Secure Physical Layer Voting

Nirnimesh Ghose, Bocan Hu, Yan Zhang, and Loukas Lazos
Dept. of Electrical and Computer Engineering, University of Arizona
Email: {nghose, bocanhu, yanzhang, llazos}@email.arizona.edu

APPENDIX A

Proposition 1: Let participants cast M votes over $2M \leq N$ subcarriers by transmitting ℓ symbol votes. Let an external adversary inject energy on $J \leq N$ subcarriers. The probability of flipping the voting outcome is

$$\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] = \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \Pr[\mathbf{Z}=z], \tag{1}$$

where $n_1 = \frac{M+\mu}{2}$ denotes the number of votes in favor of $\mathcal{T}$ and $n_2 = \frac{M-\mu}{2}$ denotes the number of votes not in favor of $\mathcal{T}$.

$$\begin{aligned}\Pr[\mathbf{Z}=z] &= \sum_x \left(\binom{n_1}{x}\binom{n_2}{x-z} \left(\frac{\binom{N-2x+z}{J-2x+z}}{\binom{N}{J}} \right)^{\ell} \right. \\ &\quad \left. - \left(\sum_{w=1}^{\min\{n_1-x,J-x\}} \sum_{k=0}^{w-z} \binom{n_1-x}{w}\binom{n_2-x+z}{k} \frac{\binom{N-n_1-n_2-4x+2z}{J-w-k-2x+z}}{\binom{N-x}{J-x}} \right) \left(\frac{1}{\binom{N}{J}} \right)^{\ell} \right). \end{aligned} \tag{2}$$

Proof: Let a vote process with M participants lead to a voting outcome $\mathcal{T}$, selected with a margin μ. Without loss of generality, assume that the votes in favor of $\mathcal{T}$ are "yes" votes. For a margin μ, it is straightforward to show that there are $n_1 = \frac{M+\mu}{2}$ "yes" votes and $n_2 = \frac{M-\mu}{2}$ "no" votes. To flip $\mathcal{T}$ through vote nullification, the adversary must nullify at least $\mu - \gamma$ more "yes" votes than "no" votes to make the vote difference less or equal to γ.

Let $\mathbf{X}$ be a random variable (RV) denoting number of nullified "yes" votes when the adversary injects energy on J subcarriers on each of the ℓ voting slots. To nullify x "yes" votes, the adversary has to pick at each slot those subcarriers that nullify the "yes" votes of a set of x participants. Similarly, let $\mathbf{Y}$ be an RV denoting the number of nullified "no" votes, when the adversary injects energy on J subcarriers on each of the ℓ voting slots. Let also $\mathbf{Z} = \mathbf{X} - \mathbf{Y}$ denote the excess number of nullified "yes" votes relative to "no" votes. The pmf of $\mathbf{Z}$ can be computed using

$$\begin{aligned}\Pr[\mathbf{Z}=z] &= \sum_x \Pr[\mathbf{X}=x, \mathbf{Y}=x-z] \\ &= \sum_x \left(\binom{n_1}{x}\binom{n_2}{x-z} \left(\frac{\binom{N-2x+z}{J-2x+z}}{\binom{N}{J}} \right)^{\ell} \right. \\ &\quad \left. - \left(\sum_{w=1}^{\min\{n_1-x,J-x\}} \sum_{k=0}^{w-z} \binom{n_1-x}{w}\binom{n_2-x+z}{k} \frac{\binom{N-n_1-n_2-4x+2z}{J-w-k-2x+z}}{\binom{N-x}{J-x}} \right) \left(\frac{1}{\binom{N}{J}} \right)^{\ell} \right) \end{aligned} \tag{3}$$

In eq. (3), the first term denotes all possible combinations of x subcarriers that nullify x out of n_1 "yes" votes, which fixes the combination of x votes that are nullified after ℓ slots. Similarly, it has all possible combinations of $x - z$ subcarriers that nullify $x - z$ out of n_2 "no" votes. This term is multiplied by the number of ways of choosing $J - 2x + z$ subcarriers from the remaining $N - 2x + z$, and divided by all possible ways of choosing J subcarriers out of N. The second multiplier is raised to the power of ℓ because the subcarrier selection is repeated with every time slot in an independent fashion. Note that the first multiplier is not raised to the power of ℓ because the set of votes to be nullified remains fixed after the first slot. The second term, excludes all possible combinations of additional "yes" votes and "no" being nullified due to the selection of the remaining $J - 2x + z$ subcarriers. This term computes all possible selections of $J - 2x + z$ subcarriers in which at least one subcarrier is assigned to the remaining $n_1 - x$ "yes" votes and $n_2 - x + z$ "no" votes and this subcarrier is present on all the ℓ slots, multiplied by the probability of occurrence for each selection.

The probability of flipping the voting outcome is equal to the probability of nullifying at least $\mu - \gamma$ more "yes" than "no" votes, i.e., $\mathbf{Z} \geq \mu - \gamma$. Summing (3) over all $z \geq \mu - \gamma$ yields,

$$\begin{aligned}\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] &= Pr[\mathbf{Z} \geq \mu - \gamma] \\ &= \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \Pr[\mathbf{Z}=z], \end{aligned} \tag{4}$$

where $\Pr[\mathbf{Z} = z]$ is given by (3). This completes the proof.

■

APPENDIX B

Corollary 1: For an external adversary, $\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] \leq p_0$ if

$$\ell > \lceil \frac{1}{\log \frac{1}{C_1}} \log \frac{C_0}{p_0} \rceil, \tag{5}$$

where

$$C_0 = \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \left(\binom{n_1}{x} \binom{n_2}{x-z} \right), \tag{6}$$

$$C_1 = \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \frac{\binom{N-2x+z}{J-2x+z}}{\binom{N}{J}}. \tag{7}$$

Proof: We wish to determine the value of ℓ for which $\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] \leq p_0$. From (4), it follows that

$$\begin{aligned}
\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] &= \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \left(\binom{n_1}{x} \binom{n_2}{x-z} \left(\frac{\binom{N-2x+z}{J-2x+z}}{\binom{N}{J}} \right)^{\ell} \right. \\
&\quad \left. - \left(\sum_{w=1}^{\min\{n_1-x,J-x\}} \sum_{k=0}^{w-z} \binom{n_1-x}{w} \binom{n_2-x+z}{k} \frac{\binom{N-n_1-n_2-4x+2z}{J-w-k-2x+z}}{\binom{N-x}{J-x}} \right) \left(\frac{1}{\binom{N}{J}} \right)^{\ell} \right) \\
&< \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \left(\binom{n_1}{x} \binom{n_2}{x-z} \left(\frac{\binom{N-2x+z}{J-2x+z}}{\binom{N}{J}} \right)^{\ell} \right) \\
&< \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \left(\binom{n_1}{x} \binom{n_2}{x-z} \right) \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \left(\frac{\binom{N-2x+z}{J-2x+z}}{\binom{N}{J}} \right)^{\ell} \\
&< \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \left(\binom{n_1}{x} \binom{n_2}{x-z} \right) \left(\sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \frac{\binom{N-2x+z}{J-2x+z}}{\binom{N}{J}} \right)^{\ell}
\end{aligned} \tag{8}$$

Limiting the right hand side of (8) by p_0 and solving for ℓ,

$$\ell > \lceil \frac{1}{\log \frac{1}{C_1}} \log \frac{C_0}{p_0} \rceil, \tag{9}$$

where

$$C_0 = \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \left(\binom{n_1}{x} \binom{n_2}{x-z} \right), \tag{10}$$

$$C_1 = \sum_{z=\mu-\gamma}^{\min\{n_1,J\}} \sum_{x=z}^{\min\{n_1,J\}} \frac{\binom{N-2x+z}{J-2x+z}}{\binom{N}{J}}. \tag{11}$$

This completes the proof.

■

APPENDIX C

Proposition 2: Let an internal adversary attempt to nullify the votes of δ participants and let $p = \Pr[v(i) = e]$ denote the probability of nullifying a singe vote, as given by (12).

$$\begin{aligned} \Pr[\hat{v}(i) = e] &= \Pr[\hat{v}_i(n_0) = e, \ldots, \hat{v}_i(n_0 + \ell - 1) = e] \\ &= 0.5^{\ell}. \end{aligned} \tag{12}$$

Under the secret vote model, an internal adversary following Strategy 1 can flip the voting outcome for a decision threshold γ and a margin μ with probability

$$\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] = \sum_{i=\mu-\gamma}^{\delta} HG(n_1, M, i, \delta) \sum_{z=\mu-\gamma}^{i} \sum_{x=z}^{\min\{i, \frac{\delta+z}{2}\}} \frac{\binom{i}{x}\binom{\delta-i}{x-z}}{\binom{\delta}{2x-z}} B(2x - z, \delta, p), \tag{13}$$

where $n_1 = \frac{M+\mu}{2}$ denotes the number of votes in favor of $\mathcal{T}$.

Proof: Let a vote process with M participants lead to a voting outcome $\mathcal{T}$, selected with a margin μ. Without loss of generality, assume that the votes in favor of $\mathcal{T}$ are "yes" votes. For a margin μ, it is straightforward to show that there are $n_1 = \frac{M+\mu}{2}$ "yes" votes and $n_2 = \frac{M-\mu}{2}$ "no" votes. To flip $\mathcal{T}$ through vote nullification, the adversary must nullify at least $\mu - \gamma$ more "yes" votes than "no" votes to make the vote difference less or equal to γ. For an adversary that attempts to nullify a total of δ votes, the probability that i of them are "yes" votes is given by a hypergeometric distribution.

$$\Pr[\mathbf{I} = i] = HG(n_1, N, i, \delta) \tag{14}$$

Each vote is successfully nullified with probability $p = \Pr[v_i = e] = 0.5^{\ell}$. Let $\mathbf{X}$ be an RV denoting the number of successfully nullified "yes" votes, when x "yes" votes are attacked. Because the nullification of each vote is an independent Bernoulli trial (the adversary randomly picks one of the two subcarriers assigned to each attacked participant), $\mathbf{X}$ follows the binomial distribution

$$\Pr[\mathbf{X} = x] = B(x, i, p), \quad p = 0.5^{\ell}. \tag{15}$$

Similarly, let $\mathbf{Y}$ be an RV denoting the number of "no" votes that are successfully nullified. For $\mathbf{Y}$,

$$\Pr[\mathbf{Y} = y] = B(y, \delta - i, p), \quad p = 0.5^{\ell}. \tag{16}$$

The probability that the number of successfully nullified "yes" votes exceeds the number of nullified "no" votes by exactly z votes is given by RV $\mathbf{Z} = \mathbf{X} - \mathbf{Y}$. The pmf of $\mathbf{Z}$ can be computed using the convolution formula.

$$\begin{aligned} \Pr[\mathbf{Z} = z] &= \sum_{x} \Pr[\mathbf{X} = x, \mathbf{Y} = x - z] \\ &= \sum_{x} \Pr[\mathbf{X} = x] \Pr[\mathbf{Y} = x - z | \mathbf{X} = x] \\ &= \sum_{x} B(x, i, p) B(x - z, \delta - i, p) \\ &= \sum_{x=z}^{\min\{i, \frac{\delta+z}{2}\}} \frac{\binom{i}{x}\binom{\delta-i}{x-z}}{\binom{\delta}{2x-z}} B(2x - z, \delta, p). \end{aligned} \tag{17}$$

The probability of flipping the voting outcome is equal to the probability of nullifying at least $\mu - \gamma$ more "yes" than "no" votes, i.e., $\mathbf{Z} \geq \mu - \gamma$. Summing (17) over all $z \geq \mu - \gamma$ yields,

$$Pr[\mathbf{Z} \geq \mu - \gamma] = \sum_{z=\mu-\gamma}^{i} \sum_{x=z}^{\min\{i, \frac{\delta+z}{2}\}} \frac{\binom{i}{x}\binom{\delta-i}{x-z}}{\binom{\delta}{2x-z}} B(2x - z, \delta, p). \tag{18}$$

Using (14) and (18), we compute

$$\begin{aligned} \Pr[\hat{\mathcal{T}} \neq \mathcal{T}] &= \sum_{i=\mu-\gamma}^{n_1} \Pr[I = i] Pr[\mathbf{Z} \geq \mu - \gamma] \\ &= \sum_{i=\mu-\gamma}^{n_1} HG(n_1, N, i, \delta) \sum_{z=\mu-\gamma}^{i} \sum_{x=z}^{\min\{i, \frac{\delta+z}{2}\}} \frac{\binom{i}{x}\binom{\delta-i}{x-z}}{\binom{\delta}{2x-z}} B(2x - z, \delta, p). \end{aligned}$$

■

APPENDIX D

Proposition 3: Under the open vote model, an internal adversary following Strategy 1 can flip the voting outcome for a decision threshold γ and a margin μ with probability

$$\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] = \sum_{i=\mu-\gamma}^{\delta} B(i, \delta, p). \tag{19}$$

where δ denotes the number of votes that the adversary attempts to nullify, with $\delta \leq n_1$.

Proof:

Let a vote process with M participants lead to a voting outcome $\mathcal{T}$, selected with a margin μ. Without loss of generality, assume that the votes in favor of $\mathcal{T}$ are "yes" votes. For a margin μ, it is straightforward to show that there are $n_1 = \frac{M+\mu}{2}$ "yes" votes and $n_2 = \frac{M-\mu}{2}$ "no" votes. Consider a voting outcome $\mathcal{T}$ with a margin μ with the in favor votes be "yes" votes. Under the open vote model, the adversary only targets subcarriers that are assigned to participants that intend to vote "yes". The voting outcome $\mathcal{T}$ is flipped if at least $\mu - \gamma$ "yes" votes are nullified. The adversary successfully nullifies an attacked vote with probability $p = 0.5^{\ell}$. As the success of nullifying each vote is an independent event (the adversary picks one of the two subcarriers assigned to each attacked participant at random), the number of nullified "yes" votes when a total of δ "yes" votes are attacked, follows the binomial distribution with parameter p.

$$\Pr[\mathbf{X} = x] = B(x, \delta, p), \quad p = 0.5^{\ell}. \tag{20}$$

Summing over all values of $x \geq \mu - \gamma$ yields,

$$\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] = \sum_{i=\mu-\gamma}^{\delta} B(i, \delta, p), \quad p = 0.5^{\ell}. \tag{21}$$

The value of δ is smaller or equal to the number n_1 of "yes" votes, as there is no benefit to nullifying "no" votes. ■

APPENDIX E

Corollary 2: For the secret vote model, $\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] \leq p_0$ if

$$\ell > \Big\lceil \frac{1}{\log 2} \log \frac{\delta \sum_{i=\mu-\gamma}^{\delta} HG(n_1, N, i, \delta) \sum_{z=\mu-\gamma}^{i} \frac{1}{z}}{p_0} \Big\rceil.$$

Proof: We wish to determine the value of ℓ for which $\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] \leq p_0$. From (17), it follows that

$$\begin{aligned} \Pr[\mathbf{Z} = z] &= \sum_{x} \frac{\binom{i}{x}\binom{\delta-i}{x-z}}{\binom{\delta}{2x-z}} B(2x - z, \delta, p) && \text{(22a)} \\ &< \sum_{x} B(2x - z, \delta, p) && \text{(22b)} \\ &< \frac{\delta p}{z} && \text{(22c)} \end{aligned}$$

In (22b), we used the fact that $\binom{N}{n}\binom{M}{m} < \binom{N+M}{n+m}$. In (22c), we used the Chernoff bound to limit the tail sum of the Binomial distribution. Substituting to (13) yields,

$$\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] < \sum_{i=\mu-\gamma}^{n_1} HG(n_1, N, i, \delta) \sum_{z=\mu-\gamma}^{i} \frac{\delta p}{z}. \tag{23}$$

Limiting the right hand side of (23) by p_0 and solving for p results in

$$p < \frac{p_0}{\delta \sum_{i=\mu-\gamma}^{n_1} HG(n_1, N, i, \delta) \sum_{z=\mu-\gamma}^{i} \frac{1}{z}}. \tag{24}$$

Substituting $p = 0.5^{\ell}$ and solving for ℓ completes the proof.

■

APPENDIX F

Corollary 3: For the open vote model, $\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] \leq p_0$ if

$$\ell \geq \Big\lceil \frac{1}{\log 2} \log \frac{n_1}{(\mu - \gamma) p_0} \Big\rceil.$$

Proof: The proof follows by using the Chernoff bound to limit the tail probability of the binomial distribution in (21).

■

APPENDIX G

Proposition 4: Under the secret vote model, an internal adversary following Strategy 2 can flip the voting outcome for a decision threshold γ and a margin μ with probability

$$\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] = \sum_{z=\mu-\gamma}^{\min\{n_1,\delta\}} \sum_{x=\lceil \frac{\delta+z}{2} \rceil}^{\min\{n_1,\delta\}} \frac{\binom{n_1}{x}\binom{n_2}{\delta-x}}{\binom{M}{\delta}}, \tag{25}$$

when attempting to nullify δ votes.

Proof: Consider a voting outcome $\mathcal{T}$ with a margin μ with the in favor votes be "yes" votes. Let an internal adversary intend to nullify a total of δ votes. Under the secret vote model, the adversary is unaware of the vote intend of each participant. Therefore, the δ votes are selected at random from the total M votes casted by the participants. Of these M votes, $n_1 = \frac{M+\mu}{2}$ are "yes" votes, whereas the remaining $n_2 = \frac{M-\mu}{2}$ are no votes. The adversary successfully flips the voting outcome if at least μ more "yes" votes are nullified relative to "no" votes, when a total of δ are nullified. Note that under Strategy 2, vote nullification occurs with certainty, because the adversary injects energy on both the subcarriers assigned to a targeted participant. This is independent of the number of symbol votes ℓ. Let $\mathbf{X}$ and $\mathbf{Y}$ be two RVs denoting the number of nullified "yes" and number of nullified "no" votes, respectively. Let also $\mathbf{Z} = \mathbf{X} - \mathbf{Y}$. It follows that

$$\begin{aligned} \Pr[\mathbf{Z} = z] &= \sum_{x-y=z} \Pr[\mathbf{X} = x, \mathbf{Y} = y] \\ &= \sum_{x=\lceil \frac{\delta+z}{2} \rceil}^{\min\{n_1,\delta\}} \frac{\binom{n_1}{x}\binom{n_2}{\delta-x}}{\binom{M}{\delta}}. \end{aligned} \tag{26}$$

In (26), we used the hypergeometric pmf to account for the selection of x votes from the n_1 "yes" votes and $x - z$ votes from the n_2 "no" votes, when a total of δ votes are nullified. Note that the adversary only targets the subcarriers assigned to the M participants and ignores any of the unassigned subcarriers if $N > 2M$ (this is not the case for an external adversary). Also, the difference between x and y is fixed to be equal to z, independent of the number of nullified votes δ. From (26), we calculate the probability that at least μ more "yes" votes are nullified relative to "no" votes, by summing over all $z \geq \mu$.

$$\begin{aligned} \Pr[\hat{\mathcal{T}} \neq \mathcal{T}] &= \sum_{z \geq \mu-\gamma} \Pr[\mathbf{Z} = z] \\ &= \sum_{z=\mu-\gamma}^{\min\{n_1,\delta\}} \sum_{x=\lceil \frac{\delta+z}{2} \rceil}^{\min\{n_1,\delta\}} \frac{\binom{n_1}{x}\binom{n_2}{\delta-x}}{\binom{M}{\delta}}. \end{aligned} \tag{27}$$

■

APPENDIX H

Proposition 5: Under the open vote model, an internal adversary following Strategy 2 can flip the voting outcome for a decision threshold γ and a margin μ with certainty, or $\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] = 1$, when injecting energy in $J \geq \mu - \gamma$ subcarriers.

Proof: The proof immediately follows by noting that the adversary must nullify $\mu - \gamma$ votes in favor of $\mathcal{T}$ to flip the voting outcome at the tallier. Each of the $\mu - \gamma$ votes is submitted by injecting energy to one of the subcarriers assigned to the corresponding participant. Injecting energy in both those subcarriers nullifies an in favor vote with certainty. Targeting a total of $J = 2(\mu - \gamma)$ subcarriers that correspond to in favor votes (the vote intend is known under an open vote model), nullifies $\mu - \gamma$ in favor votes with certainty, thus flipping the voting outcome.

■