway 1(a) and Munich City Center 1(b). In general, a dense network has a higher packet delivery ratio than a sparse network. As expected, while the attacker percentage in the network increases, packet delivery ratio decreases in both maps. Figure 1 clearly shows that the Istanbul Highway is affected more severely than Munich City Center. Because of the density, vehicles in Munich are able to find more connections than Istanbul Highway even with 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 connects two endpoints, or two network partitions [24]. Since the attacker diverts traffic through itself in a 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.

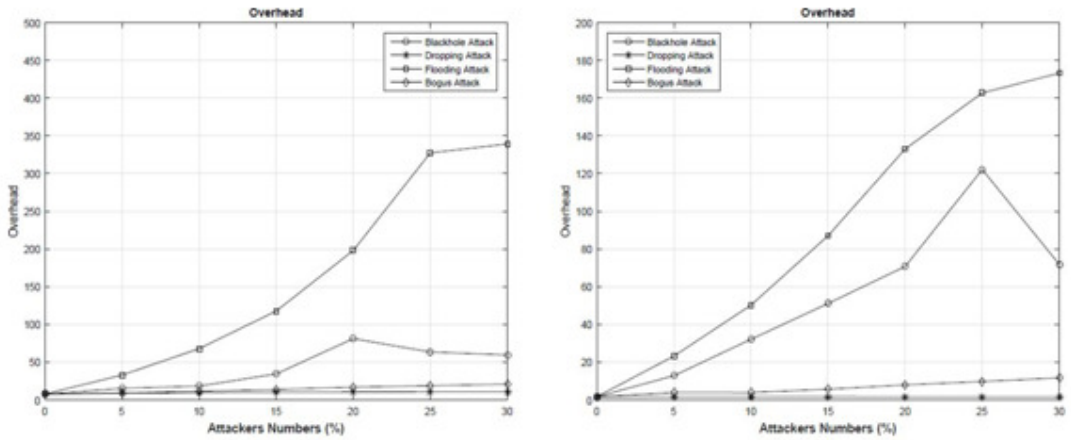
Flooding attack does not have as severe effect as blackhole and dropping attacks do. As the number of fake packets broadcast to the network increases, it will cause more packets to be dropped due to heavy traffic impacting the network. This situation applies to the increase of the number of attackers as clearly seen in the figure 1.

In the bogus attack scenario, by pro-actively forging fake routing control packets without receiving any packets (differently from a 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 (Istanbul Highway) are affected more than dense networks (Munich City Center). Moreover, as expected, when there are no malicious vehicles in the network, dense

networks have a higher packet delivery ratio than dense networks. In such networks, vehicles can find more vehicles able to continue the packet transmission.

5.2.2. Overhead – AODV

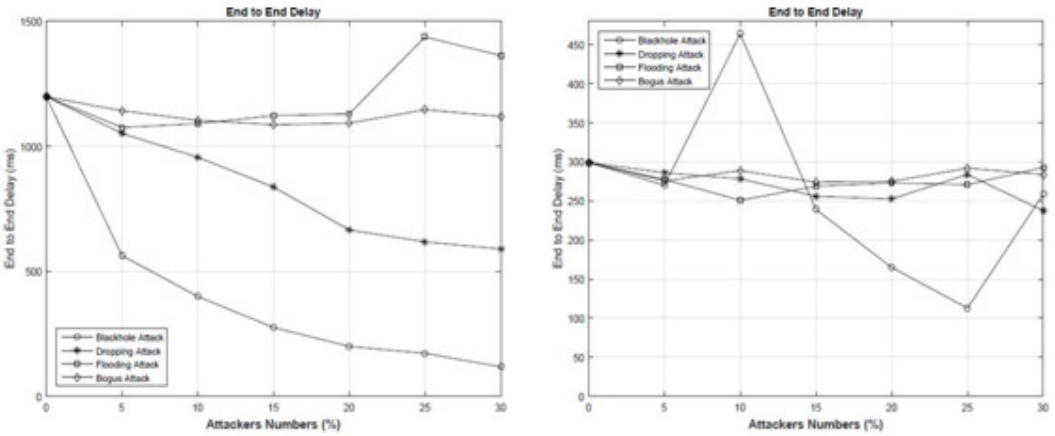


(a) Istanbul Highway (b) Munich City Center

Figure 2. Overhead – AODV

Figure 2 shows the overhead results for the attacks in both Istanbul Highway 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 overhead the most. Blackhole attack also increases the overhead considerably due to its disruption of effective routes. The density of maps affects the overhead results as well. Since the dense network provides more connectivity, less control packets are introduced to the network.

5.2.3. End-to-End Delay – AODV



(a) Istanbul Highway (b) Munich City Center

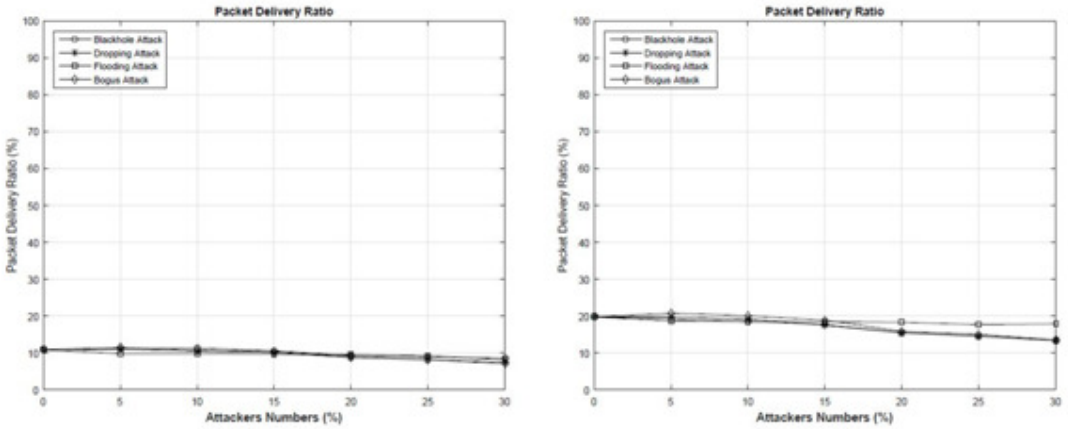
Figure 3. End - to - End Delay - AODV

Istanbul Highway 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

exceeds a 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 levels in the network. Even though the number of routing control packets increases, as shown in Figure 2, the 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 also occurred in the case of blackhole and dropping attacks. There was a fluctuation seen in the blackhole attack in Munich City map in Figure 3, probably caused by the selection of attackers, position of attackers, communication patterns, etc.

5.3. Results in GPSR

5.3.1. Packet Delivery Ratio – GPSR



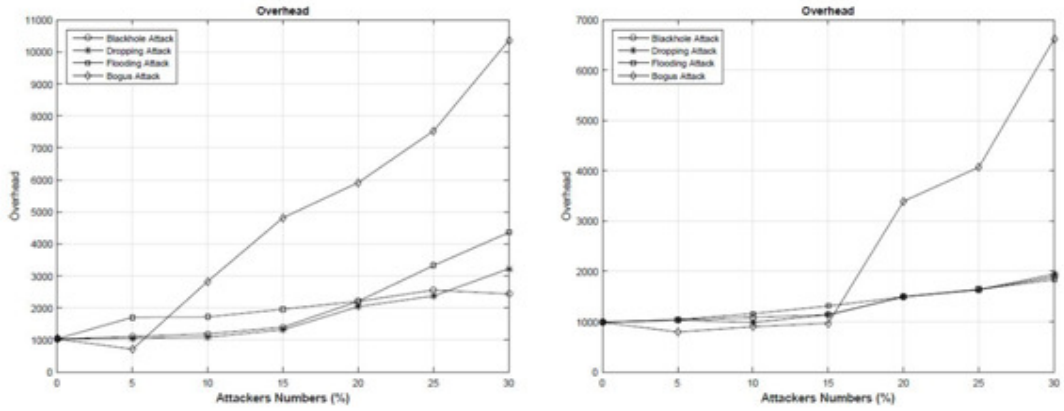
(a) Istanbul Highway (b) Munich City Center

Figure 4. Packet Delivery Ratio – GPSR

Figure 4 shows the packet delivery ratio of all attacks in both maps. GPSR's instantaneous vehicle selection to transmit a packet does not always succeed. Lack of selecting the best route for the destination might result in poor packet delivery performance. As expected the packet delivery ratio was higher on the more dense network. Since a node could find more alternative routes to a destination node in such networks, the sustainability of communication could be extended. More dense networks, consisting of more vehicles, could be more suitable to show the reaction of GPSR against attacks in the future.

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 the packet transmission begins. For this reason AODV has higher packet delivery ratio than GPSR. Also, the density of networks is significant to the packet delivery ratio. Since a node could find more alternative routes to a destination in dense networks, the sustainability of communication could be provided for longer.

5.3.2 Overhead – GPSR



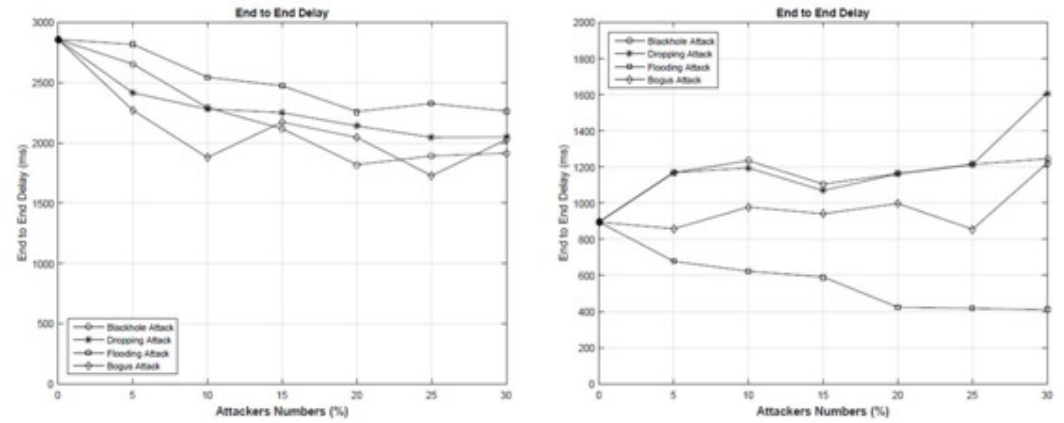
(a) Istanbul Highway (b) Munich City Center

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 [25], overhead is quite high in GPSR even when not under attack. When GPSR cannot 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 low density networks, they are slightly more affected by flooding attacks in both routing protocols. As the attacker number increases more control packets will be burst to the network, which resulting in increased overhead. Moreover, this attack is more damaging in GPSR as the attacker sends beacon packets to all its neighbors. The increase in the routing control packets can clearly be seen in Figure 5.

5.3.3 End-to-End Delay – GPSR



(a) Istanbul Highway (b) Munich City Center

Figure 6. End-to-End Delay – GPSR

Figure 6 shows the-end-to end delay for attacks in the two different maps. In Istanbul Highway map, GPSR's end-to-end delay for all attacks is decreasing. Since fewer packets are transmitted over a short period time to the destination point, end-to-end delay is decreasing. On the other hand, Munich City Center is less not affected than Istanbul Highway due to the high density of nodes in the city center traffic, and more application of GPSR's greedy forwarding mechanism under attack. It should be noted that density is not the only major factor affecting end-to-end delay. There are also other parameters such the location of attackers, the network topology, and traffic patterns.

To summarize 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. As expected, results showed that both protocols have better performance in dense networks under no attack. Although AODV demonstrates fairly good performance on networks under no attack, the pre-establishing mechanism of AODV shows a weakness 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 neighbors only. In the results, the attack which affects AODV the most is a 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 suited to showing the reaction of GPSR against attacks.

6. CONCLUSION

Vehicular ad hoc networks are an emerging technology which it is believed will be extensively used in the near future. However, security is a key issue that first needs to be addressed. 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 carefully analyzed; and which was the primary aim of this study. The attacks, namely blackhole, dropping, flooding and bogus information, are implemented on AODV and GPSR routing protocols. Although there has been some analyses of attacks specific to MANETs, their effects on more dynamic environments are lacking in the literature, hence they were explored in this current study. More popular attacks against VANETs such as bogus information attacks are also implemented and analyzed. More importantly, all attacks were 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 in such experimental settings. 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 a such highly dynamic environment. To the best of the authors' knowledge, this current study will be one of the most extensive attack analyses for VANETs to be found in the literature, helping future researchers working in this area.

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] R.W. van der Heijden, S. Dietzel, T. Leinmüller, F. Kargl. "Survey on misbehavior detection in cooperative intelligent transportation systems," arXiv preprint arXiv:1610.06810 (2016).

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] "The Network Simulator ns-2," http://www.isi.edu/nsnam/ns/, 2017.

[21] 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.

[22] 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.

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

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

[25] 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.