SCIENCE CHINA
Information Sciences

• LETTER •

April 2017, Vol. 60 049301:1–049301:3
doi: 10.1007/s11432-016-0253-x

A random linear code based secure transmission scheme for wireless fading channels

Lukman A. OLAWOYIN[1,2*], Nana ZHANG[1], A. O. OLOYEDE[2], Nasir FARUK[2] & Hongwen YANG[1]

[1]*Wireless Communication Center, Beijing University of Posts and Telecommunications, Beijing* 100876*, China;*
[2]*Department of Telecommunication Science, University of Ilorin,* PMB 1515*, Nigeria*

Received April 19, 2016; accepted July 22, 2016; published online November 28, 2016

Citation Olawoyin L A, Zhang N N, Oloyede A O, et al. A random linear code based secure transmission scheme for wireless fading channels. Sci China Inf Sci, 2017, 60(4): 049301, doi: 10.1007/s11432-016-0253-x

Dear editor,

Wireless transmissions are vulnerable to potential security threats such as eavesdropping and wiretapping since unauthorized reception is facilitated through wireless channels [1]. Traditional system security is mainly implemented in the higher layers of the communication protocol stack, relying on authentication and cryptography [2]. The recent researches explore security in the physical layer [3], which can help to protect the information in wireless transmission and prevent the unauthorized nodes from illegally receiving and extracting confidential messages. In particular, channel coding can play an important role in the techniques for physical-layer security. For example, Chen in [4] proposed secure wireless network coding to achieve physical-layer security at routers by taking advantages of interference and noise. Application of Reed Solomon (RS) code and vector coding is presented in [5], the use of scrambled code and automatic repeat request (ARQ) is proposed by [6].

In a wireless network system, the packet losses at the intended receiver and the eavesdropper are generally independent due to the independence of the thermal noise and channel fading. Based on this fact, a random linear code based secure approach is proposed in this letter where the data symbols of the transmitter (Alice) are encoded with the generators determined by the receiver (Bob). The code is constructed in a way that it would be difficult for an eavesdropper (Eve) to decode the data symbol unless it has ability to intercept all the two way transmissions between Alice and Bob. Hence, very low crack probability can be achieved.

Proposed secure transmission scheme. Consider a wireless transmission between Alice and Bob in the presence of a passive eavesdropper Eve which attempt to overhear the conversation from wireless signal.

Alice has K data symbols $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_K$ to be transmitted to Bob. Each data symbol, $\boldsymbol{x}_k$, is a binary row vector containing N bits and the whole data symbols can be expressed as a $K \times N$ matrix:

$$\boldsymbol{X} = (\boldsymbol{x}_1^{\mathrm{T}}, \boldsymbol{x}_2^{\mathrm{T}}, \ldots, \boldsymbol{x}_k^{\mathrm{T}}, \ldots, \boldsymbol{x}_K^{\mathrm{T}})^{\mathrm{T}}. \quad (1)$$

Instead of sending data symbols $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_K$ directly over the unreliable and unsecured wireless channel, Alice sends code symbols $\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_n, \ldots, \boldsymbol{s}_K$, which are linear combina-

* Corresponding author (email: lolawoyin@bupt.edu.cn)
The authors declare that they have no conflict of interest.

tions of data symbols:

$$\boldsymbol{s}_n = \boldsymbol{g}_n \boldsymbol{X}, \tag{2}$$

where n is the index of the code symbol; $\boldsymbol{g}_n$, a binary row vector of length K, is the generator for code symbol $\boldsymbol{s}_n$.

Define a set $\mathcal{B} = \{(\boldsymbol{g}_n, \boldsymbol{s}_n)\}$ such that $(\boldsymbol{g}_n, \boldsymbol{s}_n) \in \mathcal{B}$ implies Bob has correctly received a code symbol $\boldsymbol{s}_n$ which is encoded with $\boldsymbol{g}_n$. We assume that the packets exchanged between Alice and Bob contain necessary control fields and numberings such that Bob can correctly associate each received $\boldsymbol{s}_n$ with corresponding index n and generator $\boldsymbol{g}_n$.

For each code symbol $\boldsymbol{s}_n$, the generator $\boldsymbol{g}_n$ is chosen by Bob and is sent to Alice via the wireless channel. Bob chose $\boldsymbol{g}_n$ with following rules:

R1. All generators are chosen by random (pseudo-random).

R2. The weight of $\boldsymbol{g}_n$ is even for $n = 1, 2, \ldots, K-1$ and is odd for $n = K$.

R3. $\boldsymbol{g}_n$ is linearly independent with all $\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_{n-1}$ in $\mathcal{B}$.

Among these rules, R1 is to prevent Eve from knowing g_n by a priori or deducing it from packet numbering. R2 prevents Eve from decoding any single source symbol with a subset of $s_1, s_2, \ldots, s_{n-1}$. R3 is a necessary condition for Bob to decode all source symbols. For $n = 1, 2, \ldots, K-1$, Bob chooses the generator $\boldsymbol{g}_n$ with these rules, and then sends $\boldsymbol{g}_n$ to Alice together with index n. Upon receiving $\boldsymbol{g}_n$, Alice generates the code symbol $\boldsymbol{s}_n = \boldsymbol{g}_n \boldsymbol{X}$ and sends it to Bob. If Bob receives $\boldsymbol{s}_n$, the pair $(\boldsymbol{g}_n, \boldsymbol{s}_n)$ is recorded into $\mathcal{B}$. Otherwise, Bob will generate a new $\boldsymbol{g}_n$ and repeat the process until Bob receives $\boldsymbol{s}_n$. This procedure continues until $n = K$. At this moment, all pairs $(\boldsymbol{g}_n, \boldsymbol{s}_n)$ for $n = 1, 2, \ldots, K-1$ are known to both Alice and Bob. Bob will chose a generator $\boldsymbol{g}_K$ with odd weight. But instead of sending $\boldsymbol{g}_K$, it sends

$$\tilde{\boldsymbol{g}}_K = \boldsymbol{g}_K + \sum_{n=1}^{K-1} \boldsymbol{g}_n. \tag{3}$$

Since Alice knows $\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_{K-1}$, it can recover $\boldsymbol{g}_K$ from $\tilde{\boldsymbol{g}}_K$. Then Alice generates the last code symbol $\boldsymbol{s}_K = \boldsymbol{g}_K \boldsymbol{X}$. Instead of sending $\boldsymbol{s}_K$ to Bob, Alice sends

$$\tilde{\boldsymbol{s}}_K = \boldsymbol{s}_K + \sum_{n=1}^{K-1} \boldsymbol{s}_n. \tag{4}$$

If Bob can not receive $\tilde{\boldsymbol{s}}_K$, Bob will generate a new $\boldsymbol{g}_K$ and send the new $\tilde{\boldsymbol{g}}_K$ to Alice and, correspondingly, Alice will generate a new $\boldsymbol{s}_K$ and send the new $\tilde{\boldsymbol{s}}_K$ to Bob. Bob will finally receive $\tilde{\boldsymbol{s}}_K$ and then recover $\boldsymbol{s}_K$ since it has already received $\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_{K-1}$. Now, Bob has K pairs in set $\mathcal{B}$ which leads to a set of linear equations:

$$\boldsymbol{S} = \boldsymbol{G}\boldsymbol{X}, \tag{5}$$

where $\boldsymbol{G} = (\boldsymbol{g}_1^{\mathrm{T}}, \ldots, \boldsymbol{g}_K^{\mathrm{T}})^{\mathrm{T}}$, $\boldsymbol{S} = (\boldsymbol{s}_1^{\mathrm{T}}, \ldots, \boldsymbol{s}_K^{\mathrm{T}})^{\mathrm{T}}$. $\boldsymbol{G}$ has full rank due to rule R3. Hence Bob can solve $\boldsymbol{X}$, using Gaussian elimination for example.

Secure performance analysis. Define a set $\mathcal{E} = \{(\hat{\boldsymbol{g}}_n, \hat{\boldsymbol{s}}_n)\}$ such that if Eve has overheard a generator $\hat{\boldsymbol{g}}_n$ from Bob and the corresponding code symbol $\hat{\boldsymbol{s}}_n = \hat{\boldsymbol{g}}_n \boldsymbol{X}$ from Alice, then $(\hat{\boldsymbol{g}}_n, \hat{\boldsymbol{s}}_n) \in \mathcal{E}$. It should be noted that $\mathcal{E}$ may contain pairs that are not contained in $\mathcal{B}$. For example, Bob sends $\hat{\boldsymbol{g}}_n$ which is received by both Alice and Eve, Alice sends $\hat{\boldsymbol{s}}_n = \hat{\boldsymbol{g}}_n \boldsymbol{X}$, which is received by Eve but lost at Bob. In this case the pair $(\hat{\boldsymbol{g}}_n \hat{\boldsymbol{s}}_n) \in \mathcal{E}$, but $(\hat{\boldsymbol{g}}_n \hat{\boldsymbol{s}}_n) \notin \mathcal{B}$. Similarly, $\mathcal{E}$ may also contain multiple pairs having the same index n.

Based on $\mathcal{E}$, Eve can also establish a set of linear equations similar to (5):

$$S_{\mathrm{E}} = G_{\mathrm{E}} X, \tag{6}$$

where G_{E} and S_{E} consist of, respectively, generators and code symbols in $\mathcal{E}$. If $\mathcal{E}$ contains no pair with index $n = K$, then Eve cannot solve any one data symbol of $\boldsymbol{X}$ since now that all rows of G_{E} have even weight. From (3) and (4), Eve cannot have a pair with index $n = K$ (which has odd weight generator) unless it has intercepted all pairs $(\boldsymbol{g}_n, \boldsymbol{s}_n) \in \mathcal{B}$ for all $n = 1, 2, \ldots, K-1$. Thus the necessary conditions for Eve to crack $\boldsymbol{X}$ are

C1. $\forall n = 1, 2, \ldots, K-1$, if $(\boldsymbol{g}_n, \boldsymbol{s}_n) \in \mathcal{B}$, then $(\boldsymbol{g}_n, \boldsymbol{s}_n) \in \mathcal{E}$.

C2. $\exists (\hat{\boldsymbol{g}}_k, \hat{\boldsymbol{s}}_k) \in \mathcal{E}$ such that $k = K$.

Let $p_{\mathrm{XY}}, \mathrm{X}, \mathrm{Y} \in \{\mathrm{A}, \mathrm{B}, \mathrm{E}\}$ denotes the packet loss rate at links X→Y. Assume that $0 \leqslant p_{\mathrm{XY}} < 1$ and the packet losses are independent random events for different links and different transmissions. Then the probability of condition C1 is given by

$$p_{\mathrm{C1}} = (1-q)^{K-1}, \tag{7}$$

where $q \triangleq 1 - (1 - p_{\mathrm{AE}})(1 - p_{\mathrm{BE}})$. The probability of C2 is

$$p_{\mathrm{C2}} = \sum_{k=1}^{\infty} (1 - q^k)(1-p)p^{k-1} = \frac{1-q}{1-pq}, \tag{8}$$

where $p \triangleq 1 - (1 - p_{\mathrm{AB}})(1 - p_{\mathrm{BA}})$. Thus, the probability that $\boldsymbol{X}$ can be cracked by Eve is

$$p_{\mathrm{crack}} = p_{\mathrm{C1}} p_{\mathrm{C2}} = \frac{(1-q)^K}{1-pq}. \tag{9}$$

The crack probability decreases monotonically with $K, p_{\mathrm{AE}}, p_{\mathrm{BE}}$. Hence arbitrary small crack probability is achievable either by increasing the

code length of the random linear code, or by degrading the quality of links to Eve. The latter can be realized by reducing transmit power or by using techniques such as beamforming or artificial noise [3].

Numerical results. In this section we present the numerical results for the crack probability p_{crack} by considering a Rayleigh fading channel. The average packet loss rate between the link X→Y can be expressed as [7]

$$p_{\text{XY}} = 1 - \exp\left(-\frac{\gamma_{\text{th}}}{\overline{\gamma}_{\text{XY}}}\right), \tag{10}$$

where $\overline{\gamma}_{\text{XY}}$ is the average signal to noise ratio (SNR) which is given by

$$\overline{\gamma}_{\text{XY}} = \frac{P}{\sigma^2}\left(\frac{d_{\text{XY}}}{d_0}\right)^{-\lambda}, \tag{11}$$

where P and σ^2 are, respectively, the transmit power and the noise power which are assumed to be the same for all nodes. d_{XY}/d_0 is the normalized distance between node X and Y. $\lambda = 3.5$ is the path loss exponent. γ_{th} is the SNR waterfall threshold of the physical layer error control code. For Turbo or LDPC codes, the threshold can be estimated via the radius of the decision region [8]. We set $\gamma_{\text{th}} = 1/0.81$ or 0.92 dB which is a typical value for BPSK modulated rate 1/2 LDPC codes.

With (10) and (11), we have $q = 1 - \exp(-\frac{a}{d_{\text{AE}}^{-\lambda}} - \frac{a}{d_{\text{BE}}^{-\lambda}})$ where $a = \frac{\gamma_{\text{th}}\sigma^2}{Pd_0^{\lambda}}$. Since harmonic mean $\leqslant$ geometric mean $\leqslant$ arithmetic mean, so we have $\frac{1}{d_{\text{AE}}^{-\lambda}} + \frac{1}{d_{\text{BE}}^{-\lambda}} \geqslant \frac{2}{\sqrt{d_{\text{AE}}^{-\lambda} d_{\text{BE}}^{-\lambda}}} \geqslant 2\left(\frac{d_{\text{AE}}+d_{\text{BE}}}{2}\right)^{\lambda} \geqslant 2\left(\frac{d_{\text{AB}}}{2}\right)^{\lambda}$ with equality iff $d_{\text{AE}} = d_{\text{BE}} = d_{\text{AB}}/2$. This has shown that p_{crack} is maximized when Eve is located at the midpoint between Alice and Bob. The crack probability for this worst case is shown in Figure 1. It can be observed that, even under this worst condition and there is no beamforming or artificial noise to degrade the link quality of Eve, the proposed scheme can still guarantee small crack probability.

Conclusion. This letter proposes a secure transmission scheme with random linear coding for wireless communications over fading channels. Since all nodes (including the passive eavesdropper Eve) will undergo independent fading and thermal noise, the packet losses at different nodes are statistically independent. When Alice and Bob exchange a lot of packets, such independence will lead to different knowledge at Eve and at the intended receiver, hence Alice can transmit information to Bob, that is high likely unknown to Eve.

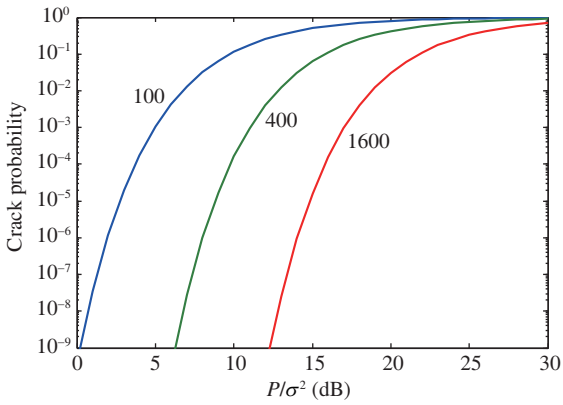

Figure 1 (Color online) p_{crack} as the function of SNR=P/σ^2. K =100, 400, 1600.

The numerical results show that, with proper setting of code length and transmit power, the proposed scheme can have very low crack probability.

Acknowledgements This work was supported by Chinese Scholarship Council.

References

1 Barros J, Rodrigues M R D. Secrecy capacity of wireless channel. In: Proceedings of IEEE International Symposium on Information Theory, Seatle, 2006. 356–360
2 Xiao L, Greenstein L J, Mandayam N B, et al. Using the physical layer for wireless authentication in time-variant channels. IEEE Trans Wirel Commun, 2008, 7: 2571–2579
3 Wang B, Mun P, Yang P, et al. Two-step transmission with artificial noise for secure wireless SIMO communications. Sci China Inf Sci, 2015, 58: 042308
4 Chen L. Wireless network coding with physical-layer security. In: Proceedings of IEEE Global Communication Conference, Atlanta, 2013. 1197–2002
5 Yamasaki S, Matsushima T K, Miyazaki S. Secure wireless communications using secret sharing and vector coding. In: Proceedings of IEEE Asia Pacific Conference of Circuits and Systems (APCCAS), Ishigaki, 2014. 731–734
6 Baldi M, Bianchi M, Chiaraluce F. Increasing physical layer security through scrambled codes and ARQ. In: Proceedings of IEEE International Conference on Communication Workshops (ICC), Kyoto, 2011. 1–5
7 Chatzigeorgiou I, Wassell I J, Carrasco R. On the frame error rate of transmission schemes on quasi-static fading channels. In: Proceedings of Information Sciences and Systems (CISS), Princeton, 2008. 577–581
8 Chen X G, Yang H W. Evaluating the word error rate of channel codes via the squared radius distribution of decision regions. IEEE Commun Lett, 2008, 12: 891–893