Proceedings of the IEEE
International Conference on Mechatronics & Automation
Niagara Falls, Canada • July 2005

Array-Transmission Based Physical-Layer Security Techniques For Wireless Sensor Networks*

Xiaohua(Edward) Li and Mo Chen
Department of Electrical and Computer Engineering
State University of New York at Binghamton
Binghamton, NY 13902
{*xli,mchen0*}*@binghamton.edu*

E. Paul Ratazzi
Air Force Research Laboratory
AFRL/IFGB
Rome, NY 13441
paul.ratazzi@afrl.af.mil

***Abstract*— This paper proposes new approaches to enhance the security of wireless sensor networks. Two randomized array transmission schemes are developed to secure wireless sensor networks at the physical layer. Transmission secrecy can be guaranteed by either the inherent ambiguities of MIMO blind equalization or the intentionally created ambiguities. Perfect secrecy is shown to be realizable under certain conditions. The schemes do not require secret keys, and work under more relaxed assumptions than existing techniques. They are useful for secure wireless data transmission or key distribution in wireless sensor networks.**

***Index Terms*— sensor networks, antenna array, perfect se crecy, physical layer information assurance**

I. INTRODUCTION

Information security has become one of the major concerns for wireless networks. This is also true for wireless sensor networks or the future robotic networks. Compared with wireline networks, wireless sensor networks lack a physical boundary due to the broadcasting nature of wireless transmissions. This unique physical-layer weakness calls for innovative physical-layer security designs in addition to, and integrated with, the traditional data encryption approaches.

Existing physical-layer security techniques may be classified into three categories: i) power approach like beamforming and directional transmissions, ii) code approach like spread-spectrum, and iii) channel approach like [1]. They usually depend on some strong assumptions for secrecy, such as the unauthorized user has null-receiving energy, has no information of the spreading codes or the propagation channel. Such strong assumptions can be easily violated. In particular, the unauthorized user may use blind equalization to estimate channels, which causes many channel-based approaches such as [1] to lose secrecy.

In this paper, we propose new physical-layer transmission techniques to realize secrecy under more reasonable assumptions. We assume that the unauthorized user may have better received signal quality and knows all the transmission protocols. There are no secret keys shared by the transmitters and the authorized user before transmission, and both of them have no knowledge of the unauthorized user.

*This work is partially supported by US AFRL/IF under grant FA8750-04-1-0213 to X. Li.

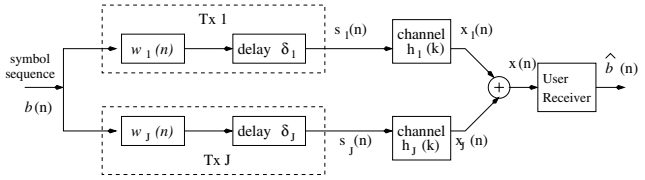

Fig. 1. The block diagram of array transmission.

We exploit two special properties of wireless transmissions for secure designs. First, signals received by the authorized sensor node (or user) and the unauthorized nodes (or user) are different because their channels are different. Second, channels between the transmitters and the authorized user can be reciprocal [2] (but they are not assumed always reciprocal). Our primary objective is to develop randomized array transmission schemes for computational secrecy, though perfect secrecy [3] is shown to be realizable under some circumstances.

This paper is organized as follows. The transmission framework is setup in Section II, whereas two transmission schemes are developed in Section III and IV. Simulations are then given in Section V and conclusions are in Section VI.

II. SYSTEM DESCRIPTION

We consider a wireless sensor network where sensors communicate with a mobile agent which has J transmitting antennas, which are denoted as J transmitters. A beamforming-like array transmission procedure shown in Fig. 1 is used by the J transmitters. A symbol sequence $\{b(n)\}$ is fed to all J transmitters, and is processed with single-tap weights $w_i(n)$ and delays δ_i. The transmitted signal from the transmitter i is $s_i(n)$.

With flat fading propagation, the authorized user receives signal

$$x(n) = \sum_{i=1}^{J} h_i^* s_i(n) + v(n) \triangleq \mathbf{h}^H \mathbf{s}(n) + v(n), \qquad (1)$$

where $v(n)$ denotes AWGN with zero-mean and variance σ_v^2, channels h_i^* are independent complex circular symmetric Gaussian distributed with zero-mean and unit variance, $\mathbf{h} \triangleq [h_1, \cdots, h_J]^T$, and

$$\mathbf{s}(n) \triangleq \begin{bmatrix} s_1(n) \\ \vdots \\ s_J(n) \end{bmatrix} = \begin{bmatrix} w_1(n) \\ \vdots \\ w_J(n) \end{bmatrix} b(n) \triangleq \mathbf{w}(n)b(n). \quad (2)$$

In this paper, $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ denote conjugation, transposition and Hermitian, respectively. Since channel estimation is required, we assume that $\mathbf{h}$ is block fading [1], i.e., it is constant or slowly time-varying when transmitting a block of symbols but may change randomly between blocks. The symbols $b(n)$ are independent uniformly distributed with zero-mean and unit variance.

The unauthorized user may use multiple receiving antennas for better interception, and the interception becomes much easier with a flat-fading channel model. Therefore, we consider the worst case (to the transmitters and the authorized user) where the unauthorized user receives synchronized signals with M receiving antennas

$$\mathbf{x}_u(n) = \mathbf{H}_u \mathbf{w}(n)b(n) + \mathbf{v}_u(n), \quad (3)$$

where $\mathbf{x}_u(n) = [x_{u,1}(n), \cdots, x_{u,M}(n)]^T$, $\mathbf{v}_u(n)$ is the corresponding noise vector, and the channel matrix

$$\mathbf{H}_u = \begin{bmatrix} h_{u,1,1}(0) & \cdots & h_{u,1,J}(0) \\ \vdots & & \vdots \\ h_{u,M,1}(0) & \cdots & h_{u,M,J}(0) \end{bmatrix}. \quad (4)$$

Each element in $\mathbf{H}_u$ has the same distribution as h_i, but is independent from h_i.

In this paper, we focus only on the security of the downlink transmission (from the mobile agent to the authorized user). Once the downlink is secured, the uplink can be easily secured by using similar techniques and/or by exchanging encryption keys frequently.

III. Secure transmission with inherent ambiguity

In this section, we assume that the unauthorized user does not know the channels $\mathbf{h}$ and $\mathbf{H}_u$. But it may try to estimate them by training/blind methods, or by a brute-force search of all possible channels. The transmitters and the authorized user do not know all channels either, and have no ways to estimate $\mathbf{H}_u$.

A. Transmission and receiving procedure

In order to achieve transmission secrecy, according to the received signal

$$x(n) = \mathbf{h}^H \mathbf{w}(n)b(n) + v(n), \quad (5)$$

our basic idea is to make $\mathbf{h}^H\mathbf{w}(n)$ deterministic but $\mathbf{H}_u\mathbf{w}(n)$ changing randomly in each symbol interval. Therefore, we design the transmitting weights vector $\mathbf{w}(n)$ such that

$$\mathbf{h}^H \mathbf{w}(n) = \|\mathbf{h}\|, \quad (6)$$

where $\|\mathbf{h}\| = \sqrt{\sum_{i=1}^J |h_i|^2}$, and exploit the degrees of freedom in $\mathbf{w}(n)$ for randomization purpose. The authorized user can detect symbols as $\hat{b}(n) = \|\mathbf{h}\|^{-1}x(n)$, where $\|\mathbf{h}\|^2$ can be estimated as $\frac{1}{N}\sum_{n=1}^N |x(n)|^2$.

To implement this transmission scheme, the channel $\mathbf{h}$ has to be known to the transmitters instead of the receiver. There are at least two ways for the transmitters to estimate the channel $\mathbf{h}$. First, if the downlink and uplink channels are reciprocal, the transmitters can estimate $\mathbf{h}$ directly from the uplink received signals. This is the case in fast time-division-duplexing (TDD) transmissions [2].

The second way is to ask the authorized user to feedback some received signal information to the transmitters. Since explicit training should be avoided, the transmitters can send a training sequence randomized by $\mathbf{w}(n)$ which are known to themselves only. The authorized user estimates and feedbacks $y(n) = \mathbf{h}^H\mathbf{w}(n)$, with which the transmitters can estimate channel $\mathbf{h}$ based on their knowledge of $\mathbf{w}(n)$.

B. Transmitting weights design

Before presenting our designs, we first show that traditional transmit beamforming methods do not guarantee secrecy although they are optimal in terms of performance and power efficiency. A typical transmit beamforming method uses $\mathbf{w}(n) = \mathbf{h}/\|\mathbf{h}\|$. In this case, the received signal of the unauthorized user is $\mathbf{x}_u(n) = (\mathbf{H}_u\mathbf{h}/\|\mathbf{h}\|)b(n)+\mathbf{v}_u(n)$, from which many blind equalizers including the constant modulus algorithm (CMA) can be applied for symbol detection. The same holds for other designs of $\mathbf{w}(n)$ that are not random. This explains why we should use randomized array transmissions.

More generally, $\mathbf{w}(n)$ can be obtained from the singular value decomposition (SVD) of $\mathbf{h}$, i.e., $\mathbf{h}^H = \mathbf{U}\mathbf{D}\mathbf{V}^H$, in which case $\mathbf{w}(n)$ can be calculated as $\mathbf{w}(n) = \mathbf{V}[1, z_2(n), \cdots, z_J(n)]^T$ where $z_j(n)$ can be arbitrary. Such a classic approach does not have any secrecy even if $\mathbf{w}(n)$ is randomized by choosing randomly $\mathbf{z}_1(n)$. For example, CMA may be used to estimate symbols from

$$\mathbf{x}_u(n) = \mathbf{H}_u\mathbf{V}\begin{bmatrix} 1 \\ \mathbf{z}_1(n) \end{bmatrix} b(n) + \mathbf{v}_u(n). \quad (7)$$

Since the above transmit beamforming are designed for optimal transmission power, there may be always a tradeoff of transmission power for secrecy. Based on this observation, we design transmitting weights with relaxed power requirement. The trade-off of transmission power for secrecy is necessary when enhanced secrecy is required. Because the mobile agent can be considered as without severe energy constraints, such

increased transmission power can be tolerable. Note that we do not increase the power consumption of receivers, i.e., sensors.

We first select randomly an h_i from $\mathbf{h}$, then choose randomly $w_j(n)$, $1 \leq j \leq J$ and $j \neq i$. For example, we can draw $w_j(n)$ from an i.i.d. complex Gaussian random process. Denote $\mathbf{z}_i(n) = [w_1(n), \cdots, w_{i-1}(n), w_{i+1}(n), \cdots, w_J(n)]^T$ and $\mathbf{h}_i = [h_1, \cdots, h_{i-1}, h_{i+1}, \cdots, h_J]^T$. The weights vector is calculated as

$$\mathbf{w}(n) = \mathbf{P}_i \begin{bmatrix} \frac{\|\mathbf{h}\| - \mathbf{h}_i^H \mathbf{z}_i(n)}{h_i^*} \\ \mathbf{z}_i(n) \end{bmatrix}. \quad (8)$$

The matrix $\mathbf{P}_i$ is a $J \times J$ commutation matrix whose function is to insert the first row of the following vector into the ith row. Since h_i is chosen randomly, $\mathbf{P}_i$ is also random.

One of the major advantages of this scheme (we denote it as Scheme 1) is linear computational complexity. Efficient computation is important because $\mathbf{w}(n)$ are recalculated in each symbol interval.

C. Transmission power

Although we do not explicitly apply any power constraints on $\mathbf{w}(n)$, the transmission power can be statistically controlled by adjusting the mean and variance of the random variables $w_j(n)$, $j \neq i$.

Let us consider the case that the mean and variance are zero and σ^2, respectively. Since small h_i in (8) increases power, we need to select proper threshold α and choose those h_i that satisfy $|h_i|^2 > \alpha$.

Proposition 1. With Rayleigh fading channels, if the coefficients are selected with threshold α, then the expected total transmission power is

$$P_t = (J-1)\sigma^2 + 1 + (J-1)(1+\sigma^2)\Gamma(0, \alpha). \quad (9)$$

Proof. See Appendix A.

If the channel $\mathbf{h}$ is slowly time-varying or even constant for a long time, we need to avoid the case that the power of one of the transmitters is exceptionally larger than the others. Otherwise the array transmission behaves as that with a single transmitter, and security can be compromised. Therefore, we have to constrain as well the ratio of the transmission power of the ith transmitter to that of the jth transmitter. The power ratio can be obtained from (9) as

$$\frac{P_{t,i}}{P_{t,j}} = \frac{1 + (J-1)(1+\sigma^2)\Gamma(0, \alpha)}{\sigma^2}. \quad (10)$$

Larger σ^2 increases P_t but decreases $P_{t,i}/P_{t,j}$. Since both P_t and $P_{t,i}/P_{t,j}$ should be small, there is a trade-off between them when choosing σ^2. The same holds for choosing α.

D. Transmission secrecy of Scheme 1

Since we have removed explicit training, the unauthorized user has no training available for channel estimation. If the channels are reciprocal, then the transmitters can estimate channel $\mathbf{h}$ from any uplink signal transmitted by the authorized user in TDD, without leaking channel information to the unauthorized user. On the other hand, if the transmitters depend on feedback from the authorized user for channel estimation, then the secrecy relies on the security of the feedback data. If the feedback data are not secure, the secrecy of the downlink transmission can be lost. For example, if the unauthorized user has intercepted the feedback data $y(n)$, $n = 1, \cdots, J$, then together with its own estimations $y_u(n) = \mathbf{H}_u \mathbf{w}(n)$, $n = 1, \cdots, J$, it can derive a vector $\mathbf{h}^H \mathbf{H}_u^{-1}$. By this vector, it can intercept symbols $b(n)$ from $\mathbf{x}_u(n)$.

Therefore, before using feedback for channel estimation, a secure initialization method has to be adopted for the subsequent feedback-based data transmission to become secure. We can exploit the reciprocal channel property to realize this objective. The advantage is that no secret keys are required before transmission, which is important considering that key distribution is usually a major weakness for traditional security techniques.

Without training, the unauthorized user may turn to blind equalizers. So the transmitters need to remove any constant modulus information from $s_j(n)$, which is done by randomizing $w_j(n)$. Then the secrecy of Scheme 1 comes from the fact that the received signal (3) of the unauthorized user is with a multiple-input multiple-output (MIMO) channel model. It is well known that blind MIMO channel estimation has an inherent matrix ambiguity if no source property can be exploited [4]. In fact, the unknown source statistics makes the ambiguity matrix arbitrary, not only unitary.

If the blind equalization is not applicable, the last way left for the unauthorized user is to try a brute-force search of all possible channels $\mathbf{H}_u$ (or, strictly speaking, all $J \times J$ ambiguity matrices) and $\mathbf{h}$. Let us assume that the unauthorized user uses K-level quantization for each single value (a complex number has two such values). Then the brute-force search needs to consider at least $K^{(2J)^2}$ possible combinations of $\mathbf{H}_u$ and K^{2J} possible combinations of $\mathbf{h}$. This gives an overall complexity $K^{2J(2J+1)}$.

With $J = 4$ and QPSK transmission, in order to achieve bit-error-rate (BER) under 0.1, by simulations we find $K \geq 4$ even in the noiseless case. When $K = 4$, the complexity becomes $4^{2\times4\times(2\times4+1)} = 2^{144}$, which gives security well above the encryption with a 128-bit key.

IV. Secure transmission with intentional ambiguity

In this section, we develop another transmission scheme which achieves secrecy even if the unauthorized user knows

its own channel $\mathbf{H}_u$. This would effectively simplify the design of physical-layer secured wireless networks. We assume that the unauthorized user knows $\mathbf{H}_u$ but not $\mathbf{h}$, and has extremely high SNR or even noiseless signal. Such assumptions make our approach distinct from most existing physical-layer security studies such as [1].

A. Create intentional ambiguity

With the known $\mathbf{H}_u$, the signals of the unauthorized user (3) can be simplified to

$$\mathbf{x}_u(n) = \mathbf{w}(n)b(n), \tag{11}$$

where the noise is skipped under the assumption of high SNR. Since the unauthorized user may know the signal model of the authorized user (5)-(6) (but does not know $\mathbf{h}$, $\mathbf{w}(n)$ and $b(n)$), a brute-force search with much reduced complexity can be applied, during which it simply checks every possible $\mathbf{h}$ with (11) to see whether the rule of finite symbol alphabet is satisfied. This procedure may break the secrecy with a complexity K^{2J} only.

To resolve this weakness, one way is to make $\mathbf{h}$ time-varying, which can increase the complexity of the brute-force method in low SNR but is not effective in high SNR or noiseless cases. To guarantee secrecy under (11), we propose to introduce intentional ambiguity in addition to creating time-varying channels.

Instead of using (8) to find $\mathbf{w}(n)$, we generate a $J\times(J-1)$ random matrix $\mathbf{F} = [\mathbf{f}_1, \cdots, \mathbf{f}_{J-1}]$, where each $\mathbf{f}_i$ is a $J \times 1$ vector. The matrix $\mathbf{F}$ is known to the transmitters only. Let

$$\mathbf{a}(n) = \begin{bmatrix} \|\mathbf{f}_1\| c_1(n) \\ \vdots \\ \|\mathbf{f}_{J-1}\| c_{J-1}(n) \end{bmatrix}, \tag{12}$$

where $\{c_i(n)\}$, $1 \le i \le J-1$, are secret sequences known only to the transmitters. We make each column of the matrix $\mathbf{F}$ to have the same distribution as $\mathbf{h}$. Then we calculate $\mathbf{w}(n)$ by solving

$$\begin{bmatrix} \mathbf{h}^H \\ \mathbf{F}^H \end{bmatrix} \mathbf{w}(n) = \begin{bmatrix} \|\mathbf{h}\| \\ \mathbf{a}(n) \end{bmatrix}. \tag{13}$$

This method is denoted as Scheme 2. For the authorized user, the received signal is still (5) and (6).

The power efficiency of this scheme can be made much higher than Scheme 1 because the problem of inverting small h_i is gone. The lower bound of total transmission power is

$$E[\|\mathbf{w}(n)\|^2] \ge E\left[\|[\mathbf{h}, \mathbf{F}]\|^{-2} \|[\|\mathbf{h}\|, \mathbf{a}^T(n)]^T\|^2\right] = 1. \tag{14}$$

However, the unit lower bound usually can not be obtained.

B. Transmission secrecy of Scheme 2

Proposition 2. The unauthorized user can not discriminate $\mathbf{h}$ from any column $\mathbf{f}_i$ of $\mathbf{F}$, i.e., $P[\mathbf{h}|\{\mathbf{x}_u(n)\}] = P[\mathbf{f}_i|\{\mathbf{x}_u(n)\}]$, $1 \le i \le J-1$, where $\{\mathbf{x}_u(n)\}$ denotes the sequence including all the available samples.

Proof. See Appendix B.

Proposition 2 means that the unauthorized user can not discriminate $b(n)$ from $c_i(n)b(n)$, which is the ambiguity created intentionally. However, if the number of vectors $\mathbf{h}$ and $\mathbf{f}_i$ that satisfy (13) is finite, then the unauthorized user can use brute-force search to determine which sequence among $\{b(n)\}$ and $\{c_i(n)b(n) : 1 \le i \le J-1\}$ is more meaningful by recovering them to message sequences.

Therefore, we need to create suitably time-varying channels in order to make the brute-force search computationally prohibitive. Time-varying channels can be intentionally created by moving randomly transmitting antennas, or by choosing different antenna subsets from a large array. Each channel realization is used to transmit a short block of symbols with a suitable $\mathbf{F}$. As long as the determination of $\{b(n)\}$ requires a sufficiently large number of blocks, computational secrecy can be achieved.

In practice, due to noise and the short block length, the unauthorized user may not have sufficient statistic measures for determining even $\mathbf{h}$ or $\mathbf{f}_i$. Hence computational secrecy can be guaranteed with a moderate number of symbol blocks.

C. Perfect secrecy

Proposition 3. $P[b(n)|\{\mathbf{x}_u(n)\}]$ can be made independent of $b(n)$ (i.e., prefect secrecy [3]) if $\mathbf{h}$ is i.i.d. for each symbol and the symbols have constant magnitude, i.e., $|b(n)| = 1$. Otherwise, $P[b(n)|\{\mathbf{x}_u(n)\}]$ may not be independent of $b(n)$ since the unauthorized user can exploit its knowledge of (6).

Proof. See Appendix C.

Note that the necessary condition, i.e., $|b(n)| = 1$, is similar to that in [1], although the latter is obtained under much stronger assumption that the unauthorized user has no information of the channel $\mathbf{H}_u$, nor can it estimate $\mathbf{H}_u$.

A possible way for implementing transmissions with perfect secrecy is to intentionally create channel variation. With each new channel realization, a training sequence can be transmitted for channel estimation. After the transmitters know the channels, a symbol is transmitted with a randomized $\mathbf{w}(n)$. The initialization based on channel reciprocity is still required. Note the channel reciprocity, if available, can be used for removing feedback and improving data rate.

V. Simulations

In this section, we show the performance of the proposed Scheme 1 and 2 for both the authorized user and the unauthorized user. For comparison purpose, we also give the performance of the optimal transmit beamforming and the theoretical BER curve of the Rayleigh fading channel without diversity. For Scheme 1, we use $\alpha = 0.5$ and $\sigma^2 = 0.5$.

From the simulation results in Fig. 2, we see that Scheme 1 and 2 both have similar performance as the optimal transmit beamforming. They all exploit the diversity of $J = 4$ transmitters. The unauthorized user can not intercept symbols

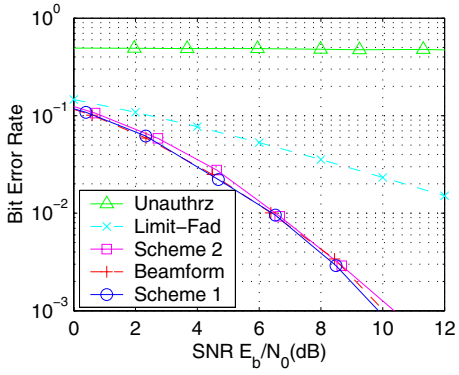

Fig. 2. Performance comparison. $J = 4$.

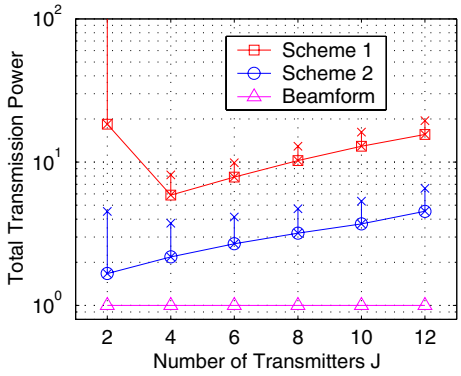

Fig. 3. Transmission power and standard deviation. Standard deviation is shown by $\times$ above the power value.

using the blind equalization with 8 receiving antennas and sufficiently good channels.

The transmission powers for Schemes 1 and 2 as well as beamforming are compared in Fig. 3. Scheme 1 requires the largest total transmitting power. Such increase in power consumption is due to the lack of optimization when calculating transmitting coefficients $\mathbf{w}(n)$. In addition, the standard deviation of power consumption among 5000 runs is also shown. For Scheme 1, when J is small, especially when $J = 2$, the standard deviation becomes large because small h_i have to be chosen.

VI. Conclusions

This paper develops two randomized array transmission schemes for transmission security in wireless sensor networks where mobile agents with antenna arrays can be used for extreme physical-layer security. Although we have considered only flat-fading channels, such schemes can be extended to frequency selective fading channels with similar performance and security [5]. The proposed methods can be useful for future wireless sensor networks, or even battle field robotic networks, where extreme security is highly required.

Appendix A
Proof of Proposition 1

If channels are random, then the ensemble average of the power becomes

$$P_t = E[P_{t,h_i}] = (J-1)\sigma^2 + 1 + E\left[\frac{\|\mathbf{h}_i\|^2}{|h_i|^2}\right](1+\sigma^2). \quad (15)$$

Since the channel coefficients are independent from each other, we have

$$P_t = (J-1)\sigma^2 + 1 + (J-1)(1+\sigma^2)E[\frac{1}{|h_i|^2}]. \quad (16)$$

Because $|h_i|^2$ has exponential distribution, we have

$$E[\frac{1}{|h_i|^2}] = \int_\alpha^\infty \frac{1}{|h_i|^2} e^{-|h_i|^2} d|h_i|^2 = \Gamma(0,\alpha). \quad (17)$$

Hence (9) is obtained.

Appendix B
Proof of Proposition 2

Considering the *maximum a posteriori* (MAP) detector for $\mathbf{h}$, the unauthorized user has

$$\begin{aligned} & P[\mathbf{h}|\{\mathbf{x}_u(n)\}] \\ &= P[\{x_u(n)\}|\mathbf{h}]\frac{P[\mathbf{h}]}{P[\{\mathbf{x}_u(n)\}]} \\ &= P[\{\mathbf{w}(n)b(n)\}|\mathbf{h}]\frac{P[\mathbf{h}]}{P[\{\mathbf{x}_u(n)\}]} \\ &= P[\{\mathbf{w}(n)\}|\mathbf{h}]P[\{b(n)\}]\frac{P[\mathbf{h}]}{P[\{\mathbf{x}_u(n)\}]}. \end{aligned} \quad (18)$$

Because of (6), one element of $\mathbf{w}(n)$ is completely determined by others given $\mathbf{h}$. Without loss of generality, let $w_1(n)$ be determined by random variables $\mathbf{z}_1(n) = [w_2(n), \cdots, w_J(n)]^T$. Then

$$P[\mathbf{h}|\{\mathbf{x}_u(n)\}] = P[\{\mathbf{z}_1(n)\}]P[\{b(n)\}]\frac{P[\mathbf{h}]}{P[\{\mathbf{x}_u(n)\}]}. \quad (19)$$

Similarly, if the unauthorized user considers $\mathbf{f}_i$ instead of $\mathbf{h}$, it has

$$P[\mathbf{f}_i|\{\mathbf{x}_u(n)\}] = P[\{\mathbf{z}_1(n)\}]P[\{b(n)\}]\frac{P[\mathbf{f}_i]}{P[\{\mathbf{x}_u(n)\}]}. \quad (20)$$

Because $P[\mathbf{f}_i] = P[\mathbf{h}]$, the proposition is proved.

Appendix C
Proof of Proposition 3

Since $\mathbf{w}(n)$ is randomly and independently generated in each symbol interval, if the channel $\mathbf{h}$ is i.i.d. for each symbol, then $\mathbf{w}(n)$ is independent from $\mathbf{x}_u(m)$ for any $m \neq n$. The same conclusion holds for $b(n)$. Therefore, $P[b(n)|\{\mathbf{x}_u(n)\}]$ is equivalent to $P[b(n)|\mathbf{x}_u(n)]$. We have

$$\begin{aligned} P[b(n)|\mathbf{x}_u(n)] &= P[\mathbf{x}_u(n)|b(n)]\frac{P[b(n)]}{P[\mathbf{x}_u(n)]} \\ &= P[\mathbf{w}(n)b(n)|b(n)]\frac{P[b(n)]}{P[\mathbf{x}_u(n)]}. \end{aligned} \quad (21)$$

The pdf of $\mathbf{w}(n)b(n)$ given $b(n)$ is $\frac{1}{|b(n)|}f_{\mathbf{w}}(\frac{\mathbf{w}(n)}{b(n)})$, where $\mathbf{f}_{\mathbf{w}}(\cdot)$ denotes the joint pdf of $\mathbf{w}(n)$.

Because the channel coefficients in $\mathbf{h}$ are jointly Gaussian with zero mean, the pdf of $\mathbf{h}$ is phase symmetric (or phase invariant), i.e., the probability of $\mathbf{h}e^{j\theta}$ is the same as that of $\mathbf{h}$ for any θ. Because $\mathbf{w}(n)$ is obtained from $\mathbf{h}$, $f_{\mathbf{w}}(\mathbf{w}(n))$ can also be phase symmetric. This can be seen from the fact that $[\mathbf{h}e^{j\theta}]^H[\mathbf{w}(n)e^{j\theta}] = \|\mathbf{h}e^{j\theta}\|$. This equation tells us that if there is a $\mathbf{w}(n)$ obtained from $\mathbf{h}$ with certain probability, then for any phase θ, $\mathbf{w}(n)e^{j\theta}$ can be obtained from $\mathbf{h}e^{j\theta}$ with the same probability. Note that different $\mathbf{h}$ and $\mathbf{h}e^{j\theta}$ do not share the same $\mathbf{w}(n)$.

Therefore, if $|b(n)| = 1$, then $\mathbf{w}(n)/b(n)$ and $\mathbf{w}(n)$ have identical probability, which means that $f_{\mathbf{w}}(\mathbf{w}(n)/b(n)) = f_{\mathbf{w}}(\mathbf{w}(n))$. Hence $P[b(n)|\mathbf{x}_u(n)] = P[\mathbf{w}(n)]P[b(n)]/P[\mathbf{x}_u(n)]$. Since $P[b(n)]$ is constant, $P[b(n)|\mathbf{x}_u(n)]$ is independent of $b(n)$.

However, if the channel $\mathbf{h}$ is not i.i.d. for each symbol, or if $|b(n)|$ are not constant, then $\frac{1}{|b(n)|}f_{\mathbf{w}}(\frac{\mathbf{w}(n)}{b(n)}) \neq f_{\mathbf{w}}(\mathbf{w}(n))$ in general. Some information about $b(n)$ may be available given $\{\mathbf{x}_u(n)\}$.

REFERENCES

[1] A. O. Hero, III, "Secure space-time communication," *IEEE Trans. Info. Theory*, vol. 49, no. 12, pp. 3235-3249, Dec. 2003.

[2] G. Xu and H. Liu, "An effective transmission beamforming scheme for frequency-division-duplex digital wireless communication system," *ICASSP'95*, vol. 3, pp. 1729-1732, May 1995.

[3] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656-715, 1949.

[4] G. B. Giannakis, Y. Hua, P. Stoica and L. Tong, editors, *Signal Processing Advances in Mobile and Wireless Communications, Volume 1: Trends in Channel Estimation and Equalization*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 2000.

[5] X. Li, "Randomized array transmissions for physical-layer secured wireless communications," report to US AFRL/IF. Available online at: *http://bingweb.binghamton.edu/∼xli/secom.pdf*.