A Method for Low-Latency Secure Multiple Access

Yingbo Hua  
University of California at Riverside  
Riverside, California, USA  
yhua@ucr.edu

Md Saydur Rahman  
University of California at Riverside  
Riverside, California, USA  
mrahm054@ucr.edu

Ananthram Swami  
DEVCOM Army Research Laboratory  
Adelphi, Maryland, USA  
ananthram.swami.civ@army.mil

Abstract—This paper studies an application of “secret-message transmission by echoing encrypted probes (STEEP)” to multiple access (MA) between users’ equipment (UEs) and an access point (AP). This method, referred to as MA-STEEP, allows all UEs to take advantage of a common sequence of probes broadcasted by AP, which helps to meet the low-latency requirement. The secrecy capacity of MA-STEEP from each UE to AP is shown to be positive with high probability (subject to a power condition) and robust against the number $M$ of UEs. A total secrecy capacity of MA-STEEP increases with $M$, unlike a common-nonce method.

Index Terms—Multiple access, security, low-latency.

I. INTRODUCTION

For applications such as Virtual Reality, Artificial Intelligence, federated learning, autonomous driving, etc., next generation networks must allow low-latency secure multiple access. Multiple access is necessary to provide local wireless connections for massive numbers of devices with limited spectral resources. Security and privacy are among the major requirements from network designers and consumers alike. Low latency is essential to ensure the feasibility of any real-time networked control systems and to provide high-quality consumer experiences.

This paper presents a method of physical layer security to achieve a combined goal of multiple access, security and low-latency.

Multiple access has been an active research topic for many decades. An extensive survey is available in [1]. There are orthogonal multiple access schemes such as TDMA, FDMA and OFDMA, as well as non-orthogonal multiple access schemes such as CDMA, random access and successive interference cancellation. In this paper, we will focus on orthogonal multiple access which is highly efficient in both computation and spectral usage for users with similar powers.

Secure multiple access can be realized with the aid of secret key generation networks. This is a research topic for decades [4], and a vast majority of the prior methods for secret key generation (SKG) require a reciprocal wireless channel. But the secret-key rate based on this approach is very limited when the channel environment is, for example, static. Many efforts to produce a positive secret-key rate with or without channel reciprocity in static environment have failed until the recent works [5], [6], [7], [8]. It is now established that regardless of channel reciprocity, one node can effectively send a secret key to another node with a positive secret-key rate even if the eavesdropper’s channel is stronger than that between the two nodes. This paper aims to extend parts of the discoveries shown in those works to the area of secure multiple access.

To achieve low latency and information security between two nodes, there have been recent papers on short-packet theory for wiretap channel (WTC) system, e.g., see [9] and the references therein. These works essentially follow the traditional WTC theory [10] while also considering the loss of secrecy rate due to finite or short length of a packet [11]. But just like the long-packet case, the secrecy rate of the short-packet scheme shown in those works is always zero whenever eavesdropper’s channel is stronger than the channel between the legitimate users. The applicability of the short-packet theory to multiple access is another major hurdle which was unresolved.

The secrecy capacity region of multi-access WTC system is still a poorly understood subject [12]. Fundamentally different from [12] and many others where “feedback” from AP is used, the proposed method in this paper uses “probing” from AP. Note that “feedback” follows a message transmission while “probing” precedes the message transmission.

The method called “secret-message transmission by echoing encrypted probes (STEEP)” was formulated in [7]. The extension of STEEP in this paper to multiple access (MA) will be referred to as MA-STEEP. There is a similarity between MA-STEEP and the common-nonce method, but there are also crucial differences explained below.
The similarity between the two methods is that before each UE transmits its message, AP sends a signal to all UEs; and this signal is then used by all UEs for privacy purposes. This is also where the similarity ends. In the common-nonce method, all UEs are required to receive the common nonce with no error, and hence unfortunately they can all eavesdrop on each other. In MA-STEEP, a sequence of random probing symbols are transmitted from AP to all UEs in phase 1 (also called probing phase), but no Eve or UE is allowed to estimate the probes exactly. This can be realized by power control at AP. In phase 2 (also called echoing phase), each UE sends back its estimated probes encrypted by (or mixed with) its secret message. At AP, the secret message from each UE can be then detected with a reliability always higher than at Eve or any eavesdropping UE. In other words, MA-STEEP transforms the physical multi-access WTC system from UEs to AP into a virtual or effective multi-access WTC system where the latter always disadvantages any eavesdropping node. MA-STEEP takes advantage of the independent noises at all nodes in the physical layer to yield an almost always positive secrecy rate for each UE in uplink. With this effective WTC system, all established coding methods for WTC can be then applied.

II. BASIC PRINCIPLE OF STEEP

For a two-user channel, STEEP shown in [7] is a round-trip transmission scheme between two nodes, which uses channel probing and echoing of encrypted probes to effectively or virtually degrade eavesdropper’s channel. The two-way scheme shown in [5] for a binary symmetric channel turns also into a virtual or effective multi-access WTC system where the latter always disadvantages any eavesdropping node. MA-STEEP takes advantage of the independent noises at all nodes in the physical layer to yield an almost always positive secrecy rate for each UE in uplink. With this effective WTC system, all established coding methods for WTC can be then applied.

In this paper, we examine the role of STEEP for multiple access (or multi-user) applications. Given an access point (AP) and multiple users’ equipment (UEs), a trivial application of STEEP would be to apply STEEP between AP and each UE in a completely orthogonal fashion, e.g., AP sends a separate sequence of probes to each of the UEs using an orthogonal channel in the probing phase, and then each UE performs its operation as described above using an orthogonal channel in the echoing phase. But in this paper, we consider a MA-STEEP where AP first broadcasts a single sequence of probes to all UEs in the probing phase, and only in the echoing phase an orthogonal channel is used for each UE to transmit to AP a secret message encrypted with the UE’s estimate of its effective sequence of the same probes.

If we want to further reduce the spectral usage, or equivalently the latency, we could also consider non-orthogonal multiple access by the UEs in the echoing phase. But in this paper we only consider orthogonal multiple access in phase 2.

III. MA-STEEP AND ITS SECRECY CAPACITY

Consider an access point (AP) with \( n_A \) antennas and \( M \) single-antenna users’ equipment (UEs). The broadcast channel from AP to UEi, in baseband is modelled by

\[
y_i = h_i^T x_A + w_i
\]

where \( h_i \in \mathbb{C}^{n_A \times 1} \) is a vector transmitted by AP, \( h_i \in \mathbb{C}^{n_A \times 1} \) is the channel vector, \( y_i \) and \( w_i \) are the received signal and noise at UEi. If there are interferences such as jamming noises from (full-duplex) Eve, then \( w_i \) also includes them.

The channels from UEs to AP are assumed to be orthogonal (such as TDMA, FDMA and OFDMA), i.e., the channel from UEi to AP can be modelled as

\[
y_{A,i} = h_{A,i} x_i + w_{A,i},
\]

where \( x_i \) is a symbol transmitted by UEi, \( h_{A,i} \in \mathbb{C}^{n_A \times 1} \) is the channel vector from UEi to AP, and \( y_{A,i} \) and \( w_{A,i} \) are the received signal and noise at AP. Like \( w_i \) in (1), \( w_{A,i} \) in (2) includes noise and all noise-like interferences.

In the probing phase (phase 1), AP broadcasts a sequence of i.i.d. probing vectors. Each of the vectors can be represented by \( \sqrt{\frac{P_A}{n_A}} x \) with \( \mathbb{E} \{ ||x||^2 \} = n_A \). Then the corresponding signal received by UEi for each of \( i = 1, \ldots, M \) is

\[
y_i = \sqrt{\frac{P_A}{n_A}} h_i^T x + w_i
\]

where \( \mathbb{E} \{ ||w_i||^2 \} = \sigma_i^2 \). We will also write

\[
y_i = \begin{cases} \sqrt{\frac{P_A}{n_A}} h_i p_i + w_i, & n_A = 1; \\ \sqrt{\frac{P_A}{n_A}} ||h_i|| p_i + w_i, & n_A \geq 2; \end{cases}
\]

with

\[
p_i = \begin{cases} x, & n_A = 1; \\ \bar{h}_i^T x, & n_A \geq 2. \end{cases}
\]

Here \( x = x \) and \( h_i = h_i \) for \( n_A = 1 \), and \( \bar{h}_i = \frac{1}{||h_i||} h_i \).

We call \( p_i \) the effective probing symbol from AP to UEi, which is always known to AP if \( n_A = 1 \). For \( n_A \geq 2 \), AP also knows \( p_i \) if AP receives the feedback of \( \bar{h}_i \) from UEi. For secrecy analysis, we will assume that \( \bar{h}_i \) is publicly known. In fact, we will also assume that all channel parameters between AP and UEs are known to Eve.

In the echoing phase (phase 2), UEi for \( i = 1, \ldots, M \) transmits \( \sqrt{\frac{P_E}{\bar{p}_i}} (\bar{p}_i + s_i) \) to AP, where \( s_i \) is a secret symbol of unit variance from UEi, and \( \bar{p}_i \) is the MMSE estimate of \( p_i \) by UEi using \( y_i \). Here each UE knows its receive channel.

Note that the above \( \sqrt{\frac{P_E}{\bar{p}_i}} (\bar{p}_i + s_i(k)) \) also corresponds to \( \sqrt{\frac{P_E}{\bar{p}_i}} (\bar{p}(k) + s_i(k)) \) if \( k \) denotes the \( k \)th probing symbol interval and the \( k \)th echoed symbol interval for UEi.
We will also assume that \( x, w_i \) and \( s_i \) for all \( i \) are circular complex Gaussian of zero mean. Then it can be shown [13] that

\[
\hat{p}_i = \sqrt{\frac{p_A}{n_A}} \frac{\|h_i\|}{\|h_i\|^2 + \sigma_i^2} y_i = \frac{\sqrt{S_i}}{S_i + 1} \frac{1}{\sigma_i} y_i,
\]

with \( S_i = \frac{p_A}{n_A \sigma^2} \|h_i\|^2 \) which is the signal-to-noise ratio (SNR) of \( y_i \). We will also use

\[
c_i = \sigma^2_{\hat{p}_i} - \mathbb{E}\{\|\hat{p}_i\|^2\} = \frac{S_i}{S_i + 1},
\]

\[
\sigma^2_{\hat{p}_i} - \mathbb{E}\{\|\hat{p}_i - p_i\|^2\} = \frac{1}{S_i + 1} = 1 - c_i.
\]

A. Effective Return Channel from UE\(_i\) to AP

The corresponding signal vector received by AP from UE\(_i\) in phase 2 of MA-STEEP is

\[
y_{A,i} = \sqrt{\frac{p_B}{2}} (\hat{p}_i + s_i) h_{A,i} + w_{A,i}.
\]

It can be shown [13] that the MMSE estimate of \( s_i \) by AP from \( y_{A,j} \) for all \( j = 1, \cdots, M \) is

\[
\hat{s}_i = \frac{p_B}{2}\left(\frac{\sigma^2_{\hat{p}_i}}{\sigma^2_{\hat{p}_i} + \sigma^2_{\hat{p}_i}}\right) h_{A,i} \Delta y_{A,i} \tag{10}
\]

with \( \Delta y_{A,i} = y_{A,i} - \mathbb{E}\{y_{A,i}|x\} = y_{A,i} - \sqrt{\frac{p_B}{2}} h_{A,i} \sigma^2_{\hat{p}_i} p_i \), and the MSE of \( \hat{s}_i \) is

\[
\sigma^2_{\Delta s_i} = \mathbb{E}\{|\hat{s}_i - s_i|^2\} = \frac{\sigma^2_{\hat{p}_i} \sigma^2_{\hat{p}_i} S_{A,i} + 1}{(1 + \sigma^2_{\hat{p}_i} \sigma^2_{\hat{p}_i}) S_{A,i} + 1} \tag{11}
\]

with \( S_{A,i} = \frac{p_B \|h_{A,i}\|^2}{2 \sigma^2_{\hat{p}_i}} \). Hence the effective return channel capacity from UE\(_i\) to AP (relative to \( s_i \)) is

\[
C_{A,i} = \log \frac{1}{\sigma^2_{\Delta s_i}} = \log \left(1 + \frac{S_{A,i}}{S_i + 1}\right) \tag{12}
\]

This capacity is achievable when UE\(_i\) knows \( S_i \) as well as \( S_{A,i} \).

B. Effective Return Channel from UE\(_i\) to Eve

The signals received by Eve during both phases of MA-STEEP are

\[
y_{E,A} = \sqrt{\frac{p_A}{n_A}} G_A x + w_{E,A},
\]

\[
y_{E,i} = \sqrt{\frac{p_B}{2}} g_i (\hat{p}_i + s_i) + w_{E,i} \tag{14}
\]

for all \( i = 1, \cdots, M \). Here \( \hat{p}_i \) for every \( i \) depends on \( x \). Also note that \( s_1, \cdots, s_M \) (from different UEs) are independent of each other.

A special case of the above is that one of the users is Eve. If user \( m \) is Eve, then \( n_E = 1 \), \( G_A = h_m \) and \( g_i = g_{m,i} \) with \( i \neq m \). Here \( g_{m,i} \) is the channel gain from UE\(_i\) to UE\(_m\).

It can be shown that the MSE of the MMSE estimate of \( s_i \) by Eve using \( y_E \) is

\[
\sigma^2_{\Delta s_i,E} = 1 - r_i^H R^{-1} r_i \tag{15}
\]

where \( r_i^H = \mathbb{E}\{s_i y_i^H\} \) and \( R = \mathbb{E}\{y_i y_i^H\} \). With no loss of generality, we can now focus on \( i = 1 \). Then, we can write

\[
r_1 = \left[ \sqrt{\frac{p_B}{2}} g_1^T, 0^T \right]^T \tag{16}
\]

and

\[
R = \begin{bmatrix} R_{1,1} & \cdots & R_{1,M+1} \\ \vdots & \ddots & \vdots \\ R_{M+1,1} & \cdots & R_{M+1,M+1} \end{bmatrix} \tag{17}
\]

Here \( 0_m \) is a zero vector of \( m \) elements, and \( R_{i,j} = r_{i,j}^H \) for all \( i \) and \( j \). For \( 1 \leq i \leq M, 1 \leq j \leq M \) and \( i \neq j \),

\[
R_{i,i} = (1 + \sigma^2_{\hat{p}_i}) \frac{p_B}{2} g_i^H + \sigma^2_{E,i} I_{n_E},
\]

\[
R_{i,j} = \epsilon_{i,j} \frac{p_B}{2} g_j^H, \tag{18}
\]

\[
R_{i,M+1} = \sqrt{\frac{p_B p_A}{2 n_A}} g_i r_x^H G_A, \tag{19}
\]

\[
R_{M+1,M+1} = \frac{p_A}{n_A} G_A G_A^H + \sigma^2_{E,A} I_{n_E}, \tag{20}
\]

where \( \epsilon_{i,j} = \mathbb{E}\{\|\hat{p}_i \|^2\} \) and \( r_{x,i} = \mathbb{E}\{\|\hat{p}_i \|^2\} \). It can be shown [13] that

\[
r_{x,i} = \sigma^2_{\hat{p}_i} q_i \tag{22}
\]

with \( q_i = \bar{h}_i^* \). Furthermore, one can verify that for \( i \neq j \),

\[
\epsilon_{i,j} = \frac{S_i S_j}{(S_i + 1)(S_j + 1)} \phi_{i,j} = \sigma^2_{\hat{p}_i} \sigma^2_{\hat{p}_j} \phi_{i,j} \tag{23}
\]

with \( \phi_{i,j} = q_i^H q_j = \bar{h}_i^* \bar{h}_j^* \) for \( n_A \geq 2 \), and \( \phi_{i,j} = 1 \) for \( n_A = 1 \).

Let us rewrite (17) as

\[
R = \begin{bmatrix} R_{1,1} & \cdots & R_{1,M+1} \\ \vdots & \ddots & \vdots \\ R_{M+1,1} & \cdots & R_{M+1,M+1} \end{bmatrix} \tag{24}
\]

where \( R_{1,1} \) is the same \( n_E \times n_E \) upper-left block of \( R \) in (17). Then

\[
R^{-1} = \begin{bmatrix} (R_{1,1} - \bar{R}_{1,1} \bar{R}_{1,1}^H)^{-1} \star \\ \star \end{bmatrix} \tag{25}
\]

where \( \star \) denotes matrix blocks of no importance. Hence, (15) with \( i = 1 \) becomes

\[
\sigma^2_{\Delta s_{1,E}} = 1 - \frac{p_B}{2} b_1^H (R_{1,1} - \bar{R}_{1,1} \bar{R}_{1,1}^H)^{-1} b_1. \tag{26}
\]

Recall

\[
R_{1,1} = (1 + \sigma^2_{\hat{p}_1}) \frac{p_B}{2} g_1^H + \sigma^2_{E,1} I_{n_E}
\]

and \( \bar{R}_{1,1} = \sqrt{\frac{p_B}{2}} g_1 c_1 \). Then

\[
c_1^H = \left[ \epsilon_{1,2} \sqrt{\frac{p_B}{2}} g_2^H, \cdots, \epsilon_{1,M} \sqrt{\frac{p_B}{2}} g_M^H, \sqrt{\frac{p_A}{n_A}} \bar{G}_{x,1}^H G_A \right]. \tag{27}
\]

Hence

\[
\bar{R}_{1,1} \bar{R}_{1,1}^H = \frac{p_B}{2} g_1 c_1^H \bar{R}_{1,1}^H c_1 g_1^H. \tag{28}
\]

Let

\[
\gamma_1 = 1 + \sigma^2_{\hat{p}_1} - c_1^H \bar{R}_{1,1}^{-1} c_1. \tag{29}
\]
We see $\sigma_{p_i}^2 > \gamma_i - 1 > 0$. Here $\gamma_i - 1$ is the MSE of the MMSE estimate of $p_i$ by Eve using $y_{E|1} = [y_{E,2}, \cdots, y_{E,M}, y_{E,A}]^T$. It follows from (26) that

$$\sigma_{s_{i,E}}^2 = 1 - \frac{p_B}{2} g_i^{H} \left( \frac{p_B}{2} g_i g_i^{H} + \sigma_{E,i}^2 I_{n_E} \right)^{-1} g_i = \frac{(\gamma_i - 1)(S_{E,i} + 1)}{\gamma_i S_{E,i} + 1}, \quad (30)$$

with $S_{E,i} = \frac{p_B \|\mathbf{h}_{i}^{E} \|^2}{2_{\sigma_{E,i}^2}}$. In [13], “1/2” is not included in $S_{E,i}$. The capacity of the effective return channel from UE$_i$ to AP relative to $s_i$ is

$$C_{E|i} = \log \frac{1}{\sigma_{s_{i,E}}^2} = \log \left( 1 + \frac{S_{E,i}}{(\gamma_i - 1)(S_{E,i} + 1)} \right). \quad (31)$$

C. Secrecy Capacity of MA-STEEP

**Theorem 1:** For MA-STEEP, the secrecy capacity of the effective wiretap channel from UE$_i$ to AP (in bits per return symbol) is

$$\tilde{C}_{s,i} = (C_{A|i} - C_{E|i})^+ = \left[ \log \left( 1 + \frac{S_{A,i}}{S_{S,i} + 1} \right) \right]^+, \quad \log \left( 1 + \frac{S_{E,i}}{(\gamma_i - 1)(S_{E,i} + 1)} \right)^+, \quad (32)$$

Here only $\gamma_i$ is affected by all UEs, which in fact depends on $S_i$ and $S_{E,i} = \frac{p_B \|\mathbf{h}_{i}^{E} \|^2}{2_{\sigma_{E,i}^2}}$ for all $2 \leq i \leq M$. In [13], “1/2” is not included in $S_{E,i}$.

**Proof:** The effective return channel from UE$_i$ to AP and the effective return channel from UE$_i$ to Eve constitute an effective wiretap channel (EWT) system (relative to $s_i$) whose secrecy capacity is $(C_{A|i} - C_{E|i})^+$. The property of $\gamma_i$ follows from (29).

D. Analysis of the Special Case of $n_A = 1$

**Theorem 2:** Assume $n_A = 1$ and hence $G_A$ reduces to a vector $\mathbf{g}_A$. Recall the SNRs $S_i = \frac{p_B \|\mathbf{h}_{i}^{E} \|^2}{\sigma_{E,i}^2}$, $S_{A,i} = \frac{p_B \|\mathbf{h}_{i}^{E} \|^2}{2_{\sigma_{E,i}^2}}$ and $S_{E,i} = \frac{p_B \|\mathbf{h}_{i}^{E} \|^2}{2_{\sigma_{E,i}^2}}$. Also let $S_{E,A} = \frac{p_B \|\mathbf{h}_{A}^{E} \|^2}{\sigma_{E,A}^2}$, $\alpha_i = \frac{S_{E,A}}{S_i}$ and $\beta_i = \frac{S_{E,A}}{S_{E,i}}$. Here $\alpha_i$ is the ratio of Eve’s receive strength from Alice over UE$_i$’s, and $\beta_i$ is the ratio of Eve’s receive strength from UE$_i$ over AP’s.

$$\gamma_i - 1 = \frac{S_i}{(S_i + 1)^2} \left( 1 + \frac{S_i}{\alpha_i S_i + 1} \right) \left( 1 - \frac{t_{1,M}}{\alpha_i S_i + 1} \right) \quad (33)$$

where $t_{1,M} = 0$ for $M = 1$, and $t_{1,M}$ for $M \geq 2$ is a function of $S_{E,A}$ and $S_{E,i}$ for all $i \neq 1$, i.e.,

$$t_{1,M} = v_M^H \mathbf{B}_M^{-1} v_M \quad (34)$$

with $v_M^H = [c_2 \mathbf{g}_2^H, \cdots, c_{M-1} \mathbf{g}_{M-1}^H | c_M \mathbf{g}_M^H] = [v_{M-1}^H | c_M \mathbf{g}_M^H]$, and $C_{M-1} = \frac{c_M}{S_{E,A} + \gamma_i} \mathbf{g}_M \mathbf{g}_M^H + 1$.

$C_{M-1} = \frac{c_M}{S_{E,A} + \gamma_i} \mathbf{g}_M \mathbf{g}_M^H$ and $\mathbf{g}_M = \sqrt{\frac{p_B}{2 \gamma_i^2}} \mathbf{g}_i$. Furthermore, for $M \geq 2$, $t_{1,M} < \min(M - 1, \alpha_i S_i + 1)$. Consequently, for all $M \geq 1$, $\tilde{C}_{s,i} > 0$ if and only if

$$S_{A,i} > \left( 1 - \frac{1}{\beta_i} \right) \frac{(S_i + 1)^2 (\alpha_i S_i + 1)}{S_i^2 (1 - t_{1,M}/\alpha_i S_i + 1)} = \tilde{S}_{A,i}. \quad (37)$$

**Proof:** Available in [13]. Our simulations have validated the above stated bound on $t_{1,M}$ for $M \geq 2$.

E. Total Secrecy Capacity of MA-STEEP

A total secrecy capacity of MA-STEEP can be expressed as

$$\tilde{C}_s = \tilde{C}_{s,1} + \tilde{C}_{s,2|1} + \cdots + \tilde{C}_{s,M|1,\cdots,M-1}. \quad (38)$$

Here $\tilde{C}_{s,i|1,\cdots,i-1} \geq 0$ denotes the secrecy capacity from UE$_i$ to AP subject to $s_{1}, \cdots, s_{i-1}$ being known to Eve, the details of which are omitted. Assuming i.i.d. conditions of UEs, $\tilde{C}_{s,i|1,\cdots,i-1}$ is expected to be statistically larger than $\tilde{C}_{s,i+1|1,\cdots,i}$. More details are in [13].

IV. DISCUSSION ON IMPLEMENTATION OF MA-STEEP

We now discuss some of the implementation issues of MA-STEEP. Before the probing phase, each of the UEs could send a pilot to AP so that AP can estimate its receive channel vectors $h_{A,i}$ for all $i$. Each of the pilots should also include necessary information (such as an initial shared key) for AP to perform authentication.

In the probing phase (phase 1), the packet broadcasted by AP should have a header which allows each UE to authenticate the legitimacy of the packet from AP. The header should also include a pilot to allow each UE to perform channel estimation and to obtain its receive channel SNR, i.e., UE$_i$ now knows $\tilde{S}_i$. The header should also include $S_{A,i}$ for all $i$. The payload in the packet should contain uncoded random probing symbols, i.e., the entries of $\mathbf{x}(k) \in \mathbb{C}^{n_c \times 1}$ for probing instant $k = 1, \cdots, m$. Since UE$_i$ now knows $\tilde{S}_i$, it also knows the MSE $c_i$ of its MMSE estimate of its effective probe (see (7)). Equivalently, UE$_i$ now knows the capacity $C_{A,i}$ in (12) for the effective channel from UE$_i$ to AP, which allows UE$_i$ to encode its message for reliable transmission to AP.

In the echoing phase (phase 2), each UE applies orthogonal multiple access to AP (such as OFDMA - a good option for low latency). The header of the packet from each UE should allow AP to conduct authentication. The payload of the packet from UE$_i$ now contains a sequence of encrypted probes, i.e., $\tilde{p}_i(k) + s_i(k)$ with $k = 1, \cdots, m$. Here $s_i(k)$ should be encoded for reliable reception at AP, which should be guided by the knowledge of $C_{A,i}$. The detection of the message in $s_i(k)$ should be done optimally at AP (for example using a convolutional encoder and Viterbi’s decoder). In this way, the detection performance at any eavesdropping node (Eve) is always worse than that at AP even if Eve is much closer to AP.
than each (legitimate) UE is. Since the message from each UE is received by AP with a positive secrecy, it can also be used for secret-key update needed for future packet authentication.

Any existing encryption method (which may not be strong enough) can still be used. MA-STEEP simply adds a new layer of security, which is a strong physical layer security. How to exactly integrate MA-STEEP with a real-life multiple access system remains a future topic of research.

V. NUMERICAL ILLUSTRATIONS

For all the simulation results, we assume that the noises are i.i.d. circular complex Gaussian with zero mean and unit variance, i.e., $\mathcal{C}\mathcal{N}(0,1)$, and all channel parameters are also i.i.d. $\mathcal{C}\mathcal{N}(0,1)$. Each of the statistical distributions is based on $10^4$ independent realizations.

A. Illustration of per-user secrecy capacity $\bar{C}_{s, 1}$

It is shown in [7] and [13] that the secrecy capacity of STEEP (for $M = 1$) approaches the secret-key capacity based on the data sets collected in the probing phase if the users’ channel in the echoing phase is relatively noiseless compared to the user’s channel in the probing phase. Since the secret-key capacity is almost always positive, so is the secrecy capacity of STEEP subject to the above conditions.

We now illustrate that the secrecy capacity of MA-STEEP for each UE is also almost always positive even if $M > 1$ provided $p_B \gg p_A$. (Regardless of AP’s power capacity, $p_A$ for the probing symbols can be always chosen to meet the above condition for any given $p_B$.) Since all UEs are now statistically equivalent, we will choose $i = 1$ among $i = 1, \cdots, M$ without loss of generality. In Figs. 1-2, we see that the distributions of $\bar{C}_{s, 1}$ subject to $p_A = 10\, \text{dB}$ and $p_B = 30\, \text{dB}$ are virtually always positive. We also see that the mean of $\bar{C}_{s, 1}$ decreases as $M$ increases, but the reduction rate of $\bar{C}_{s, 1}$ is significantly smaller than the increasing rate of $M$.

For example, Fig. 1 shows that after $M$ is increased from 1 to 16, the mean of $\bar{C}_{s, 1}$ is reduced by only 13.5%.

Unlike Figs. 1-2 where $p_A = 10\, \text{dB}$ and $p_B = 30\, \text{dB}$, Figs. 3-4 show the distributions of $\bar{C}_{s, 1}$ subject to $p_A = 20\, \text{dB}$ and $p_B = 30\, \text{dB}$. In this case, we see a small probability that $\bar{C}_{s, 1}$
becomes zero when \( n_A \) is small (i.e., \( n_A = 1 \)).

**B. Illustration of the threshold \( \hat{S}_{A,1} \)**

Recall \( \hat{S}_{A,1} \) in (37) for \( n_A = 1 \), which must be exceeded by AP’s receive SNR \( S_{A,1} = \frac{p_A |h_{A,1}|^2}{2\sigma_h^2} \) for the raw channel from UE1 in order to achieve a positive secrecy rate for UE1. Fig. 5 shows the distributions of \( S_{A,1} \) in dB for \( n_E = 4 \), \( p_A = 20\)dB and \( M = 2, 4, 8, 16 \). We see that in these cases there is only a small probability that \( \hat{S}_{A,1} \) is larger than 30dB. We also see that the mean of \( \hat{S}_{A,1} \) increases very slowly as \( M \) increases. This explains the small probability that \( C_{s,1} \) becomes zero, as shown in Fig. 3.

**C. Illustration of total secrecy capacity \( \bar{C}_s \)**

In Fig. 6, we show the distributions of \( \bar{C}_s \) for \( M = 2, 4, 8, 16 \) subject to \( n_A = n_E = 4 \), \( p_A = 10\)dB and \( p_B = 30\)dB. Notice that Fig. 6a is the distribution of the sum of \( C_{s,1} \) (as shown in Fig. 2b) and \( C_{s,2|1} \). Fig. 6 suggests that the corresponding distribution of \( C_{s,2|1} \) is also strongly positive. (Note that the bin size used for the distribution in Fig. 6a differs from that in Fig. 2b.) However, we have also observed that if \( n_A < n_E \), the probability for \( C_{s,2|1} = 0 \) increases.

Since \( \bar{C}_s \) in general has contributions from \( C_{s,i|1,\cdots,i-1} \) for all \( i = 1, \cdots, M \), the mean value of \( \bar{C}_s \) typically increases with \( M \). This phenomenon differs from that for the common-nonsense method at the networking layer, of which the total secrecy is no larger than a per-user secrecy. In other words, if Eve knows the secret message from one user, then she (who received all packets) knows the corresponding nonce and hence the secret messages from all users using the same nonce.

**VI. CONCLUSION**

In this paper, we have examined MA-STEEP for secure multiple access from UEs to AP. MA-STEEP allows all UEs to effectively share a common stream of probes from AP, which makes MA-STEEP useful to meet future low-latency requirement. We have shown that, using MA-STEEP subject to a power condition, the secrecy capacity from each UE to AP is positive with high probability and robust against an increasing number \( M \) of UEs, and the total secrecy capacity in general increases with \( M \). Although the secrecy capacity loss from finite-length packets is not addressed in this paper, such a consideration would not change the novel advantage of MA-STEEP. To our knowledge, there has been no prior method which has similar properties as MA-STEEP.

**REFERENCES**


