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 if there is always a strong secret key between an access point (AP) and each user equipment (UE). A secret key used repeatedly in general loses its secrecy due to, for example, plain-text attacks [2]. The traditional methods for key generation and management are costly [3]. The use of nonce at the networking layer for communications between AP and each UE can be effective for privacy but is not spectrally efficient or of low latency. To reduce the spectral usage or latency of the transmissions between AP and all UEs, a common nonce could be broadcasted by AP and later be used by all UEs for uplink. In this case, however, any of the UEs could eavesdrop on the transmissions from other UEs.

A secret key between AP and each UE can be locally generated by the two nodes exploiting the wireless channel between them. This has been 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 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 "*s*ecret-message *t*ransmission by *e*choing *e*ncrypted *p*robes (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.

This work was supported in part by the Department of Defense under W911NF-20-2-0267. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

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 out to be a special case of STEEP. A predecessor of STEEP, called iSAT, is also shown in [6].

More specifically, in order for node B to transmit a secret message to node A, node A first transmits probing symbols to node B in what we call a "probing" phase (phase 1). The estimated probing symbols (or estimated effective probes) obtained by node B are then encrypted with the secret message and echoed back to node A in what we call an "echoing" phase (phase 2). Since node A knows the exact probing symbols while Eve only knows a noisy version of the probes, node A almost always has an advantage over Eve in detecting the secret message from node B. This results in a positive secrecy rate as long as Eve's receive channel from node A is not infinitely stronger than node B's receive channel from node A, which is the case if Eve's channel is not noiseless.

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 UE$_i$ in baseband is modelled by

$$y_i = \mathbf{h}_i^T \mathbf{x}_A + w_i \tag{1}$$

where $\mathbf{x}_A \in \mathbb{C}^{n_A \times 1}$ is a vector transmitted by AP, $\mathbf{h}_i \in \mathbb{C}^{n_A \times 1}$ is the channel vector, y_i and w_i are the received signal and noise at UE$_i$. 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 UE$_i$ to AP can be modelled as

$$\mathbf{y}_{A,i} = \mathbf{h}_{A,i} x_i + \mathbf{w}_{A,i}. \tag{2}$$

where x_i is a symbol transmitted by UE$_i$, $\mathbf{h}_{A,i} \in \mathbb{C}^{n_A \times 1}$ is the channel vector from UE$_i$ to AP, and $\mathbf{y}_{A,i}$ and $\mathbf{w}_{A,i}$ are the received signal and noise at AP. Like w_i in (1), $\mathbf{w}_{A,i}$ 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 $\sqrt{\frac{p_A}{n_A}}\mathbf{x}$ with $\mathcal{E}\{\|\mathbf{x}\|^2\} = n_A$. Then the corresponding signal received by UE$_i$ for each of $i = 1, \cdots, M$ is

$$y_i = \sqrt{\frac{p_A}{n_A}} \mathbf{h}_i^T \mathbf{x} + w_i \tag{3}$$

where $\mathcal{E}\{|w_i|^2\} = \sigma_i^2$. We will also write

$$y_i = \begin{cases} \sqrt{p_A} h_i p_i + w_i, & n_A = 1; \\ \sqrt{\frac{p_A}{n_A}} \|\mathbf{h}_i\| p_i + w_i, & n_A \geq 2; \end{cases} \tag{4}$$

with

$$p_i = \begin{cases} x, & n_A = 1; \\ \bar{\mathbf{h}}_i^T \mathbf{x}, & n_A \geq 2. \end{cases} \tag{5}$$

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

We call p_i the effective probing symbol from AP to UE$_i$, 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 $\bar{\mathbf{h}}_i$ from UE$_i$. For secrecy analysis, we will assume that $\bar{\mathbf{h}}_i$ 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), UE$_i$ for $i = 1, \cdots, M$ transmits $\sqrt{\frac{p_B}{2}}(\hat{p}_i + s_i)$ to AP, where s_i is a secret symbol of unit variance from UE$_i$, and $\hat{p}_i$ is the MMSE estimate of p_i by UE$_i$ using y_i. Here each UE knows its receive channel.

Note that the above $\sqrt{\frac{p_B}{2}}(\hat{p}_i + s_i)$ also corresponds to $\sqrt{\frac{p_B}{2}}(\hat{p}_i(k) + s_i(k))$ if k denotes the kth probing symbol interval and the kth echoed symbol interval for UE$_i$.

We will also assume that $\mathbf{x}$, w_i and s_i for all i are circular complex Gaussian of zero mean. Then it can be shown [13] that

$$\hat{p}_i = \frac{\sqrt{\frac{p_A}{n_A}}\|\mathbf{h}_i\|}{\frac{p_A}{n_A}\|\mathbf{h}_i\|^2 + \sigma_i^2} y_i = \frac{\sqrt{S_i}}{S_i+1}\frac{1}{\sigma_i} y_i, \tag{6}$$

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

$$c_i \doteq \sigma_{\hat{p}_i}^2 \doteq \mathcal{E}\{|\hat{p}_i|^2\} = \frac{S_i}{S_i+1}, \tag{7}$$

$$\sigma_{\Delta p_i}^2 \doteq \mathcal{E}\{|\hat{p}_i - p_i|^2\} = \frac{1}{S_i+1} = 1 - c_i. \tag{8}$$

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

$$\mathbf{y}_{A,i} = \sqrt{\frac{p_B}{2}}(\hat{p}_i + s_i)\mathbf{h}_{A,i} + \mathbf{w}_{A,i}. \tag{9}$$

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

$$\hat{s}_i = \frac{\frac{p_B}{2}}{\frac{p_B}{2}(\sigma_{\hat{p}_i}^2 \sigma_{\Delta p_i}^2 + 1)\|\mathbf{h}_{A,i}\|^2 + \sigma_{A,i}^2}\mathbf{h}_{A,i}^H \Delta\mathbf{y}_{A,i} \tag{10}$$

with $\Delta\mathbf{y}_{A,i} = \mathbf{y}_{A,i} - \mathcal{E}\{\mathbf{y}_{A,i}|\mathbf{x}\} = \mathbf{y}_{A,i} - \sqrt{\frac{p_B}{2}}\mathbf{h}_{A,i}\sigma_{\hat{p}_i}^2 p_i$, and the MSE of $\hat{s}_i$ is

$$\sigma_{\Delta s_i}^2 \doteq \mathcal{E}\{|\hat{s}_i - s_i\|^2\} = \frac{\sigma_{\hat{p}_i}^2\sigma_{\Delta p_i}^2 S_{A,i} + 1}{(1+\sigma_{\hat{p}_i}^2\sigma_{\Delta p_i}^2)S_{A,i} + 1} \tag{11}$$

with $S_{A,i} = \frac{p_B\|\mathbf{h}_{A,i}\|^2}{2\sigma_{A,i}^2}$. Hence the effective return channel capacity from UE_i to AP (relative to s_i) is

$$C_{A|i} = \log\frac{1}{\sigma_{\Delta s_i}^2} = \log\left(1 + \frac{S_{A,i}}{\frac{S_i S_{A,i}}{(S_i+1)^2} + 1}\right). \tag{12}$$

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

$$\mathbf{y}_{E,A} = \sqrt{\frac{p_A}{n_A}}\mathbf{G}_A\mathbf{x} + \mathbf{w}_{E,A}, \tag{13}$$

$$\mathbf{y}_{E,i} = \sqrt{\frac{p_B}{2}}\mathbf{g}_i(\hat{p}_i + s_i) + \mathbf{w}_{E,i} \tag{14}$$

for all $i = 1, \cdots, M$. Here $\hat{p}_i$ for every i depends on $\mathbf{x}$. 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 $n_E = 1$, $\mathbf{G}_A = \mathbf{h}_m$ and $\mathbf{g}_i = g_{m,i}$ 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 $\mathbf{y}_E \doteq [\mathbf{y}_{E,1}^T, \cdots, \mathbf{y}_{E,M}^T, \mathbf{y}_{E,A}^T]^T$ is

$$\sigma_{\Delta s_{i,E}}^2 = 1 - \mathbf{r}_i^H \mathbf{R}^{-1}\mathbf{r}_i \tag{15}$$

where $\mathbf{r}_i^H = \mathcal{E}\{s_i \mathbf{y}_E^H\}$ and $\mathbf{R} = \mathcal{E}\{\mathbf{y}_E\mathbf{y}_E^H\}$. With no loss of generality, we can now focus on $i = 1$. Then, we can write

$$\mathbf{r}_1 = \left[\sqrt{\frac{p_B}{2}}\mathbf{g}_1^T, \mathbf{0}_{n_E M}^T\right]^T \tag{16}$$

and

$$\mathbf{R} = \begin{bmatrix} \mathbf{R}_{1,1} & \cdots & \mathbf{R}_{1,M+1} \\ \cdots & \cdots & \cdots \\ \mathbf{R}_{M+1,1} & \cdots & \mathbf{R}_{M+1,M+1} \end{bmatrix}. \tag{17}$$

Here $\mathbf{0}_m$ is a zero vector of m elements, and $\mathbf{R}_{i,j} = \mathbf{R}_{j,i}^H$ for all i and j. For $1 \leq i \leq M$, $1 \leq j \leq M$ and $i \neq j$,

$$\mathbf{R}_{i,i} = (1 + \sigma_{\hat{p}_i}^2)\frac{p_B}{2}\mathbf{g}_i\mathbf{g}_i^H + \sigma_{E,i}^2\mathbf{I}_{n_E}, \tag{18}$$

$$\mathbf{R}_{i,j} = \epsilon_{i,j}\frac{p_B}{2}\mathbf{g}_i\mathbf{g}_j^H, \tag{19}$$

$$\mathbf{R}_{i,M+1} = \sqrt{\frac{p_A p_B}{2n_A}}\mathbf{g}_i\mathbf{r}_{x,i}^H\mathbf{G}_A^H, \tag{20}$$

$$\mathbf{R}_{M+1,M+1} = \frac{p_A}{n_A}\mathbf{G}_A\mathbf{G}_A^H + \sigma_{E,A}^2\mathbf{I}_{n_E}, \tag{21}$$

where $\epsilon_{i,j} = \mathcal{E}\{\hat{p}_i\hat{p}_j^*\}$ and $\mathbf{r}_{x,i} = \mathcal{E}\{\mathbf{x}\hat{p}_i^*\}$. It can be shown [13] that

$$\mathbf{r}_{x,i} = \sigma_{\hat{p}_i}^2\mathbf{q}_i \tag{22}$$

with $\mathbf{q}_i = \bar{\mathbf{h}}_i^*$. Furthermore, one can verify that for $i \neq j$,

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

with $\phi_{i,j} = \mathbf{q}_i^H\mathbf{q}_j = \bar{\mathbf{h}}_i^T\bar{\mathbf{h}}_j^*$ for $n_A \geq 2$, and $\phi_{i,j} = 1$ for $n_A = 1$.

Let us rewrite (17) as

$$\mathbf{R} = \begin{bmatrix} \mathbf{R}_{1,1} & \bar{\mathbf{R}}_1 \\ \bar{\mathbf{R}}_1^H & \bar{\mathbf{R}}_{1,1} \end{bmatrix} \tag{24}$$

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

$$\mathbf{R}^{-1} = \begin{bmatrix} (\mathbf{R}_{1,1} - \bar{\mathbf{R}}_1\bar{\mathbf{R}}_{1,1}^{-1}\bar{\mathbf{R}}_1^H)^{-1} & * \\ * & * \end{bmatrix} \tag{25}$$

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

$$\sigma_{\Delta s_{1,E}}^2 = 1 - \frac{p_B}{2}\mathbf{g}_1^H(\mathbf{R}_{1,1} - \bar{\mathbf{R}}_1\bar{\mathbf{R}}_{1,1}^{-1}\bar{\mathbf{R}}_1^H)^{-1}\mathbf{g}_1. \tag{26}$$

Recall $\mathbf{R}_{1,1} = (1 + \sigma_{\hat{p}_1}^2)\frac{p_B}{2}\mathbf{g}_1\mathbf{g}_1^H + \sigma_{E,1}^2\mathbf{I}_{n_E}$ and $\bar{\mathbf{R}}_1 = \sqrt{\frac{p_B}{2}}\mathbf{g}_1\mathbf{c}_1^H$ with

$$\mathbf{c}_1^H = \left[\epsilon_{1,2}\sqrt{\frac{p_B}{2}}\mathbf{g}_2^H, \cdots, \epsilon_{1,M}\sqrt{\frac{p_B}{2}}\mathbf{g}_M^H, \sqrt{\frac{p_A}{n_A}}\mathbf{r}_{x,1}^H\mathbf{G}_A^H\right]. \tag{27}$$

Hence

$$\bar{\mathbf{R}}_1\bar{\mathbf{R}}_{1,1}^{-1}\bar{\mathbf{R}}_1^H = \frac{p_B}{2}\mathbf{g}_1\mathbf{c}_1^H\bar{\mathbf{R}}_{1,1}^{-1}\mathbf{c}_1\mathbf{g}_1^H. \tag{28}$$

Let

$$\gamma_1 = 1 + \sigma_{\hat{p}_1}^2 - \mathbf{c}_1^H\bar{\mathbf{R}}_{1,1}^{-1}\mathbf{c}_1. \tag{29}$$

We see $\sigma^2_{\hat{p}_1} > \gamma_1 - 1 > 0$. Here $\gamma_1 - 1$ is the MSE of the MMSE estimate of $\hat{p}_1$ by Eve using $\mathbf{y}_{E|1} \doteq [\mathbf{y}^T_{E,2}, \cdots, \mathbf{y}^T_{E,M}, \mathbf{y}^T_{E,A}]^T$.

It follows from (26) that

$$\sigma^2_{\Delta s_{1,E}} = 1 - \frac{p_B}{2}\mathbf{g}_1^H \left(\frac{p_B}{2}\gamma_1 \mathbf{g}_1\mathbf{g}_1^H + \sigma^2_{E,1}\mathbf{I}_{n_E}\right)^{-1}\mathbf{g}_1 = \frac{(\gamma_1 - 1)S_{E,1} + 1}{\gamma_1 S_{E,1} + 1}, \quad (30)$$

with $S_{E,1} = \frac{p_B\|\mathbf{g}_1\|^2}{2\sigma^2_{E,1}}$. In [13], "1/2" is not included in $S_{E,1}$.

The capacity of the effective return channel from UE_1 to AP relative to s_1 is

$$C_{E|1} = \log\frac{1}{\sigma^2_{\Delta s_{1,E}}} = \log\left(1 + \frac{S_{E,1}}{(\gamma_1 - 1)S_{E,1} + 1}\right). \quad (31)$$

C. Secrecy Capacity of MA-STEEP

***Theorem** 1:* For MA-STEEP, the secrecy capacity of the effective wiretap channel from UE_1 to AP (in bits per return symbol) is

$$\bar{C}_{s,1} = (C_{A|1} - C_{E|1})^+ = \left[\log\left(1 + \frac{S_{A,1}}{\frac{S_1 S_{A,1}}{(S_1+1)^2} + 1}\right) - \log\left(1 + \frac{S_{E,1}}{(\gamma_1 - 1)S_{E,1} + 1}\right)\right]^+. \quad (32)$$

Here only γ_1 is affected by all UEs, which in fact depends on S_1 and $S_{E,i} = \frac{p_B\|\mathbf{g}_i\|^2}{2\sigma^2_{E,i}}$ 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_1 to AP and the effective return channel from UE_1 to Eve constitute an effective wiretap-channel (eWTC) system (relative to s_1) whose secrecy capacity is $(C_{A|1} - C_{E|1})^+$. The property of γ_1 follows from (29). ■

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

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

$$\gamma_1 - 1 = \frac{S_1}{(S_1+1)^2}\left(1 + \frac{S_1}{\alpha_1 S_1 + 1}\left(1 - \frac{t_{1,M}}{\alpha_1 S_1 + 1}\right)\right) \quad (33)$$

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.,

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

with

$$\mathbf{v}_M^H = [c_2\tilde{\mathbf{g}}_2^H, \cdots, c_{M-1}\tilde{\mathbf{g}}^H_{M-1}|c_M\tilde{\mathbf{g}}_M^H] = [\mathbf{v}^H_{M-1}|c_M\tilde{\mathbf{g}}_M^H], \quad (35)$$

$$\mathbf{B}_M = \left[\begin{array}{c|c} \mathbf{B}_{M-1} & \mathbf{C}_{M-1} \\ \hline \mathbf{C}^H_{M-1} & \left(1 + \frac{c_M^2}{S_{E,A}+1}\right)\tilde{\mathbf{g}}_M\tilde{\mathbf{g}}_M^H + \mathbf{I} \end{array}\right] \quad (36)$$

and $\mathbf{C}_{M-1} = \frac{c_M}{S_{E,A}+1}\mathbf{v}_{M-1}\tilde{\mathbf{g}}_M^H$ and $\tilde{\mathbf{g}}_i = \sqrt{\frac{p_B}{2\sigma^2_{E,i}}}\mathbf{g}_i$. Furthermore, for $M \geq 2$, $t_{1,M} < \min(M-1, \alpha_1 S_1 + 1)$. Consequently, for all $M \geq 1$, $\bar{C}_{s,1} > 0$ if and only if

$$S_{A,1} > \left(1 - \frac{1}{\beta_1}\right)\frac{(S_1+1)^2(\alpha_1 S_1 + 1)}{S_1^2\left(1 - \frac{t_{1,M}}{\alpha_1 S_1 + 1}\right)} \doteq \tilde{S}_{A,1}. \quad (37)$$

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

The above result says that for any $M \geq 1$, there is a finite threshold $\tilde{S}_{A,1}$ such that the secrecy capacity $\bar{C}_{s,1}$ for UE_1 is positive if and only if $S_{A,1} = \frac{p_B\|\mathbf{h}_{A,1}\|^2}{2\sigma^2_{A,1}} > \tilde{S}_{A,1}$. Again UE_1 is effectively any of the M UEs.

E. Total Secrecy Capacity of MA-STEEP

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

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

Here $\bar{C}_{s,i|1,\cdots,i-1} \geq 0$ 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, $\bar{C}_{s,i|1,\cdots,i-1}$ is expected to be statistically larger than $\bar{C}_{s,i+1|1,\cdots,i}$. 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 $\mathbf{h}_{A,i}$ for all i. Each of the pilots should also include necessary information (such as an initial shared key) for AP to perform authentication.

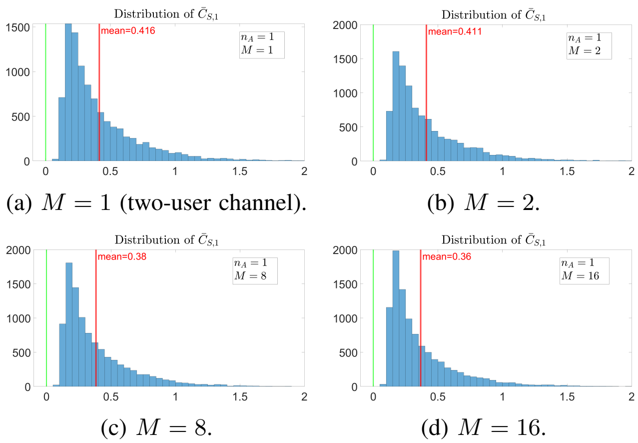
In the probing phase (phase 1), the packet broadcasted by AP should have a header which allows each UE to authenticate the legitimacy of the packet from AP. The header should also include a pilot to allow each UE to perform channel estimation and to obtain its receive channel SNR, i.e., UE_i now knows 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 $\mathbf{x}(k) \in \mathbb{C}^{n_A\times 1}$ for probing instant $k = 1, \cdots, m$. Since UE_i now knows 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., $\hat{p}_i(k) + s_i(k)$ 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.

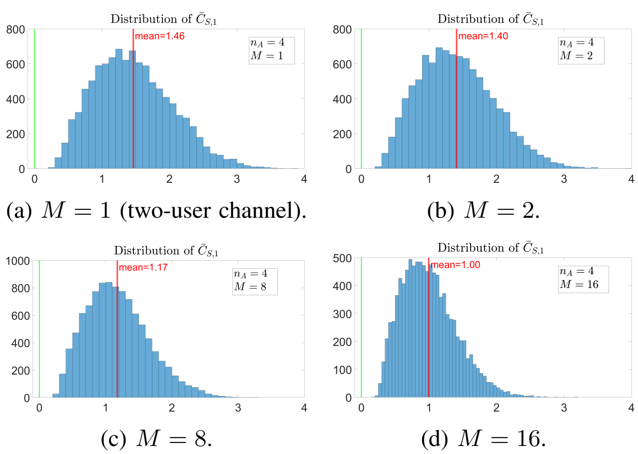
V. Numerical Illustrations

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., $\mathcal{CN}(0,1)$, and all channel parameters are also i.i.d. $\mathcal{CN}(0,1)$. Each of the statistical distributions is based on 10^4 independent realizations.



(a) $M = 1$ (two-user channel). (b) $M = 2$. (c) $M = 8$. (d) $M = 16$.

Fig. 1: Distributions of $\bar{C}_{s,1}$ for $\underline{n_A = 1}$, $n_E = 4$, $\underline{p_A = 10\text{dB}}$ and $p_B = 30$dB.

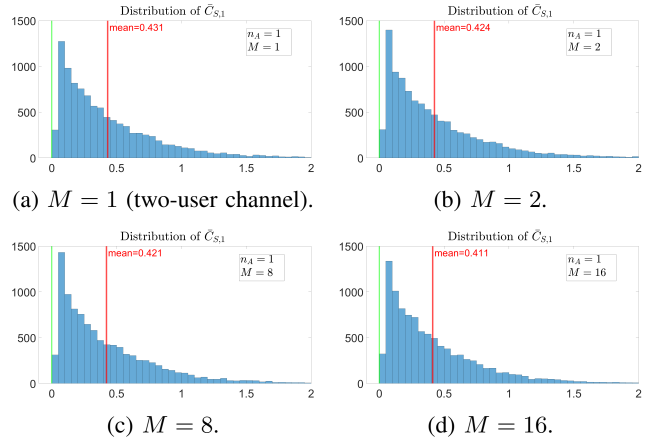


(a) $M = 1$ (two-user channel). (b) $M = 2$. (c) $M = 8$. (d) $M = 16$.

Fig. 2: Distributions of $\bar{C}_{s,1}$ for $\underline{n_A = 4}$, $n_E = 4$, $\underline{p_A = 10\text{dB}}$ and $p_B = 30$dB.

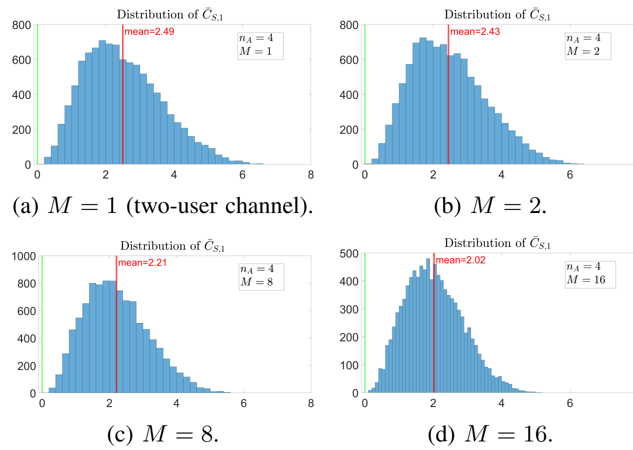
A. Illustration of per-user secrecy capacity $\bar{C}_{s,1}$

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.



(a) $M = 1$ (two-user channel). (b) $M = 2$. (c) $M = 8$. (d) $M = 16$.

Fig. 3: Distributions of $\bar{C}_{s,1}$ for $\underline{n_A = 1}$, $n_E = 4$, $\underline{p_A = 20\text{dB}}$ and $p_B = 30$dB.



(a) $M = 1$ (two-user channel). (b) $M = 2$. (c) $M = 8$. (d) $M = 16$.

Fig. 4: Distributions of $\bar{C}_{s,1}$ for $\underline{n_A = 4}$, $n_E = 4$, $\underline{p_A = 20\text{dB}}$ and $p_B = 30$dB.

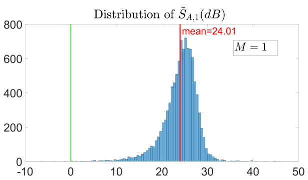
We now illustrate that the secrecy capacity of MA-STEEP for each UE is also almost always positive even if $M > 1$ provided $p_B \gg p_A$. (Regardless of AP's power capacity, p_A for the probing symbols can be always chosen to meet the above condition for any given p_B.) Since all UEs are now statistically 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 $p_A = 10$dB and $p_B = 30$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 $p_A = 10$dB and $p_B = 30$dB, Figs. 3-4 show the distributions of $\bar{C}_{s,1}$ subject to $p_A = 20$dB and $p_B = 30$dB. In this case, we see a small probability that $\bar{C}_{s,1}$

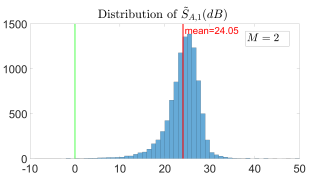
becomes zero when n_A is small (i.e., $n_A = 1$).

B. Illustration of the threshold $\tilde{S}_{A,1}$

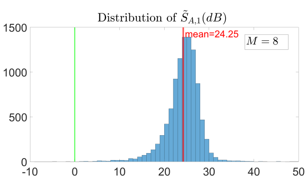
Recall $\tilde{S}_{A,1}$ in (37) for $n_A = 1$, which must be exceeded by AP's receive SNR $S_{A,1} = \frac{p_B\|\mathbf{h}_{A,1}\|^2}{2\sigma_{A,1}^2}$ for the raw channel from UE_1 in order to achieve a positive secrecy rate for UE_1. Fig. 5 shows the distributions of $\tilde{S}_{A,1}$ in dB for $n_E = 4$, $p_A = 20$dB and $M = 2, 4, 8, 16$. We see that in these cases there is only a small probability that $\tilde{S}_{A,1}$ is larger than 30dB. We also see that the mean of $\tilde{S}_{A,1}\,(\mathrm{dB})$ increases very slowly as M increases. This explains the small probability that $\bar{C}_{s,1}$ becomes zero, as shown in Fig. 3.



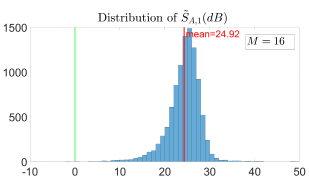
(a) $M = 1$ (two-user channel).



(b) $M = 2$.



(c) $M = 8$.



(d) $M = 16$.

Fig. 5: Distributions of $\tilde{S}_{A,1}\,(\mathrm{dB}) = 10\log_{10}\tilde{S}_{A,1}$ for $n_A = 1$, $n_E = 4$ and $p_A = 20$dB.

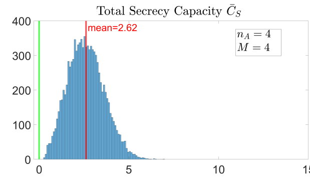
C. Illustration of total secrecy capacity $\bar{C}_s$

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 $\bar{C}_{s,1}$ (as shown in Fig. 2b) and $\bar{C}_{s,2|1}$. Fig. 6 suggests that the corresponding distribution of $\bar{C}_{s,2|1}$ 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 $\bar{C}_{s,2|1} = 0$ increases.

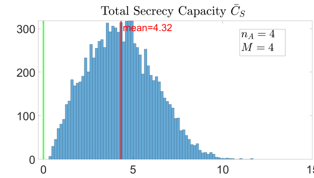
Since $\bar{C}_s$ in general has contributions from $\bar{C}_{s,i|1,\cdots,i-1}$ for all $i = 1, \cdots, M$, the mean value of $\bar{C}_s$ typically increases with M. This phenomenon differs from that for the common-nonce method at the networking layer, of which the total secrecy is no larger than a 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

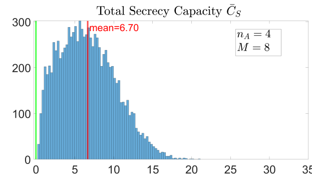
In this paper, we have examined MA-STEEP for secure multiple access from UEs to AP. MA-STEEP allows all UEs to effectively share a common stream of probes from AP, which makes MA-STEEP useful to meet future low-latency requirement. We have shown that, using MA-STEEP subject



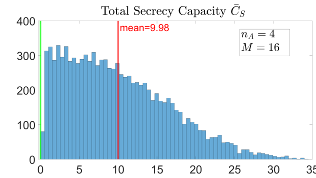
(a) $M = 2$.



(b) $M = 4$.



(c) $M = 8$.



(d) $M = 16$.

Fig. 6: Distributions of $\bar{C}_s$ for $n_A = 4$, $n_E = 4$, $p_A = 10$dB and $p_B = 30$dB.

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

[1] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5G and beyond," *Proc. of the IEEE*, vol. 105, no. 12, pp. 2347–2381, Dec. 2017.

[2] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*. Pearson, 2005.

[3] A. Barki, A. Bouabdallah, S. Gharout, and J. Traoré, "M2M security: challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, p. 1241–1254, 2nd Quart. 2016.

[4] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, p. 138406–138446, 2020.

[5] M. Hayashi and A. Vazquez-Castro, "Two-way physical layer security protocol for Gaussian channels," *IEEE Transactions on Communications*, vol. 68, no. 5, p. 3068–3078, May 2020.

[6] Y. Hua, "Generalized channel probing and generalized pre-processing for secret key generation," *IEEE Transactions on Signal Processing*, vol. 71, pp. 1067–1082, April 2023.

[7] ——, "Secret-message transmission by echoing encrypted probes — STEEP," Sept. 2023, arxiv.org.

[8] Y. Hua and A. Maksud, "Secret-key capacity from MIMO channel probing," *IEEE Wireless Communications Letters*, vol. 13, no. 5, pp. 1434–1438, May 2024.

[9] C. Feng, H.-M. Wang, and H. V. Poor, "Reliable and secure short-packet communications," *IEEE Trans. Wireless Communications*, vol. 21, no. 3, pp. 1913–1926, Mar. 2022.

[10] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge University Press, 2011.

[11] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: nonasymptotic fundamental limits," *IEEE Trans. Information Theory*, vol. 65, no. 7, pp. 4069–4093, July 2019.

[12] P. Xu, G. Chen, Z. Yang, Y. Li, and S. Tomasin, "Multiple access wiretap channel with partial rate-limited feedback," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 3279–3294, 2024.

[13] Y. Hua, "On secret-message transmission by echoing encrypted probes," *IEEE Transactions on Communications*, submitted Jan. 2024, revised May 2024.