Friendly Jamming for Secure Localization in Vehicular Transportation

Bhaswati Deka[1], Ryan M. Gerdes[1](✉), Ming Li[1], and Kevin Heaslip[2]

[1] Utah State University, Logan, UT 84322, USA
{bhaswati.deka,ryan.gerdes,ming.li}@usu.edu
[2] Virginia Tech, Arlington, VA 22203, USA
kheaslip@vt.edu

Abstract. In this paper we explore the prospect of using friendly jamming for the secure localization of vehicles. In friendly jamming confidential information is obscured from eavesdroppers through the use of opportunistic jamming on the part of the parties engaged in communication. We analyze the effectiveness of friendly jamming and compare it to the traditional localization approaches of distance bounding and verifiable trilateration for similar highway infrastructures. We present our results in terms of the probability of spoofing a given position by maliciously-controlled vehicles.

Keywords: Intelligent transportation · Friendly jamming · Secure localization · Automated vehicles

1 Introduction

The goals of an intelligent transportation system (ITS) are to reduce the number and severity of accidents, lessen congestion, and decrease emissions through the creation of a transportation system utilizing vehicle-to-vehicle and vehicle-to-infrastructure communication [1]. To accomplish this a suitable deployment of wired and wireless networking technologies and sensors are used to report and disseminate information about vehicle positions, speeds, and destinations; obstacles on the roadway; weather conditions; and accidents [2]. In order to utilize this information it is important to securely localize vehicles; e.g. to prevent the dissemination of bogus information that causes traffic to be sub-optimally routed [3].

In this work we propose a secure localization method that utilizes radio interference (friendly jamming) to ensure that messages passed between a prover (vehicle) and verifier can only be received at a given locality. We show how this approach can be used to verify the velocity and position information provided by vehicles. The method is analyzed for the case of a single vehicle moving down the highway, as well as for multiple vehicles colluding to prove spurious position and velocity claims. To evaluate the relative security of ITS infrastructures using a particular localization approach, we introduce a metric based upon the probability of a given position on a segment of highway being spoofed. Specifically,

J. Tian et al. (Eds.): SecureComm 2014, Part I, LNICST 152, pp. 212–221, 2015.
DOI: 10.1007/978-3-319-23829-6_16

we compare our approach to the traditional secure localization approaches of distance bounding (DB) [4] or verifiable trilateration (VT) [5].

1.1 Paper Structure

This section concludes with a brief review of existing localization techniques and the defining of our threat model. Our friendly jamming based approach is then introduced in Sect. 2. A performance metric to compare localization approaches for ITS is presented and used in Sect. 3. As our method requires that certain signals be obscured by interference, Sect. 4 discusses several approaches to frustrate interference cancellation techniques that could be employed by attackers to recover the obscured signals. Finally, the conclusion discusses future work in the area of friendly jamming for secure localization.

1.2 Related Work

Several methods have been studied and implemented for the secure localization of nodes in wireless sensor networks [5–7]. However, existing approaches are secure against a lone attacker but are vulnerable to multiple, colluding attackers. In [6] mobile or hidden verifiers offer some additional security, at the cost of keeping the verifier locations secret or continually moving them, each of which is impractical at the scale of a transportation system. We refer the reader to [8] for a survey of the strengths and weaknesses of existing secure localization techniques.

As mentioned by Zeng et al., secure localization under the assumption of mobility has not been as thoroughly studied as the static case. Two representative works [9,10] in this area focus on filtering out spurious location claims through comparison with other node claims. In contrast, our approach is to invalidate such claims without respect to other nodes by leveraging the physical and kinematic limitations of vehicles. Furthermore, [9] assumes that attackers are not able to directly corrupt the measurements of other nodes, while wormhole attacks are not addressed in [10]. Our approach considers both possibilities.

Friendly jamming for fading, multipath channels was proposed in [11] as a physical layer method of preventing eavesdropping between a transmitter and legitimate receiver. By opportunistically contaminating the channel with additive white Gaussian noise (AWGN) channel, Vilela et al. showed that is possible to prevent the leaking of secret information. They note that secrecy can increased by either increasing the signal to noise ratio (SNR) of the legitimate receiver or by reducing the SNR for the eavesdropper by introducing controlled interference. In this work, we make use of the latter technique to ensure that a vehicle outside the locale of a verifier cannot receive messages necessary to prove a spoofed position. Our approach is conceptually similar to that of [12], in which jamming was used to prevent outside observers from eavesdropping on wireless communications.

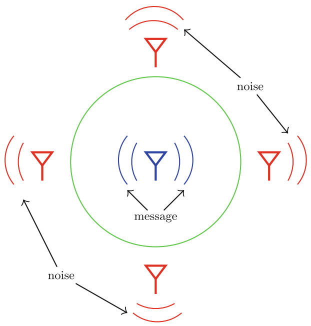
1.3 Threat Model and Assumptions

In what follows we assume an ITS infrastructure consisting of a single highway lane. Vehicles are able to transmit/receive information to/from a trusted infrastructure through the use of onboard radios and roadside transceivers. To prevent eavesdropping and provide authentication, vehicles utilize a secure and identity-preserving method for authentication and message passing, with non-repudiation, along the lines of [13]. In addition, vehicles are equipped with GPS and transmit their position and velocity to the infrastructure periodically.

The goal of an attacker(s) is to falsely claim (spoof) a position on the highway. In our analysis we consider two colluding attackers who are willing to share identities and transmit/receive messages on the others behalf. We assume that attackers are traveling along the same single lane and thus cannot overtake each other. They also do not have control over their initial position on the highway. Finally, for our proposed localization approach we assume that attackers are capable of accelerating and decelerating up to a given limit.

2 Friendly Jamming for Localization

In our proposed secure localization approach, a vehicle proves its position claim by responding to messages from verifiers that can *only* be received within the locale of the verifiers. To ensure that communication between provers and verifiers can only take place within a certain radius of the verifiers we utilize friendly jamming at the verifiers. To accomplish this each verifier would employ one set of antennas to transmit the verification message, with a second set placed outside the first and transmitting noise in an outward direction so as to obscure the verification message (Fig. 1). The granularity of position measurements would



$P \rightarrow I$:	$x_0, v_0, SIG_{K_P}(x_0, v_0)$
I :	**Calculate** time $t_1 = \frac{x_1 - x_0}{v_0} + t_0$ at which P reaches V_1 and
:	$t_2 = \frac{x_2 - x_0}{v_0} + t_0$ at which P reaches V_2
I :	**Generate** random nonces N_1, N_2
$I \rightarrow V_1$:	N_1, t_1
$I \rightarrow V_2$:	N_2, t_2
V_1 :	**Wait** until t_1
$V_1 \rightarrow P$:	$N_{V_1}, SIG_{K_{V_1}}(N_{V_1})$
V_2 :	**Wait** until t_2
$V_2 \rightarrow P$:	$N_{V_2}, SIG_{K_{V_2}}(N_{V_2})$
$P \rightarrow I$:	$N_{V_1}, N_{V_2}, SIG_{K_P}(N_{V_1}, N_{V_2})$
I :	**Verify** x_0, v_0 for P if received nonces match transmitted

Fig. 1. (LEFT) A friendly jamming verifier design using jammers (red) that ensures a verification message (blue) can only be received at given locality (green circle). A vehicle's position can be verified as it would have to be within the green circle to receive a message. (RIGHT) Verifying a vehicle's location via friendly jamming: A vehicle's claimed position and velocity are used to determine when the infrastructure will transmit nonces at specified locations (Color online figure).

depend on the number and spacing of these verifiers. In addition, establishing the veracity of a vehicle's position claim using friendly jamming requires separate channels for communication between the vehicle and a coordinating agent (part of the local verification infrastructure) and the vehicle and two verifiers. So as not to interfere with regular vehicle-to-vehicle and vehicle-to-infrastructure communication, it is assumed that a dedicated set of channels is set aside for position verification purposes. Adjacent verifiers operate on separate channels.

The protocol is as follows (Fig. 1): First, the vehicle under consideration (prover P) is queried for its current location, x_0, and velocity, v_0. Having received this information, the infrastructure (I), calculates the time t_1, based on the reported position/velocity and current time, t_0, at which the vehicle should reach the nearest upcoming verifier, V_1 (located at x_1). A random nonce, N_1, is then generated and sent to V_1 along with the time, t_1, at which it should be transmitted. This process is repeated for a second verifier, V_2 (located at x_2), using a new nonce, N_2, and transmit time, t_2. At time t_1 and t_2 the vehicle passes within the range of V_1 and V_2, respectively, and collects N_1 and N_2. To prove its original position claim the vehicle retransmits the nonces to the infrastructure.

It is assumed that the infrastructure, verifiers, and vehicles are equipped with public/private key pairs, denoted by K_I, K_{V_n}, and K_P, respectively, and participate in the same public key infrastructure. Communication between the infrastructure and verifiers is encrypted and digital signatures are used to authenticate messages.

For a preliminary analysis of the security of this approach, let us assume that an attacker located at x_a and traveling with a uniform velocity v_a attempts to spoof the position P by reporting, at time $t = 0$, its location and velocity as x_0 and v_0, respectively (Fig. 2). Allowing the verifiers V_1 and V_2 to be located at x_1 and x_2, respectively, at times $t_1 = (x_1 - x_0)/v_0$ and $t_2 = (x_2 - x_0)/v_0$ the verifiers will transmit their respective nonces. The attacker's actual position and velocity must be such that at times t_1 and t_2 they are at x_1 and x_2; i.e. x_a, v_a must satisfy $x_1 = x_a + v_a t_1$ and $x_2 = x_a + v_a t_2$. By rearranging these expressions

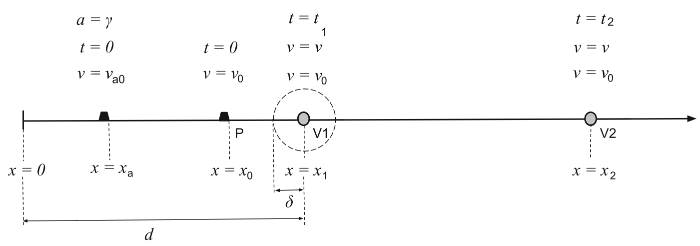


Fig. 2. Friendly Jamming infrastructure: verifiers V_1 and V_2 are used to verify a position/velocity claim along the highway segment d. At times t_1 and t_2 the system will transmit nonces that can only be received within a radius δ of the verifier. An attacker claiming position x_0 with velocity v_0, while their actual position and velocity are x_a and v_a, must arrive at x_1 and x_2 at $t_1 = (x_1 - x_0)/v_0$ and $t_2 = (x_2 - x_0)/v_0$ to receive and then retransmit the nonces in order prove a position/velocity claim.

and taking the ratios of t_1 and t_2, we have that

$$\frac{t_1}{t_2} = \frac{x_1 - x_0}{x_2 - x_0} = \frac{x_1 - x_a}{x_2 - x_a} \tag{1}$$

which shows that the attacker must be at the position P $(x_a = x_0)$ in order to acquire both nonces. Thus, it is not possible for an the attacker traveling at a constant velocity to prove any position but their actual position. We consider the case of a single attacker accelerating or decelerating in order to be able to reach the verifiers at the correct times, as well as multiple attackers sharing the same identity and coordinating their movements, in Sect. 3.2.

3 Spoofing Probability

To compare localization methods for ITS we propose to use a measure based on the probability of a randomly placed attacker(s) successfully spoofing an arbitrary point along the highway. Calculating the probability at all positions along the highway gives us an overall idea of how secure the localization method is for the defined threat model.

Definition 1. *Spoofing Probability: The likelihood of a verifier calculating the vehicle position of a legitimate vehicle erroneously, due to false information provided by malicious vehicles randomly situated on the highway.*

3.1 Sample Space and Probability Density Function

We use σ-algebra to define our sample space and then we assign a probability measure to each element of this sample space. Following the three criteria for a set to defined as a σ-algebra [14], we consider a set of points, (Σ) lying within the verification scope of a given verifier to be a σ-algebra defined over the set,(Ω) which is the set of all points on the highway. In set-notation,

$$\Omega = \{x\,(P) \in [0, \infty)\} \text{ and } \Sigma \subset \Omega \text{ defined by}$$
$$\Sigma = \{y\,(P) \in [0, d] : y\,(P) = |x\,(P) - x\,(V)|\}$$

where $x\,(P)$ = position of the point P from $x = 0$, $x\,(V)$ = position of the verifier V from $x = 0$, and d = distance between adjacent verifiers. The cardinality of the set is the verifier scope for the given infrastructure. Suppose the position of the attacker A is at $x(A)$. It can then spoof the point at $x(P)$ from the verifier at $x(V)$ if

$$|x\,(A) - x\,(V)| \leq |x\,(P) - x\,(V)| \tag{2}$$

where the value of $|x\,(P) - x\,(V)|$ is half the spoofing range of P from verifier V.

3.2 Spoofing Probability for Friendly Jamming

We assume that an attacker would spoof only those positions that are not already occupied by another vehicle. This is because if a position is occupied by a legitimate vehicle, then this vehicle crosses the verifiers at the times calculated by the verifiers from its position/velocity (PV) information, thus denying the attacker the opportunity to verify its spoofed claim.

We will find the spoofing probability as a ratio of the available positions within the range of velocity differences available for spoofing and the sum of all possible positions along the verification unit. To find the available positions and the range of velocity differences, we establish an upper and lower bound on the difference between the actual and target PV information and then find a condition such that for an instant of verifying a point from a given verifier, the outcome S (that the position cannot be spoofed) is true. We provide a sketch of the derivation for the spoofing probability for a single attacker below; for a detailed derivation, including the case of two colluding attackers, see [15].

Let $\{x_0, v_0\}$ be the PV information that an attacker wants to spoof, $\{x_a, v_a\}$ the attacker's actual PV, and $\Delta x = x_a - x_0$ and $\Delta v = v_a - v_0$. The infrastructure determines the times of crossing $t_1 = (x_1 - x_0)/v_0$ and $t_2 = (x_2 - x_0)/v_0$. As per Sect. 2, the attacker must accelerate in order to be able to reach the verifiers on time. Allow a_1 and a_2 to be the accelerations required to reach verifier V_1 in time t_1 and V_2 in time t_2. As vehicles are limited in their ability to accelerate, allow the magnitude of maximum acceleration to be denoted by γ.

Now, using the equations of motion for an attacker moving from the beginning of the verification segment (considered to be the origin) to V_1 and then from V_1 to V_2 with the bounds on a_1 and a_2, we have

$$|a_1| \leq \gamma \Rightarrow |\Delta x|\, v_0 + |\Delta v|\,(d - x_0) \leq \frac{\gamma}{2} \frac{(d - x_0)^2}{v_0} \tag{3}$$

$$|a_2| \leq \gamma \Rightarrow 2\,|\Delta x|\, v_0 + |\Delta v|\,(d - x_0) \leq \frac{\gamma}{2} \frac{d\,(d - x_0)}{v_0} \tag{4}$$

Considering (3) and (4) with the limit $\Delta v \rightarrow 0$, we find the maximum value of Δx; similarly with limit $\Delta x \rightarrow 0$ we find the maximum value of Δv. The range of values Δx and Δv are then given by

$$\begin{aligned} 0 < |\Delta x| < \frac{\gamma}{2} \frac{(d - x_0)^2}{v_0^2} \text{ and } 0 < |\Delta v| < \frac{\gamma}{2} \frac{d - x_0}{v_0} \text{ for verifier } V_1 \\ 0 < |\Delta x| < \frac{\gamma}{4} \frac{d\,(d - x_0)}{v_0^2} \text{ and } 0 < |\Delta v| < \frac{\gamma}{4} \frac{d - x_0}{2v_0} \text{ for verifier } V_2 \end{aligned} \tag{5}$$

Equation 5 provides limits on much an attacker can deviate from its reported position (x_0) and velocity (v_0). The spoofing probability then will be the number of (Δx, Δv) combinations which satisfy (3) for verifier V_1 and (4) for verifier V_2 divided by the total number of such (Δx, Δv) combinations.

For illustrative purposes, let us define the spoofing probability for a constant difference in velocities; i.e. $\Delta v = 0, ..., v_n, ..., \Delta v_{max}$, where v_n is an arbitrary value of Δv and Δv_{max} is the maximum value of Δv given by Eq. 5. The formula of spoofing probability for verifiers V_1 and V_2, when v_0 and Δv are constants and x_0 varies, are given by

$$P_{V_1,v_0,\Delta v}\left(x = x_0, \Delta v = v_n\right) = \frac{\frac{\gamma}{2}\frac{(d-x_0)^2}{v_0^2} - v_n\frac{(d-x_0)}{v_0}}{\sum_{x_0=0}^{d}\frac{\gamma}{2}\frac{(d-x_0)^2}{v_0^2} - v_n\frac{(d-x_0)}{v_0}} \tag{6}$$

$$P_{V_2,v_0,\Delta v}\left(x = x_0, \Delta v = v_n\right) = \frac{\frac{\gamma}{4}\frac{d(d-x_0)}{v_0^2} - v_n\frac{(d-x_0)}{2v_0}}{\sum_{x_0=0}^{d}\frac{\gamma}{4}\frac{d(d-x_0)}{v_0^2} - v_n\frac{(d-x_0)}{2v_0}} \tag{7}$$

The probabilities P_{V_1} and P_{V_2} are not independent of each other. Therefore, the spoofing probability is their intersection

$$P_{V_1,v_0,\Delta v} \bigcap P_{V_2,v_0,\Delta v} = P(V_2|V_1)P(V_1). \tag{8}$$

As the bounds for V_2 are calculated assuming that the attacker has already crossed V_1, $P(V_2|V_1) = P_{V_2,v_0,\Delta v}$. Therefore

$$P_{V_1,v_0,\Delta v} \bigcap P_{V2,v_0,\Delta v} = P_{V_1,v_0,\Delta v} P_{V_2,v_0,\Delta v} \tag{9}$$

3.3 Results and Discussion

We calculated the maximum spoofing probability for all pair-wise combinations of $v_0 = \{18, 36, 54\}$ m/s and $\gamma = \{1, 5, 10\}$ m/s^2. We note that $\gamma = 10$ m/s^2 is well beyond the capabilities of all but the most high performance vehicles available today. We allowed the attackers' actual velocities to vary from $\Delta v = 0$ to Δv_{max}. A verifier separation of 100 meters was assumed. Our findings are summarized in Table 1; for the sake of comparison the maximum spoofing probabilities for DB (two verifiers placed in the middle of the roadway) and VT (verifiers placed in a triangular configuration beside the roadway) are given in Table 1. See [15] for details on DB and VT infrastructures and spoofing probability derivations.

We see that the friendly jamming approach has a significantly lower spoofing probability than either distance bounding or verifiable trilateration. We also notice that as the attackers' ability to accelerate increases and the reported

Table 1. (LEFT) Maximum spoofing probability for friendly-jamming based secure localization for three attacker accelerations (γ) and nominal velocities of $v_0 = \{18, 36, 54\}$ kmph. (RIGHT) Maximum spoofing probability for DB and VT.

Targeted velocity, v_0 (kmph)	Max Spoofing Probability $\gamma = 1$ m/s^2	$\gamma = 5$ m/s^2	$\gamma = 10$ m/s^2
18	0.0372	0.0382	0.0383
36	0.0361	0.0379	0.0382
54	0.0356	0.0377	0.0381

Distance between verifiers, d (m)	Max Spoofing Probability DB	VT
100	0.25	0.11
500	0.25	0.11
1000	0.25	0.11

velocity v_0 decreases the spoofing probability for the friendly jamming approach increases, though even under the worst circumstances ($v_0 = 18$ kmph and $\gamma = 10\,\mathrm{m/s}^2$) the spoofing probability is still substantially lower than either DB or VT. Finally, while it is true that any position on the highway having a non-zero spoofing probability could be spoofed by attackers, we intend to explore continuous or mandatory verification, occurring at random times, as a counter-measure to attackers opportunistically verifying spoofed positions.

4 Interference Cancellation and Friendly-Jamming

In this section, we identify anti-jamming techniques that could otherwise be used to recover the verification messages outside the interference-free regions surrounding the verifiers, and then analyze the security of our scheme against them.

4.1 Overview of Threats to Friendly Jamming

Friendly jamming signals could be cancelled out by an attacker equipped with multiple antennas. In [16], Tippenhauer et al. examined the case of a jamming unit equipped with a single antenna and an attacker using a pair of antennas to recover a message obscured by interference. The attacker's two antennas are positioned such that the jamming signal was received by each with a relative phase difference of 180 degrees. Specifically, the attacker's antennas were positioned at the same distance r from the jammer and the two received signals subtracted to remove the common interference. We note that a line-of-sight channel condition was assumed, which presents a worst case scenario from the perspective of the jammer.

4.2 Security Analysis Against Cancellation Attacks

In our scheme we deploy multiple outward facing jamming antennas (M) surrounding the transmitter that simultaneously send out random jamming signals. Suppose that the attacker has N antennas. The channel state (CSI) between each pair of antennas can be represented as a matrix: $\mathbf{H} = [h_{i,j}], 1 \leq i \leq M, 1 \leq j \leq N$. In the worst case that the all the CSI values are static and known by the attacker (e.g., a stable line-of-sight channel condition), the attacker only needs to have $N = \lfloor M/2 \rfloor + 1$ antennas because only $M/2$ of the jamming antennas will affect each direction, and $\lfloor M/2 \rfloor + 1$ linear equations can be established to solve for all the $\lfloor M/2 \rfloor$ jamming signals and cancel them out, leaving the transmitted signal. Therefore, the defense reduces to an antenna race against the attacker.

However, the above case is too ideal in practice. The wireless channel on a highway is typically not stable, as it is affected by multiple factors such as multi-path fading, shadowing by the vehicles passing by, and doppler effects. It will be very difficult for the attacker to fully measure or gain the knowledge of all the $M \times N$ CSI in $\mathbf{H}$. Especially, if the attacker does not have any prior knowledge of the CSI matrix, the jamming signals cannot be recovered no matter how many antennas the attacker possesses. Of course this is another extreme, but in reality we expect the attacker with some prior knowledge of the CSI matrix to use $N \in [\lfloor M/2 \rfloor + 1, \infty]$ antennas to cancel out the jamming signals. The difficulty and cost of such signal cancellation depend upon the intrinsic randomness and unpredictability of the channels themselves. We can employ artificial external disturbance to change the channel condition in real-time, for example, rotating the jamming antennas [17]. This direction will be part of our future work.

5 Conclusion

We proposed a method for secure localization based on friendly jamming and found it to be less prone to spoofing attacks than either distance bounding or verifiable trilateration for an ITS infrastructure. We are in the process of evaluating its performance in terms of other metrics such as cost and complexity. An analysis of the verification protocol under varying network conditions and vehicle densities is also required. Near-term efforts will also include the creation and validation of a jammer-based verifier. The number and position of the verifier's antennas, along with their radiating characteristics and interference signals, will be selected to counter anti-jamming techniques, as per Sect. 4.

Acknowledgements. This work was supported in part by the Mountain Plains Consortium under Grant No. MPC-435 and the National Science Foundation under Grant No. 1410000.

References

1. Unsal, C.: Intelligent navigation of autonomous vehicles in an automated highway system: learning methods and interacting vehicles approach. Ph.D. Dissertation, Virginia Tech, Blacksburg, Virginia (1997)
2. U. D. of Transportation: Faq: Intelligent transportation systems joint program office (2012). http://www.its.dot.gov/faqs.htm. Accessed December 05, 2013
3. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
4. Brands, S., Chaum, D.: Distance bounding protocols. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994)
5. Capkun, S., Hubaux, J.-P.: Secure positioning in wireless networks. IEEE J. Sel. Areas Commun. **24**(2), 221–232 (2006)
6. Capkun, S., Rasmussen, K., Cagalj, M., Srivastava, M.: Secure location verification with hidden and mobile base stations. IEEE Trans. Mobile Comput. **7**(4), 470–483 (2008)
7. Fiore, M., Casetti, C., Chiasserini, C.-F., Papadimitratos, P.: Secure neighbor position discovery in vehicular network. In: IEEE/IFIP MedHocNet 2011 (2011)
8. Zeng, Y., Cao, J., Hong, J., Zhang, S., Xie, L.: Secure localization and location verification in wireless sensor networks: a survey. J. Supercomputing **64**(3), 685–701 (2013). doi:10.1007/s11227-010-0501-4

9. Chang, C., University, N.C.S.: Secure localization and tracking in sensor networks. Ph.D. Dissertation, North Carolina State University (2008)
10. Zeng, Y., Cao, J., Hong, J., Zhang, S., Xie, L.: Secmcl: A secure monte carlo localization algorithm for mobile sensor networks. In: IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, 2009. MASS 2009, pp. 1054–1059, October 2009
11. Vilela, J.P., Bloch, M., Barros, J., McLaughlin, S.W.: Wireless secrecy regions with friendly jamming. IEEE Trans. Inf. Forensics Secur. **6**(2), 256–266 (2011)
12. Kim, Y.S., Tague, P., Lee, H., Kim, H.: Carving secure wi-fi zones with defensive jamming. In: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS 2012, pp. 53–54. ACM, New York (2012)
13. Huang, D., Misra, S., Verma, M., Xue, G.: Pacp: an efficient pseudonymous authentication-based conditional privacy protocol for vanets. IEEE Trans. Intell. Transp. Syst. **12**(3), 736–746 (2011)
14. Halton, J.H.: Sigma-algebra theorems. Monte Carlo Methods and Appl. **14**(2), 171–189 (2008)
15. Deka, B., Gerdes, R.M., Li, M., Heaslip, K.: Methods for secure localization in vehicular transportation (2014). http://sats.engr.usu.edu/sites/default/files/transloc.pdf
16. Tippenhauer, N., Malisa, L., Ranganathan, A., Capkun, S.: On limitations of friendly jamming for confidentiality. In: 2013 IEEE Symposium on Security and Privacy (SP), pp. 160–173 (2013)
17. Wang, J., Hassanieh, H., Katabi, D., Kohno, T.: Securing deployed rfids by randomizing the modulation and the channel. In: Technical report (2013). Accessed April 03, 2015