A Physical Layer Security Key Generation Technique for Inter-Vehicular Visible Light Communication

Imam Uz Zaman, Anthony Bahadir Lopez, Mohammad Abdullah Al Faruque, and Ozdal Boyraz
Department of Electrical Engineering and Computer Science, University of California, Irvine, California, USA
{zamani, anthl10, alfaruqu, oboyraz} @ uci.edu

Abstract: A physical layer secret key generation scheme exploiting randomness of the road surface and the driving behavior is being proposed. 128bits encryption key is generated based on real world vehicle trajectory big-data to prove the concept.
OCIS codes: (060.2605) Free-space optical communication; (060.4785) Optical security and encryption

1. Introduction

Visible light communication (VLC) is a rapidly growing wireless optical communication technology in which visible light is employed as the transmission medium exploiting the advantage of omnipresent LEDs and photodiodes. Recently VLC has also been proposed as an effective alternative to radio-based (RF) wireless networks for short range communication due to its many intrinsic advantages over RF such as high spectral availability, precise pointing due to high directional Line of Sight (LOS) propagation, and immunity to the multipath fading. All these qualities make VLC the best choice for Vehicle to Vehicle (V2V) communication, especially where vehicles need to be driven in a controlled close formation to increase traffic fluidity, road throughput and hence to decrease traffic jam. Data flow among vehicles is so vital in delivering vehicle information such as speed, brake, acceleration and any kind of warning for safety operation of vehicles. Like any other communication medium, VLC is susceptible to many security threats including jamming, eavesdropping, interception and physical infrastructure attack [1], and hence securing the communication with a reliable cryptographic design is desirable. However, the key management is the hardest problem in cryptography. The state-of-the-art cryptographic algorithm requires pre-shared keys, which is easily accessible to attackers if they have comprehensive knowledge of the system. In this paper, we present a novel symmetric secret key generation scheme for vehicular VLC link. In particular, we utilized a low data rate (1Kbps to 1Mbps) probe signal and the random intensity variation at the detector to generate symmetric keys. The random intensity variation is caused by the totally stochastic nature of road surface roughness and driving behavior of vehicle drivers. To increase the reliability a market weighted headlamp beam model [2] and vehicle trajectory data by Next Generation SIMulation (NGSIM) program (by Federal Highway Administration) [3] are incorporated into our mathematical model. We successfully generated, with extremely low error, high entropy, secret keys with lengths up to 128-bits using a 1kbps probe signal with the proposed scheme. We also found that the vehicular visible light channels have high entropy (e.g., 12-14 bits for 5000 samples) and that separate channels are highly uncorrelated to one another (e.g., Pearson correlation coefficient of 0.32).

2. Method overview

The proposed physical layer secret key generation method utilizes the randomness in the received signal due to road conditions and driving behavior. To prove the concept we develop a model that is based on the stochastic vehicle trajectory data provided by NGSIM program and the road surface roughness, and the headlight modeling [4]. Since the Lambertian model is not an accurate model to simulate the intensity pattern of a vehicle's headlight and taillight, we utilize a market weighted headlamp beam model [5]. Using the luminous intensity (candela) table provided in this model we can calculate the corresponding illuminance value at any point of interest. In this paper, we limit ourself in the Line of Sight (LOS) communication to generate symmetric secret keys. The illuminance (L) at the photodetector (PD) at the vertical angle (θ) and horizontal angle (ϕ) with respect to headlamp axis is determined by the following equation [6],

$$L = I(\phi,\theta)\times(d\omega/dA) = I(\phi,\theta)\times(\cos\tau / r^{2})$$

where $r, dA, d\omega, \tau, I(\phi,\theta)$ are communication distance, photodetector (PD) area, solid angle, the angle between the photodetector normal and the incident direction, and luminous intensity. Then the received Line of Sight (LOS) optical power ($P_{RX\text{-}LOS}$) is calculated by $P_{RX-LOS} = (L\times A_r)/LER$ when $0 \le \tau \le \Omega$ otherwise $P_{RX-LOS} = 0$ [7] where A_r, Ω, and LER are the PD's total area, the half angle of PD's field of view (FOV) and the luminous efficacy of radiation, respectively. From the equation mentioned, we can effectively calculate the received optical power and hence photodetector current. Moreover, we assumed that the taillight follows the same model as the headlight but with much

lower intensity. In this paper, we mainly considered shot noise due to background solar radiation and other artificial lights. We also added thermal noise associated with the receiver as mentioned in **[7]**.Relative velocity and hence relative lateral and longitudinal distances among vehicles result in random variation in intensity pattern. This randomness can readily be exploited to generate symmetric cryptographic keys.

To generate symmetric keys and to assess the feasibility of the key generation scheme we developed a model of communication links between the vehicular transceivers ***Alice(A)*** and ***Bob(B)*** and another communication link between ***Alice(A)*** and the adversary ***Eve (E)*** (Fig.1). When *Alice* and *Bob* want to generate a symmetric key, they need to exchange a pre-defined probe signal (PRBS modulated bit pattern with a predefined length). To increase the

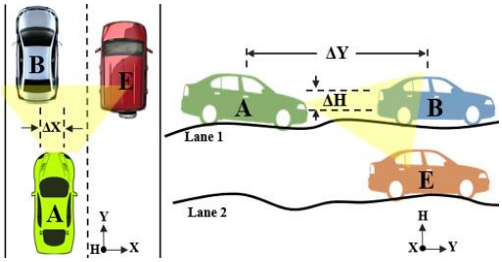

Fig. 1. Vehicles Key Generation Model

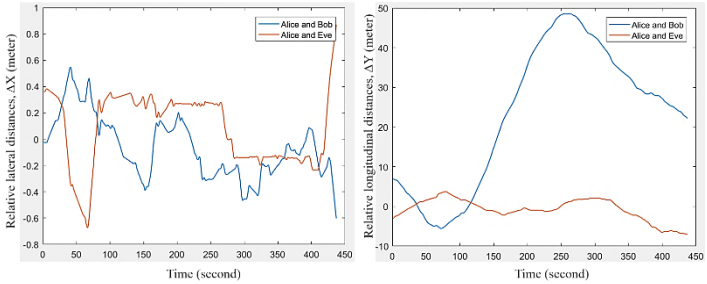

Fig. 2. Relative lateral and longitudinal distances among *Alice*, *Bob* and *Eve*

reliability of the proposed method, the data of the vehicles such as speed, lateral coordinate (X), longitudinal coordinate (Y), time etc. are extracted from the vast amount of data provided by the NGSIM program [3]. Moreover, Using big data analysis we have chosen a combination three vehicle (Alice, Bob and Eve), where *all three are omnipresent in* the vicinity of each other in the real world with the intended point to point link establishment between Alice and Bob**.** This satisfies our communication link model (Fig.1). Then from the NGSIM data, we have calculated the relative lateral (ΔX) and longitudinal (ΔY) distances between selected transceivers over a time duration. These relative distances are totally stochastic (Fig.2) We also add stochastic road surface roughness (ΔH) in our mathematical model [4]. From all these information we were able to find received intensity distribution at the photodetector. We have interpolated NGSIM data to generate keys due to the lack of available data points. In our simulation, we found that there is a high reciprocity of the modulated probe signal (>.9 Pearson correlation coefficient between Alice and Bob's signal) and there is also high randomness (approx.> 12 bits of Shanon entropy for each group of samples). We found that the data received by both Alice and Bob is reciprocal and hence we successfully generate symmetric keys. Conventionally, the adversary *Eve (E)* does not have direct access to the transceiver systems but might have access to the communication link. Furthermore, even if Eve has all the information regarding the communication system or features, Eve will not be able to generate same keys as *Alice* and *Bob* due to the stochastic nature of vehicle trajectory and road surface roughness. In our key generation technique, each transceiver will take a set of samples from the pre-defined probe signal (PRBS) and quantize their signal strengths (in Amps) into symmetric key bits. Each transceiver will compute upper (Thr_{upper}) and lower (Thr_{lower}) thresholds of a group of samples, SampleGroup, with group size *(g)*, based on their mean and variance by the following algorithm:

$$Thr_{upper} = < SampleGroup > + \alpha \times \sigma(SampleGroup)$$

$$Thr_{lower} = < SampleGroup > - \alpha \times \sigma(SampleGroup)$$

$$if \ \ SampleStrength \ \geq Thr_{upper} then \ Key \ Bit \ = 1$$

$$if \ \text{else if} \ SampleStrength < Thr_{lower} then \ Key \ Bit \ = 0$$

$$else \ do \ not \ quantize$$

Where <x> and σ(x) represent mean and variance of *x* respectively. Both *g* and α parameters that can be derived or altered according to the variance of the system (the higher the variance, the higher α, and *g* should be).

3. Simulation results and model verification

Signal propagation between the vehicles, the reciprocity check, entropy calculation, noise calculations and the key generation algorithm are modeled in Matlab. We have utilized the **US 101** (Hollywood Freeway) data from NGSIM to extract vehicles position related information and include it in our mathematical model. For key generation phase, we have performed simulation by using 1Mbps probe signal. Fig.3 and Fig.4 show the sample randomly modulated electrical signal received by *Alice* and *Bob* and corresponding thresholding to generate keys respectively. The generated keys of different lengths with parameters of group size, *g*, equal to 16 and α equal to 0.3 are shown in Fig.5 and Fig.6. The final bit mismatching rate is 0 (0 mismatching key bits/640 key bits) over 10 different 64-bit keys and

0 (0 mismatching key bits/1280 key bits) over 10 different 128-bit keys, demonstrating the applicability of this algorithm. To minimize the simulation time, we used 2^7-1 Pseudo Random Bit Sequence (PRBS) as the probe signal and 512 bits to emulate data propagation. When the key generation is done the vehicles can communicate just as conventional VLC link up to 1Gbps data rate.

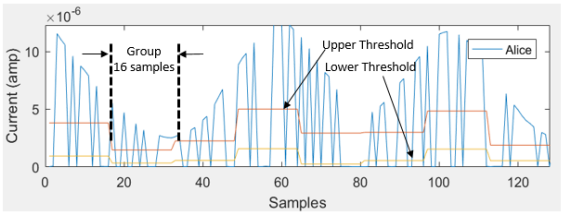

Fig. 3. Sample signal and thresholding for Alice

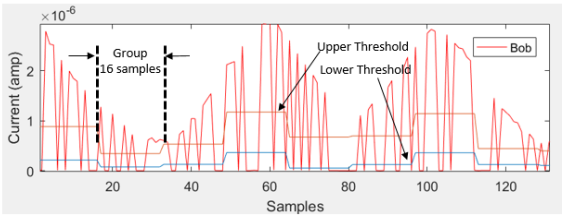

Fig. 4. Sample signal and thresholding for Bob

For the *Alice* and *Eve* channel, using the same algorithm as we used in *Alice-Bob* channel and with the similar PRBS (as we assumed *Eve* has all the information of the link) we generated keys for the adversary *Eve* in Fig. 6. We calculated a final key bit mismatching rate value of 0.0063 (4 mismatching key bits/640 key bits) for the *Alice-Eve* channel after creating 10 different 64-bit keys, and, interestingly, the same value of 0.0063 (8 mismatching key bits/ 1280 key bits) after creating 10 different 128-bit keys. As can be shown, it is clear that the resulting keys from the *Alice-Bob* channel are different than those generated from the *Alice-Eve* channel. Furthermore considering 5000 samples of received current values we computed entropy values (H, in bits) for each channel, $H_{Alice->Eve}$ = 14.77, $H_{Eve->Alice}$ = 12.95, $H_{Alice->bob}$ = 13.36 and $H_{Bob->Alice}$ = 11.97, demonstrating the high channel variation. We also computed the correlations for each channel: $Corr_{Alice-Eve}$ = 0.78 and $Corr_{Alice-Bob}$ = 0.77 showing clear symmetricity, and $Corr_{Alice-Bob}$ to Alice-Eve = 0.3163, demonstrating that the two main channels *Alice-Bob* and *Alice-Eve* are uncorrelated to each other.

Generated 64- bit matched symmetric keys by *Alice* and *Bob* g= 16 α= 0 .3	**0110101010111101011010001010001010101110100011100011000010111110**	**Generated 128-bit matched symmetric keys by *Alice* and *Bob* g= 16 α= 0 .3**	**01101010101111010110100010100010101011101000111000110000010111110100001001010001110001011000010110000001000101100101110001001100**

Fig. 5. Sample generated security keys by *Alice* and *Bob*

Generated 64- bit keys by *Eve* g= 16 α= 0 .3	**0110101010111100110100010100010101011101000000110000010111011000001**	**Generated 128- bit keys by *Eve* g= 16 α= 0 .3**	**01101010101111001101000101000101010111010000001100000101110110001011000001011101000000000000001011100010011100111000011100001111100 1**

Fig. 6. Sample generated security keys by Eve

4. Conclusion

In this paper, we propose and simulated a novel symmetric key generation scheme which can be implemented in any existing V2V visible light communication. By analyzing and simulating numerous samples taken from NGSIM vehicle trajectory data, we showed that natural driving behavior and road surface roughness can be exploited as a source of randomness to generate symmetric cryptographic security keys.

5. References

[1] G. Blinowski, Security issues in visible light communication systems, IFAC-Pap. 48 (2015) 234–239. doi:10.1016/j.ifacol.2015.07.039.

[2] B. Schoettle, M. Sivak, M.J. Flannagan, High-Beam and Low-Beam Headlighting Patterns in the U.S. and Europe at the Turn of the Millennium, ResearchGate. (2002). doi:10.4271/2002-01-0262.

[3] V. Punzo, M.T. Borzacchiello, B. Ciuffo, On the assessment of vehicle trajectory data accuracy and application to the Next Generation SIMulation (NGSIM) program data, Transp. Res. Part C Emerg. Technol. 19 (2011) 1243–1262. doi:10.1016/j.trc.2010.12.007.

[4] K. Bogsjö, K. Podgórski, I. Rychlik, Models for road surface roughness, Veh. Syst. Dyn. 50 (2012). /view.aspx?id=1144091 (accessed December 13, 2016).

[5] B. Schoettle, A market-weighted description of low-beam headlighting patterns in the U.S.: 2004, ResearchGate. (n.d.).

[6] P. Luo, Z. Ghassemlooy, H.L. Minh, E. Bentley, A. Burton, X. Tang, Fundamental analysis of a car to car visible light communication system, in 2014 9th Int. Symp. Commun. Syst. Netw. Digit. Sign CSNDSP, 2014: pp. 1011–1016. doi:10.1109/CSNDSP.2014.6923977.

[7] P. Luo, Z. Ghassemlooy, H.L. Minh, E. Bentley, A. Burton, X. Tang, Performance analysis of a car-to-car visible light communication system, Appl. Opt. 54 (2015) 1696–1706. doi:10.1364/AO.54.001696.