# Disrupting Adaptive Traffic Lights Cycles through Selective Jamming Attacks

Heather Hinze
Department of Computer Science
Texas State University
hh1183@txstate.edu

Michael Ruth
Department of Computer Science
University at Buffalo
maruth@buffalo.edu

Mina Guirguis
Department of Computer Science
Texas State University
msg@txstate.edu

*Abstract*— **Adaptive traffic lights are critical components in Intelligent Transportation Systems (ITS) aiming to minimize the trip times for vehicles as well as reduce their fuel emission rates. With the recent advances in embedded systems and communication technologies, traffic lights receive signals from nearby vehicles to learn about the current load conditions as well as the types of vehicles on various lanes. This information is used by the traffic lights to adjust the traffic cycles appropriately to optimize efficiency. In this paper, we study the impact of selective jamming attacks in which a subset of the signals from the vehicles to the traffic light are jammed. This causes the traffic light to adapt its cycle to incorrect load estimates, leading to an increase in the trip times for vehicles and higher fuel emission rates. We focus on stealthy types of attacks that take the cost of the attack in consideration when mounting attacks. In particular, the attacker aims to maximize the marginal utility of the jamming attack. We evaluate the effect of our exposed attacks using SUMO simulations under various types of scenarios and for different metrics of damage and cost.**

## I. Introduction

Recent advances in wireless technologies have enabled the development of many Intelligent Transportation Systems (ITS) with the focus on ensuring the safety and efficiency of our roads. Vehicle-to-vehicle and vehicle-to-infrastructure communications enable many applications such as collision avoidance, cooperative driving, congestion avoidance, and traffic optimization (e.g., [1]–[4]).

The shared nature of the wireless channels, however, presents a serious challenge for such applications. Through transmitting on the same wireless channels used by the ITS (e.g., the 75 MHz licensed spectrum around 5.9 GHz), an adversary can hinder communication leading to unchecked behaviors. For example, by placing jamming devices in bridges, tunnels and close to cell towers, an adversary can prevent critical information from reaching a neighboring subset of vehicles, or exploit the adaptation of the drivers to make abrupt decisions, impacting the overall traffic flow.

Traffic lights are an important factor in transportation systems. Currently, the predominant systems for traffic lights are either fixed timed or adaptive based on cameras and sensors. Most of the sensors used in today's systems are inductive loop sensors that lie beneath the road and detect when vehicles move over them. The sensors are not accurate all the time as they can only detect traffic that moves over them, and are not aware of any cars waiting behind the sensor or are stuck in an intersection. With the use of wireless technologies in ITS, adaptive traffic lights get estimates about the load on various lanes and adapt the traffic cycle accordingly (e.g., [5]).

In this paper, we investigate the impact of stealthy attacks on adaptive traffic lights. In particular, we envision an adversary who can interfere with a small subset of the signals from vehicles to the traffic light, causing it to get incorrect load estimates of the flows. This will lead to an improper calculation of the cycle length, causing congestion and increasing the fuel emissions. These attacks are very plausible due to the following reasons: (1) given the wireless technology in use, vehicles must be within a specific "range" to the traffic light/other vehicles to be heard. This means that the attacker can well anticipate when a vehicle is going to transmit its information (e.g., as it is approaching the traffic light) and thus can time the jamming attack, (2) attackers can also launch reactive jamming attacks as soon as the signals are actually heard [6], and (3) attackers can directly observe the effect of the attack (e.g., by observing the new traffic cycles, queues and patterns). Moreover, the attackers can tune the parameters of the attack in an online fashion.

We study various types of attacks/scenarios from the standpoint of an adversary who aims to maximize the damage caused by the attacks – measured as increase in trip time and fuel emissions – while minimizing the cost of the attack – measured in the number of signals jammed or the duration of the jamming attack.

**Paper organization:** This paper is organized as follows: Section II describes related work. Section III describes the adaptive traffic lights model, along with the possible attacks and assessment metrics. In Section IV we present our assessment of the attacks on adaptive traffic lights in simulation experiments. We conclude the paper in Section V with a summary of our findings and future work.

## II. Related Work

The work in this paper relates to the following two areas of research:

**Traffic safety and management applications:** There has been a large body of work in the area of ITS that utilizes wireless signals for various safety and congestion management applications. In [7], the authors relied on wireless communication to develop different cooperative collision warning assistants for forward collision warning, intersection collision and lane changes. In [1], the authors investigate the impact of Dedicated Short Range Communications (DSRC) on the latency and the success probability in Forward Collision Warning applications. The work in [8] proposes a safety application in which each vehicle is aware of its nearest $k$ neighbors through V2V communication. The architecture is envisioned for various safety scenarios, such as collision avoidance, pre-crash sensing, traffic optimization and lane changes warning. In [9], Dresner et al. devised a scheme in which vehicles can avoid congestion in intersections by not stopping at all. The idea is that vehicles, through wireless communications, reserve slots in space and time at the intersection managers.

**Security in vehicular networks:** There has also been a large body of research that focused on the security of vehicular networks. Leinmüller et al. studied the effects of false-position data on geographic routing in VANETs [10]. It was shown that malfunctioning and/or malicious nodes broadcasting false position information can lead to packet losses, routing delays and traffic interception, and hence can drastically affect the performance, reliability and security of position-based routing networks. A model for attacks on inter-vehicle communication systems was proposed in [11] wherein the goals and logistics of various attacks are expressed in terms of attack trees. These trees, which help understand and classify attacks, are used to expose weaknesses and identify potential threats facing such systems. In [12], the authors discuss stealthy jamming attacks on a load balancing scheme with the goal to increase traffic congestion. Stealthy attacks in which an attacker partitions an ad-hoc network or hijacks traffic were studied in [13]. A key idea is to keep a low exposure and to minimize the cost of the attack through manipulating the routing information of well-behaving nodes.

Other attacks on vehicular networks include Sybil attacks that inject false messages into a vehicular network through the use of false identities [14], DoS attacks through jamming the communication channels, impersonation by using fake identities, and bogus information attacks wherein wrong data could be diffused in the network, for example to divert traffic from a given road. In this paper, we consider the effect of jamming attacks on the operation of an adaptive traffic lights.

## III. Methodology

### A. An Approximate Model

We start with a simple approximate model that can give us intuition about the effect of traffic light adaptation on the flow of vehicles and the impact of the attack parameters on its performance. In the next subsection, we remove many of the constraints in this model and we work directly with the adaptive traffic light controllers that take many factors into consideration. Consider a simple intersection composed of 2 lanes that we will model as 2 M/M/1 queues. Let $\lambda_1$ be the average arrival rate for lane group 1 and $\lambda_2$ be the average arrival rate for lane group 2. Assume that intersection can serve traffic at an average rate of departure $\mu$. In particular, let the departure rate for lane group 1 be $\alpha\mu$ and for lane group 2 be $(1-\alpha)\mu$. Thus, the average utilization of lane group 1, $\rho_1$, is $\frac{\lambda_1}{\alpha\mu}$ and of lane group 2, $\rho_2$, is $\frac{\lambda_2}{(1-\alpha)\mu}$. Figure 1 shows this model. The goal of the traffic light is to choose $\alpha$ to minimize the average trip times for vehicles in both lanes. From queuing theory, we know that the average turnaround time, $T_q$, is $\frac{q}{\lambda}$, where $q$ is the average queue size which is given by $\frac{\rho}{1-\rho}$. Thus, we seek to find $\alpha$ that minimizes the average turnaround times for both lane groups $T_{q_1} + T_{q_2}$ which are given by:

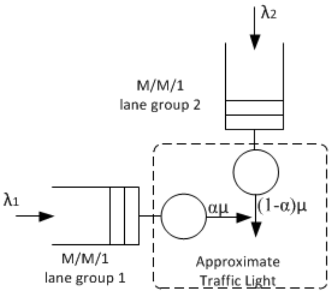

Fig. 1. An M/M/1 queuing model.

$$\begin{aligned} T_{q_1} + T_{q_2} =& \frac{q_1}{\lambda_1} + \frac{q_2}{\lambda_2} \\ =& \frac{1}{\alpha\mu - \lambda_1} + \frac{1}{(1-\alpha)\mu - \lambda_2} \end{aligned} \quad (1)$$

Differentiating the above expression with respect to $\alpha$ and equating it to zero gives the following expression:

$$\frac{-\mu}{(\alpha\mu - \lambda_1)^2} + \frac{\mu}{((1-\alpha)\mu - \lambda_2)^2} = 0 \quad (2)$$

This yields $\alpha$ to be

$$\begin{aligned} \alpha =& \frac{\mu^2 - \lambda_1^2 + \lambda_2^2 - 2\mu\lambda_2}{2\mu * (\mu - \lambda_2 - \lambda_1)} \\ =& \frac{1}{2} + \frac{\lambda_1 - \lambda_2}{2\mu}. \end{aligned} \quad (3)$$

Notice that traffic light does not follow an M/M/1 queuing discipline since the traffic light *alternates* between the two lanes, where our model assumes they can simultaneously serve both lane groups at a rate of $\alpha\mu$ and $(1-\alpha)\mu$, for lane group1 and lane group 2, respectively. The usefulness of the model can be seen if we can think of $\alpha$ as the average duration of the green light for lane group 1 and $(1-\alpha)$ as the duration of the green light for lane group 2. Clearly, we assume no wasted cycles (all red or yellow) – we will relax this assumption later. Equation 3 gives the optimal value that would minimize the average turnaround time for vehicles.

**Illustrative Example:** Consider the above model with the following parameters: $\lambda_1$ be 1 and $\lambda_2$ be 7. Let $\mu$ be 10. This means that the intersection as a whole is operating below capacity since the total average rate of arrivals is 8. Computing $\alpha$ from Equation 3 yields 0.2. Figure 2 shows the average turnaround time for all vehicles as a function of $\alpha$. We only plot the *valid* range of $\alpha$ which is between $\frac{1}{10}$ and $\frac{3}{10}$ (otherwise, one of the $\rho$'s would exceed 1). One can see that this is indeed minimized at $\alpha$ = 0.2.

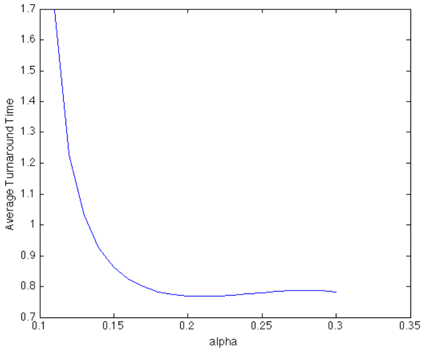

Fig. 2. Average Turnaround Time (weighted by percentage of arrivals) as a function of alpha ($\alpha$).

Since we are considering jamming attacks in which a subset of the signals are jammed, the traffic light would get incorrect load estimates leading to incorrect calculations of the proper green light duration (as reflected by $\alpha$ in our approximate model). This corresponds to shifting the operating point (as in Figure 2) from the optimal value to the right or to the left as the attacker decides which signals and from which lane groups to attack. Furthermore, it looks more damaging if we were to shift the operating point to the left (resulting in a much higher turnaround time) than to the right. We will explore such trade-offs through the potency metric that gives the marginal utility of the attack.

### *B. Adaptive Traffic Lights Model*

We now relax some of the assumptions we made above and we consider a single four-way intersection with two-lanes in each direction as shown in Figure 3. The intersection uses an adaptive traffic light model that has been proposed in [5]. We summarize the model below.

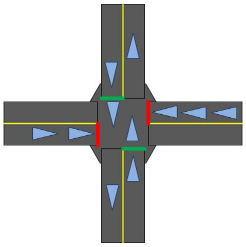

Fig. 3. A four-way intersection with an adaptive traffic light.

The model uses Webster's equation that is given by:

$$C_O = \frac{1.5 \times L + 5}{1 - \frac{1}{X_C} \times \sum_{i=1}^{n} \frac{v_i}{s_i}} \tag{4}$$

$C_O$ is the optimal cycle length. $L$ is the lost time in the cycle, which is all times where there are no green lights. For example, when all critical links have red lights. $\frac{1}{X_C}$ is the degree to which the intersection is at capacity. In our simulation experiments, we used 0.95, which is just under full capacity. $i$ is a critical lane group, which is any group of lanes that access the intersection at the same time. $\sum_i^n \frac{v_i}{s_i}$ is the sum of the maximum flow ratios for the intersection.

The green time calculation we used as provided in [5] is the following:

$$G_i = (C_O - L) \times \frac{\frac{v_i}{s_i}}{\sum_{j=1}^{n} \frac{v_j}{s_j}} \tag{5}$$

$G_i$ is the green time for critical lane group $i$. It is calculated by subtracting the lost time $L$ from $C_O$, the optimal cycle length obtained from Equation 4, and then multiplying that by the volume over saturation flow ratio for lane group $i$. Unlike the model above, we consider here the lost time and one can think of $G_i$ as the percentage $\alpha$ of the traffic cycle.

We assume that the traffic lights receive signals from vehicles either directly, or through an ad-hoc network of vehicles. However, these signals are subject to an adversary who can jam the wireless signals by transmitting on the same channel/frequencies. We assume that the attack duration lasts enough time to hinder communication from a subset of the vehicles to the traffic light.

The effect of the jamming attacks on the green light calculations changes Equation 5 to the following one:

$$G_i' = (C_O - L) \times \frac{\frac{v_i'}{s_i}}{\sum_{j=1}^{n} \frac{v_j'}{s_j}} \tag{6}$$

where $v_i'$ is the new volume of traffic that registers with the traffic light and is used in deriving the green light calculations. The attacker has a choice to attack all lanes or a subset of lanes and with varying intensities. If a lane is not attacked, then its $v_i'$ is the same as $v_i$.

### *C. Attack Scenarios and Types*

In this paper, we consider the following different scenarios for selective jamming attacks:

- **Uniform Random Attack with a Probabilistic Emission Model:** In this attack, we study the effect of a uniform random jamming attack with varying intensities on the trip times for vehicles and their fuel emission rates. We consider a probabilistic emission model. This attack gives us a base case for comparison to other attacks.
- **Uniform Random Attack with a Deterministic Emission Model:** In this attack, a deterministic vehicle emission schedule is used. The emissions produced under this case is the same as the expected emission rates under the probabilistic random schedule.
- **Isolated Random Attack with Deterministic Emission Model:** In this attack, the attack is only carried when the traffic cycle durations have converged to their optimal values. This eliminates the effect of transient behaviors observed at the beginning when the traffic light is initially adapting. The attack also stops once the traffic light cycles converge again to the optimal duration, albeit under attack.
- **Uniform Random Attack with Deterministic Emission Model with smoothing functions:** In some cases, traffic patterns could be bursty, making it challenging

to use the patterns as a control signal to derive the traffic light cycles. Under this attack, we consider a smoothing function that is applied to the results of Webster's equation. The smoothing function is a simple Exponentially Weighted Moving Average (EWMA) that is given by:

$$C'_n = \beta C'_{n-1} + (1-\beta)C_O \tag{7}$$

where $C'_n$ is the smoothed optimal cycle length for cycle n, and $C_O$ is the optimal cycle length calculated from Webster's equation. The parameter $\beta \in [0,1]$ was chosen to ensure smoothness of operation without affecting the convergence value of optimal cycle length. Under this scenario, we consider continuous attacks that are never released.

- **Targeted Random Attacks with Deterministic Emission Model:** In this attack, a single lane group is attacked. Thus, the traffic light would get incorrect estimates only from one lane group. The attack is also isolated (i.e., starts when the traffic light cycles have converged and it stops when the cycles converge to their new value under attack).

### D. Assessment Metrics

To assess the impact of the exposed jamming attacks on the performance of adaptive traffic lights, we follow the definition of attack potency, $\pi$, given in [15]. The attack potency is defined as the damage inflicted divided by the cost in mounting the attack, i.e.,

$$\pi = \frac{Damage}{Cost} \tag{8}$$

Damage and cost can be instantiated using several metrics. In this paper, we focus on damage as the difference in trip times that vehicles experience due to the attack. The cost of the attack is instantiated as the number of signals attacked. Thus, the definition gives the marginal utility of the jamming attack to be maximized by the attacker.

## IV. Evaluation

In this section, we report on our findings as we study the effect of jamming attacks on adaptive traffic lights.

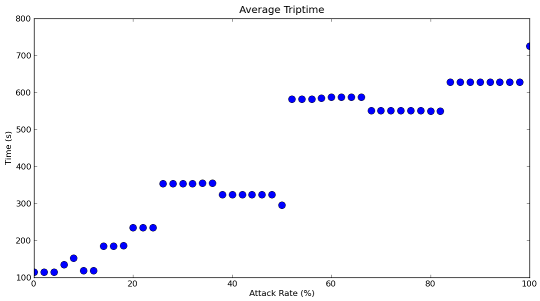

Fig. 4. Average trip times under uniform random attack.

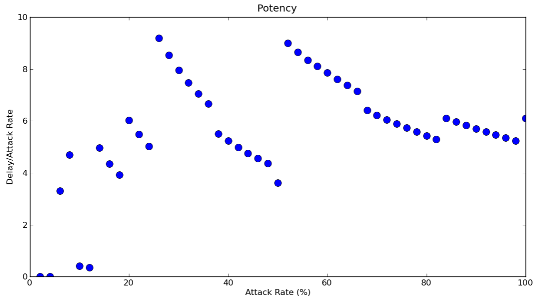

Fig. 5. Attack potency under a uniform random attack.

All our experiments were conducted using the SUMO simulator [16]. A 4-way intersection with 2 lanes in each direction is setup. The intersection is controlled by an adaptive traffic light similar to the model explained in the previous section that uses Equations 4 and 6. Vehicles are emitted with probability of 0.1 from the tail of each lane at each time step. The step size used for all experiments is 1 second. Each simulation experiment emits vehicles until the simulation times reaches 1000 seconds, at that point, the simulation continues to run until all vehicles arrive at their destination. We vary the intensity of the jamming attack from 0% (no attack) to 100% (DoS-like attack) with increments of 10%. When randomization is used, we ran each experiment 10 independent times and the results reported were averaged over those runs. Traffic volumes are calculated based on the number of signals transmitted from vehicles to the traffic light. The jamming attacks are simulated by multiplying the number of the signals received by the factor indicating the strength of the attack. This is done prior to computing the cycle length and the green cycle length. Data capturing trip times and fuel consumption rates are written to files after the simulation is completed.

We first observe the effect of a uniform random attack with varying intensities on the average trip times for vehicles. Figure 4, shows the average trip times against the attack rate. One can observe that the average trip times increase as the attack rate is increased due to registering incorrect load estimates and using them in control. It also shows that for a small change in the attack rate, the average trip time is somewhat resilient to attacks. Figure 5 shows the potency as calculated by the damage (increase in the average trip times when compared to no-attack) divided by the cost (number of signals attacked. The steps in the average trip times in Figure 4 correspond with the spikes in the potency plot in Figure 5.

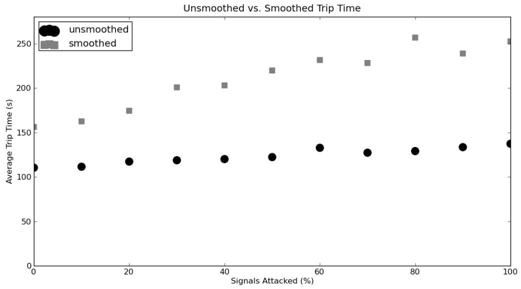

Fig. 6. Average trip times under smoothed and unsmoothed traffic.

Figure 6 shows the effect of smoothing under different attack rates on the average trip times. While there is no noticeable difference between the behavior of the two sets of trip times, smoothing additionally slowed the convergence

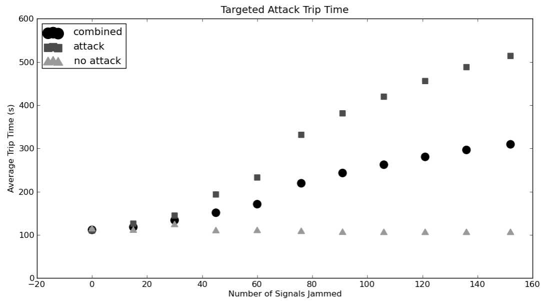

Fig. 7. Effect of targeted attack on attacked, unattacked and combined average trip times.

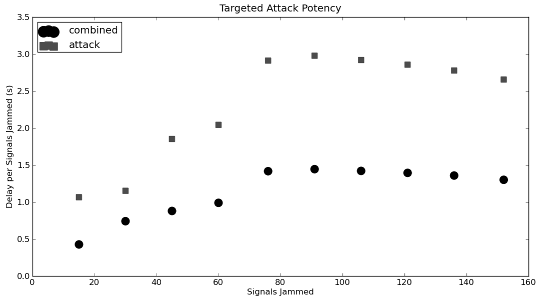

Fig. 8. Potency of targeted attack on combined and attacked segments.

of cycle lengths.

Figure 7 shows the effect of a targeted jamming attack on one lane group as a function of the number of signals attacked, and its impact of the attacked traffic (attack), the unattacked traffic (no-attack), along with the average trip times (combined). As expected, the average trip times increase as the number of signals attacked are increased (except for the no-attack traffic). An interesting observation is that the average trip times for the unattacked traffic actually decreased, albeit slightly, as the number of signals attacked is increased. This plot suggests that if an attacker would like to minimize its own average trip times, a very effective policy is to attack signals from the opposing lane.

Figure 8 shows the potency of the attack on the combined and attacked segment's delay time. The potency of the attack on the attack segment is roughly double the potency of the attack on the entire system. Maximum potency is achieved in both cases when 91 signals are jammed, which corresponds to an attack rate of only 23%. This shows that a complete Denial-of-Service type of an attack may not be the best attack strategy for an attacker who is concerned about the cost of the attack and the risk of getting detected.

## V. Conclusions and Future Work

In this paper, we have investigated the impact of low-rate jamming attacks on adaptive traffic lights. We have shown that both system-wide and targetted attacks do have a significant impact on the average trip times. The most potent attack for a system-wide attack occurs at a similar rate of attack as a targeted one. We have shown that an attacker mounting an attack on one segment can increase the average trip time more when compared with a similar strength attack on the entire system. Similarly, a driver who seeks to attack opposing lane groups is able to reduce their own trip time. We also observed that Webster's equation is somewhat tolerant of these jamming attacks, holding trip time constant while attack rate is increased over short intervals.

One direction in our current work is to expose attacks that are timed based on the current state of the system. For example, by observing the traffic flow over some lanes and the queue lengths over other lanes, an attacker can identify an optimized attack policy. We believe this paper provides the basic structure for jamming attacks so that we can consider more optimized ones in our future work.

## Acknowledgment

This research is funded by NSF REU award #1156712 that is co-funded by the Department of Defense and by the NSF CNS award #1149397.

## References

[1] T. Elbatt, S. Goel, G. Holl, H. Krishnan, and J. Parikh, "Cooperative Collision Warning Using Dedicated Short Range Wireless Communications," in *Proceedings of VANET*, Los Angeles, CA, Sept. 2006.

[2] G. Yan, W. Yang, M. Weigle, S. Olariu, and D. Rawat, "Cooperative Collision Warning through Mobility and Probability Prediction," in *IEEE Intelligent Vehicles Symposium (IV)*, San Diego, CA, June 2010.

[3] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety," *IEEE Communications Magazine*, vol. 44, no. 1, pp. 74–82, 2006.

[4] M. Sichitiu and M. Kihl, "Inter-vehicle Communication Systems: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 10, 2008.

[5] V. Gradinescu, C. Gorgorin, R. Diaconescu, V. Cristea, and L. Iftode, "Adaptive Traffic Lights Using Car-to-Car Communication," in *Proceedings of the IEEE VTC*, Dublin, Ireland, April 2007.

[6] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, "Short Paper: Reactive Jamming in Wireless Networks: How Realistic is the Threat?" in *Proceedings of the fourth ACM conference on Wireless network security*, 2011.

[7] J. Misener, R. Sengupta, and H. Krishnan, "Cooperative Collision Warning: Enabling Crash Avoidance with Wireless Technology," in *Proceedings of 12th World Congress on ITS*, San Francisco, CA, 2005.

[8] B. Xu, O. Wolfson, and H. Cho, "Monitoring Neighboring Vehicles for Safety via V2V Communication," in *IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, 2011.

[9] K. Dresner and P. Stone, "Multiagent Traffic Management: An Improved Intersection Control Mechanism," in *In The Fourth International Joint Conference on Autonomous Agents and Multiagent Systems*, Utrecht, The Netherlands, July 2005.

[10] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Influence of Falsified Position Data on Geographic Ad-hoc Eouting," in *Proceedings of the ESAS*, Berlin, Heidelberg, 2005. [Online]. Available: http://dx.doi.org/10.1007/11601494_9

[11] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller, "Attacks on Inter Vehicle Communication Systems- An Analysis," in *Proceedings of the International Workshop on Intelligent Transportation (WIT)*, Hamburg, Germany, March 2006.

[12] M. Guirguis and G. Atia, "Stuck in traffic (sit) attacks: A framework for identifying stealthy attacks that cause traffic congestion," in *Proceedings of the IEEE VTC*, Dresden, Germany, June 2013.

[13] M. Jakobsson, S. Wetzel, and B. Yener, "Stealth Attacks on Ad-hoc Wireless Networks," in *IEEE VTC*, October 2003.

[14] T. Z., R. Choudhury, P. N., and K. Chakrabarty, "P2DAP-Sybil Attacks Detection in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582 –594, march 2011.

[15] M. Guirguis, A. Bestavros, and I. Matta, "Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources," in *Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP)*, Berlin, Germany, October 2004.

[16] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO - Simulation of Urban MObility: An Overview," in *Proceedings of the 3rd International Conference on Advances in System Simulation*, Barcelona, Spain, October 2011.