Key Agreement Algorithms for Vehicular Communication Networks Based on Reciprocity and Diversity Theorems

Bin Zan, *Student Member, IEEE*, Marco Gruteser, *Member, IEEE*, and Fei Hu, *Member, IEEE*

***Abstract*—Creating secure communication channels in vehicular communication networks is one of the important topics that have not been well studied. A critical question is how to distribute secret keys between the communication partners. Vehicular networks typically include two different types of communication modes: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). In this paper, we propose two key agreement algorithms for V2V and V2I respectively. The first algorithm allows two legitimate users (vehicles) to derive a common secret key through an information-theoretic manner. The second algorithm uses the channel diversity property to generate secret key between a central server and the individual user. Through evaluation we show that the proposed V2V key agreement algorithm achieves strong information-theoretic security with a secret bit generation rate much faster than previous work. Numerical analysis also shows that the proposed V2I key agreement scheme can prevent attacks from an adversary with high probability even it has a large number of eavesdroppers following the target user.**

I. Introduction

It is expected that vehicular communication systems can be more effective in avoiding accidents and traffic congestion than if each vehicle tries to solve these problems individually. A general vehicular network system includes two types of communications: Vehicle-to-Infrastructure (V2I) communication and Vehicle-to-Vehicle (V2V) communication. In V2I, an individual vehicle speaks to the RoadSide Unit(RSU) to obtain or upload information to a remote traffic server or other application server. In V2V, private data communication can be performed between a pair of vehicles. Both communications are supported by Dedicated Short-Range Communications (DSRC) radio devices, which offer high data rate communication up to 1000 meters [1].

It is desired that two separate sets of secret keys can be used for V2I and V2V communications. For example, a driver may query the traffic center for a section of road along his/her route to the destination through V2I communication. Without a secret key shared between the server and the individual user, this query may be overheard and disclosed to the other users. On the other hand, sometimes a driver may want to query for the local traffic condition without disclosing his/her exact current location to the remote server.

Traditional key agreement approaches include public key (asymmetric) cryptography (such as Diffie-Hellman key establishment) and trusted third parties (TTP) [2]. However, neither approach fits the V2V communication or V2I communication very well. To be more specific, TTP requires a trusted central server, while in vehicular networks there is not such a trusted third party or a central authority. It is also unsecure for V2I communication because even though we can assume the infrastructure is connected to a trusted central server, the key distribution procedure itself is not secure, especially if the secret keys are distributed through wireless channels.

In this work, we are looking for untraditional methods to create secret keys for V2V and V2I communications. By significantly extending our previous work [3], [4] and addressing the special characteristics of vehicular networks, we develop a novel set of key agreement schemes for both V2V and V2I communications. The core of the proposed schemes can be summarized into two words: **Reciprocity** and **Diversity**. Reciprocity represents the channel reciprocity theorem. Diversity includes frequency diversity, space diversity and time diversity.

To summarize, the main contributions of this work are:

1) We propose a secret key agreement scheme for V2V communication. It achieves strong information-theoretic security by extracting secret bits from the wireless channel between two legitimate users. The amount of increasing or decreasing of the Received Signal Strength (RSS) value is used to identify a secret bit instead of using the RSS value itself. This helps to increase the key generation rate and prevent the attacks that have been found in prior methods.
2) We propose a secret key agreement scheme for V2I communication. This scheme exploits random channel hopping mechanism to create frequency diversity when distributing different seeds through RSUs. Due to the space and time diversities, the security can be further improved through seed exchanging between vehicles via the secure V2V communication.
3) We evaluate the proposed V2V key agreement and the V2I key agreement schemes through extensive simulation, experiment and numerical analysis. By comparing to a baseline, we show that the proposed V2V secret key agreement scheme can generate a strong secret

B. Zan is the the Wireless Information Network Laboratory, Rutgers University, North Brunswick, NJ 08902 USA (e-mail: zanb@winlab.rutgers.edu).

M. Gruteser is with the Wireless Information Network Laboratory, Rutgers University, North Brunswick, NJ 08902 USA (e-mail: gruteser@winlab.rutgers.edu).

F. Hu is with the Department of Electrical and Computer Engineering, The University of Alabama, Tuscaloosa, AL 35487 USA (e-mail: fei@eng.ua.edu).

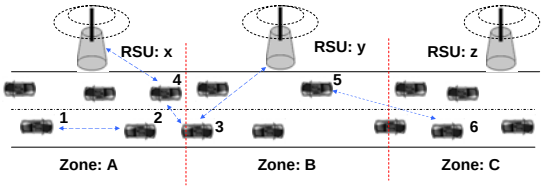

Fig. 1: Illustration of A Vehicular Communication Networks.

key 100% faster than the baseline. We also show that the proposed V2I secret key agreement scheme can achieve strong security with extremely high probability even when the adversary has impractical capabilities compared to a legitimate user.

The remainder of this paper is organized as follows. Section 2 describes the system model. Section 3.1 describes the V2V secret key agreement scheme and section 3.2 describes the V2I secret key agreement scheme. Section 4.1 and section 4.2 evaluates the two schemes respectively. Section 5 reviews some related work. Section 6 concludes our work.

II. System Model

Fig. 1 shows the infrastructure of a typical vehicular communication networks. V2V communication can happen when two vehicles are in each other's communication area. A vehicle conducts V2I communication through RSUs. Each RSU can only cover a segment of the road, labelled as zone in the figure. When vehicles are in the same zone, they can listen to the same RSU.

We assume two types of adversaries. (1) The first kind is interested in knowing the content of the private communication between two mobile users. The adversary could be any other vehicle as long as it is not the users themselves. The adversary could have much more powerful hardware than the users have. It could even be the traffic server which can access and control all the RSUs to monitor the communication between the two users. Finally, the adversary can even have the ability to combine information obtained from the server and multiple vehicles. However, we do assume that any device used by the adversary is not installed less than 1/2 wavelength away from any of the two vehicles' DSRC antennas and the adversary cannot communications inside the vehicle. This assumption is reasonable since otherwise, the user may notice the eavesdropper. (2) The second kind of adversary is interested in eavesdropping the communication content between a vehicle and the server. Thus, the adversary should not be the target vehicle itself and also cannot be the server or the RSUs controlled by the server. The adversary can cooperate with multiple vehicles which are also moving on the same area near the target vehicle. We also assume that deploying multiple radio devices at every RSU along the entire vehicular networks is infeasible to the adversary. Finally, we assume none of the adversaries is interested in interrupting the key agreement process.

III. Main Algorithm

In this section, we describe the V2V and V2I secret key agreement schemes in detail. First, we give an overview on both schemes through Fig. 2 and Fig. 3 respectively.

As shown in Fig. 2, because of channel reciprocity, two vehicles - Alice and Bob - observe similar channel characteristic. Through the proposed differential approach, they can extract a sequence of bits from the channel at each side. The unique sequence of bits can be used to form a secret key for V2V communication. On the other side, Eve can observe either channel A to E or B to E. However, due to the spatial decorrelation, both channel characteristics are different from channel A to B (and B to A). Therefore, the bit Eve can extract from the channel is different from the bits extracted at Alice or Bob side.

Fig. 3 describes the V2I key agreement scheme. Alice receives a seed from the RSU x at channel 1 and time t_1. Because of frequency, space and time diversity, Eve doesn't receive the same seed. For example, 1) she is not on the channel 1 and/or 2) she is not inside the communication range of the RSU x. Later, Eve receives seed from RSU x at channel 3 and time t_1'. However, these two seeds are totally independent. Alice continues collecting seeds along the road as well as exchanging seeds with other legitimate users when possible. In the end, Alice selects some of the seeds and uses XOR operation to form a secret key. The index of the selected seeds are disclosed to the server, thus, the server can execute the XOR operation on the same set of seeds to regenerate the key. On the other hand, if Eve misses one seed, she cannot form the same key. Every index (or ID) is unique, which is the combination of RSU ID, channel number and timestamp as shown in Fig. 3 (e.g. index $x1t_1$ and $x3t_1'$). On the other hand, the value of a seed does not need to be unique. Since the length of a seed is limited, e.g. 128 bits, different IDs may correspond to seeds with the same value.

Next, we will describe the V2V key agreement scheme and V2I key agreement scheme in more detail.

A. Vehicle-to-Vehicle: The Differential Approach

The V2V key agreement scheme is based on the channel reciprocity theorem and the spatial decorrelation property. A secret bit 1 or 0 can be extracted from the channel while the channel characteristic changes. Therefore, we propose a differential approach to capture such variations and generate secret bits.

1) Principle: Channel reciprocity describes the phenomenon that the communication nodes at the two ends of a channel will observe identical channel characteristic, such as channel impulse response or Received Signal Strength (RSS) value. Fig. 4 shows a period of RSS measurement under a multi-path (office) environment. Two users, Alice and Bob, alternatively transmit wireless signal to each other while moving in about 1 meter per second. Both Alice and Bob probe the channel and measure the RSS values at a rate of 40 per second. Due to the channel reciprocity, the RSS values observed at Alice and Bob's sides for Alice-Bob and Bob-Alice channels respectively are highly correlated (=0.9120).

On the other hand, Eve, who is at a different location from Bob, observes different RSS values from Alice-Eve channel compared to Bob's observation of the Alice-Bob channel, as

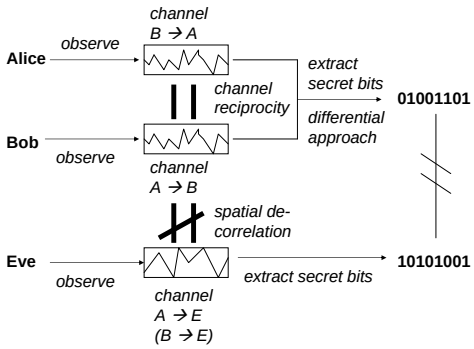

Fig. 2: The V2V Key Agreement Flow Chart.

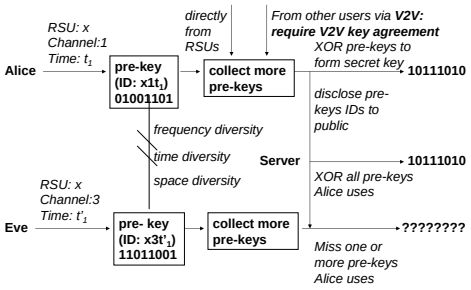

Fig. 3: The V2I Key Agreement Flow Chart.

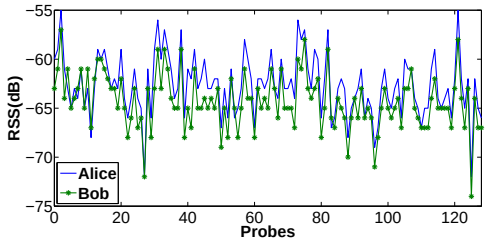

Fig. 4: Illustration of the channel reciprocity.

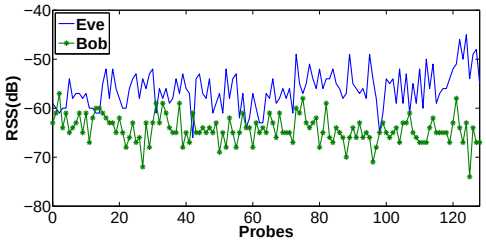

Fig. 5: Illustration of the spatial decorrelation.

shown in Fig. 5. The two curves shown in the figure are highly uncorrelated (=-0.1937) due to the spatial decorrelation property in a multi-path (Rayleigh) fading channel. Theoretically, the spatial decorrelation property can be described by a Bessel function:

$$J_0(x) = \frac{1}{\pi}\int_0^{\pi} cos(xsin\theta)d\theta \tag{1}$$

in which x is the distance between Bob and Eve in the unit of wavelength λ, and θ is phase offset.

The wireless channel between Alice and Bob can be described as complex and discrete function of time $h_t = H(t)e^{j\gamma_t}$. Alice sends Bob a signal $s(t_1) = A_{t_1}e^{j\phi_{t_1}}$ at time t_1, then the received signal at Bob can be written as:

$$y_{t_1} = H_{t_1}A_{t_1}e^{j(\phi_{t_1}+\gamma_{t_1})} + n^b_{t_1} \tag{2}$$

where n^b_t is the noise terms which are independently and identically distributed complex Gaussian random variables. A signal $s(t_2) = A_{t_2}e^{j\phi_{t_2}}$ sent from Bob to Alice is received as:

$$y_{t_2} = H_{t_2}A_{t_2}e^{j(\phi_{t_2}+\gamma_{t_2})} + n^a_{t_2} \tag{3}$$

From t_1 to t_2, if the total changes in location on both Alice and Bob sides are much smaller than $\frac{\lambda}{2}$, then good estimated values of $\hat{h}_{t_1} \approx H_{t_1}e^{j\gamma_{t_1}}$ at Bob side and $\hat{h}_{t_2} \approx H_{t_2}e^{j\gamma_{t_2}}$ at Alice side are highly correlated according to equation 1. On the other side, assume Eve is not close to either Alice or Bob, she cannot obtain a proper estimation on either h_{t_1} or h_{t_2}. Furthermore, when Alice and Bob alternatively send each other probe signals, then the sequences of probed channel characteristics $[\hat{h}_{t_1}, \hat{h}_{t_3}, ..., \hat{h}_{t_{2n-1}}]$ are highly correlated to the sequence of probed channel characteristics $[\hat{h}_{t_2}, \hat{h}_{t_4}, ..., \hat{h}_{t_{2n}}]$.

2) Challenges: Several research groups have proposed key agreement schemes based on the channel reciprocity theorem and spatial decorrelation property. The core idea of most existing works to extract secret key from RSS values is Quantization, in which, one or two threshold values are either determined through a pre-probe phase such as in [5], [6] or post-phase process [7], [8]. The value of a secret bit is obtained by comparing the RSS values to the threshold values. By studying existing works, we feel the proposed scheme must at least fulfill the following challenges.

Prevent Entropy Reduction. We introduce a metric, entropy, to evaluate the strength of a secret key:

$$H_i = -p_0 \log p_0 - p_1 \log p_1 \tag{4}$$

$$H_{average} = \frac{1}{N}\sum_{i=0}^{i=N} H_i \tag{5}$$

where N is the total length of the secret key, and p_0 is the post test probability of a bit being 0 based on adversary's knowledge. The closer to 1 the value of $H_{average}$ is, the stronger the secret key is.

In the pre-probe method, the thresholds are determined in a pre-probe phase. This method relies on the assumption that the future probes are roughly and evenly distributed around the thresholds. However, this is not always true. As shown in Fig. 6, in which the thresholds q_+ and q_- are calculated according to [5]. If an adversary notices that the Euclidean distance between two vehicles is dramatically increasing during the bits extracting phase, he might easily predict the results. Therefore, the entropy of the resulted secret key is very low.

In the post-probe method, thresholds are determined after all RSS samples have been collected. As shown in [7], by inserting or removing intermediate objects between Alice and

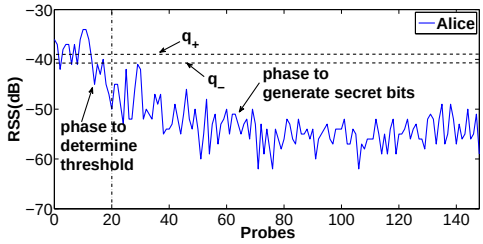

Fig. 6: The failure of the Pre-Probe method.

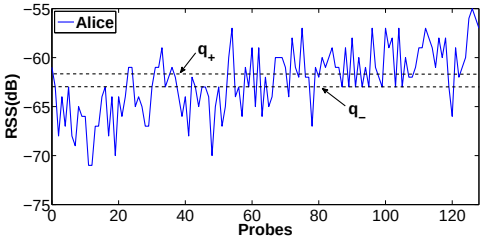

Fig. 7: The failure of the Post-Probe method.

Bob, Eve can force the RSS curves following certain trends as shown in Fig. 6 and Fig. 7. Secret keys based on these two curves are very predictable from Eve's point of view. Therefore they have very low entropy.

Reduce the Impact of Small Fluctuation. It is known that small fluctuation may reduce the effect of channel reciprocity. When the real channel variation is smaller than the small fluctuation caused by noise, interferes etc, no secret bit can be correctly extracted from the channel. The proposed algorithm should be able to reduce the impact of small fluctuation.

Increase the Secret Bit Generation Rate. In V2V, the communication is limited by the period of the encounter duration between two vehicles. When vehicles moving out of radio range, the communication stops. In this work, we pursue a more efficient and fast key agreement scheme comparing to previous works.

3) Algorithm: Instead of using absolute thresholds, the proposed differential approach determines a secret bit based on the difference between two neighbor RSS values. To illustrate the basic concept, an example is shown in Fig. 8. In this method, whenever an increase between two RSS values is observed, a bit 1 is generated, and a bit 0 is generated for a decrease.

The differential approach can be summarized in the following steps:

1) Sample collection: Both Alice and Bob collect a period T of RSS values using their maximum probe rate.
2) Segments division: To improve bit matching rate, we divide the sequence of probes into segments by every τ number of probes. A secret bit is generated based on the value of the first probe and last probe in each segment or the last probes between two neighboring segments. For example, by comparing probe 3 and 5, Alice obtains bit 1 for segment 2.
3) Small fluctuation removal: Using moving average method to reduce the influence of small fluctuation by width d number of segments[1].

$$Y = \frac{x_1 + x_2 + x_3 + ... + x_d}{d} \tag{6}$$

4) Bit extraction: Secret bit is generated by comparing a RSS sample of each segment (for example the first RSS value of the segment). Set bit to 1 if there is an increase by more than ϵ/d, and 0 if there is a decrease by more than ϵ/d. ϵ is an approximate estimate of the small fluctuation, it could be different for Alice and Bob. Note, to reduce the computational load, we only need to calculate the moving average of one value in each segment.
5) Information exchange: Alice sends Bob only the positions of those probes which are used by her to generate secret bits. From those positions, Bob picks the ones he can also extract secret bits and replies back to Alice.

Fig. 9 gives a more concrete example for the key agreement scheme. For the sake of simplicity, in this example, we assume the moving average width $d = 1$, $\tau = 2$ and the value of ϵ for both Alice and Bob is equal to 3. Alice obtains a sequence of bits 010?1?0??010 by comparing the first RSS value of each segment. She is unsure of the bit values at positions '4,6,8,9' in the sequence. Then she sends Bob a message to disclose this information. On the other hand, Bob obtains bit sequence 0?0?1?01?010. In addition to what Alice is not sure of, Bob adds position '2' to the unsure bit list and informs Alice. After taking out the unsure bits, both Alice and Bob obtain the final bit sequence 0010010. To further improve efficiency, we introduce another parameter ϵ_2 related to the small fluctuation, $\epsilon_2 = a * \epsilon$, $0 < a < 1$. When only one of Alice and Bob is not sure about a bit at a specific position, she/he uses ϵ_2 instead of ϵ to identify a bit value. Through this way, more secret bits can be generated since ϵ_2 is smaller than ϵ. For the case in Fig. 9, assume $\epsilon_2 = 0.5 * \epsilon$, two more bits 1 will be generated from segment 2 and 8. One of the advantages of using differential method is that it can prevent the attack described in [7]. Because, even the channel condition is improving or downgrading following an observable trend, this method will not generate bits all in 1 or 0 values.

To further reduce parameter dependence, we propose a dynamic differential approach in which the fixed interval τ is removed. In this approach, the first RSS sample is used as a reference. Every RSS sample starting from the second one will be compared with the reference until a difference larger than ϵ/d is observed. A bit is extracted depending on whether the difference is an increase or decrease. Reference is updated at the position where a bit is extracted. The balance RSS samples will be compared with the updated reference until the next large difference appears. In the end, Alice sends Bob the positions of which she is able to extract secret bits.

[1] d and τ are two different concepts. Every segment includes τ number of probes. However, we perform moving average based on every d number of segments. Therefore, τ determines how frequently a bit we expect to generate directly related to the true channel condition various, and d determines how to remove small fluctuation noise which is directly related to the impact of the noise.

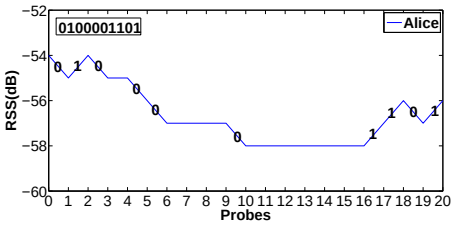

Fig. 8: Differential approach example.

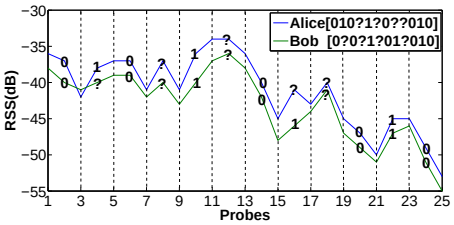

Fig. 9: Fixed interval method.

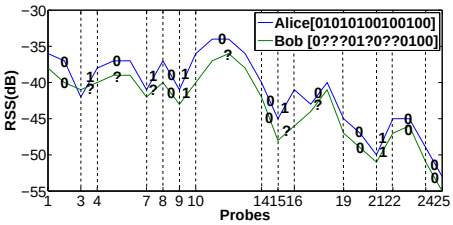

Fig. 10: Dynamic differential method.

Upon receipt, Bob checks if he can also extract bits from these positions and then, sends the results back.

In Fig. 10, we assume $d = 1$ and $\epsilon = 3$. Based on the method described above, Alice extracts a bit sequence 01010100100100. Bob recognizes 0???01?0??0100 and recommends Alice to remove unsure bits at positions '2,3,4,7,9,10'. Therefore the resulted common bit sequence is 00100100. If using two ϵ thresholds, for example $\epsilon_2 = 0.5 * \epsilon$, the bit sequence Bob obtains becomes 0?0101001?0100. This updates the common bit sequence to 001010010100.

B. Vehicle-to-Infrastructure: All About Diversity

As shown in Fig. 3, the proposed V2I key agreement scheme is a combination of different kind of diversities.

1) Problem Statement: We have shown that traditional key agreement approaches are not good candidates for secure V2I communication. The V2V secret key agreement scheme does not fit V2I either. That is because: 1) The V2V secret key agreement scheme requires a multi-path (Rayleigh) fading environment, however, in V2I, this may not exist. For example, when the RSU is installed on a much higher position comparing to all the moving vehicles, channel characteristic is dominated by line-of-sight propagation. 2) RSUs are installed at fixed locations and may not be checked by people for certain time. Thus, an adversary may have an eavesdropper installed very close to the RSU device for a long period before anyone notices that. 3) Relying on a particular RSU to generate secret key between the vehicle and the server is not a very strong secure manner. If the adversary compromises the RSU, the secret key is no longer a secret.

2) The Frequency Hopping Method: Since it is not adequate to reuse the solution of V2V in V2I, we propose to use a frequency hopping method and its extension based on time and space diversity properties. The main principle of the frequency hopping method has been studied in our work [3]. Below we give a short introduction.

Assume an RSU (Alice) is the transmitter, one legitimate vehicle receiver (Bob) and one passive vehicle eavesdropper (Eve). Everyone can communicate on multiple, non-interfering channels, but receive on a single (or a few) channel at a given time. As in [9], we assume that the hardware Eve has is similar to Alice's and Bob's. Alice and Bob seek to establish a secret key without any prior shared information.

Basic Packet-Based Scheme. The idea underlying this scheme is that both parties of the key agreement process—Alice and Bob—randomly select a channel to send and listen to, respectively. If they are on the same channel, key information is successfully transferred and Bob sends an acknowledgment (ACK). Otherwise, a timeout occurs. Alice and Bob may select other channels and repeat the process. Alice must use a different key material, which we refer to as a seed, for every transmission attempt. If Alice receives an ACK, she knows that this seed will be used, otherwise she discards the seed.

Analysis. Given n channels, the probability that Alice and Bob are on the same channel is $p = \frac{1}{n}$. Assume that Eve can monitor one channel at a time as Bob, the probability she overhear Bob's secret key is $p_e = \frac{1}{n}$. To achieve a high level of security, the basic scheme requires a large number of channels. This is impractical because the number of available channels is often limited by the radio hardware, and the time required for a successful key exchanging increases with the number of channels. In fact, the probability that Alice and Bob successfully exchange a secret key in x attempts follows the *Geometric* distribution $P_X(x) = p(1-p)^{x-1}$. Thus the expected number of exchange attempts is $E[X] = \frac{1}{p} = n$, where n is the number of channels. This means that halving the probability of key overhearing p_e requires twice the number of channels and time required for key agreement.

Multi-Agreement Scheme. To address the limitation, we introduce a multi-agreement scheme. In this scheme, Bob and Alice will repeat the seed agreement multiple times. The process will end when Bob receives k seeds and the final secret key will be a XOR of all the seeds. For detailed analysis, please refer [3].

Application. In V2I communication, RSUs controlled by the server will be the legitimate senders (Alice) who broadcasts seeds through random channel hopping scheme. There is no immediate feedback: ACK. Instead, after a vehicle (Bob) has received enough seeds, it sends the server a message about the seeds it will use to form secret key, as shown in Fig. 3. The message tells the server information about the time and from which RSUs the seeds are collected. Based on above knowledge, the server can also reproduce the key from its side.

3) Enhancements: **Space Diversity.** Spatial differences increase the chance that an adversary misses a seed. Furthermore, a vehicle, especially one from the opposite direction, has a very high probability of hearing different seeds somewhere else. Thus, we could improve the frequency hopping scheme by exchanging seeds between vehicles via the secure V2V channel created before. **Time Diversity.** A vehicle does not need use all received seeds to form a secret key, instead it leaves some seeds for future use. The time diversity makes it

even harder for an adversary to get all the seeds for forming a key, especially when those seeds are collected over a long time and are exchanged randomly between vehicles.

IV. Experimental Results and Numerical Evaluation

In this section, we first evaluate the proposed V2V key agreement scheme based on real experimental data. Then, we show the simulation and numerical analysis results for the V2I key agreement scheme.

A. Vehicle-to-Vehicle Case

The following results shown in this subsection are based on real experimental data.

In the experiment, two mobile nodes, Alice and Bob, are moving in a multipath fading channel environment and collecting 50000 RSS value samples at the same time. We use Orbit mobile nodes [10] equipped with Atheros AR5212 Mini PCI wireless interfaces[2]. Our baseline is based on the protocol proposed in [5]. However, we have updated the scheme from pre-probe to post-probe. In [5], the authors use level-crossings and quantization to extract bits from correlated stochastic processes. To be more specific, two legitimate users use the channel statistics to determine scalars, q_+ and q_- serve as reference levels for quantizing. A secret key bit 1 or 0 is agreed if enough channel magnitude measurements are higher than q_+ or lower than q_- on both sides. Since post-probe method generally can achieve higher performance than pre-probe method due to its better threshold setting, we update the baseline by using post-probe method.

In Fig. 11, we compare the bit generation rates among four schemes: baseline [5], fixed interval differential (interval $\tau = 10$ and interval $\tau = 30$) and dynamic differential schemes. Fig. 12 shows the bit matching rate. Note, the results of baseline are already enhanced by subtracting the moving average and setting $\alpha = 0.125$ and $m = 4$. In all proposed schemes, $\epsilon = 6$ and $\epsilon_2 = 3$. Estimated value of $\lambda/2v$ is around 25, which means ideally, an uncorrelated secret bit can be generated every 25 probes. As shown in the figure, all differential approaches perform better than the baseline. In fixed interval method, the smaller τ, the higher generation rate. This is easy to be understood because small τ results in more RSS values to be compared and consequently more large scale variations may be caught. However, the negative part is it may generate correlated bits that have low entropy. This fact is shown in Fig. 13. In the figure, x indicates the length of a continuous 1 or 0 bit sequence, and y is the probability distribution of different length. Both fixed interval with $\tau = 10$ and the dynamic approach do not have the same distributions as the ideal one. Since a long set of 1 or 0 due to the correlation is easy to be predicted by an adversary, these two cases will generate bit sequence with low entropy. There are some methods to convert such a low entropy bit sequence into a high entropy bit sequence, e.g. removing some redundant bits. After taking a properly bits converting step (from low entropy to high entropy), we show the results in Fig. 14. The dynamic approach and the fixed interval with $\tau = 10$ have similar and the highest bit rate, while the dynamic approach reduces the parameter dependence.

Above figures also show the affect of moving average width. For all differential methods, the width should not be too small in order to remove the small fluctuations. Otherwise, it leads to a low bit generation rate. For the baseline, small width also doesn't work since it cannot remove large scale fading. On the other hand, moving average width should not be too large, because it will screen out some useful large variations. In the proposed approaches, the width could be estimated by $\lambda/2v$. However, for the baseline there is no proper method to estimate the width[3].

B. Vehicle-to-Infrastructure Case

In this subsection, we study the V2I key agreement scheme through simulation.

The simulation data are generated from Paramics Traffic Simulation model for South New Jersey vehicular networks. Total data includes 984,445 records from 5000 cars in a 3395-second period. We assume every 1500 meters in vertical or horizontal distance, an RSU is deployed. Every 0.5 seconds, each RSU randomly picks one of three pre-defined channels to broadcast a seed. A vehicle receives the seed if it is tuning to the right channel and is in the right distance (less than 1000 meters Euclidean distance away). It is possible that a location is covered by more than one RSU. If a vehicle hear signal from multiple RSUs, it only receives the seed from the closest one.

In Fig. 15, the histogram chart describes the number of vehicles sharing the same seed. As can be seen, a seed tends to be shared only by small number of vehicles. On average a seed is shared by 7 vehicles and the maximum number of vehicles sharing the same seed is 83. Recall that even if a seed is known by multiple vehicles include the adversary, as long as one seed is unknown to the adversary, she cannot form the right secret key. This is because the final key is based on the XOR operations on a set of seeds, thus the security of the key is always guaranteed by the remaining unknown seeds from an adversary.

One of the strategies the adversary can use is to cooperate with multiple vehicles and collect as many seeds as possible. In Fig. 16, we compare the seeds that are collected by an adversary through this strategy with the seeds collected by all the vehicles. Although it is helpful to cooperate with other vehicles, at 99.9% cooperation rate, an adversary still cannot guarantee to obtain all the seeds a vehicle received during the simulation.

In Fig. 17, we study the successful attacking rate by the adversary when it has multiple partners. In this figure, the secret key is assumed generated based on all the seeds a vehicle collected during the simulation. The successful attacking rate is only 0.174 when 99.9% vehicles are cooperating with the

[2]Although it use 802.11a instead of 802.11p for wireless communication and at a relative slow moving speed, the results is still instructive.

[3]This is because for the proposed methods, we need to remove the small fluctuations only, however in the baseline, it needs to remove a large scaling fading which is harder to estimate.

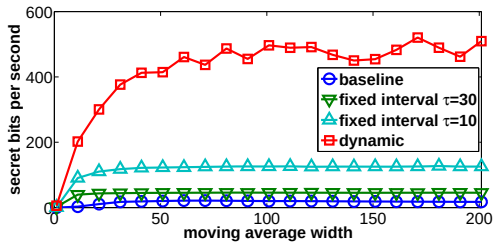

Fig. 11: Illustration of the bit generation rate.

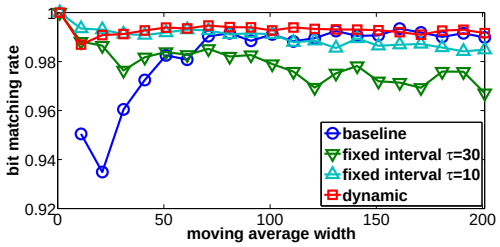

Fig. 12: Illustration of the bit matching rate.

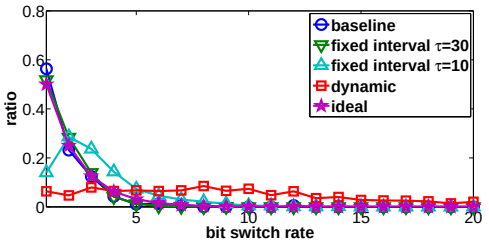

Fig. 13: Illustration of the bit switch rate.

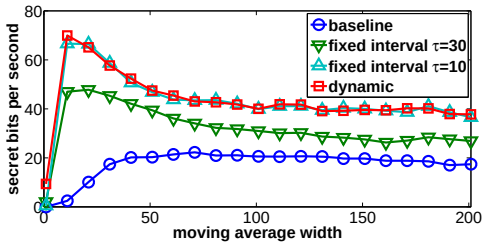

Fig. 14: High entropy (full) secret bit generation rate.

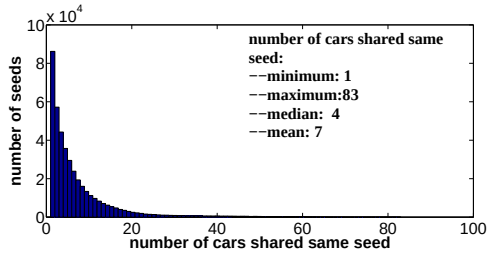

Fig. 15: Histogram of the number of cars sharing the same seed.

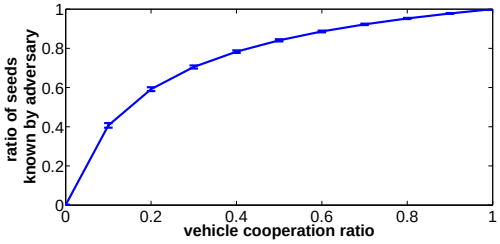

Fig. 16: Illustrate the impact of cooperation between adversary and other vehicles (comparing to total seeds collected in the networks).

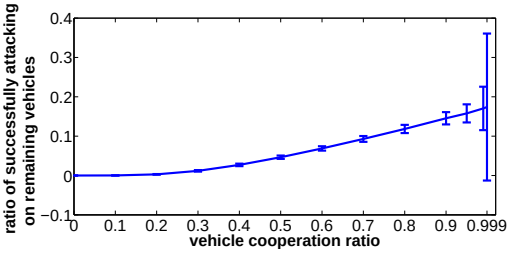

Fig. 17: Illustrate the impact of cooperation ratio on an adversary's successful attacking rate.

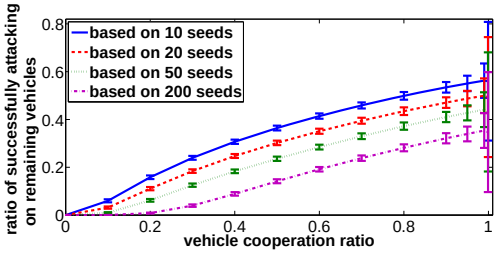

Fig. 18: Successful attacking rate v.s. cooperation ratio v.s. number of seeds required.

adversary. This result is a disaster to the adversary. First, it is impossible to cooperate with so many vehicles in a large vehicular network. Second, the success rate is still very low. Thirdly, the standard deviation is too large to make the success rate reliable.

In practice, a fix number of pre-keys may be used to form a final secret key. Thus, in Fig. 18, we study the performance based on fixed number of seeds. When forming a secret key with more seeds, the success rate of an adversary to break the key becomes low. For example, 200 seeds correspond to 0.0003 for 10% vehicles, and 0.3472 for 99.9% vehicles. Even for small number of seeds, as long as the cooperation ratio is low, the success rate of an adversary is still low.

V. Related Work

Traditional key distribution protocols rely on infrastructure with online trusted third parties (TTP), such as the well-known Kerberos [11] scheme and Otway-Rees protocol [12]. However, in V2V communication, there is no central authority can be relied on as we discussed before. Furthermore, since the node mobility is unrestricted, the topology may be unpredictable making central authority assumption infeasible.

Diffie and Hellman discussed a public key distribution system and how it can be transformed into a one-way authentication system [13]. Other well-known public key algorithms include RSA [14], Elliptic curves [15] and Digital Signature

Algorithms (DSA), etc. Several research works [16], [17], [18] have shown that cost-effective processors with limited computational abilities make public-key cryptography almost impractical for embedded intelligence and ubiquitous computing applications, even without power consumption considerations. Another issue with public key protocols is the number of certificates that need to be exchanged. With the proposed approach, certificates exchanging are avoided.

In [19], Rolf Blom presented a symmetric key generation system (SKGS), where each pair of users share one master key that is distributed at the start up time by a key generation authority. Eschenauer and Gligor [20] proposed a key management scheme that relies on probabilistic key sharing among the nodes of a random graph and uses a simple shared-key discovery protocol for key distribution, revocation and node re-keying for large-scale distributed sensor networks. Chan [21] introduced Distributed Key Pre-distribution Scheme (DKPS) which is a fully distributed and self-organized key pre-distribution scheme without relying on any infrastructure support. However, the strict requirement for pre-distribution might not be available always. For example, in vehicular networks, the cars (sharing no prior secret information) may just meet on the spot where there is likely to be no single trustable proxy or TTP for key pre-distribution.

Hershey et al. [22] first presented the concept of using physical layer characteristics for key management. Using Espar (Electronically Steerable Parasitic Array Radiator) antenna to measure the RSSI, the authors of [8] create secret key based on the median value of the RSSI profiles. More recent work can be found in [5], [23]. However, all existing work require a relative accurate measurement on end users. However, consider the difference between each individual communication device, accurate and uniform threshold may not be available at different end users even with the channel reciprocity theorem.

Finally, some researchers started to exploit multi-channel characteristic of wireless devices to help improving security recently. Interested readers can refer [9], [3].

VI. Conclusion

In this paper, we have presented a set of key agreement schemes to help establish secure communication channels in vehicular networks for both V2V and V2I modes. The proposed algorithm is based on two novel key agreement schemes: differential and channel hopping key agreement schemes and their extensions. It takes advantage of physical layer characteristics of a wireless channel and the natural characteristics of vehicular networks. Specifically, besides the channel reciprocity property, it makes use of different kinds of diversity properties existing in the channel and in vehicular networks. The security of the proposed algorithm is rooted in two factors: first is the well-known spatial decorrelation property and the second one is the complexity of the vehicular networks and individual randomness.

References

[1] "Dsrc standards: What's new?" Retrieved 2008-02-17. [Online]. Available: http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm

[2] A. Perrigand, K. Szewczyk, V. Wen, D. Culler, and J. Tygar, "Spins: Security protocols for sensor networks," *Wireless Nets*, vol. 8, no. 5, pp. 521–534, 2002.

[3] B. Zan and M. Gruteser, "Random channel hopping schemes for key agreement in wireless networks," in *PIMRC '09: Proceedings of the 20th Personal, Indoor and Mobile Radio Communications Symposium 2009*, Tokyo, Japan, 2009.

[4] B. Zan, M. Gruteser, and F. Hu, "Improving robustness of key extraction from wireless channels with differential techniques," in *ICNC '12: Proceedings of the International Conference on Computing, Networking and Communications 2012*, Maui, Hawaii, USA, 2012.

[5] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2008, pp. 128–139.

[6] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2007, pp. 401–410.

[7] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *MobiCom '09: Proceedings of the 15th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2009, pp. 321–332.

[8] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *Antennas and Propagation, IEEE Transactions on*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[9] M. J. Miller and N. H. Vaidya, "Leveraging channel diversity for key establishment in wireless sensor networks," April 2006, pp. 1–12.

[10] D. Raychaudhuri, I. Seskar, M. Ott, S. Ganu, K. Ramachandran, H. Kremo, R. Siracusa, H. Liu, and M. Singh, "Overview of the orbit radio grid testbed for evaluation of next-generation wireless network protocols," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 3, march 2005, pp. 1664 – 1669 Vol. 3.

[11] J. Steiner and J. I. Schiller, "Kerberos: An authentication service for open network systems," in *Usenix Conference Proceedings*, 1988, pp. 191–202.

[12] D. Otway and O. Rees, "Efficient and timely mutual authentication," *SIGOPS Oper. Syst. Rev.*, vol. 21, no. 1, pp. 8–10, 1987.

[13] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976. [Online]. Available: citeseer.ist.psu.edu/diffie76new.html

[14] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[15] N. Koblitz, "An elliptic curve implementation of the finite field digital signature algorithm," in *CRYPTO '98: Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 1998, pp. 327–337.

[16] A. C. f. Chan, "Distributed symmetric key management for mobile ad hoc networks," *IEEE INFOCOM*, vol. 4, pp. 2414–2424, 2004.

[17] M. Al-Shurman and S.-M. Yoo, "Key pre-distribution using mds codes in mobile ad hoc networks," in *Information Technology: New Generations, 2006. ITNG 2006. Third International Conference on*, april 2006, pp. 566 –567.

[18] C. Castelluccia, N. Saxena, and J. H. Yi, "Self-configurable key pre-distribution in mobile ad hoc networks," in *in: IFIP Networking Conference*, 2005, pp. 1083–1095.

[19] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 335–338.

[20] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *ACM Conference on Computer and communication Security(CCS)*, 2004.

[21] A. C.-F. Chan, "Distributed symmetric key management for mobile ad hoc networks," *IEEE INFOCOM*, vol. 4, pp. 2414–2424, 2004.

[22] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *Communications, IEEE Transactions on*, vol. 43, no. 1, pp. 3–6, Jan 1995.

[23] A. Kitaura, T. Sumi, K. Tachibana, H. Iwai, and H. Sasaoka, "A scheme of private key agreement based on delay profiles in uwb systems," March 2006, pp. 1–6.