Outdoor secret key agreement scenarios using wireless MIMO fading channels

VICTOR YAKOVLEV  
State University of Telecommunications, St. Petersburg, Russia  
viyak@bk.ru

VALERY KORZHIK  
State University of Telecommunications, St. Petersburg, Russia  
val-korzhik@yandex.ru

PAVEL MYLNIKOV  
Research & Design Institute for Information Technology,  
Signaling and Telecommunications on Railway Transport, Saint-Petersburg, Russia  
paul.mylnikov@gmail.com

GUILLERMO MORALES-LUNA  
Computer Science, CINVESTAV-IPN, Mexico City, Mexico  
gmorales@cs.cinvestav.mx  
<http://delta.cs.cinvestav.mx/~gmorales>

The method of key sharing between a mobile unit and a base station through a wireless MIMO-based fading channel is investigated. The expressions to estimate the correct keybit agreement based on a quantization with the use of guard interval are proved. The generated key sequences are tested on pseudo randomness and improved by application of some transforms. It provides that these key sequences pass all NIST tests. A leakage of information on the key to eavesdropper is estimated in terms of correlation between signals received by legal users and eavesdropper. The parameters of key distribution protocol are optimized in order to maximized the key rate under the conditions of given probability key string agreement for legal users.

Keywords: Key distribution scenarios, MIMO fading channel, multi-phase detection, NIST tests.

1. Introduction

Secure transmission is still a concern for wireless mobile devices due to broadcast nature of signals. Although traditional secure systems employ private or public-key cryptography independently of physical transmission, there is a growing interest in physical layer security methods that exploit noisy telecommunication channels and channels with multi-path wave propagation.

In a pioneered paper [Wyner (1975)], Wyner introduced the wire-tap channel concept with two types of channels: the main channel (less noisy) and the wire-tap channel (more noisy). Wyner’s theorem states that under some (not very strong conditions) there exist such encoding and decoding procedures that reliable transmission
on the main channel and zero information leakage on the wire-tap channel can be
provided with an increasing of the coding block lengths if the transmission rate is less
than the so called secrecy capacity $C_s$. In the post-Wyner’s period there appear a lot of
paper devoted to a generalization of wire-tap channel models [Carleial and Hellman
(1985), Barros and Rodrigues (2006)] and to a specification of the amount of information
leaking to eavesdropper [Korzhik and V. Yakovlev (1981)]. But unfortunately it is still
unknown constructive encoding and decoding procedures providing a transmission rate
close to secrecy capacity. Next advance in the physical security area occurs due to
Maurer’s paper [Maurer (1993)] at the cost of public discussion between legitimate users.
Such approach allows to share secret keys between legitimate users even in the case
when the wire tapper observes a “better” channel than one used by the legitimate users
but only if the wire tapper is passive (that is in another words if legal channel is
authenticated). After a common key sharing the legitimate correspondents can use ideal
Shannon’s one-time pad cipher [Shannon (1949)].

The idea of a common key sharing and the execution of an ideal cipher is very
positive especially in the so called post-quantum period when it is assumed that many
cryptographic algorithms can be broken by a quantum computer [Micciancio and Regev
(2008)]. But such approach requires to share a very long secret key string before ideal
encryption. Moreover, in order to provide a secure key sharing that means to get a
negligible amount of Shannon information leaking to an eavesdropper about this key, it is
necessary to be sure that signal-to-noise ratio at the input of wire tapper receiver is fixed
and known for legitimate users. In order to avoid such strong requirements it has been
proposed to execute (for mobile users) a multipath wave propagation in some wireless
channels [Sayeed and Perrig (2008), Liu et al. (2011)]. Unfortunately if mobile unit stops
it may result in a very slow and small channel fluctuation. In order to take for granted
some given randomness level it would be better to create this randomness artificially by
means of legitimate users. In [Aono et al. (2005)] it has been proposed a method using
smart antenna excited randomly by electronic means. More detailed investigation of such
approach was undertaken in [Yakovlev et al. (2012)]. But this requires a special
construction of a Variable Directional Antenna.

The explosion of interest to multiple-input multiple-output (MIMO) systems soon
led to a realization that exploiting the available spatial dimensions can also enhance the
secrecy capabilities of wireless channels [Wallace and Sharma (2010)].

An advantage of MIMO system for key sharing is its property that a presence of
many antennas results in a better randomization even for very small transfer of mobile
units. It is worth to note that in contrast to communication system where a presence of
MIMO devices results in interference of signals at the receiving antennas, key sharing
occurs avoidable of such interference because in that case it is necessary to form any but
only coinciding key bits. The last property is provided thanks to the Reciprocity Theorem
of radio wave propagation between transmitting and receiving sides of MIMO-based
link. Further investigation of MIMO-based key distribution protocols (KDP) was
undertaken in [Li et al. (2007), Shafiee and Ulukus (2007)]. But a final solution of this
problem is very far from a termination. First of all it is requested to increase the key
generation rate providing simultaneously high secrecy and good statistical properties of
Outdoors secret key agreement scenarios using wireless MIMO fading-channels

the shared keys that should be close to truly random data. Namely solution of these questions forms the main contribution of our investigations undertaken in the current paper.

The remainder of the article is organized as follows. Section 2 describes the main scenarios of key distributions. The mathematical model of MIMO-based channel with random reflections is given in Section 3. Section 4 describes the algorithm for key distribution on the MIMO channel model. Investigation of key stream statistic and information leaking to eavesdropper appears in Section 5. Section 6 concludes the paper and poses open problems for further investigations. The appendix presents the proof of the relation for the error probability given in Section 4.

2. Main scenarios for key distribution under the existence of MIMO-fading channels

The scheme of a general scenario for key distribution between a mobile unit and a base station is presented in Fig. 1.

Fig. 1. The scheme of a general key distribution scenario between a mobile unit and a base station.

The mobile unit (MU) and the base station (BS) are supplied both by MIMO antenna devices, test signal generators and estimators of signal parameters for key extraction.

The mobile unit contains also a GPS receiver connected with an electronic map of the mobile unit traffic route. The radiation pattern controller allows to change in some cases the antenna diagram. It is assumed that an eavesdropper is able to intercept all information transmitted both from the base station or the mobile unit.
The movement of the mobile unit results in a changing of environment and as a consequence it changes the electromagnetic wave propagation conditions.

Several different models of MIMO channels corresponding to the description of this environment are well known. Among them are: green field [Tse and Viswanath (2005)], city canyon [Driessen and Foschini (1999)], group of random reflectors [Gesbert (2002)] including experimental statistical channel models WINNER II [Kyosti et al. (2007)], and some other developments. For the first two models it is typical a presence of direct visibility (Line-Of-Sight (LOS) scenario) between the mobile unit and the base station. In the model group of random reflectors, direct visibility is absent and the signal propagates from transmitter to receiver only due to scatters that are located randomly in the environment (Non-Line-Of-Sight (NLOS) scenario).

The key distribution protocol is initiated by the mobile unit. Next, using a GPS receiver, the MU investigates its current location on the electronic map and selects to which channels models above does it correspond. In the case of LOS scenario, it is performed a procedure known as beamforming. Then the MU antenna diagram is excited randomly by electronic means. (This approach was mentioned already in Section 1 and it has been studied in [Aono et al. (2005), Yakovlev et al. (2012)].) The same method can be recommended as well whenever the MU is stopped within some time period.

Let us consider in the next section the case when direct visibility is absent but there are a group of random reflectors.

3. Mathematical model of MIMO-based channel

We assume that a key distribution protocol (KDP) is performed between a mobile unit $A$ and a base station $B$ that have the same number of antennas $N_A$ and the signal power radiated of each antenna is equal to $P_s / N_A$.

For a frequency-flat fading MIMO channel, the commonly used discrete-time input-output relation for test-signal is given by

$$ y = Hs + z, $$

where $H$ is a square ($N \times N$)-matrix, $s$ is a transmitted test-signal ($N \times 1$)-vector, $y$ is a received signal ($N \times 1$)-vector, and $z$ is an additive noise ($N \times 1$)-vector at the MIMO channel output. Due to the Reciprocity Theorem, the relation for back channel:

$$ y' = H^T s + z'. $$
Outdoor secret key agreement scenarios using wireless MIMO fading-channels

However the elements of the matrix $H$ can change during the test signal transmission, generally speaking, and therefore in order to approximate equally channel matrices in direct and back channels it is necessary that the following inequalities hold [Biglieri et al. (2007)]:

$$\Delta t << T_c, \Delta f << B_c,$$

where $\Delta t$ is the delay in transmission between direct and back test signals, $\Delta f$ is the frequency (Doppler) shift, $T_c$ is the coherent time and $B_c$ is the coherent band width for the MIMO channel.

In order to specify the values of the matrix $H$, it is necessary to describe the channel model in detail.

Let us consider the multi-path MIMO channel model with Rayleigh fading according to [Yigit and Kavak (2012)] and presented in Fig. 2.

![Fig. 2. General model of MIMO channel between mobile unit and base station.](image)

We denote the number of rays as $L$ and denote by $\beta_l$ the attenuation in the $l$-th ray, by $\phi, \psi$ the transmitted and received angles, respectively, by $\Phi, \Psi$ the antenna diagram angles, and by $\omega$ the frequency shift due to mobile units transfer (Doppler effect). Then the matrix $H(t)$ of the test signal at time $t$ can be presented as

$$H(t) = \sum_{l=1}^{L} \beta_{l} (a_{R,l} a_{T,l}^T) e^{-j\omega t},$$

being

- $\beta_l = a e^{\psi}$: signal complex attenuation resulting by reflection in the $l$-th ray,
Yakovlev et al.

- \( a_{R,j}' \), \( a_{T,j}' \): response vectors in the \( j \)-th ray at the receiver and at the transmitter respectively.

\[
\begin{align*}
a_{R,j}' &= \left[ 1, e^{-j\Omega_{R,j}}, \ldots, e^{-j(\Omega_{R,j})^{N_{R,j}-1}} \right]^T, \\
a_{T,j}' &= \left[ 1, e^{-j\Omega_{T,j}}, \ldots, e^{-j(\Omega_{T,j})^{N_{T,j}-1}} \right]^T,
\end{align*}
\]

- \( \Omega_{T,j} = \left( \frac{2\pi}{\lambda} \right) d_r \sin \phi_r \): angular receiver frequency,
- \( \Omega_{R,j} = \left( \frac{2\pi}{\lambda} \right) d_s \sin \psi_s \): angular transmission frequency,
- \( \lambda \): wave length corresponding to carrier frequency,
- \( d_r \): diversity interval between receiving antennas, and
- \( d_s \): diversity interval between transmission antennas.

A typical example of the above channel model is the octal-rays model of the railway telecommunication system having 8 antennas with distances \( \lambda/2 \), between them, mobile object speed 100 km/h, \( \Phi = 28^\circ \), \( \Psi = 180^\circ \), and carrier frequency 2.6 GHz [Guan et al. (2011)].

Investigation of such model has been undertaken in many papers (e.g. [Jakes and C. Cox (1994), Guan et al. (2011)] and others). Results of our investigations show that the entries of matrix \( H \) can be correctly approximated by zero mean Gaussian distribution with equal variances.

The space correlation is determined just by mutual antenna locations. The space-time correlation can be presented following to the results of [Bakulin et al. (2014), Biglieri et al. (2007)] as

\[
R_{H}(t) = R_{H} \rho(t),
\]

where \( R_{H} \) is the matrix of space correlation between antennas, and \( \rho \) is the time correlation function of antenna signals. For Jakes fading model [Jakes and C. Cox (1994)], the function \( \rho \) can be determined as

\[
\forall t : \rho(t) = J_0 \left( 2\pi f_D(t) \right),
\]

where \( f_D \) is the Doppler spread and \( J_0 \) is the Bessel function of zero order.

4. KDP based on MIMO channel model

The KPD is described in the following steps:
Outdoor secret key agreement scenarios using wireless MIMO fading-channels

1. Estimation of the environment on the electronic map and a selection of MIMO channel model by MU.
2. For the case of direct visibility, the MU sends the test signal to the BS forming random diagram by electronic means. For the case of the NLOS scenario, the MU sends the test signal using MIMO based channel.
3. The BS calculates some parameter of the received signals.
4. Just after step 3, the BS sends the same test signal to the MU.
5. The MU calculates the same (selected in advance by both users) parameters of the received signals.
6. Both users BS and MU form the key bits from the found parameters using a quantization procedure (see in sequel).

It is worth to note that the knowledge of the MIMO-based channel model parameters can be ignored in KDP design if during its execution time these parameters are approximately constant. But this knowledge is necessary to estimate a reliability of KDP (the probability of key bits coincidence for both correspondents), the statistical properties of key strings and its security (in terms of the key information leakage to an eavesdropper near users A and B).

We can see from relation (1) that each coordinate $y_i$ of the vector $y$ is a complex Gaussian random value with amplitude $\mu_i = \sqrt{\Re(y_i)^2 + \Im(y_i)^2}$ (here $\Re$ and $\Im$ are the maps that take the real and the imaginary parts of a complex number) and phase $\theta_i = \tan^{-1}\left(\frac{\Im(y_i)}{\Re(y_i)}\right)$. These variables have Rayleigh distribution and uniform distribution, respectively. It has been proved in [Yakovlev et al. (2011)] that phases are less correlated versus distance between legal users and eavesdroppers than amplitude. Therefore our selection as parameter for the key bit generation, namely the phase quantization procedure into $q$ integers, is determined as:

$$\begin{align*}
\text{if } & \theta_i \in \left[\frac{2\pi(q-1)}{Q}, \frac{2\pi q}{Q}\right] \text{ with } 1 \leq q \leq Q, \\
\text{then } & f_Q(\theta_i) = q,
\end{align*}$$

where $Q$ is the number of quantization levels. Then the probability of an integer $q$ equals $1/Q$. Since the channel noise results in a transition from $q$ to $q'$, with $q'$ $\neq q$, and it is more likely closer to the bounds of the decision areas in (2), we propose to introduce guard intervals between decision areas as key symbols may be erased. Then the decision function (2) can be modified as:
Let us consider one of the decision areas (or sector) in Fig. 3, determined by $y_i = (\mu_i, \theta)$, $x_i = Hs = (a_i, \phi_i)$, $z_i = (b_i, \psi_i)$. Under the decision taken about the phase $\phi_i$ when $y_i$ is received, the following events may occur:

- $y_i$ is in the same area that the vector $x_i$ (correct decision area with angle $\Omega - \gamma$),
- $y_i$ belongs to the guard interval (erasure area with angle $\gamma$),
- $y_i$ appears outside of both previous areas (incorrect decision).

Let us denote the probabilities of previous events by $P_{cor}$, $P_{er}$, $P_{error}$, respectively.

It is proved in the Appendix that
Outdoor secret key agreement scenarios using wireless MIMO fading-channels

\[
 F(\phi) = \int_{\frac{\phi - \gamma}{\frac{\pi}{2}}}^{\frac{\phi + \gamma}{\frac{\pi}{2}}} \left[ 1 + \frac{h \tan \left( \frac{\phi + \frac{\pi}{2}}{2} \right)}{\sin \psi} \right]^{-1} d\psi ,
\]

(3)

where \( P_{\text{cor}} \) is given by eq. (A.10) in the Appendix after combining (A.5)–(A.9).

In Fig. 4 there are plotted the dependences of \( P_{\text{cor}}, P_{\text{er}}, P_{\text{error}} \) with respect to signal to noise ratio for \( Q = 8 \) and different guard intervals (GI) that were calculated after numerical computations of corresponding integrals. We observe that it is possible to trade off \( P_{\text{error}} \) to the value of the guard interval but it affects also on \( P_{\text{er}} \). Hence there appears the problem of KDP parameters optimization, given some final requirements, as key generation rate maximization for given SNR and the number of antennas \( N_{\text{t}} \) in MIMO system. From Fig. 4, it can be seen that a guard interval (GI) allows to decrease the error probability but simultaneously the probability of erasure increases. (We remark that it is not obtained a precise expression for the corresponding probabilities but some bounds, namely an upper bound for \( P_{\text{error}} \), a lower bound for \( P_{\text{er}} \) and lower bound for \( P_{\text{cor}} \) because it was not taken into account that correct key bits can be obtained sometimes even if both legal users got incorrect phase. But such incorrectness is acceptable).

In reality a final decision about key bit has to be taken no by the single user B but by both users A and B. Thus the final probabilities \( P_{\text{cor}}, P_{\text{er}}, P_{\text{error}} \) should be changed as:

Fig. 4. Curves of \( P_{\text{cor}}, P_{\text{er}}, P_{\text{error}} \) against the values of SNR for \( Q = 8 \).
\[ P_{\text{cor}}^* = P_{\text{cor}}(A) \cdot P_{\text{cor}}(B), \]

\[ P_{\text{error}}^* = P_{\text{error}}(A) \cdot P_{\text{cor}}(B) + P_{\text{error}}(B) \cdot P_{\text{cor}}(A) + P_{\text{error}}(A) \cdot P_{\text{error}}(B), \]

\[ P_{\text{er}}^* = 1 - P_{\text{cor}}^* - P_{\text{error}}^*. \]

The KDP should be also slightly corrected under the condition of symbol erasures. Namely the numbers of the erased symbols are transmitted from both users to opposite ones in addition and an extra signal should be transmitted if it is necessary. A relation for the probability \( P_{n_0}(k) \) of the correct key bit string sharing of length \( n_0 \) is:

\[ P_{n_0}(k) = \left( \frac{P_{\text{cor}}^*}{1 - P_{\text{er}}^*} \right)^{n_0} \log Q, \]

where \( Q \) is the number of quantization levels. The key bit stream rate for the use of all \( N_A \) antennas is

\[ R = N_A \log_2 Q \left( 1 - P_{\text{er}}^* \right) \frac{\text{bit}}{\text{sample}}. \]

Then the following optimization problem arises:

\[ \left( \gamma^*, Q^*, N_A^*, h_{2*}^* \right) = \arg \max R_{\gamma, Q, N_A} \]

subject to the restrictions \( P_{\ell}(k) \geq P_{\ell}(k)_{\text{reqmin}}, \gamma \in [0, \frac{2\pi}{Q}], Q \in [2, Q_{\text{max}}], N_A \in [1, (N_A)_{\text{max}}], \) and \( h \in [1, (h_{2*})_{\text{max}}], \) where the values \( P_{\ell}(k)_{\text{reqmin}}, Q_{\text{max}}, (N_A)_{\text{max}}, (h_{2*})_{\text{max}} \) have to be conditioned by the general requirements of the MIMO system design.

The solution of problem (6) has been found by the branch and bound algorithm [Land and G. Doig (1960)].

In Fig. 5 there are presented the dependences \( R \) from SNR under the conditions \( n_0 = 256, P_{\ell}(k)_{\text{reqmin}} = 0.9, 0.95 \) and 0.99, and \( N_A = 1, 2, 4, 8, 16. \)
Outdoor secret key agreement scenarios using wireless MIMO fading-channels

In Table 1 the optimal values for $a = \frac{\gamma}{\Omega}$ and $Q$ are displayed maximizing the rate $R$ for a given SNR.

\[ a) \quad P_{n}(k)_{\text{requested}} = 0.9 \]

\[ b) \quad P_{n}(k)_{\text{requested}} = 0.95 \]
Table 1. Optimal parameters $\gamma$ and $Q$ providing the maximum rate $R$ for a given SNR.

Fig. 5. The key sharing bit rate of the length 256 bits with $P_{n_0}(k)_{\text{requested}} \in \{0.9, 0.95, 0.99\}$ for optimization of the system parameters.
Outdoor secret key agreement scenarios using wireless MIMO fading-channels

An analysis of the curves in Fig. 5 shows that the key generation rate $R$ increases with an increasing of the number of antennas in the MIMO-based channel. Key generation rate increases obviously as SNR increases. For every SNR value there exist optimal number of phase quantization levels and value of guard interval providing the requested probability of correct key sharing for both legal users.

5. Investigation of keystream statistic and information leaking to eavesdropper

The statistics of the key stream distributed due to KDP is very important because if it is very far from uniform distribution it may result in effective attacks for cipher breaking. In order to investigate the key stream statistic after phase quantization from different antennas they will be combined in a serial sequence containing bits from all antennas and this sequence was investigated by statistical tests. In Fig. 6 there are presented the empirical density distributions for the length of binary strings from 1 to 16.
In order to get this distribution, it was investigated the sequence of length $10^6$ bits obtained for the WINNER II model with the use of the following parameters:

- SNR: 36 dB;
- number of quantization levels: $Q = 4$;
- value of guard interval (GI): 24%;
- number of antennas $N_{MU} = N_{BS} = 4$.

From Fig. 6 it is clear that the length of the key sequence $\ell \geq 3$, the block probability distributions are not uniform. In fact, for $\ell \geq 5$ there are even peaks on some subsequences. It was calculated the values of entropy function for the sequences of fixed length $\ell$ with the use of well-known formula [Shannon (1949)]:

$$H(x) = \sum_{i=1}^{2^\ell} p_i^{(\ell)} \log_2 p_i^{(\ell)},$$

where $p_i^{(\ell)}$ is the probability of the $i$-th key subsequence of length $\ell$. As we can see, the entropy function values differ from those which should be equal to $\log_2 \ell$ for uniformly distributed key sequences.
Outdoor secret key agreement scenarios using wireless MIMO fading-channels

In order to improve the statistics of the key string it was undertaken two types of deterministic transforms recommended in [Schneier (1995)]. The first type is the so called transposition of symbols and the second transform is adjacent bit XOR-ing. The results of testing after such transforms are presented in Table 2 in which were used some NIST STS tests [Bassham et al. (2010)]. We see that after both transforms the key bit sequence passes the most of NIST tests.

Now let us face with the eavesdropping problem and let us assume that the following parameters hold [Guan et al. (2011)]:

- frequency carrier: 2600 MHz;
- MIMO antennas: 8 × 8;
- distance between MIMO antennas at the departure unit: 0.5\(λ\);
- distance between MIMO antennas at the arrival unit: 0.5\(λ\);
- number of rays: 8;
- departure ray angle: 28°;
- arrive ray angle: 180°;
- speed of mobile unit motion: 50 km/h;
- number of simulated channel matrices: 1000.

The mutual correlation \(r\) between the phases of legal user \(B\) and an eavesdropper located at a distance \(d\) from \(B\) (in terms of wave length factors) is presented in Fig. 7.

![Fig. 7. Mutual correlation between phases of legal user and eavesdropper against distance between them in terms of wave length factors.](image)
We see from this figure that in line with similar results presented in [Yakovlev et al. (2012)] the correlation has not a monotonically decreasing dependence from \( d \) but it has a randomly-looking dependence. But in contrast to [Yakovlev et al. (2012)] it has significantly less values from all distances between \((0.1\lambda, \ldots, 20\lambda)\). This is a consequence of the multi-phase functional used for key bit generation and another channel model. Thus, we can believe that it can be neglected an opportunity of key eavesdropping in large area of eavesdropper locations. (It is worth to note that if phase had Gaussian distribution and even for binary quantization values it would be results in the error probability for eavesdropper about one key bit near 0.47 [Yakovlev et al. (2012)] that it is very close to “break of eavesdropper channel”.)

Table 2. Experimental testing based on NIST STS of the key sequences after two types of transforms.

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Name of test</th>
<th>Transposition</th>
<th>TXOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Frequency (Monobit) Test</td>
<td>10/10</td>
<td>10/10</td>
</tr>
<tr>
<td>2</td>
<td>Frequency Test within a Block</td>
<td>10/10</td>
<td>10/10</td>
</tr>
<tr>
<td>3</td>
<td>The Runs Test</td>
<td>9/10</td>
<td>10/10</td>
</tr>
<tr>
<td>4</td>
<td>Tests for the Longest-Run-of-Ones in a Block</td>
<td>0/10</td>
<td>10/10</td>
</tr>
<tr>
<td>5</td>
<td>The Binary Matrix Rank Test</td>
<td>10/10</td>
<td>10/10</td>
</tr>
<tr>
<td>6</td>
<td>The Discrete Fourier Transform (Spectral) Test</td>
<td>0/10</td>
<td>9/10</td>
</tr>
<tr>
<td>7</td>
<td>The Non-overlapping Template Matching Test</td>
<td>1/10</td>
<td>8/10</td>
</tr>
<tr>
<td>8</td>
<td>The Overlapping Template Matching Test</td>
<td>0/10</td>
<td>10/10</td>
</tr>
<tr>
<td>9</td>
<td>Maurer’s “Universal Statistical” Test</td>
<td>10/10</td>
<td>10/10</td>
</tr>
<tr>
<td>10</td>
<td>The Linear Complexity Test</td>
<td>5/5</td>
<td>7/7</td>
</tr>
<tr>
<td>11</td>
<td>The Serial Test</td>
<td>5/5</td>
<td>7/7</td>
</tr>
<tr>
<td>12</td>
<td>The Approximate Entropy Test</td>
<td>0/10</td>
<td>10/10</td>
</tr>
<tr>
<td>13</td>
<td>The Cumulative Sums (Cusums) Test</td>
<td>3/10</td>
<td>10/10</td>
</tr>
<tr>
<td>14</td>
<td>The Random Excursions Test</td>
<td>1/10</td>
<td>10/10</td>
</tr>
<tr>
<td>15</td>
<td>The Random Excursions Variant Test</td>
<td>10/10</td>
<td>10/10</td>
</tr>
</tbody>
</table>

TXOR: Transposition plus XOR of adjacent bits. The numerators of fractions are number of “passed” tests and the denominators are the total number of tests.

6. Conclusion

We considered different scenarios for key distribution protocols between base station and mobile unit connected through MIMO fading channel. The main attention has been focused on a study of Winner channel model with reflection of electromagnetic waves. Key distribution protocol has been proposed where the feature of key bit generation is based on a quantization procedure with the usage of guard interval. After an optimization of KDP parameters we get that it can provide a key sharing of size 256 bits and with the probability of its reliable performance about 0.99 for SNR equal to 35 dB, and 16 antennas after execution of about 74 test signals on average.

It was also shown that key sequence after simple transforms is very close to i.i.d. one because it satisfied to all NIST tests. Interception of key sequence by eavesdropper is prevented by a very small correlation between phases of legal users and eavesdroppers if the distance between them is not lesser than 0.5\(\lambda\).
Outdoor secret key agreement scenarios using wireless MIMO fading-channels

It is worth to note that a presence of massive MIMO fading channel gives a significant improvement of KDP in comparison of single antennas because it results in a larger key distribution rate and better approaching of key string to i.i.d. sequence.

We believe that a future work can be undertaken in order to increase the key distribution rate and to short a delay in its delivering at the cost of the of error correction codes application.

References


Proof of formula (3)

Let us consider one of the decision areas, namely $\angle TOL = \Omega$ (see Fig. 8). Assume that the vector $y$ is in the sector $\angle SOX$ (area $D_1'$) and that it is a sum of the vectors $x$ and $z$. Then the error for taking a decision on the phase of $y$ occurs if $y$ lays on the axis $OS$ or at left to it. This event will occur if and only if:
Outdoor secret key agreement scenarios using wireless MIMO fading-channels

\[
\angle BOA \geq \angle SOA = \Omega - \varphi + \frac{\gamma}{2}.
\]  

(A.1)

Let us draw the perpendicular from the point B on the axis OX. Then \(BC = b\sin(\pi - \psi) = b\sin\psi\), \(AC = -b\cos\psi\). We have

\[
\angle BOA = \tan^{-1} \frac{BC}{a - AC} = \tan^{-1} \frac{b\sin\psi}{a + b\cos\psi},
\]

(A.2)

where \(a\) is the amplitude of vector \(x\), and \(b\) is the amplitude of vector \(z\). By substituting (A.2) into (A.1) we get

\[
\frac{b\sin\psi}{a + b\cos\psi} \geq \tan \left( \Omega - \varphi + \frac{\gamma}{2} \right).
\]

If \(a \gg b\) (which is very likely) then the term \(b\cos\psi\) can be neglected and it results in the following condition to produce error:

\[
u := \frac{b}{a} \geq \frac{\tan \left( \Omega - \varphi + \frac{\gamma}{2} \right)}{\sin \psi} = l_{\Omega - \varphi, \psi}.
\]
Let us denote by \( f(u) \) the probability density of the random variable \( u \). Then the error probability \( P_{\text{error}} \), of event that the received vector \( y \) lies at the left of line \( OS \), can be expressed by the following formula, on the assumption that phases \( \phi \) and \( \psi \) are distributed uniformly:

\[
P_{\text{error}}^I = \frac{1}{\Omega} \int_0^\Omega d\phi \frac{1}{2\pi} \int_{\Omega-\phi+\frac{\gamma}{2}}^{\infty} d\psi \int_{\Omega-\phi,\psi} f(u) du.
\]  

(A.3)

(thesuperindex \( I \) emphasizes that it is true whenever the received vector occurs to the left of line \( OS \)).

For the area \( D_1'' = \angle LOX \), we can repeat the derivation of (A.3) in order to get
Outdoor secret key agreement scenarios using wireless MIMO fading-channels

\[ P_{error}^{II} = \frac{1}{\Omega} \int_0^\Omega \frac{1}{2\pi} d\phi \int_{\pi}^{2\pi-\phi+\frac{\gamma}{2}} d\psi \int_{l_{\psi,\phi}}^\infty f(u) du. \] (A.4)

Let us specify the formula for the probability of correct decision after quantization and introducing of guard interval. We can see such areas at Fig. 8. Having received the vector \( y \) we get the following cases:

1. \( x \in D_1, y \in D_1 \), with \( D_1 = D_1' \cup D_1'' \). After repeating the procedure to obtain (A.3) and (A.4), we get

\[ P_{cor, D_1} = \frac{1}{\Omega} \int_0^{\frac{\gamma}{2}} d\phi \frac{1}{2\pi} \int_{\frac{\phi-\frac{\gamma}{2}}{2}}^{2\pi-\phi+\frac{\gamma}{2}} d\psi \int_{l_{\psi,\phi}} f(u) du. \] (A.5)

2. \( x \in D_2 \cup D_3, y \in D_1 \), with \( D_1 = D_1' \cup D_1'' \). After repeating the procedure to obtain (A.3) and (A.4), we get

\[ P_{cor, D_2 \cup D_3} = \frac{1}{\Omega} \int_0^{\frac{\gamma}{2}} d\phi \frac{1}{2\pi} \int_{\frac{\phi-\frac{\gamma}{2}}{2}}^{2\pi-\phi+\frac{\gamma}{2}} d\psi \int_{l_{\psi,\phi}} f(u) du. \] (A.6)

3. \( x \in D_1, y \in D_0 \). In such situation the vector \( x \) transfers to the area of correct decision from the area of erasure due to noise.

\[ P_{cor, D_0} = \frac{1}{\Omega} \int_0^{\frac{\gamma}{2}} d\phi \frac{1}{2\pi} \int_{0}^{\frac{\gamma}{2}} d\psi \int_{0}^{\infty} f(u) du = \frac{(\Omega - \gamma)^2}{\Omega \cdot 2\pi}. \] (A.7)

4. \( x \in D_2, y \in D_0 \) (in this case, \( D_2 \) and \( D_0 \) are intersected)
\[ P_{\text{cor} \ D_2 \rightarrow D_0} = \frac{1}{\Omega} \int_{0}^{\frac{\gamma}{2}} d\varphi \frac{1}{2\pi} \int_{\frac{\gamma}{2}}^{\infty} dy \int_{l_{\varphi,y}} f(u) du. \] (A.8)

5. \( x \in D_3, y \in D_0 \). It is easy to see that

\[ P_{\text{cor} \ D_3 \rightarrow D_0} = P_{\text{cor} \ D_2 \rightarrow D_0}. \] (A.9)

Combining (A.5)–(A.9) we get:

\[ P_{\text{cor}} = P_{\text{cor} \ D_1} + P_{\text{cor} \ D_2 \cup D_3} + P_{\text{cor} \ D_0} + 2P_{\text{cor} \ D_2 \rightarrow D_0}. \] (A.10)

It is very easy to see that \( P_{\text{erase}} = 1 - P_{\text{cor}} - P_{\text{error}}. \)

In order to prove the relations (A.3)–(A.8) in a closed form it is necessary to derive the probability density function of the random variable \( u = b/a \), where \( a \) and \( b \) have the Rayleigh distribution and they are mutually independent. This means:

\[ f(a) = \begin{cases} \frac{a}{\sigma_a^2} e^{-\frac{a^2}{2\sigma_a^2}} & \text{if } a \geq 0 \\ 0 & \text{if } a < 0 \end{cases}, \quad f(b) = \begin{cases} \frac{b}{\sigma_b^2} e^{-\frac{b^2}{2\sigma_b^2}} & \text{if } b \geq 0 \\ 0 & \text{if } b < 0 \end{cases} \]

The distribution function of \( u \) can be found as follows [Ventsel (2000)]:

\[ f(u) = \int_{0}^{\infty} a e^{-\frac{a^2}{2\sigma_a^2}} e^{\frac{au}{\sigma_a^2}} da = \int_{0}^{\infty} u e^{-\frac{u^2}{2\sigma_b^2}} e^\frac{u^2}{2\sigma_b^2} da = \int_{0}^{\infty} u e^{-\frac{u^2}{2\sigma_b^2}} da. \] (A.11)

Let us write \( r = \left( \frac{1}{2\sigma_a^2} + \frac{u^2}{2\sigma_b^2} \right) \), then we get

\[ f(u) = \frac{u}{\sigma_a^2 \sigma_b^2} \int_{0}^{\infty} a^3 e^{-ra^2} da. \] (A.12)
The indefinite integral in (A.12) is [Gradshteyn and Ryzhik (2007)]

\[ \int r^2 e^{-ra^2} \, dr = \frac{ra^2 + 1}{2r^2} e^{-ra^2}. \] (A.13)

By substituting (A.13) into (A.11) and passing to definite integral we can write

\[
f(u) = \frac{u}{\sigma_a^2 \sigma_b^2} \left( \frac{ra^2 + 1}{2r^2} e^{-ra^2} \right)_{r=0}^{\infty} = \frac{u}{\sigma_a^2 \sigma_b^2} \left( -\frac{1}{2r^2} \right) \\
= \frac{u}{2\sigma_a^2 \sigma_b^2} \left( \frac{1}{2\sigma_a^2} + \frac{u^2}{2\sigma_b^2} \right)^2 = \frac{4u(\sigma_a^2 \sigma_b^2)^2}{2\sigma_a^2 \sigma_b^2 \left( u^2 \sigma_a^2 + \sigma_b^2 \right)^2} \\
= \frac{2u^2 \sigma_a^2 \sigma_b^2}{(u \sigma_a^2 + \sigma_b^2)^2}. \]

Thus the probability density function for ratio of two Rayleigh variables is

\[ f(u) = \frac{2u^2 \sigma_a^2 \sigma_b^2}{(u \sigma_a^2 + \sigma_b^2)^2}. \] (A.14)

Denoting \( \delta^2 = \frac{\sigma_b^2}{\sigma_a^2} \), the noise to signal ratio, we get

\[ f(u) = \frac{2\delta^2 u}{(\delta^2 + u^2)^2}. \] (A.15)

In Fig. 9, the probability density function by (A.15) is presented.
We can see from Fig. 9 that the probability density function of two Rayleigh variables is very close to a Rayleigh distribution.

Substituting (A.15) into (A.3) and (A.4) we obtain

\[
P_{\text{error}} = \frac{1}{2\pi\Omega} \int_0^\Omega d\phi \int_{\phi+\frac{\gamma}{2}}^{\frac{\pi-\phi-\frac{\gamma}{2}}{}2} d\psi \int_0^\infty \frac{2\delta^2 u}{\sin \psi (\delta^2 + u^2)^2} du. \tag{A.16}
\]

Last integral in (A.16) can be expressed in a closed form:

\[
\int \frac{2\delta^2 u}{(\delta^2 + u^2)^2} du = -\frac{\delta^2}{\delta^2 + u^2}.
\]

Then we get for the definite integral

\[
\int_{\phi}^{\phi+\frac{\gamma}{2}} \frac{2\delta^2 u}{\delta^2 + u^2} du = \left[ \frac{1}{1+(hV)^2} - \frac{1}{1+(hW)^2} \right], \tag{A.17}
\]
where $h = \frac{1}{\delta}$ is the signal-to-noise ratio. Substituting (A.17) into (A.16) we get finally

$$P_{\text{error}} = \frac{1}{2\pi \Omega} \int_0^{2\pi} d\varphi \int_{\varphi + \frac{\gamma}{2}}^{2\pi - (\varphi + \frac{\gamma}{2})} \left[ 1 + \frac{h \tan \left( \frac{\varphi + \gamma}{2} \right)}{\sin \psi} \right]^2 d\psi.$$  

Q.E.D.