INTERLOC: An Interference-Aware RSSI-Based Localization and Sybil Attack Detection Mechanism for Vehicular Ad Hoc Networks

Mevlut Turker Garip, Paul Hyungmin Kim, Peter Reiher, Mario Gerla
Department of Computer Science, University of California Los Angeles
{mtgarip, reiher, gerla}@cs.ucla.edu, paulmkim@ucla.edu

***Abstract*—Vehicular ad hoc networks (VANETs) are designed to provide traffic safety by exploiting the inter-vehicular communications. Vehicles build awareness of traffic in their surroundings using information broadcast by other vehicles, such as speed, location and heading, to proactively avoid collisions. The effectiveness of these VANET traffic safety applications is particularly dependent on the accuracy of the location information advertised by each vehicle. Therefore, traffic safety can be compromised when Sybil attackers maliciously advertise false locations or other inaccurate GPS readings are sent. The most effective way to detect a Sybil attack or correct the noise in the GPS readings is localizing vehicles based on the physical features of their transmission signals. The current localization techniques either are designed for networks where the nodes are immobile or suffer from inaccuracy in high-interference environments. In this paper, we present a RSSI-based localization technique that uses mobile nodes for localizing another mobile node and adjusts itself based on the heterogeneous interference levels in the environment. We show via simulation that our localization mechanism is more accurate than the other mechanisms and more resistant to environments with high interference and mobility.**

***Keywords*—Vehicular Ad hoc Networks, VANET Security, Sybil Attacks, Sybil Attack Detection, Localization, Location Accuracy**

I. Introduction

Due to the large number of injuries and fatalities caused by traffic-related crashes, traffic safety is a big concern worldwide [11]. Traffic accidents are mainly caused by human error, such as a driver's slow reaction to local visual and acoustic cues or unsafe actions due to insufficient traffic information [18]. Vehicular ad hoc networks (VANETs) have emerged as a promising approach to increasing traffic safety and preventing collisions by enhancing both the accuracy of traffic information and the delivery of alarms.

In a VANET, vehicles communicate with each other over a wireless channel and exchange routine traffic information through Basic Safety Messages (BSMs) [19], which contain current speeds, locations, and directions, as well as emergency alarms, such as notifications of emergency braking, etc. With VANETs, vehicles can collect more accurate traffic information electronically than drivers can visually. The direct activation of commands (brakes, accelerator, steering wheel, etc.) by an alarm will ensure a vehicle's prompt reaction to abrupt traffic events without depending on the driver's alertness. These VANET traffic safety applications, however, rely highly on the correctness of location data. If the location information is compromised, by Sybil attacks, inaccurate GPS data, or other bugs in a vehicle's software, the safety of the vehicular network will be jeopardized. Intelligent Sybil attacks use the most extreme forms of inaccuracy to achieve their goals, so mechanisms resistant to such attacks are likely to also handle accidental errors and inaccuracies. It is therefore necessary for VANETs to deploy a localization mechanism with built-in support for Sybil attack detection to defend against such attacks and enhance the safety of the network. Such a mechanism can also improve traffic safety by providing location data to VANET traffic safety applications since GPS is unreliable and sometimes unavailable in indoor locations such as a tunnel [6].

There are numerous localization mechanisms proposed in the literature. However, most of them are either designed for networks with stationary nodes—such as sensor networks—and therefore perform poorly in networks with high mobility, or they have requirements that are unrealistic in the presence of malicious nodes. Most of the existing localization mechanisms that are specifically designed for VANETs do not provide Sybil attack detection. The state-of-the-art localization mechanism that also defends against Sybil attacks is presented in [20] and will be referred as POEST in this paper.

POEST is an RSSI-based localization mechanism that uses the stationary roadside units (RSUs) to localize a vehicle. It estimates the location of the vehicle as a point and detects possible Sybil attacks using this point. It uses a radio propagation model that is—to some extent—interference-aware; however, due to its several drawbacks, which are discussed throughout paper, it suffers from inaccuracy in case of high interference levels and mobility. In this paper, we propose our localization mechanism, INTERLOC, that is resistant to extreme levels of interference and mobility. It continuously learns and adapts to heterogeneous and changing interference levels by using an interference-aware radio propagation model more effective than POEST. It uses the vehicles on the map to localize another vehicle to minimize the effect of mobility on accuracy. Using multiple vehicles as observers also provides faster interference adaptation. For Sybil attack detection, it estimates an area that contains the localized vehicle rather than a point, which provides a better detection accuracy than POEST. We also designed another version of INTERLOC by just replacing its radio propagation model with FRIIS [16]—an interference-unaware model—in order to show the importance of taking interference levels into account in localization.

In Section II, we present the existing localization mechanisms and their drawbacks. In Section III, we give an overview of the POEST and FRIIS mechanisms as alternatives to INTERLOC. We describe the design of the INTERLOC mechanism in Section IV, along with a detailed comparison with its alternatives in Section IV-E. In Section V, we show the results of our experiments conducted on FRIIS, POEST and INTERLOC, and demonstrate that INTERLOC performs better than its alternatives even under highly challenging conditions.

II. Related Work

Wireless localization is a well-studied area and there is a significant body of related work. The existing work on localization is mostly for sensor networks [3], [10], [13], [14], [15] and the localization approach used—exploiting the properties of radio signals—generally involves using one of these four methods: time of arrival (ToA), time difference of arrival (TDoA), angle of arrival (AoA) and RSSI.

The use of ToA and TDoA [10], [14], [15] must assume that the localized node is cooperative, which is not realistic since a Sybil attacker will not cooperate. Also, they both require the time that a signal was sent and received by all nodes, which can easily be faked by a malicious node. [15] uses AoA but it requires specialized hardware to detect the angle of a signal. [10] attempts to circumvent the need for specialized hardware, but states that calculating and normalizing the angle of a signal require at least two antennas (stationary and rotational), which is not applicable for VANETs.

We believe that exploiting RSSI for localization is the most effective and lightweight approach. Other localization methods have also concluded that measurements of RSSI is the most reliable mechanism, while maintaining the freedom to work in a dynamic environment without expensive hardware [14]. Unfortunately, RSSI values can be affected significantly by the interference levels in an environment. Some methods overcome this problem by having a dense network of highly repetitive values, as well as the limited mobility of their environment [14]. RSSI also has a tendency to reach extremely low values, which can easily be solved by a filtering strategy [5]. INTERLOC is especially designed to be robust with noisy RSSI values in high-interference environments.

Most existing localization mechanisms are designed for and work well in networks with stationary nodes, but are infeasible in high mobility networks. They either require a phase to learn the map prior to localization [3] or require anchor points (special stationary nodes) on the map [13]. An algorithm without these requirements is clearly preferable. Localization mechanisms for VANETs should specifically be designed for high mobility and optimized based on the VANET specifications and their expected deployments and uses.

There are some localization mechanisms designed for VANETs. [7] does not actually localize but improves the already advertised locations by a prediction model. [1] and [4] rely on the localized car to be cooperative, which is again not realistic due to the aforementioned reason. [12] proposes using RSUs for localization; however, RSUs might have limited availability since they are expensive. [8] has some similarity with INTERLOC in a way that vehicles use inter-vehicular communication to calculate the distance to a vehicle; however, the motion and GPS information are used to increase the accuracy, which can easily be faked by malicious nodes. [2] uses signal strength obtained from BSMs for localization but it is only for vehicles to localize themselves. Furthermore, all these localization mechanisms for VANETs neither have a Sybil attack detection mechanism nor guidelines on how they can be used for that purpose. We believe that every VANET localization mechanism should be designed either with a built-in support for Sybil attack detection or in a way that makes later deployment of such mechanism convenient. In that manner, POEST [20] is the state-of-the-art localization mechanism with already built-in Sybil attack detection. We discuss the drawbacks of POEST mechanism in Section IV-E.

III. POEST and FRIIS Overview

A. POEST

POEST is mainly designed for Sybil attack detection and uses RSUs for localization. Each RSU samples the RSSIs from the vehicle being localized and sends these values to the RSU that is responsible for estimating the location of the vehicle in question. Localization is then performed by minimizing the following Mean-Square Error (MSE) formula:

$$MSE(p) = \frac{\sum_{i=1}^{k}(S_r(w_i) - S_m(w_i, p))^2}{k}$$

p is a potential position of the sender vehicle, k is the number of RSUs (witnesses) that participate in the localization, S_r is the received signal strength at witness w_i, S_m is the signal strength that witness w_i is supposed to observe from a sender node given its position p, according to the radio propagation model presented in [9]. The formula of the radio propagation model that is used by the S_m function after the input p is converted to distance is:

$$P_T - P_R = PL_0 + 10\gamma\, log_{10}(\frac{d}{d_0}) + X_g$$

P_T is the transmission power (in dBm) of the sender node and P_R is the power of the signal measured at the receiver side. PL_0 represents the path loss ($P_{T_0} - P_{R_0}$) at the reference distance d_0. The initialization variables PL_0 and d_0 have to be set in the beginning before the formula is used and they have to stay the same afterwards. These variables configure the formula according to the general path loss of the environment according to the map size. γ is the coefficient that can be used to fine-tune the formula based on the interference levels on the map. POEST sets γ to a value that, to some extent, represents the overall interference level on the map before it starts localizing any vehicle and never changes it after that. X_g is a normal random variable and is set to zero in this case.

POEST minimizes the MSE by varying p, and the $\hat{p}$ that gives the minimum MSE becomes the optimal estimated position while the resulting minimum MSE indicates the error in the localization. After comparing this estimated location against the advertised location, POEST reports a Sybil attack if the locations are different.

B. FRIIS

FRIIS [16] is another radio propagation model that can be used by any localization algorithm as an alternative to the shadowing model presented in [9]. It demonstrates the relationship between transmitted and received signal strength based on distance in an ideal environment. In other words, unlike the shadowing model, FRIIS does not consider path loss or interference levels in the environment. The formula of this propagation model is:

$$\frac{P_R}{P_T} = G_T G_R \left(\frac{\lambda}{4\pi R}\right)^2$$

P_R and P_T represent the received power and the transmission power respectively. G_T and G_R are the antenna gains, which are both set to 1 in our simulations since the test environment does not incorporate any antenna gain. λ is the wave length of the transmitted signal, and R is the radius/distance that is traveled by the transmitted signal.

IV. INTERLOC Mechanism

A. Overview

INTERLOC is a RSSI-based localization algorithm that is designed both for detecting Sybil attacks and providing the location of any vehicle—when its GPS is not available or noisy—to improve traffic safety. It dynamically learns the new interference levels and adjusts itself accordingly, and is therefore robust to high and changing interference levels in the environment. INTERLOC does not depend on the existence of RSUs or any other stationary roadside infrastructure for localization. Since we believe that the most effective way of localizing a mobile node is using other mobile nodes to collect the RSSI values, INTERLOC uses the vehicles (observers) on the map to localize another vehicle. Therefore, it is also highly robust to the extreme levels and change rates of mobility in the network, since observers will have the same mobility at that time as the vehicle being localized.

B. Localization Algorithm

INTERLOC uses the same radio propagation model as POEST but does not perform MSE minimization to estimate the position of the vehicle. Instead of estimating the exact point with an error, INTERLOC estimates an area where the vehicle is certainly located without an error. Each observer samples the RSSI values by listening to the BSMs that are continuously broadcast from the vehicle being localized and estimates its distance to the vehicle using the following formula:

$$d = d_0 * 10^{\left(\frac{P_T - P_R - PL_0}{10\gamma}\right)}$$

d is the estimated distance between the observer and the localized vehicle. Other variables were explained earlier in Section III-A. After all observers in the vicinity of the localized car estimate their individual d, they send their current location and the estimated d to the chosen observer for it to process this aggregated data. Time lags due to various delays (propagation, the observer selection, etc.) are resolved by this processing observer using the timestamps of the received measurements.

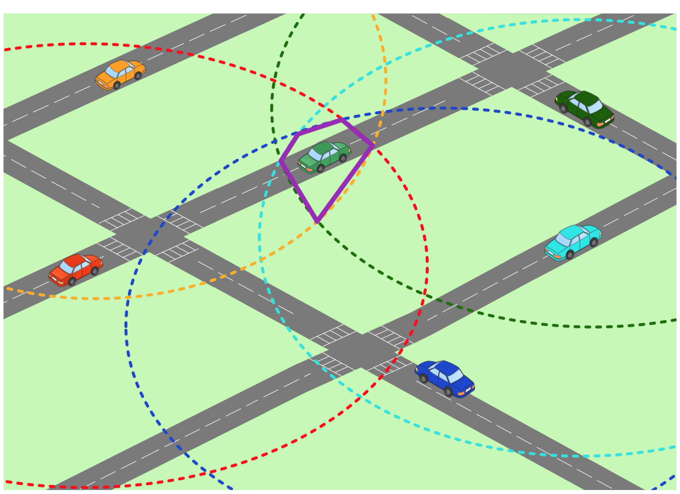

Figure 1. Localization performed by the observers and the estimated area

The chosen observer then creates a circle for each participating observer, where the centre point is equal to the location of the corresponding participating observer and the radius is the d estimated by that observer. After all the circles are created, the chosen observer calculates the polygon whose corners are the intersection points of these circles. The localized car will be inside this polygon without any estimation error, since each d will always be greater than or equal to the actual distance between the observer and the localized car. In an ideal environment without any interference in the RSSI values, the estimated polygon will just be a point on top of the localized car. As the interference levels increase, RSSI values will get lower increasing each d based on the interference measured by the associated observer. Therefore, the size of the polygon will get bigger but it will always contain the localized car inside due to the way d values are updated.

C. Mechanism for Learning Interference Levels

Learning and adapting to the changing interference levels are performed by exploiting the two variables of the radio propagation model: PL_0 and γ.

PL_0 is used to represent the initial overall interference levels before the localization can be performed. POEST sets this variable after a few iterations among a small number of stationary observers. INTERLOC sets it after measuring power losses between every vehicle that is d_0 away from each other on the map, which enables sensing interference levels with a finer granularity and a wider range of angles than POEST. The value of d_0 is set in a way that maximizes the number of observers participating in the PL_0 calculation. As a result, INTERLOC represents the initial interference levels on the map much better and more thoroughly than POEST.

Learning the initial interference levels alone is not sufficient for achieving a high localization accuracy. Configuring only the PL_0 is considering interference levels to be the same everywhere on the map. However, interference levels differ based on where the localized vehicle is on the map and the angle between the vehicle and each observer. Also, the position of the vehicle being localized and the angle between the vehicle and each observer will continuously change. Therefore, we exploit the γ in the radio propagation model to dynamically adapt to the heterogeneous and changing interference levels.

Each observer has a set of (θ, γ) pairs, where each γ is calculated by sampling the interference level in the direction to another observer in the communication range and θ is the angle to that observer. Each observer recycles its set periodically due to the constant changes in positions and angles in order to adapt to the changing interference levels. Each (θ, γ) pair is calculated by the following formulas where the positions of the sampling and the other observer are (x_1, y_1) and (x_2, y_2):

$$\gamma = \frac{P_T - P_R - PL_0}{10\,\log_{10}(\frac{d}{d_0})} \qquad d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

$$\theta = \begin{cases} arctan(\frac{x1-x2}{y1-y2}), & \text{if } x_1 \le x_2 \text{ and } y_1 < y_2 \\ 180^\circ + arctan(\frac{x1-x2}{y1-y2}), & \text{if } y_1 \ge y_2 \\ 360^\circ + arctan(\frac{x1-x2}{y1-y2}), & \text{if } x_1 > x_2 \text{ and } y_1 < y_2 \end{cases}$$

d is set to the distance between the advertised positions of the two observers and θ is the clockwise angle from true north of the sampling observer to the other observer. An example of the θ calculation is shown in Figure 2.

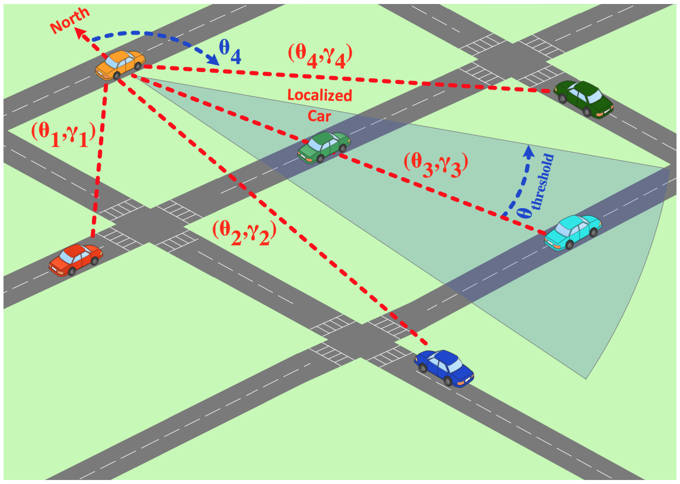

Figure 2. γ selection performed by each observer based on $\theta_{threshold}$ value

When a vehicle is to be localized, every observer in the vicinity of the vehicle attempts to choose the best (θ, γ) pair to use from its set, based on the angle to the vehicle being localized (θ_{loc}). Since θ_{loc} cannot be calculated without first knowing the estimated location of the vehicle, the initial estimation is performed by each observer using a default γ. Similarly to PL_0, the default γ is set to the value that minimizes the estimation error at setup time.

After the initial estimation of the vehicle's location by using the default γ, each observer then calculates its own θ_{loc} and determines the best (θ, γ) pair to use from its own set based on this θ_{loc}. The pair with the closest θ to θ_{loc} is regarded as the best choice $(\theta_{best}, \gamma_{best})$ and will be subjected to the final threshold test. If $|\theta_{best} - \theta_{loc}| \leq \theta_{threshold}$, then the γ_{best} will be used in the localization; otherwise, the default γ will be used until there is a θ_{best} that passes the threshold test.

Figure 2 depicts the γ selection mechanism along with how an observer calculates θ using true north. In this scenario, γ_3 will be used by the observer on top since currently θ_3 is the angle that passes the threshold test. Every observer participating in the localization performs this γ selection based on its own set and can use different γ values than the other observers. This makes INTERLOC take the heterogeneity of interference levels into account for localization. Since the angles and locations of the vehicles are constantly changing, each observer periodically updates its γ value used in localization along with periodically recycling its set with new (θ, γ) pairs, which ensures the adaptation to changing interference levels.

D. Sybil Attack Detection and Traffic Safety

INTERLOC uses the estimated localization areas to detect active Sybil attacks. Every observer continuously participates in the localization of all the vehicles in its communication range while listening to their location advertisements in the BSMs at the same time. All the chosen observers—each of which is responsible for processing the data obtained from the other observers to calculate its localization area—check if any advertised location falls outside the area where the advertising vehicle is estimated to be in. If such an inconsistency gets detected, the chosen observer that detected it will mark the vehicle as a Sybil node and notify the authorities about it.

When a legitimate car wants to advertise its location, it uses the built-in GPS unit to find the location and broadcasts it through the BSMs. However, there might be some minor fluctuations from its true location due to the natural noise in GPS [6]. If a localization mechanism estimates a point and compares the advertised location with this point to detect Sybil attacks, a legitimate vehicle might be marked as a Sybil node due to these fluctuations. INTERLOC gets rid of these false positives by estimating the smallest *area* that *certainly* contains the vehicle being localized even with all the GPS fluctuations that might occur. Therefore, if the advertised location of a vehicle is outside the localization area, then it is safe to mark the vehicle as a Sybil node. There still might be false negatives when the localization area is large and the Sybil attacker is advertising a relatively close location to the true location. However, the radii of the localization areas estimated by INTERLOC are generally smaller than the differences from the true location that are caused by Sybil attacks; therefore, false negative rates of INTERLOC are also fairly low.

INTERLOC can also significantly improve traffic safety. Due to the fluctuations from the true locations of vehicles caused by the noise in GPS, or to the absence of GPS data in the places like tunnels, the advertised locations in BMSs can sometimes be inaccurate or not available. This can cause serious accidents since the VANET traffic safety applications are highly dependent on the correctness of the advertised location data. In order to resolve this problem, vehicles can use the "Positioning Accuracy" field in the BSM [19], which indicates the error in GPS. If GPS is erroneous beyond some threshold, vehicles can switch to the localization mode and ask the responsible observer for the associated localization area. Afterwards, all traffic safety applications can use this area for avoiding collisions, which increases their tolerance to the noisy or unavailable location data.

E. Comparison with POEST and FRIIS

POEST uses the RSUs to collect RSSI values from a vehicle and localize it. The RSUs are stationary and not available in many places since it is expensive to install them. Therefore, using RSUs to defend against Sybil attackers is not an effective method since once they leave the area covered by the RSUs that POEST uses for localization, the attackers cannot be found anymore. RSUs also lose the vehicles when they enter a tunnel even if the vehicles are in their communication range. Since INTERLOC uses vehicles to localize other vehicles, localization can continuously be performed virtually anywhere on the map—even in a tunnel. While POEST uses a static γ value for all the nodes performing the localization, which introduces high inaccuracy due to the heterogeneous and changing interference levels, it is even more severe for the tunnel cases. On the other hand, INTERLOC is likely to perform very well in these cases since the measurements of the observers in the tunnel will be weighed more in the localization formula than the observers outside the tunnel—thanks to the usage of different and always up-to-date γ values. Furthermore, localization by mobile nodes makes INTERLOC more resistant to the mobility than POEST.

POEST estimates a point after the localization and uses this point to detect a Sybil attack, which causes a high false positive rate. INTERLOC has no false positives due to the usage of localization area instead—without increasing the false negative rate. Since the only difference between INTERLOC and FRIIS is the deployed propagation model, FRIIS also has no false positives. However, its false negative rate is much higher than INTERLOC's—the localization areas estimated by FRIIS are much bigger since it does not incorporate the interference levels into its propagation model.

V. Evaluation

We used Veins [17] (which combines the SUMO and OMNeT simulators) to evaluate the three localization algorithms. SUMO is responsible for simulating realistic vehicular traffic while OMNeT simulates the communication capabilities of the vehicles, with IEEE 802.11p integration [19].

We benchmarked FRIIS, POEST and INTERLOC in environments that are intentionally designed to be highly challenging and to reveal the worst-case-scenario accuracies of these three mechanisms. Any localization algorithm designed for VANETs will face such worst-case scenarios very often due to the nature of these networks, where extreme sparsity or density levels occur very often, and nodes are highly mobile. Therefore, this approach provides a more realistic performance analysis of these three mechanisms and a more thorough comparison between them. We ran one simulation for the Sybil attack detection accuracy graph and a separate simulation for each value on the x-axis of the remaining graphs (e.g., one simulation for 5% observers, one for 10%, etc.), each of which was 1000 seconds long. In each of these simulations, all three mechanisms were evaluated at the same time with the same number of observers (stationary for POEST and mobile for INTERLOC and FRIIS), and there were approximately 300 localizations performed.

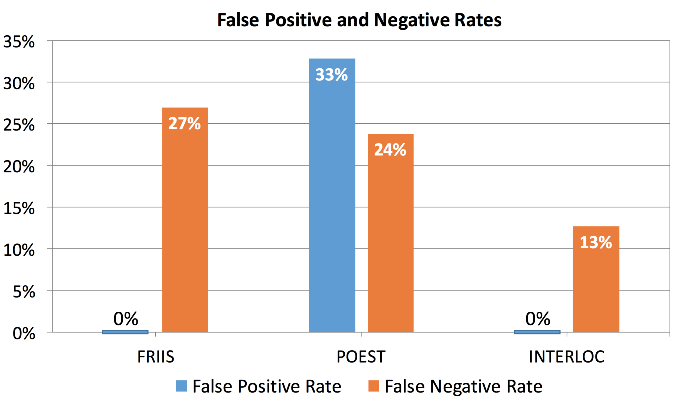

Figure 3. False positive and false negative rates during Sybil attack detection

We first evaluated the success of the localization mechanisms against a Sybil attack scenario we implemented. In our scenario, any vehicle can be a Sybil attacker and begin advertising false locations with a probability that is input to the simulation. In order to challenge the precision of each algorithm, each malicious vehicle advertises locations only subtly different ($\approx 10\,meters$ away in any direction) than its actual location. Figure 3 shows the false positive and false negative percentages during the detection of Sybil attacks by the three mechanisms. INTERLOC performs approximately twice as well as FRIIS and POEST in detecting Sybil attacks. FRIIS and INTERLOC do not have any false positives since they estimate a localization area rather than a point and use this for Sybil attack detection, as discussed in Section IV-D.

The following experiments measure the localization accuracy of the three mechanisms in case they are used to provide locations for traffic safety when GPS is not available or is highly noisy. We discussed earlier that calculating a localization area rather than a point is a better way for both Sybil attack detection and localization; however, to fairly compare POEST with FRIIS and INTERLOC, we calculate the centroid of the estimated localization area of FRIIS and INTERLOC just for comparison of point estimation and to evaluate the success rate of these three mechanisms. If the estimated point is closer to another vehicle than the vehicle being localized, then it is a failure case; otherwise, we regard it as a successful localization. Note that the point estimation for FRIIS and INTERLOC is just for the sake of a fair comparison with POEST, and is *not* a representation of how they will actually perform Sybil attack detection or localization.

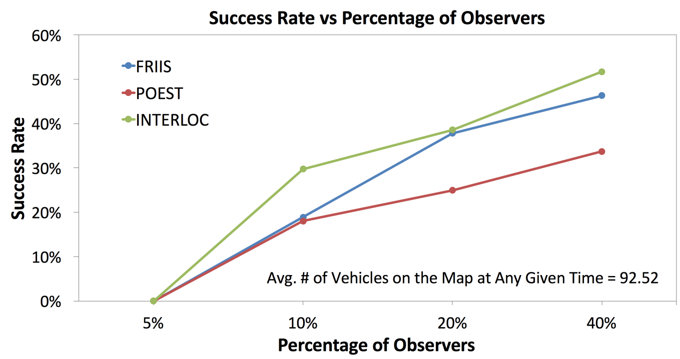

Figure 4. Accuracy graph with different percentages of observers

Figure 4 shows the accuracies of each localization mechanism with different percentages of observers, which are used for localization. The more observers are used for sampling RSSI readings, the more accurate each localization mechanism will be. However, INTERLOC always stays above the other mechanisms since it exploits the number of observers also for learning the interference levels on the map more effectively, therefore, adjusting to them better and faster.

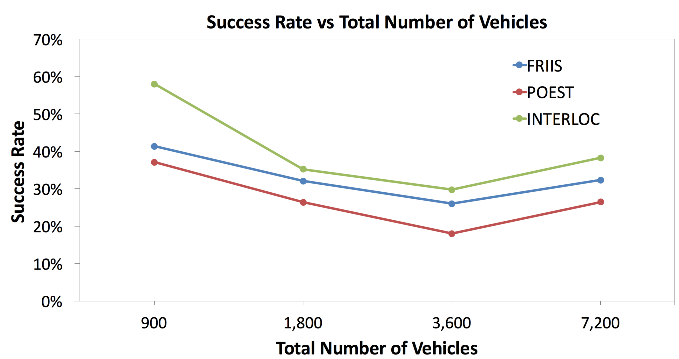

Figure 5. Accuracy graph based on the total number of cars on the map

Due to the way we calculate the accuracy of each localization mechanism, the total number of vehicles on the map has an adverse effect on the success of the localization. As the total number of vehicles increases, the probability of each estimated point to be closer to the other cars than the localized car gets higher, thus decreases the accuracy of the localization mechanisms, as shown in Figure 5. INTERLOC has a higher overall accuracy comparing to the other mechanisms despite these challenging conditions. Since the percentage of observers is kept constant during this experiment, the adverse effect is later counterbalanced—to some extent—by the increase in the number of observers along with the total number of vehicles.

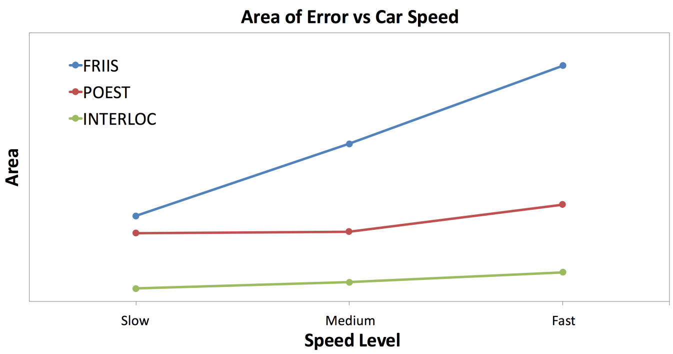

Figure 6. Size of the area of localization error with different mobility levels

In order to evaluate the resistance of the localization mechanisms to the environments with high mobility, we use a different metric: the area of localization error. We define the area of localization error as the area of a circle with the radius that is equal to the distance between the estimated point and the true location of the car being localized—the area gets larger as the localization error gets bigger. Figure 6 shows the changes in the area of error for each localization mechanism based on the different average speeds of the car being localized. We observe that the localization error increases as the localized car moves faster. The actual values on the y-axis of the graph in Figure 6 are missing since SUMO is using a Cartesian coordinate system, which makes the conversion from a coordinate distance to a meter distance too inaccurate to be used for measuring the localization area in m^2. The experiment results clearly show that INTERLOC has a much smaller area of localization error at each mobility level, and is very resistant to the changes in the mobility of the vehicle being localized.

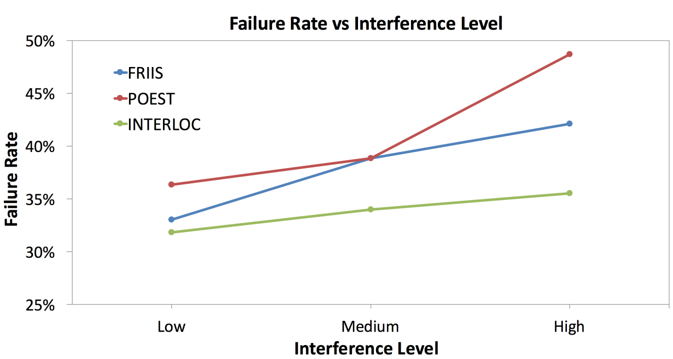

Figure 7. Failure rates with different obstacle densities and interference levels

Finally, we evaluate the localization mechanisms with different interference levels on the map, as shown in Figure 7. Even the interference-unaware FRIIS performs better than POEST since POEST's estimation of the overall interference levels in the beginning decreases its accuracy when the subparts of the map have significantly different interference levels than its initial estimation. Being interference-aware without periodically adapting to the new interference levels produces less accuracies than being interference-unaware. The localization accuracy of INTERLOC, however, changes negligibly with higher interference levels since it learns and dynamically configures itself to adjust to each new interference level.

VI. Conclusion

In this paper, we demonstrated INTERLOC—a localization mechanism with built-in Sybil attack detection for VANETs—that is designed to withstand extreme levels of interference and mobility. Unlike most localization mechanisms in the literature, INTERLOC is specifically designed for highly mobile and noisy networks and takes the existence of malicious nodes into account. We showed through experiments with highly challenging test cases that INTERLOC performs much better than its alternatives in terms of both localization and Sybil attack detection accuracy. The high accuracy and resilience of our localization mechanism not only enable an effective defense against Sybil attackers, but also improve traffic safety significantly, making INTERLOC a reliable alternative to GPS when that system's positioning is erroneous or not available.

References

[1] O. Abumansoor and A. Boukerche. A secure cooperative approach for nonline-of-sight location verification in vanet. *IEEE Transactions on Vehicular Technology*, 61(1):275–285, 2012.

[2] L. Altoaimy, I. Mahgoub, and M. Rathod. Weighted localization in vehicular ad hoc networks using vehicle-to-vehicle communication. In *Global Information Infrastructure and Networking Symposium*, 2014.

[3] P. Bahl and V. N. Padmanabhan. Radar: An in-building rf-based user location and tracking system. In *IEEE INFOCOM*, 2000.

[4] A. Benslimane. Localization in vehicular ad hoc networks. In *IEEE Systems Communications*, 2005.

[5] G. Blumrosen, B. Hod, T. Anker, D. Dolev, and B. Rubinsky. Continuous close-proximity rssi-based tracking in wireless sensor networks. In *IEEE International Conference on Body Sensor Networks*, 2010.

[6] A. Boukerche, H. A. Oliveira, E. F. Nakamura, and A. A. Loureiro. Vehicular ad hoc networks: A new challenge for localization-based systems. *Computer Communications*, 31(12):2838–2849, 2008.

[7] A. Boukerche, C. Rezende, and R. W. Pazzi. Improving neighbor localization in vehicular ad hoc networks to avoid overhead from periodic messages. In *IEEE GLOBECOM*, 2009.

[8] N. Drawil and O. Basir. Toward increasing the localization accuracy of vehicles in vanet. In *IEEE ICVES*, 2009.

[9] I. K. Eltahir. The impact of different radio propagation models for mobile ad hoc networks (manet) in urban area environment. In *IEEE AusWireless*, 2007.

[10] G. Mao, B. Fidan, and B. D. Anderson. Wireless sensor network localization techniques. *Computer Networks*, 51(10):2529–2553, 2007.

[11] W. Odero, P. Garner, and A. Zwi. Road traffic injuries in developing countries: a comprehensive review of epidemiological studies. *Tropical Medicine & International Health*, 2(5):445–460, May 1997.

[12] C. H. Ou. A roadside unit-based localization scheme for vehicular ad hoc networks. *International Journal of Communication Systems*, 27(1):135–150, 2014.

[13] C. Savarese, J. Rabaey, and K. Langendoen. Robust positioning algorithms for distributed ad-hoc wireless sensor networks. In *USENIX Annual Technical Conference*, 2002.

[14] C. Savarese, J. M. Rabaey, and J. Beutel. Locationing in distributed ad-hoc wireless sensor networks. In *IEEE ICASSP*, 2001.

[15] A. Savvides, C. Han, and M. Strivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In *ACM SIGMOBILE*, 2001.

[16] J. A. Shaw. Radiometry and the friis transmission equation. *American Journal of Physics*, 81(1):33–37, 2013.

[17] C. Sommer. Veins: Vehicles in network simulation. http://veins.car2x.org, 2015.

[18] U.S. Department of Transportation. National motor vehicle crash causation survey. *DOT HS 811 059*, 2008.

[19] Wireless LAN Working Group. Wireless access in vehicular environments. *IEEE Standards*, July 2010.

[20] B. Xiao, B. Yu, and C. Gao. Detection and localization of sybil nodes in vanets. In *DIWANS'06*, 2006.