# Artificial Fast Fading-Aided Key Agreement Algorithm for Vehicle-to-Infrastructure Networks

Fábio César Schuartz, João Luiz Rebelatto and Richard Demo Souza

***Abstract*— The communication in vehicular ad hoc networks (VANETs) is commonly divided in two scenarios, namely vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Aiming at establishing secure communication against eavesdroppers, recent works have proposed the exchange of secret keys based on the variation in received signal strength (RSS). However, the good performance of such scheme directly depends on the channel variation rate, being more suitable to the V2V scenario since, in V2I, the channel commonly undergoes slow fading. In this work we propose the use of multiple "dumb" antennas in order to artificially generate a fast fading channel so that the extraction of secret keys out of the RSS becomes feasible in a V2I scenario. Numerical analysis shows that the proposed model can outperform, in terms of secret bit extraction rate, a frequency hopping-based method proposed in the literature.**

***Keywords*— Key agreement, security, vehicular networks, multiple antennas, channel diversity, secret key generation, artificial fast fading.**

## I. Introduction

With the increase of road traffic volume in cities and highways, the use of advanced intelligent road information systems capable of monitoring the movements of vehicles, such as the vehicular ad hoc networks (VANETs) [1], becomes important towards minimizing congestion, accidents and increasing safety on the roads. A general communication system in VANETs commonly encompasses two different scenarios: the communication between two vehicles (V2V) and between a vehicle and a infrastructure (V2I), where the last corresponds to a road-side unit (RSU) placed along the highway [2].

Regardless the scenario, secure communication protocols are needed in order to protect the confidentiality of information against potential eavesdroppers. Traditional security approaches adopt the exchange of secret keys between the legitimate pair of transmitter-receiver (commonly referred to as Alice and Bob, respectively), where secure communication is established after a key agreement between Alice and Bob. It becomes then of paramount importance to provide secure ways for the legitimate nodes to exchange the keys.

Traditional key agreement protocols include public key cryptography and trusted third parties (TTP) [3]. However, both do not fit in V2V and V2I communication. For example, TTP requires a trusted central server which does not exist in V2V. Also, it is also not safe in V2I due to the fact that, even if the infrastructure is connected to a trusted central server, the key distribution procedure in wireless channel is not safe. In [4], a one-way authentication public key distribution system is presented. A symmetric key generation system is presented in [5], with each pair of users sharing a master key, distributed initially by a key generation authority. In [6], an algorithm for key management is proposed, using a simple shared key discovery protocol for key distribution. However, the requirement for predistribution of keys may not always be available, such as in a spot without a trusted proxy or TTP.

Unlike encryption-based traditional methods, recent works exploit physical layer information to extract secret keys between two wireless communication devices [2], [7], [8]. The idea behind this method is that, through the exchange of public information, Alice and Bob can obtain reciprocal observations of temporal and spatial randomness of the channel state between them, which will serve as the basis for the generation of secret keys. The security of secret keys generated by the physical layer information of a channel is ensured by the fact that the wireless channel between two devices is uncorrelated from other channels [8], making the physical layer based secret key extraction methods an alternative to existing encryption methods for wireless mobile devices with limited resources or without key management infrastructures.

In [2] the authors propose two methods for key agreement, for both V2V and V2I scenarios. In the V2V, the model uses the amount of increase or decrease in the RSS value to identify a secret bit, instead of using the RSS value itself. Such scheme, which we referred to as differential RSS (D-RSS), makes use of the reciprocity and high correlation from the channel between the legitime users. In this environment, the rate of secret bits extracted depends on the channel variation rate, which, due to the movement between the vehicles, has been shown to be large enough [2]. In V2I model, one of the participants is fixed and the channel characteristic may be dominated by line-of-sight propagation, resulting in a more slowly varying channel when compared to V2V method [2] and compromising the performance of the D-RSS scheme in this scenario. In order to overcome this issue, the authors in [2] propose a frequency-hopping (FH)-based method to key extraction in a slow-fading V2I scenario, which exploits random channel-hopping mechanism to create diversity when distributing different seed through different RSUs.

In this work, we focus on the V2I scenario and resort to multiple "dumb" antennas [9] placed at the RSU in order to artificially transform the aforementioned slow fading channel into a fast fading channel, so that the extraction of secret keys out of the RSS becomes feasible in a V2I scenario. An important feature of the proposed multiple antenna D-RSS (MD-RSS) scheme is that the multiple antennas placed at the

Fábio César Schuartz, João Luiz Rebelatto and Richard Demo Souza CPGEI, Federal University of Technology - Parana, Av. Sete de Setembro, 3165, Rebouças, Curitiba, PR, 80230-901, Brazil. E-mails: phabyo@gmail.com, {jlrebelatto, richard}@utfpr.edu.br.

This work was partially supported by Fundação Araucária, CAPES and CNPq (Brazil).

RSU are transparent to the vehicles [9]. Our results show that the proposed scheme can outperform the FH-based method from [2] in terms of secret bit extraction rate in a V2I scenario.

The rest of this paper is organized as follows: Section II describes the system model and the D-RSS and FH algorithms. Section III presents the proposed MD-RSS scheme, followed by numerical results in Section IV. Finally, Section V concludes the paper.

## II. Preliminaries

### A. System Model

We consider a V2I scenario composed of three nodes: one legitimate vehicle (referred to as Alice - $A$), one RSU (called Bob - $B$) and a malicious passive eavesdropper (Eve - $E$).The frame transmitted by node $i \in \{A, B\}$ and received by the node $j \in \{A, B, E\}, i \neq j$ is

$$\mathbf{y}_j(t) = h_{ij}(t)\,\mathbf{x}_i(t) + \mathbf{n}_j(t), \tag{1}$$

where $h_{ij}(t)$ is the quasi-static fading coefficient, whose envelop is modeled as a Rayleigh independent and identically distributed random variable and which changes independently from frame to frame, $\mathbf{x}_i(t)$ is the average unit energy transmitted frame, and $\mathbf{n}_j(t)$ is the zero-mean complex Gaussian noise with variance $\sigma_j^2$.

### B. D-RSS Key Agreement Algorithm for V2V Communication

The D-RSS scheme presented in [2] is based on channel reciprocity theorem (which states that $h_{ij}(t)$ is highly correlated to $h_{ji}(t)$) and spatial decorrelation ($h_{ij}(t)$ is decorrelated from $h_{iz}(t)$) property. Based on the channel variations over time, the D-RSS scheme proposes the extraction of a secret bit 0 or 1 according to a decrease or increase of the RSS measured at every two instants of time. Obviously, the key extraction rate depends on the channel variation rate.

Figure 1 (top) illustrates a period where the RSS was collected in a multipath environment where the channels are highly correlated (approximately 0.9120 of correlation). However, an observer, called Eve, which is in a different location than Bob, observes different values of RSS in the Alice-Eve channel, compared to those observed by Bob on Alice-Bob channel, as shown in Figure 1 (bottom). It is observed that the curves are highly uncorrelated (approximately 0.1937 of correlation).

The D-RSS scheme from [2] is illustrated in Figure 2 and works as follows: When an increase between two RSS measures is observed, a bit 1 is generated. When it is observed a decrease, a bit 0 is extracted. This increase or decrease must be greater than $\epsilon/d$ where $\epsilon$ is a rough estimation of small fluctuations in the channel and $d$ corresponds to the number of segments used to obtain an average for the removal of small fluctuations [2]. If the increase or decrease is lesser or equal than $\epsilon/d$, no bit is generated, and we represent the indertemination by using the question mark symbol.

After performing the collection of a set of secret bits, Alice informs Bob about the positions where the samples were used to generate her secret bit, not the bits themselves. From these positions, Bob chooses the locations where he also

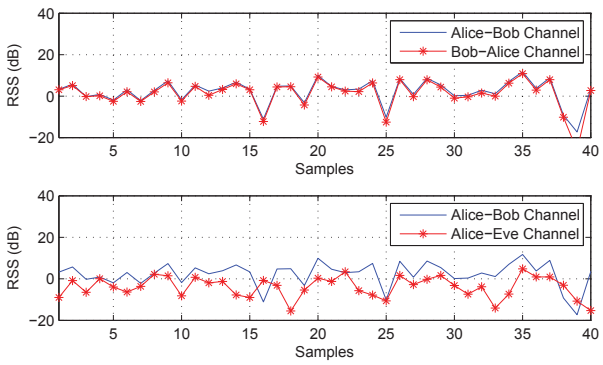


Fig. 1. Figure on top is an example of high-reciprocity of the channels. Figure on the bottom illustrates an example of poor channel reciprocity. Figure adapted from [2].

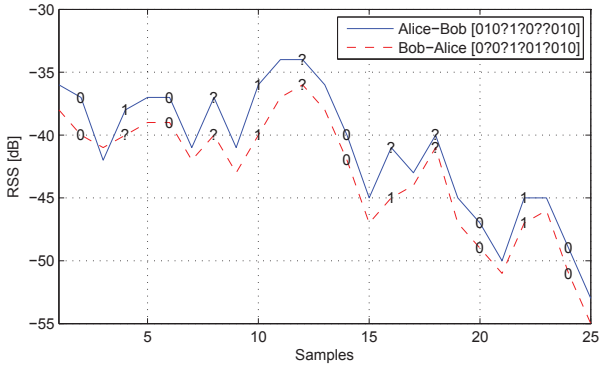


Fig. 2. Example of D-RSS key agreement scheme. Figure adapted from [2].

managed to extract secret bits and responds to Alice. Eve, however, should get the same values that Alice and Bob in the same positions chosen by both to compose the secret key. An example can be observed in Figure 2. Failure to extract a single secret bit prevents composing the necessary key to compromise the communication security between Alice and Bob. Thus, increasing the number of bits necessary to compose the secret key, it decreases the chance of Eve obtaining all bits in the instants of time selected by Alice and Bob, reducing the likelihood of Eve obtaining the secret key.

**Secure Extraction Rate:** We define the secure extraction rate, in bits per second, as the maximum rate a scheme can extract secret bits that are secure from Eve, that is, the bits that both Alice and Bob have simultaneously obtained but Eve has not. Every secret key or seed that was obtained by Eve is discarded, but the time it required to be generated impacts on the extraction rate.

*1) FH-based Key Agreement Algorithm for V2I Communication:* As presented in [2], the D-RSS scheme presented in the previous subsection does not perform well in situation where the channel variations are not fast enough, as is the case of the V2I scenario with slow fading. Thus, the authors of [2] propose another key agreement scheme to V2I, which is based on the frequency hopping (FH) method. In the FH-based scheme, both Alice and Bob randomly select a channel to establish communication out of the set of $c$

available channels. Everyone can communicate on multiple, non-interfering channels, but can only receive on a single channel at a given time. If they are on the same channel, the key information (seed) is transferred successfully and Bob sends an acknowledgment signal (ACK) to Alice. Otherwise, there is a timeout. Alice and Bob select other channels and repeat the process, where Alice uses different seeds for each transmission attempt. If Alice receives an ACK, she knows that the seed can be used. If not, she drops the seed. The probability that Alice and Bob are in the same channel is then $p = 1/c$. The probability of Eve listen to the seed received by Bob is $p_e = 1/c$. According to [2], to obtain a high level of security the scheme requires a large number of channels, which is impractical due to hardware constraints and the time required for a successful seed exchange increases with the number of channels. To address this problem, it is introduced a multiagreement scheme, where Alice and Bob will repeat the seed agreement multiple times. The process ends when Bob receives $s$ seeds. In the end, Bob selects all the seeds and uses an XOR operation to form the secret key. Which seeds were used is known to the server, allowing it to perform an XOR operation on the same seed set and retrieve the key. On the other hand, if Eve miss a single seed, she cannot form the same key.

The security in the FH is determined by the number of available channels $c$ for transmission and the amount of seeds $s$ used to compose a secret key. The probability function for Alice and Bob generate a secret key after $z$ exchange attempts becomes a Pascal distribution [10]:

$$P_Z(z) = \binom{z-1}{s-1} p^s (1-p)^{z-s}, \tag{2}$$

where $p = 1/c$ and the number of seed exchange attempts is expected to be

$$E[Z] = \frac{s}{p} = sc. \tag{3}$$

The probability for Eve generating the final key is $p_e = (1/c)^s$. Also, the seed's size determines the bit extraction rate, since a whole seed is transmitted in each transmission. The seed containing more bits will generate a final secret key with more bits, therefore safer. However, even when Eve does not overhear the entire seed, she can still get some information from the incomplete data [10]. So, the longer the seed transmission takes, the higher the possibility that the seed will be exposed.

## III. Proposed Scheme

Our proposal is to place multiple antennas at the RSU in order to artificially induces fast fading in the V2I scenario. The proposed scheme, which we refer to as MD-RSS, adopts the concept of multiple "dumb" antennas introduced in [9]. The term dumb comes from the fact that the multiple antennas are completely transparent to the users (in our case, the vehicles). Figure 3 shows an example of a slow fading channel, before and after applying the MD-RSS scheme.

Considering a system with $N$ transmit antennas at the base station and $h_{ij}^n(t)$ the complex gain of the channel between nodes $i$ and $j$ regarding the $n$-th antenna, in time slot $t$. The

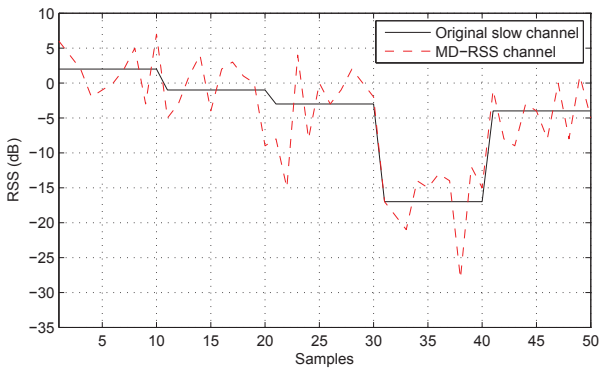


Fig. 3. Example of a channel, before and after being applied the MD-RSS scheme to transform a slow channel into a fast fading channel.

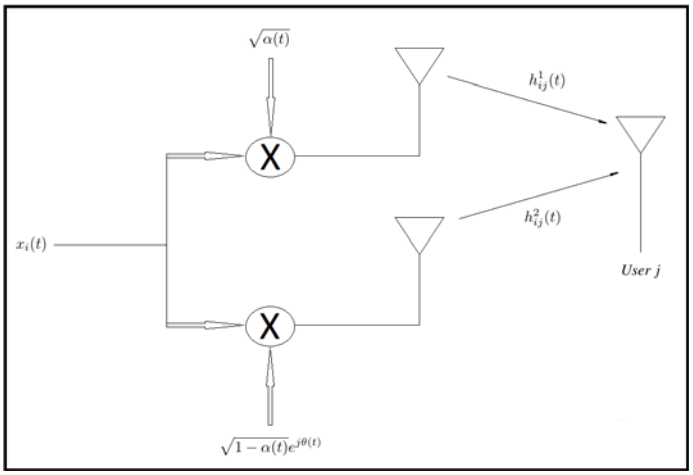


Fig. 4. Model of two antennas transmitting the same signal with time-varying phase and power. Figure adapted from [9].

RSU transmits the same frame $\mathbf{x}_i(t)$ by all the antennas, after multiplying it by a complex number $\sqrt{\alpha_n(t)}e^{j\theta_n(t)}$ at antenna $n$, for $n = 1, ..., N$, such that $\sum_{n=1}^{N} \alpha_n(t) = 1$, preserving the total power transmitted. This is illustrated in Figure 4 for the particular case with $N = 2$.

The signal received by the user $j$ is then given by:

$$\mathbf{y}_j(t) = \left( \sum_{n=1}^{N} \sqrt{\alpha_n(t)} e^{j\theta_n(t)} \, h_{ij}^n(t) \right) \mathbf{x}_i(t) + \mathbf{n}_j(t), \tag{4}$$

where $\alpha_n(t)$ and $\theta_n(t)$ are the power fractions and phase shifts allocated to each transmit antenna, respectively. The gain of the average channel seen by receiver $j$ is:

$$h_{ij}(t) = \sum_{n=1}^{N} \sqrt{\alpha_n(t)} e^{j\theta_n(t)} h_{ij}^n(t). \tag{5}$$

Thus, by varying these values over time - $\alpha_n(t)$ varies between 0 and 1 and $\theta_n(t)$ between 0 and $2\pi$, one can induce fluctuations in the mean channel even if the fluctuations in the channel $h_{ij}(t)$'s gains are very small. The rate of $\alpha_n(t)$ and $\theta_n(t)$ in time is defined in the system specification and should be sufficiently slow and occurring on a time scale that allows the channel to be estimated reliably by users and with SNR feedback. Measuring individually channel $h_{ij}(t)$'s

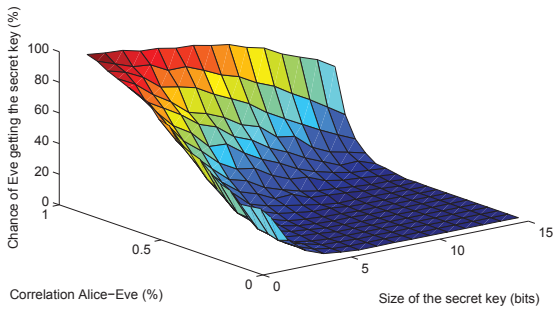


Fig. 5. Chance of Eve getting the secret key as a function of the Alice-Eve correlation and the size of the secret key, for $\epsilon = 3$, $d = 1$ and $N = 2$ antennas.

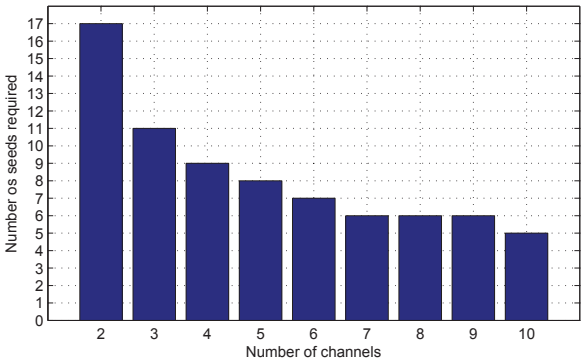


Fig. 6. Number of seeds $s$ required for each number of channels $c$ available in order to keep the secure secret key extraction error rate under $10^{-5}$.

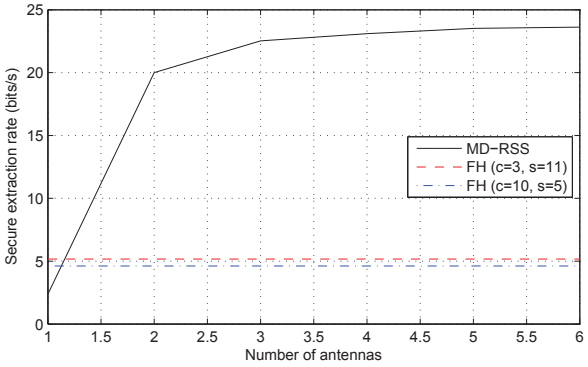


Fig. 7. Number of secure bits extracted per second as a function of the number of antennas at the transmitter.

gains is not required - phase or magnitude, since the existence of multiple transmission antennas is completely transparent to the receiver, where a single pilot signal is required for channel measurement. The pilots symbols are repeated by each transmitting antenna, just like the data symbols.

Factors influencing safety in RSS model with multiple antennas are the degree of correlation between Alice-Eve channel and the size, in bits, of the secret key. The correlation between the Alice-Bob channel determines the extraction rate of secret bits. In the RSS method with multiple antennas, the correlation of the channel between Alice and Eve will determine at which points of time Eve can extract secret bits from the received signal. However, these bits only have value when both Alice and Bob can extract them properly as well. Thus, the more correlated is the channel between Alice and Eve, the greater the chance, at a given time, that Alice, Bob and Eve all extract the same secret bit.

## IV. Numerical Results

In this section we provide some numerical results and discussion on the performance of the MD-RSS and FH key agreement schemes. We evaluate the frequency and sampled channel coefficients with their correlation matrices and numerically calculate the empirical secure secret bit extraction between Alice and Bob, based on our simulated time domain channel coefficients, for different channel environments.

Figure 5 presents the chance of Eve getting the secret key as a function of both the correlation Alice-Eve and the size of the secret key. As expected, Eve's capability in getting the secret key is severely reduced with the reduction in the correlation to Alice's channel. Moreover, it can also be seen that increasing the size of the secret key also reduces the chance of Eve extracting all the bits at the same time slots that Alice and Bob.

In the following results, we set the target secure secret key extraction error rate to be equal $10^{-5}$. For this value, the relationship between the number of channels $c$ and minimum number of seeds $s$ for the FH scheme is presented in Figure 6. Thus, we adopt the pairs $(c = 3, s = 11)$ and $(c = 10, s = 5)$ for the FH scheme in what follows.

The secure bits extraction rate between the MD-RSS and FH schemes is compared in Figure 7, where we set the FH to have 2 transmission per second, and each seed is 128 bits long. For the MD-RSS scheme, we assume 19,37% channel correlation between Alice and Eve, secret key is also 128 bits long and we vary the number of antennas $N$ from 1 to 10. Comparing the D-RSS scheme (which is equivalent to the MD-RSS scheme with $N = 1$ antenna) to the FH scheme, we can see that with the use of a single antenna the extracted bit rate is much lower than FH. However, as the number of antennas increases, there is a gain in rate, even with only two antennas. Nevertheless, it should be noted that such gain is not directly proportional to the number of antennas, that is, it can be observed that after a certain number of them, the bit rate tends to a finite ceiling value. Note also that the bit extraction rate for the frequency hopping method is not dependent on the number of transmit antennas and for two or more antennas, the MD-RSS scheme outperforms the secret bit extraction rate of FH.

For the next results, unless stated otherwise, we evaluate the MD-RSS by adopting $N = 2$ antennas, secret key 128 bits long and channel correlation between Alice and Eve set to 19,37%. In Figure 8 we evaluate the secure secret bit extraction rate versus the number of available channels $c$, for both MD-RSS (which does not depend on $c$) and FH schemes, considering that size of the seed $\in \{64, 128, 256\}$ bits and we are varying the number of available channels $c$ from 3 to 10. Even tough the MD-RSS scheme presented small change of

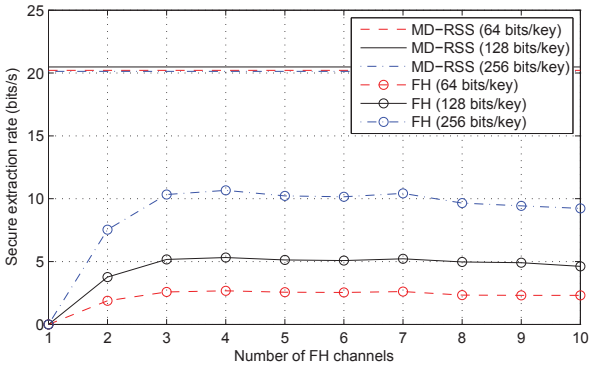


Fig. 8. Number of bits extracted per second, varying the number of frequency hopping's channels.

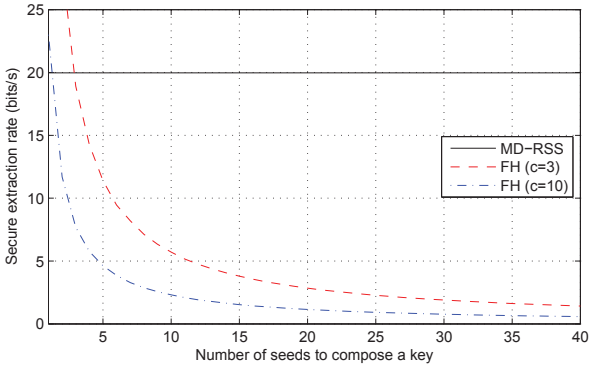


Fig. 9. Number of bits extracted per second, varying the number of seeds used to compose a key.

rate for different seed sizes, one can see that it provide a better secure secret bit extraction rate than the FH scheme, regardless the number of channels as well as the seed sizes under consideration. We can also note that increasing the number of channels in FH decreases the bit extraction rate decreases, while increasing the size of the seed offers better bit extraction rate.

Another variable that influences in the performance is the number of seeds $s$ required to form the secret key. This is illustrated in Figure 9. It can be seen that the number of extracted bits per second is constant for the MD-RSS, but the rate decreases for the FH as more seeds are need. Also, increasing the number of channels $c$ reduces the extraction rate. As the results show, the MD-RSS presents a higher extraction rate than FH. However, for $c = 3$ and $s < 3$, the FH results in better secure extraction rate, but greatly at the cost of security, since it is required at least $s = 11$ to guarantee the $10^{-5}$ error rate.

Finally, we compare in Figure 10 the two methods by varying the size of the seed up to 512 bits. For the FH model we note an increase of the rate as we increase the size of the seed, in bits, as expected. We can see that, for seeds over approximately 494 bits in size, $c = 3$ and $s = 11$, the FH method has a better bit rate than the MD-RSS scheme. However, according with [10], the longer the seed transmission

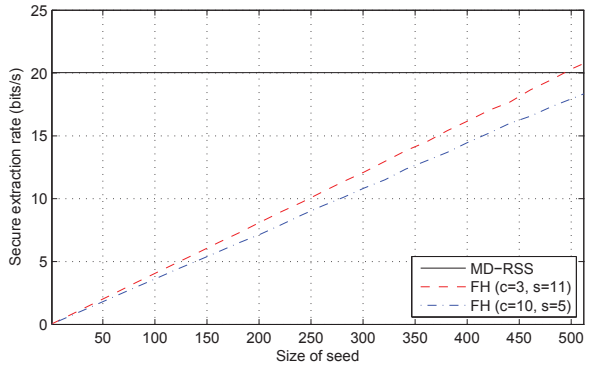


Fig. 10. Number of bits extracted per second, varying the size of the seed used to compose a key.

takes, the higher the possibility that the seed will be exposed.

As illustrated by the various forms of comparison, the proposed MD-RSS scheme, even with only two transmit antennas, is capable of outperforming the FH scheme in the bit extraction rate in a V2I scenario.

## V. Final Comments

In this paper, we proposed the use of multiple dumb antennas in a RSU of a V2I network in order to artificially increase the channel variation, turning a slow fading channel in a fast fading channel. This enabled us to apply a key agreement algorithm based on the channel variation (which we call MD-RSS) to the aforementioned scenario, showing that it is capable of outperforming a recently proposed frequency hopping-based scheme in terms of secure bit extraction rate.

## References

[1] H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, June 2008.

[2] B. Zan, M. Gruteser, and F. Hu, "Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems," *IEEE Transactions on Vehicular Technology*, 2013.

[3] A. Perrig, K. Szewezyk, V. Wen, D. Culler, and J. Tygar, "Spins: Security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, Sep 2002.

[4] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, Nov 1976.

[5] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. EUROCRYPT, New York, NY, USA*, 1985, pp. 335–338.

[6] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM Conf. CCS*, 2002, pp. 41–47.

[7] 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.

[8] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, March 2008, pp. 3013–3016.

[9] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antenas," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1277 – 1294, June 2002.

[10] B. Zan and M. Gruteser, "Random channel hopping schemes for key agreement in wireless networks," in *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, Sept 2009, pp. 2886–2890.