Open Access
Full Length Article

ORIGINAL ARTICLE

Detection and Minimization of Jamming Attacks to Enhance String Stability in VANETs

Abid Israr[1], Majid Ashraf[2], Sadeeq Jan[3], Fazal Qudus Khan[4]

[1,2]Faculty of Electrical and Computer Engineering, University of Engineering and Technology, Peshawar, Pakistan
[3]National Center for Cyber Security-UETP, Dept. of CS&IT, University of Engineering and Technology, Peshawar, Pakistan
[4]Department of IT, Faculty of Computing & IT, King Abdulaziz University, Jeddah, Saudi Arabia

ABSTRACT

Vehicular Adhoc Networks (VANETs) is an emerging area and have achieved popularity in the last decade. Due to its increased use, attacks on such networks have also increased. In this paper, we have evaluated an approach for Jamming attack's detection and also to minimize such attacks for string stability of vehicles. String stability is essential for safety of the vehicles because if the string stability is disturbed then there are chances of rear end collisions among the vehicles. String Stability among the vehicles is maintained by the periodic broadcasting of beacon messages which contains information about vehicles acceleration, direction, velocity, speed etc. Jamming disturbs the transmission of beacons from transmitter to the receiver and hence string stability is also disturbed. Jamming attack is detected by the calculation of time delay Δt of the beacon message from the source to the receiver along with the beacon's Bit-Error-Rate (BER). Upon detection of the jamming, the mitigation algorithm is called which is a mixture of interpolation and plausibility check. Interpolation is done if the BER is decreasing with time which means that nodes are coming out from the range of adversary or jamming area. But if BER is increasing with time it means that nodes are moving towards the jamming area or adversary, then a plausibility check is done to check whether switching the frequency of communication is safe or not. And after that channel is switched and the effects of jamming are mitigated. Satisfying results in terms of maintaining the string stability among the nodes are achieved.

Keywords: Vehicular Adhoc Networks, String Stability, Jamming, Mitigation

Author`s Contribution
[1,2,3,4]Manuscript writing, Data analysis, interpretation, Conception, synthesis, planning of research, Interpretation and discussion, Data Collection

Address of Correspondence
Majid Ashraf
Email: majid@uetpeshawar.edu.pk

Article info.
Received: March 04, 2019
Accepted: Dec 11, 2019
Published: December 30,2019

Cite this article: *Israr A, Ashraf M, Jan S, Khan FQ. Detection and Minimization of Jamming Attacks to Enhance String Stability in VANETs. J. Inf. commun. technol. robot. appl.2019; 10(2):9-17.*

Funding Source: *Nil*
Conflict of Interest: *Nil*

INTRODUCTION

Vehicular Adhoc Networks (VANETs) are infrastructure less networks which are temporarily created among the vehicles moving on the road for the ease and safety of the passengers and drivers [1]. According to statistics [2], road accidents cause death of around 150K per year. With the help of VANETs vehicles are made intelligent so that they don't rely on drivers and can communicate with each other about the conditions and hazards of the roads [3]. VANETs have been allocated 75MHz bandwidth by Federal Communication

Commission (FCC). This uses 5.9GHz spectrum and is called Dedicated Short-Range Communication (DSRC) [4] which is used by vehicles for their communication. This 75MHz bandwidth of DSRC is further divided into 7 channels of 10MHz where each includes a Control Channel (CCH) and 4 Service Channels (SCH). The CCH is utilized for information related to safety while the SCH is for non-safety applications. Unfortunately, because of its wireless nature, the networks are more prone to different kinds of security threats [5,6,7] out of which, Jamming is one [8]. Jamming refers to the condition when network is not available for sharing information when the vehicles need it.

In this work, we focus on how jamming attacks can be detected and mitigated for maintaining the string stability of the vehicles on the road to avoid accidents. String stability means the inter vehicular gap between the vehicles moving on the road over some given time should remain same, and that can be maintained when each vehicle will have knowledge of the speed, acceleration, direction, location etc. of the other cars moving on the road. This information is shared among vehicles by the beacon messages. When beacon messages are jammed, the information will not be shared and hence chances of accidents arose.

LITERATURE REVIEW

With the increased use of VANETs, the security has become a concern [1,7,9,10,11]. Various types of attacks are possible on VANETs [12]. Such attacks can affect the various aspects including confidentiality, authenticity, anonymity and reliability [13,14]. In particular, availability is very important in VANETs which means that the network is available when the nodes/vehicles try to access it [15]. Jamming attacks affect the availability of the network [16]. In this type of attack, the attackers use noise signals on the network which have the same frequencies upon which the network nodes are communicating with each other. The aim is to create interference between the noise signals and original signals and reduce the signal to Noise Ratio (SNR) and jamming the network. Several other attacks also affect availability of the network e.g., Denial of Service (DoS) and Distributed Dos(DDoS) attack, Broadcast Tampering Attack [17,18, 19]. Our work is focused on jamming attack which affects the availability of the network. Jamming attacks are broadly divided into 4 major types based on their behavior [20], i.e.,

- **Constant Jamming**: This type of attack works by sending random bits upon the channel continuously, i.e., whether the channel is idle or not.
- **Reactive Jamming**: In this type, the attacker works as a listener where it the channel is continuously sensed and as soon as any type of transmission is detected, noise signals are sent.
- **Deceptive Jamming**: In this the attacker sends stream of random data constantly, i.e., no gap is kept between the transmission of packets.
- **Random Jamming**: Here, the fluctuation between the sleep and jamming mode is created by the attacker to conserve the energy in the network.

In our research, we have addressed a method for the detection of constant jamming and then presented a solution for the mitigation of that jamming to maintain the string stability among the vehicles.

Jamming attacks target the availability factor of communication when sharing information. The other factors (e.g., accuracy, relevancy) are not affected directly by such attacks if the messages are transmitted successfully. However, when the jamming attacks succeed, the resulting information is inaccurate and irrelevant because the failure to reach its destination [21]. To launch jamming attacks, the attacker monitors the behavior of the wireless network. Upon the discovery of the frequency, the attackers then transmit noise signals at that frequency to interfere with the original signals affecting the communication [22]. An intrusion detection system for connected vehicles is proposed in [23]. Similarly, a mitigation technique called channel surfing has been suggested by [24]. In this technique, a number of frequencies is used to alter the communication to hide the actual communication frequency from the attackers. There also exist several other techniques for detection/minimization of jamming attacks. The author of [25] has designed a method for the detection of radio interference which depends upon the Correlation Coefficient (CC). In his technique, every node in a network compares CC with Error Probability (EP). The network jamming occurs when the value CC > EP. The author of [26] has studies the Denial-of-Services type

jamming attack. In this author have only discussed method for how to get rid of the jammed area and didn't describe any method for the detection.

According to the work of [27], the transmitted packets have no sensitive data in them, as such we do not requires confidentiality in VANETs based communication that takes place between vehicles. He proposed solutions to various attacks on VANETs.

The author of [20] has divided jamming attacks into Active and reactive jamming attacks and also concluded that the reactive jamming attacks are very difficult to detect. The author of also has described many techniques like beam forming, GPS Verification, Double anchoring to mitigate the effects of jamming. The authors [28] also investigated jamming attacks on wireless networks. They evaluated different models of such attacks and checked their effectiveness and capability of blocking the network. According to their results, jammers cannot be detected by only the information about signal strength and carrier concluded that the Strength of signals and the time of carrier sensing.

Detailed surveys and analysis of communication in VANETs and their challenges are provided in [29,30].

RESEARCH METHODOLOGY

We have created a platoon of 5 vehicles for the purpose of simulation. The leading car is named as Platoon leader, and the rest 4 cars are the followers. The followers will follow the instruction from the leader. And leader will broadcast that information through beacon messages. Depending upon the information in beacons, the following vehicles will adjust their speeds, acceleration, and direction for the maintenance of the gap between them so that the string stability will be achieved. Total length of the road is 5km and single lane is used by the vehicles. After each Km there is a junction on the road. Jammer is standing at the first junction. We have checked the string stability by speeding up and speeding down the vehicles. Nature of the jammer which jams the beacons of the network is static, which means that jammer has a limited range and has limited knowledge about the platoon, like upon which frequency platoon is communicating. It does not have any knowledge about the channel switching. Pictorial view of vehicle platoon and jammer is shown in figure. The red car is the platoon leader and the following four blue cars are the followers which follow the instructions of the leader. The blue car standing at the junction is jammer, having effective range of 500m radius. Total simulation time is 300 seconds. At about 10 second when the simulation starts the platoon will enter into the range of adversary or jammer and will remain in its range till 50 seconds. We have tested our simulation without jamming, with jamming and in the presence of mitigation, and satisfying results in achieving the string stability are gained.

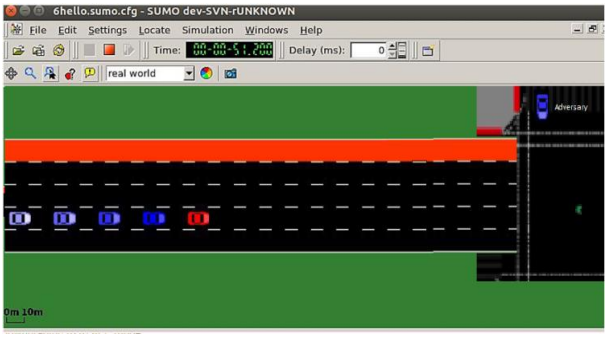

Figure 1. Pictorial View of Vehicle Platoon and Jammer

Simulation is done inside OmNet++ [31]. The log files are taken from the OmNet and are plotted in MatLab for the results. SUMO (Simulation of Urban Mobility) is installed over the Omnet++. SUMO thus allows for mimicking a network commination infrastructure. For the creation of Communication among the vehicles, VENTOS a simulator of vehicle based networks which provides a platform for SUMO and Omnet++ and is executed with SUMO/Omnet.

Two modes Co-operative Adaptive Cruise Control (CACC) [32] and Adaptive Cruise Control (ACC) [33] are used. In CACC each vehicle of the platoon has the knowledge of every other vehicle and that knowledge is received by the beacons which are periodically broadcasted by the vehicles. In ACC mode, vehicles in the platoon have only knowledge of the immediate preceding vehicle speed, distance between them through the sensors installed in their bumpers.

Our work has two steps:

A. Detection of Jamming Attack

In order to limit the effects of an attack the initial step is detection. As such, at the start of the simulation, the platoon of the vehicles follows their leader on a straight path. The leader is continuously broadcasting the beacon

messages upon the network which contains the information about the speed, acceleration, location and velocity and according to those beacons the vehicles will adjust their speed and velocity. A transmission delay of 0.5 second in the first message is a sign of attack on wireless network. Vehicle will automatically switch mode by downgrading from CACC mode to ACC mode. It happens because the vehicles have information of the acceleration and velocity of preceding ones in CACC mode. Such information exists because of the periodic beacons upon the network according to which the following cars setup their speed to maintain a distance between them. But as the network is jammed, the beacons are jammed, thus CACC is downgraded to ACC. In ACC mode, each following car judges the speed of its immediate preceding car through the sensors installed and does not rely upon the network. This is achieved as per the CACC protocol as declared in the platoon control algorithm. When the vehicles switch mode from CACC to ACC, their speed decreases and the gap between them increases. This decrease in the speed results in increased safety of the vehicle from a possible rear end collision. Next, the Bit-Error-Rate (BER) is checked. If the it increases based on time, this confirms that an attack is under way on the network. BER is checked for 3 seconds after the Δt crosses the threshold. For our experiments, we have used a time delay of 0.5 seconds, it can be increased and decreased. But as the vehicles are moving very fast on the roads and the topology of the network is continuously changing that's why we have taken the delay limit not less than 0.5 seconds.

Time delay is calculated by each vehicle using the formula:

$\Delta t = T2 - T1$ (1)

T2= Time at which beacon is transmitted

T1= Time at which beacon is received

If $\Delta t > 0.5$ seconds

When $\Delta t > 0.5$ then BER is also observed which is calculated via the following formula:

$$BER = \frac{1}{2}\left(1 - \frac{\sqrt{SNR}}{\sqrt{(2+SNR)}}\right) \quad (2)$$

SNR is Signal to Noise Ratio. When the platoon moves towards jammer SNR decreases and BER increases. Hence jamming attack is confirmed.

B. Minimization of Jamming Attack

When the attack is detected, it needs to be minimized. This can be achieved by continuously monitoring the BER. A decreasing BER with time, the vehicles in the platoon keeps moving using the previous (normal) values. However, in case of an increased BER, the plausibility check is performed and the decision is taken to switch the channel. By plausibility check we mean that the network will check whether other channels are free from jamming or not, if free then switching is done.

$$v_{safe}(g, v) = -b\tau + \sqrt{(b\tau)^2 + v^2 + 2bg}$$

In our simulation we have assumed that only one channel is under attack and all the other available channels are free. First communication is done on Control Channel (CCH) of DSRC band, which means the data, is transmitted upon the frequency of 5.890GHz. When the channel is jammed, and the detection is done by calculating the communication delay and BER, the frequency is altered upon the Service Channel 1 (SCH1), having the transmission frequency of 5.870GHz. The information about the channel switching is embedded in the code of the simulation, that when the jamming is detected upon one channel then the alternate channel will be SCH1 for the communication. And all the vehicles have knowledge that if one channel is jammed then automatically switches to SCH1. It is assumed that jammer do not have any knowledge of channel switching. And we have assumed that the adversary is only single channel jammer and does not have any idea about the channel switching. To maintain the string stability among the vehicles, the gap between the vehicles is maintained by the formula given by equation 3.

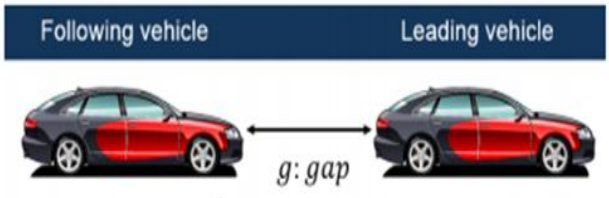

Figure 2. Gap Between two Vehicles

(3) Where g is the safe gap between vehicles to maintain string stability

τ= response time after receiving the beacon
v= speed of the following vehicle
b= maximum deceleration of the vehicle

Table 1 Various Network/Platoon's Parameters			
Parameter		Variable	Value
Road's length			5000m
Number of Lanes			5(only one is used)
ΔT			0.5 seconds
Platoons default Mode			CACC
Minimum gap between vehicles		G	2m
Acceleration		a	1.5m/s²
Deceleration	B	2m/s²	

The following flow chart summarizes the working of whole simulation.

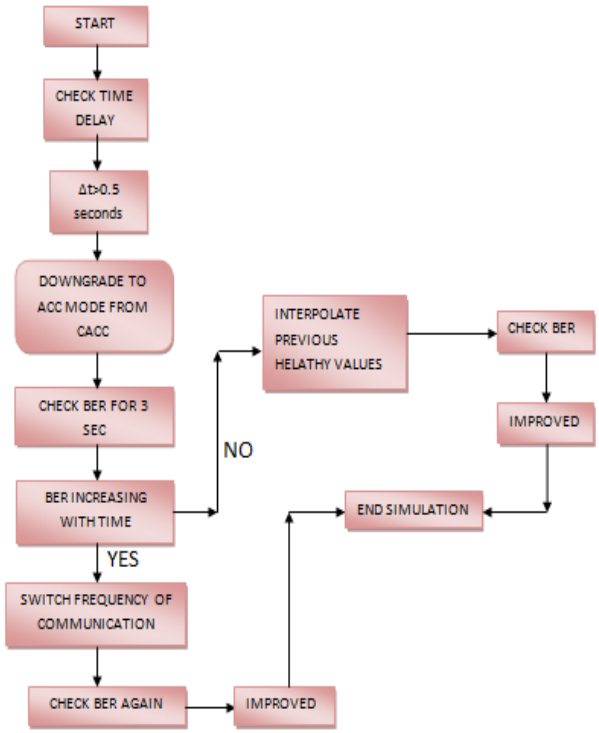

Figure 3. Flow chart of the Gap between Vehicles

RESULTS AND DISCUSSION

We have tested our simulation in normal mode (without jamming and mitigation), with jamming and in the presence of mitigation algorithm. Satisfying results are obtained and string stability among the vehicles is maintained to avoid any collision among the vehicles. Figure 4 is the graph of BER. We can see that when the simulation is running without jamming the beacon messages are delivered to the following vehicles from the leader with minimum BER. When jamming attack is applied in the second simulation, the graph show that BER is increasing after the 10 seconds mark. Which means that platoon is moving towards the jammer. When the mitigation algorithm is applied the, as the BER is increased for the 3 seconds, channel is switched. Now the channel which is provided to the network for communication is free from jamming, hence abrupt decrease in BER can be seen. Percentage of BER is along y-axis while x-axis shows time in seconds.

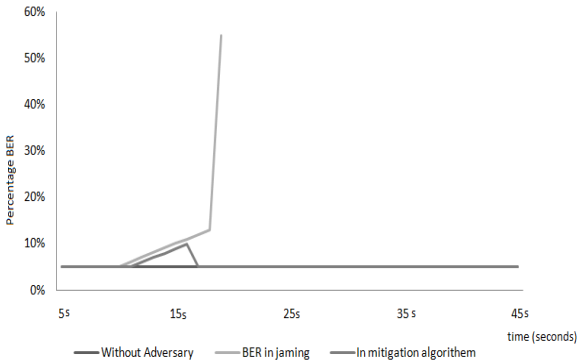

Figure 4. Percentage of Bit Error Rate (BER)

A. Platoon's Behavior in the absence of Jamming

Figure 5 depicts the speed of the platoon with respect to time. We observe how the platoon behaves in scenario when the speed is constant as well as when speeding up and down. A Platoon consisting of five cars is shown in figure with the starting speed of 0 m/s and accelerating at 1.5 m/s2. As shown in the figure, in about 20 seconds, the platoon reach at a speed of 20m/s. The first vehicle (leader) in the platoon reaches its target faster compared to the other vehicles because there are no vehicles at the front of it and therefore it is not concerned of the gaps between vehicles. All the other following vehicles reach their targets in 20 seconds. Next, the vehicles in the platoon move at a steady speed for 40 seconds duration before the speed goes to 5m/s. The String stability can be seen in the figure when the speed is increased or decreased. It can be seen that all the cars of the platoon are speeding up and down with the same manner and at the same time as that of platoon leader. It means that the beacon message is being transmitted without any delay to the followers. The dotted line shows the platoon leader.

Figure 6 depicts the acceleration of the platoon with respect to time when there is no adversary. We can see in the figure that the first vehicle (leader) accelerates from 0 to the 1.5 m/s2 (the upper limit). Next the other vehicles do the same as their leader as shown by the ripples. It is important to note that these ripples do not represent the string instability. As the time passes, the string instability is increased and the platoon keeps propagating. The string stability is achieved and can be seen with the 10 seconds interval points marked in the figure. The vehicle's acceleration is reduced to 0 first. Afterwards, a steady rate of 20m/s is achieved as discussed in the previous section (Figure 5). The platoon, upon receiving an instruction/command to decelerate, it should do so in a short span of time to keep a smaller value of deceleration than the one defined in vehicle class. On the other hand, when a vehicle responds in less than 0.5 seconds, the ripples are created as shown in the graph at mark 50 and subsequent times. However, please note that in the next 10 seconds stabilization is achieved when the vehicles reach constant velocity. In this current scenario shown in the figure, the stabilization is achieved after 70 seconds after the constant velocity at 60 seconds.

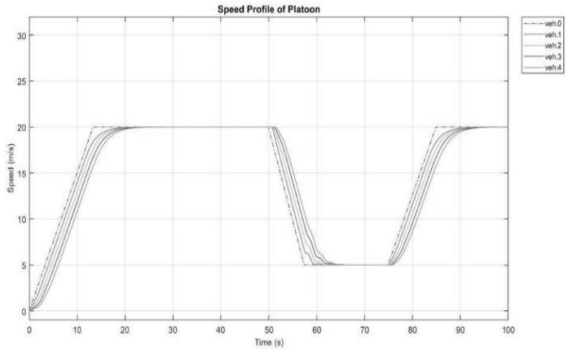

Figure 5. Platoon Behavior with no Jammers

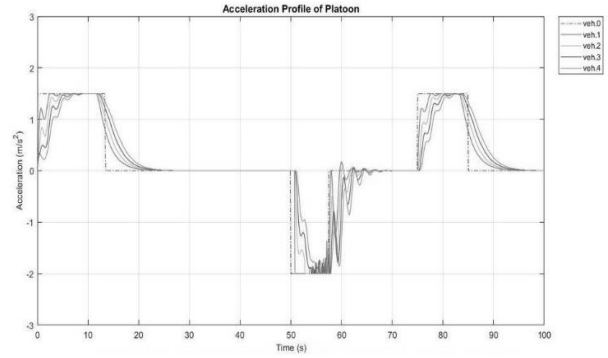

Figure 6. Platoon's behavior for Acceleration with no jammer

B. Platoon's Behavior when jamming is present but no mitigation

As explained in the previous sections, the same commands are used for increasing and decreasing the speed of the vehicles in the platoon. As depicted in Figure 1, the attacker's location is at the first junction in the car. The attacker is producing constant jamming signals. As soon as the platoon enters the radio range of the adversary the communication between the members of the platoon members will be disturbed and the beacon messages will not be delivered to the members of the platoon from the leader of the platoon. When the jamming attack is applied, it slows down the vehicles drastically compared to the first one (leader). Since, there is no mitigation for the attack in the current scenario, the string stability is achieved in a longer duration of time.

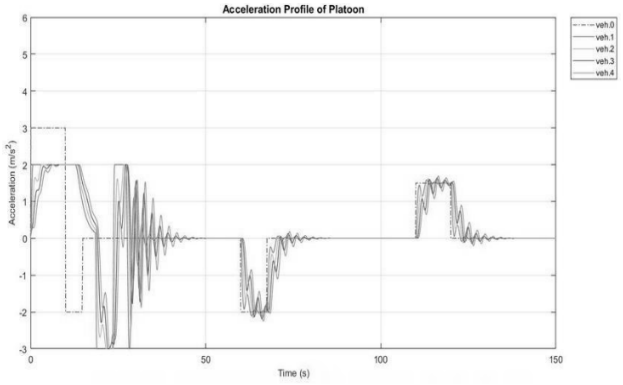

Figure 7. Speed Behavior of the Platoon when the adversary is present

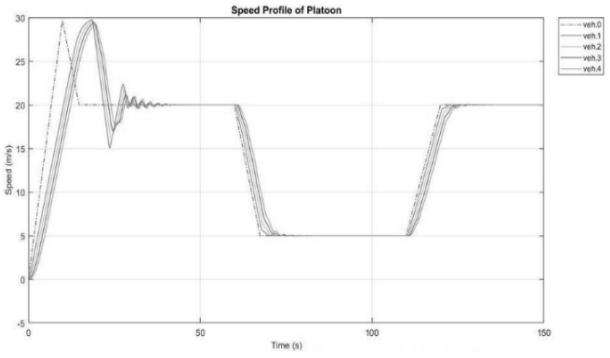

Figure 8. Acceleration Behavior when the adversary is present

Figure 7 depicts the behavior of the platoon in terms of speed/time when the adversary is present. At the start, the first vehicle (leader) speeds up and broadcasted a beacon about its increased speed. The following cars also received the message and also speeded up. As there are

no cars in front of the leader so it did not care for inter vehicular gaps and speeds up. When the leader reaches at about 10sec mark, it is the point from where the range of adversary is started. After attaining the speed of 30m/s leader slows down its speed. The message is again broadcasted, but as the network is jammed, the following cars have not received the information about decreased speed. This is the time following vehicles are downgraded to ACC mode, and become dependent upon the sensors. The ripples generated in the graph can be seen and hence disturbance in the string stability can be observed. String instability can be more clearly understood from the Gap profile of the vehicles (Figure 9)

Figure 8 shows that the platoon's leader has an acceleration of 3m/s² for 10 seconds. And in 10 seconds it has achieved the speed of 30m/s as explained in Figure 7. After that the leader decreased its speed to 20m/s, following the instructions the leader decelerated with the -2m/s², when leader has decelerated to 20m/s, at this point

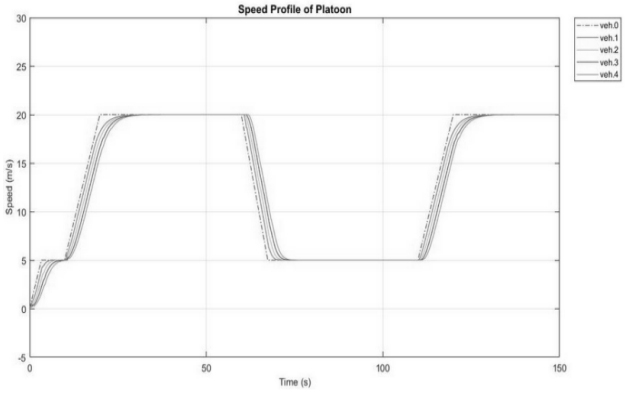

Figure 9. Speed Profile when mitigation is applied

the platoon entered the range of the adversary and it can be seen that the following cars have ripples in their acceleration graph as they are not getting beacons from the leader so the disturbance can be seen clearly from the graph. After the 50 second's mark the platoon has come out of the range of the adversary and after that the normal behavior can be seen.

The ripples seen at 50 seconds in the figure are created because of reduction in speed, the larger value of deceleration constant than the acceleration threshold, and slow response time of the vehicle. However, such ripples do not depict disturbance as a stability is achieved in the next 10 seconds.

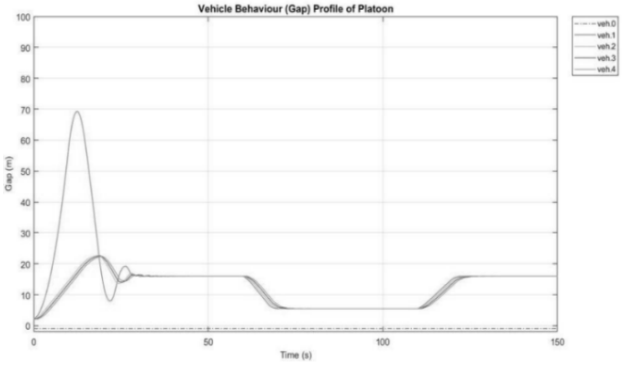

Figure 10. Gap Behavior of The Platoon in when the adversary is present

In Figure 9, it is shown how the vehicles in the platoon come closer to each other when a steady speed is maintained. We have observed (from Figure 7) that around 10 second mark, the attacker's range is started where the vehicles enter. At that particular time, the message from the leader about increase in its speed is not delivered to the other vehicles. Therefore, it can be clearly seen in figure 9 that the distance between the leader and the following vehicles has increased up to 70m because of the adversary. But the distance of the following vehicles except leader, is maintained because they are downgraded to ACC mode. Hence the string stability between the leader and the following members of the platoon is strongly disturbed.

C. Effect of mitigation on platoon's profile

Figure 10 depicts the behavior of platoon (in terms of speed) when mitigation algorithm is applied. As shown in the figure, the platoon is initially at rest, it starts and in about 10 seconds, it reaches the area accessible by the attacker.

After the threshold value (0.5 seconds) for the delay, the speed of the first vehicle (leader) is reduced and the gap between vehicles is maintained. This is achieved when the leader downgrades from CACC to ACC mode. Regarding the Bit Error Rate, it was observed to be increased because the vehicles are moving in the direction of the attacker. Therefore, a decision is made to switch the channel from CCH to SCH. This behavior can be observed from the figure as the effect of the attack is visible after 10 seconds mark. Since the channel was switched, a more accurate channel is now available for vehicles to communicate for the path. The directions for the correct path are given by the leader and followed by

others for increasing speed. The platoon achieves its initial target in the given time (20m/s in 20 sec). The vehicles in the platoon maintains a constant speed till 60 seconds. As evident from the figure, the platoon keeps the same behavior in this period when there was no attacker.

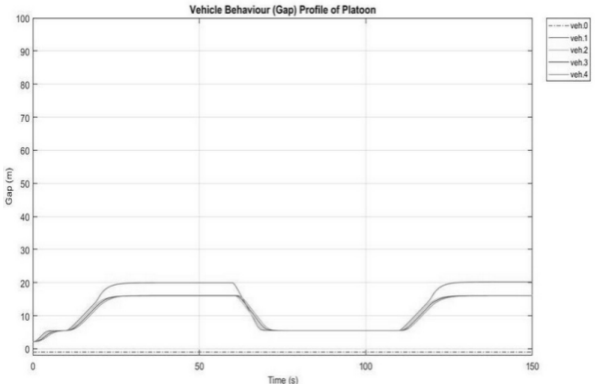

Figure 11. Acceleration Profile in The Presence of Mitigation

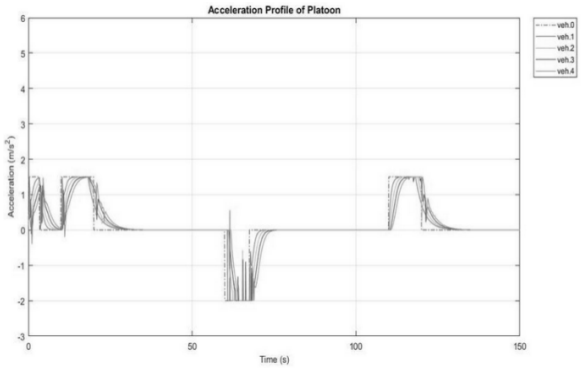

Figure 12. Gap Profile when mitigation is applied

Figure 11 depicts the behavior of the platoon for acceleration when mitigation is applied. It can be seen in the figure that instability (ripples) are created at around 10 second mark. However, the mitigation algorithm takes care of these ripples in the subsequent 5 seconds.

The string stability is achieved when the vehicles moves back and forth slowly. It is worth noting that most of the time the last vehicle is affected and the mitigation technique does not remove the complete instability, however, it does so from most of the vehicles. Such behavior for string stability is also described in [34].

Figure 12 depicts how mitigation affects the gap behavior among the vehicles. By comparing this figure with the previous one (Figure 9), it can be observed clearly that the mitigation algorithm maintains string stability in the platoon of vehicles.

CONCLUSION

The results of our approach are promising, i.e., our proposed algorithm has been found successful in achieving string stability for the vehicles in the network. String stability is important for vehicles when speeding up/down via beacons in the network. Jamming attack is timely detected and mitigated, thus string stability is maintained. By calculating the BER periodically and time delay, jamming attack can be detected in time. And channel switching is proven to be an effective technique for mitigation of jamming. For our experiments, we have used the open source packages VENTOS AND SUMO in Omnet++. The operating system used was Ubuntu 16.

For the future work, a mobile adversary can be introduced which can launch an attack upon all the channels and some technique can be designed to mitigate the effect of that adversary. In addition, other artificial intelligence techniques can be investigated in the application layer to increase the effectiveness of detecting jamming attacks.

REFERENCES

1. S. Sharma and B. Kaushik, “A survey on internet of vehicles: Applications, security issues & solutions,” Vehicular Communications, vol. 20, p. 100182, 2019.
2. “WHO | Road traffic injuries,” WHO, 2017. [Online]. Available:http://www.who.int/mediacentre/factsheets/fs358/en/ . [Accessed: 10-Nov-2019].
3. Y. Tang, N. Cheng, W. Wu, M. Wang, Y. Dai, and X. Shen, “Delay-minimization routing for heterogeneous VANETs with machine learning based mobility prediction,” IEEE Transactions on Vehicular Technology, vol. 68, no. 4, pp. 3967–3979, 2019.
4. W. Li, X. Ma, J. Wu, K. S. Trivedi, X.-L. Huang, and Q. Liu, “Analytical model and performance evaluation of long-term evolution for vehicle safety services,” IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 1926–1939, 2016.
5. J. A. Onieva, R. Rios, R. Roman, and J. Lopez, “Edge-assisted vehicular networks security,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8038–8045, 2019.
6. A. Yang, J. Weng, N. Cheng, J. Ni, X. Lin, and X. Shen, “Deqos attack: Degrading quality of service in vanets and its mitigation,” IEEE Transactions on Vehicular Technology, vol. 68, no. 5, pp. 4834–4845, 2019.
7. A. Nanda, D. Puthal, J. J. P. C. Rodrigues, and S. A. Kozlov, “Internet of autonomous vehicles communications

security: overview, issues, and directions," IEEE Wireless Communications, vol. 26, no. 4, pp. 60–65, 2019.
8. S. Feng and S. Haykin, "Cognitive risk control for anti-jamming V2V communications in autonomous vehicle networks," IEEE Transactions on Vehicular Technology, vol. 68, no. 10, pp. 9920–9934, 2019.
9. G. Blinowski, "Security of Visible light communication systems—A survey," Physical Communication, vol. 34, pp. 246–260, 2019.
10. N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," Ad Hoc Networks, vol. 90, p. 101740, 2019.
11. A. K. Malhi, S. Batra, and H. S. Pannu, "Security of Vehicular Ad-hoc Networks: A Comprehensive Survey," Computers & Security, p. 101664, 2019.
12. M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," Vehicular Communications, p. 100179, 2019.
13. R. Mishra, A. Singh, and R. Kumar, "VANET security: Issues, challenges and solutions," in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp. 1050–1055.
14. J. Arshad, M. A. Azad, K. Salah, R. Iqbal, M. I. Tariq, and T. Umer, "Performance analysis of content discovery for ad-hoc tactile networks," Future Generation Computer Systems, vol. 94, pp. 726–739, 2019.
15. S. Wen and G. Guo, "Observer-based control of vehicle platoons with random network access," Robotics and Autonomous Systems, vol. 115, pp. 28–39, 2019.
16. D. Kosmanos, A. Argyriou, and L. Maglaras, "Estimating the Relative Speed of RF Jammers in VANETs," Security and Communication Networks, vol. 2019, 2019.
17. J. M. De Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," in Handbook of research on mobility and computing: Evolving technologies and ubiquitous impacts, IGI global, 2011, pp. 894–911.
18. 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, 2012.
19. I. A. Sumra and H. Bin Hasbullah, "Effects of attackers and attacks on availability requirement in vehicular network: a survey," in 2014 International Conference on Computer and Information Sciences (ICCOINS), 2014, pp. 1–6.
20. S. D. Babar, N. R. Prasad, and R. Prasad, "Jamming attack: Behavioral modelling and analysis," in Wireless VITAE 2013, 2013, pp. 1–5.
21. R. Poisel, Modern communications jamming: Principles and techniques. Artech House, 2011.
22. G. Patounas, Y. Zhang, and S. Gjessing, "Evaluating defence schemes against jamming in vehicle platoon networks," in 2015 IEEE 18th International Conference on Intelligent Transportation Systems, 2015, pp. 2153–2158.
23. M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," Ad Hoc Networks, vol. 90, p. 101842, 2019.
24. B. Anouar, B. Mohammed, G. Abderrahim, and B. Mohammed, "Vehicular navigation spoofing detection based on V2I calibration," in 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), 2016, pp. 847–849.
25. A. Hamieh, J. Ben-Othman, and L. Mokdad, "Detection of radio interference attacks in VANET," in GLOBECOM 2009-2009 IEEE Global Telecommunications Conference, 2009, pp. 1–5.
26. I. K. Azogu, M. T. Ferreira, J. A. Larcom, and H. Liu, "A new anti-jamming strategy for VANET metrics-directed security defense," in 2013 IEEE Globecom Workshops (GC Wkshps), 2013, pp. 1344–1349.
27. R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," International journal of network security & its applications, vol. 5, no. 5, p. 95, 2013.
28. W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, 2005, pp. 46–57.
29. H. A. Ameen et al., "A Deep Review and Analysis of Data Exchange in Vehicle-to-Vehicle Communications Systems: Coherent Taxonomy, Challenges, Motivations, Recommendations, Substantial Analysis and Future Directions," IEEE Access, vol. 7, pp. 158349–158378, 2019, doi: 10.1109/ACCESS.2019.2949130.
30. S. A. A. Shah, E. Ahmed, M. Ahsan Qureshi, S. Jan, and R. MD Noor, "An effective back-off selection technique for reliable beacon reception in VANETs," International Journal of Communication Systems, vol. 32, no. 13, p. e4019, 2019.
31. A. Varga, "A practical introduction to the OMNeT++ simulation framework," in Recent Advances in Network Simulation, Springer, 2019, pp. 3–51.
32. B.-J. Chang, R.-H. Hwang, Y.-L. Tsai, B.-H. Yu, and Y.-H. Liang, "Cooperative Adaptive Driving for Platooning Autonomous Self Driving Based on Edge Computing," International Journal of Applied Mathematics and Computer Science, vol. 29, no. 2, pp. 213–225, 2019.
33. C. Wang, S. Gong, A. Zhou, T. Li, and S. Peeta, "Cooperative adaptive cruise control for connected autonomous vehicles by factoring communication-related constraints," Transportation Research Part C: Emerging Technologies, 2019.
34. Feng, S., Zhang, Y., Li, S. E., Cao, Z., Liu, H. X., & Li, L. String stability for vehicular platoon control: Definitions and analysis methods. Annual Reviews in Control, 2019.