In-band Secret-Free Pairing Protocol for COTS Wireless Devices

Nirnimesh Ghose, *Member, IEEE,* Loukas Lazos, and Ming Li, *Senior Member, IEEE.*

Appendix

A. Proof of Proposition 1

Proposition. *Test 1 detects any Type 1 adversary located at distance d_{MD} from D, satisfying* ${}^{(d_{MD}+d_{DA})^{\alpha_A}}/{}_{(d_{MD}-d_{DH}^{\max})^2} < ({}^{d_{DA}}/{}_{d_{DH}^{\min}})^2$*. Parameter α_A is the attenuation factor of the M-to-A channel.*

Proof. We first consider a single sweep of H over D. The threshold for detecting an invalid transmission using Test 1 is given by:

$$\tau_{peak} = \frac{G_H}{G_A} \cdot \frac{(d_{DA})^2}{(d_{DH}^{\min})^2}. \tag{1}$$

where we have considered the best case scenario for the adversary by setting the attenuation factor for the D-to-A channel to two. This minimizes the τ_{peak} that needs to be met by the adversary to pass Test 1. Let the adversary be located at distance d_{MH} from H and d_{MA} from A. The RSS ratio achieved by a Type 1 adversary transmitting with power P_M is

$$\gamma_M = \frac{G_H}{G_A} \cdot \frac{(d_{MA})^{\alpha_A}}{(d_{MH})^2}. \tag{2}$$

As H is swept over D, the RSS ratios computed by A when M is active form a set $\mathbf{s}_M = \{s_M(1), s_M(2), \ldots, s_M(n)\}$, where $s_M(i)$ corresponds to the i^{th} RSS ratio sample collected by A while H moves over D. To detect a Type 1 adversary, it must follow that the maximum RSS ratio obtained during the motion of H does not exceed τ_{peak}.

$$\max_{\mathbf{s}_M}(s_M(i)) < \tau_{peak}$$

$$\max_{d_{MA},\mathbf{d}_{MH}} \frac{G_H}{G_A} \cdot \frac{(d_{MA})^{\alpha_A}}{(d_{MH})^2} < \tau_{peak} \tag{3a}$$

$$\frac{G_H}{G_A} \cdot \frac{(d_{MD}+d_{DA})^{\alpha_A}}{\max\limits_{\mathbf{d}_{DH}}(d_{MD}-d_{DH}(j))^2} < \tau_{peak} \tag{3b}$$

$$\frac{G_H}{G_A} \cdot \frac{(d_{MD}+d_{DA})^{\alpha_A}}{(d_{MD}-d_{DH}^{\max})^2} < \frac{G_H}{G_A} \cdot \frac{(d_{DA})^2}{(d_{DH}^{\min})^2} \tag{3c}$$

$$\frac{(d_{MD}+d_{DA})^{\alpha_A}}{(d_{MD}-d_{DH}^{\max})^2} < \frac{(d_{DA})^2}{(d_{DH}^{\min})^2}. \tag{3d}$$

In (3a), we replaced the expression of $s_M(i)$ from (2). In (3b), we considered the distances of M to H and A that maximize the RSS ratio. We further fixed the distance between M and D and considered all possible locations of M relative to H and A that maximize the RSS ratio achieved by M. This occurs when M, D, H, and A to be co-linear as shown in Fig. 1. In (3c), we further minimized the denominator by considering the location of H closest to M.

The sweeping motion of H over D is repeated multiple times. The maximum RSS ratio must exceed τ_{peak} for every motion of H. Given that the sweeps are of approximately equal length, the same inequality as in (3d) must be satisfied for all sweeps. This concludes the proof.

□

N. Ghose is with the Department of Computer Science and Engineering, University of Nebraska–Lincoln, Lincoln, NE, 68588 USA e-mail: (nghose@unl.edu).

L. Lazos and M. Li are with Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, 85721 USA e-mail: (llazos,lim@email.arizona.edu).

Manuscript received April 03, 2019; revised February 28, 2020.

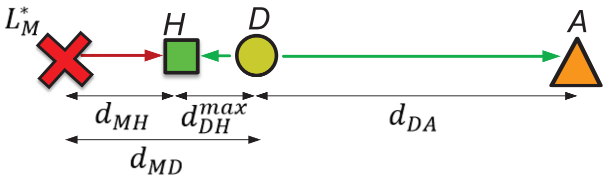


Fig. 1: The optimal position L_M^* for defeating Test 1 when the distance d_{MD} is fixed, lies co-linearly with D and A.

B. Proof of Proposition 2

Proposition. *A Type 2 adversary is detected by Test 2 when* $d_{MD} > d_{DH}^{\max}(d_{DH}^{\max}+d_{DH}^{\min})/(d_{DH}^{\max}-d_{DH}^{\min})$.

Proof. Without loss of generality due to the similar nature of every sweep, consider a single sweep $\mathbf{s}$ of H over D. The true RSS ratio range (Δ) for a legitimate device D is given by,

$$\begin{aligned}\Delta &= \frac{\max(s(j))}{\min(s(j))}\\ &= \frac{G_A}{G_H}\left(\frac{d_{DH}^{\max}}{d_{DA}}\right)^2\frac{G_H}{G_A}\left(\frac{d_{DA}}{d_{DH}^{\min}}\right)^2\\ &= \left(\frac{d_{DH}^{\max}}{d_{DH}^{\min}}\right)^2, \end{aligned}\tag{4}$$

where $d_{DH}^{\min}$ and $d_{DH}^{\max}$ are minimum and maximum distances between D and H respectively during $\mathbf{s}$. The value of τ_{range} is selected to be equal to Δ, given conservative estimates for the user's range of motion during sweeps.

$$\tau_{range} \leq \Delta = \left(\frac{d_{DH}^{\max}}{d_{DH}^{\min}}\right)^2. \tag{5}$$

The RSS ratio range (Δ_M) for a Type 2 adversary that is active during a sweep $\mathbf{s}_M$ is given by,

$$\Delta_M = \frac{\max\limits_{\mathbf{s}_M}(s_M(j))}{\min\limits_{\mathbf{s}_M}(s_M(j))} \tag{6a}$$

$$\begin{aligned}&= \frac{G_A}{G_H}\frac{G_{MA}}{G_{MH}}\frac{P_A}{P_H}\cdot\left(\frac{(\max\limits_{\mathbf{d}_{DH}}[(d_{MD}+d_{DH}(j)\cos\theta)\sec\theta'])^2}{(d_{MA})^{\alpha_A}}\right)\\ &\quad\cdot\frac{G_H}{G_A}\frac{G_{MH}}{G_{MA}}\frac{P_H}{P_A}\cdot\left(\frac{(d_{MA})^{\alpha_A}}{(\min\limits_{\mathbf{d}_{DH}}[(d_{MD}+d_{DH}(j)\cos\theta)\sec\theta'])^2}\right)\end{aligned}\tag{6b}$$

$$= \left(\frac{\max\limits_{\mathbf{d}_{DH}}[(d_{MD}+d_{DH}(j)\cos\theta)\sec\theta']}{\min\limits_{\mathbf{d}_{DH}}[(d_{MD}+d_{DH}(j)\cos\theta)\sec\theta']}\right)^2 \tag{6c}$$

$$= \left(\frac{d_{MD}+d_{DH}^{\max}}{d_{MD}-d_{DH}^{\max}}\right)^2. \tag{6d}$$

In (6b), G_{MA} denotes the gain of the directional antenna of M aimed at A whereas G_{MH} denotes the gain of the directional antenna of M aimed at H. Moreover, P_A and P_H denote the transmission power of M to A and H, respectively. Finally, θ and θ' are the angles formed by the D-to-A, D-to-H and M-to-D, M-to-H lines, respectively, as shown in Fig. 2 In (6d),

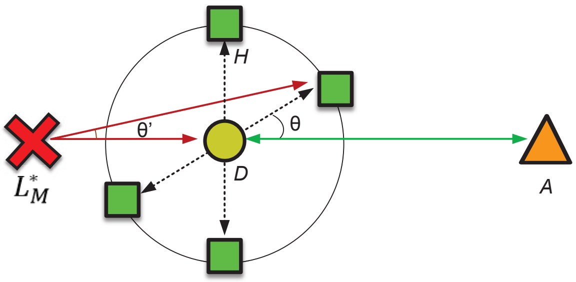


Fig. 2: Various motions for the helper.

$\max[(d_{MD} + d_{DH}\cos\theta)\sec\theta']$ is achieved when, $\theta = \theta' = 0°$. In addition, $\min[(d_{MD} + d_{DH}\cos\theta)\sec\theta']$ is achieved when, $\theta = 180°$ and $\theta' = 0°$. To pass Test 2,

$$\Delta_M < \tau_{range} \tag{7a}$$

$$\left(\frac{d_{MD} + d_{DH}^{\max}}{d_{MD} - d_{DH}^{\max}}\right)^2 < \left(\frac{d_{DH}^{\max}}{d_{DH}^{\min}}\right)^2 \tag{7b}$$

$$\left(\frac{d_{MD} + d_{DH}^{\max}}{d_{MD} - d_{DH}^{\max}}\right) < \left(\frac{d_{DH}^{\max}}{d_{DH}^{\min}}\right) \tag{7c}$$

$$(d_{MD} + d_{DH}^{\max})\, d_{DH}^{\min} < (d_{MD} - d_{DH}^{\max})\, d_{DH}^{\max} \tag{7d}$$

$$d_{MD}d_{DH}^{\min} + d_{DH}^{\max}d_{DH}^{\min} < d_{MD}d_{DH}^{\max} - (d_{DH}^{\max})^2 \tag{7e}$$

$$d_{MD}d_{DH}^{\max} - d_{MD}d_{DH}^{\min} > d_{DH}^{\max}(d_{DH}^{\max} + d_{DH}^{\min}) \tag{7f}$$

$$d_{MD}(d_{DH}^{\max} - d_{DH}^{\min}) > d_{DH}^{\max}(d_{DH}^{\max} + d_{DH}^{\min}) \tag{7g}$$

$$d_{MD} > \frac{d_{DH}^{\max}(d_{DH}^{\max} + d_{DH}^{\min})}{d_{DH}^{\max} - d_{DH}^{\min}} \tag{7h}$$

In (7c), it is assumed that $d_{MD} > d_{DH}^{\max}$. The inequality in (7h) yields the distance of M from D after which a Type 2 adversary is detectable by Test 2. Note that for nominal user motions it holds that $d_{DH}^{\max} >> d_{DH}^{\min}$) in which case $d_{MD} > d_{DH}^{\max}$. That is the adversary, becomes detectable if it is at a distance longer than the boundary of H's motion. This concludes the proof. □

C. Proof of Proposition 3

Proposition. *A Type 3 adversary is always detected by Test 3 if (a) the user performs at least two sweeps* s_1 *and* s_2*, (b) sweep* s_1 *starts and ends in area* X*, whereas sweep* s_2 *starts and ends in area* Y*, and (c)* $d_{MD} > \min_i(d_{DH}^{\max}(i))\ \forall\ i = 1, \ldots, \ell$.

Proof. To defeat Test 2, a Type 3 adversary applies power control to achieve the desired RSS ratio dynamic range τ_{range}. This is achieved by injecting a maximum power P_H when H is the closest to M and a minimum power P_H' when H is farthest from M thus maximizing the range achieved measured by H. However, we show that this approach leads to a violation of Test 3.

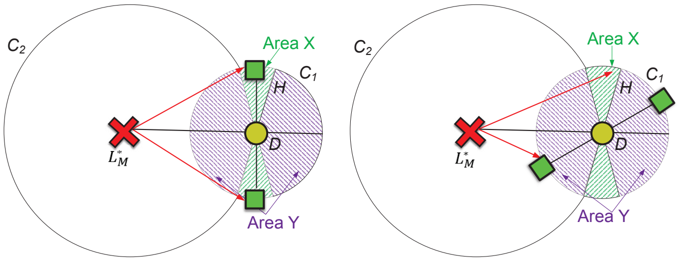
Consider two sweeps s_1 and s_2 performed by the user. The ratio of the sweep periods is given by

$$\frac{T(i)}{T(j)} = \frac{d_{DH}^{\max}(i)}{d_{DH}^{\max}(j)}, \tag{8}$$

where we have assumed a constant average speed for both s_1 and s_2. Let the threshold for passing Test 3 be set to $\tau_{period} = {}^{d_{DH}^{\max}(i)}/_{d_{DH}^{\max}(j)}$. Under equal sweep lengths, this ratio is equal to one[1]. Let the area where H moves around D be divided into two sub-areas X and Y, as shown Figure 3. The sub-areas are defined by the intersection of two circles. Circle C_1 is centered at D and has a radius of $d_{DH}^{\max}$, whereas circle C_2 is centered at L_M^* and has a radius of d_{MD}. Sub-area Y consists of the sector S_1 formed by the intersection between C_1 and C_2 and the sector of C_1 that is symmetric to S_1 over the y-axis. Sub-area X is the complement of sub-area Y within C_1.

Let the adversary perform its power control attack during sweeps s_1 and s_2. Let also $\mathrm{s}_1 \in X$ and $\mathrm{s}_2 \in Y$. From the sub-area geometry, it follows that any sweep (sweeps are assumed to form a straight line) that originates in X ends in X and any sweep

[1] In reality, the sweep lengths are unequal but approximately the same. Based on the experiments presented in the evaluation section, we have found the $\tau_{period} = 1.4$. That is, the sweep period can vary as much as 40%.



(a) (b)

Fig. 3: (a) Sweep with H starting and ending in area X, (b) Sweep with H starting and ending in area Y.

that originates in Y ends in Y. Moreover, for any point $R \in X$, it follows that $d_{MR} \geq d_{MD}$. Therefore, when a sweep is performed in X, the D is the closest point to L_M^* (also the point where M transmits with P_H.) In this case, the sweep period, i.e., time between two successive peaks, equals the time until two successive visits of H over D. Equivalently, this is equal to the time required to travel the diameter of circle C_1, denoted by $d_{DH}^{\max}$.

On the other hand. for any sweep in Y, it is straightforward to show from the sub-area geometry that the minimum separation between M and H is achieved when H is the farthest from D (i.e., at a point in C_1). In this case, the sweep period, equals the time until two successive visits of H at maximum separation from D. Equivalently, this is equal to the time required to travel *two times* the diameter of circle C_1, denoted by $2d_{DH}^{\max}$. Assuming a constant average speed of motion for H, the ratio ${T(i)}/{T(j)} = 2 > \tau_{period}$. Therefore, a violation of Test 3 will be recorded. If the two sweeps $\mathbf{s}_1$ and $\mathbf{s}_2$ belong to the same sub-area, the same sweep period will be recorded for both of them and a Type 3 adversary will pass Test 3.

Note that a Type 3 adversary incorporates the Type 1 and Type 2 capabilities and therefore a successful test will defend against all three adversaries.

□

D. Proof of Proposition 4

Proposition. *Test 4 detects a Type 3 adversary with probability no smaller than* p_0*, when the user performs at least*

$$\ell^* \geq \max\left[1, \left\lceil \frac{\sqrt{1 + {48\epsilon^2}/{\delta^2(1-p_0)^2}} - 3}{4} \right\rceil\right]$$

sweeps, the sweep period estimation error is uniformly distributed in $[-\delta, \delta]$*, and the threshold for passing Test 4 is set to* ϵ*.*

Proof. To pass Test 4, a Type 3 adversary must synchronize the RSS ratio minima measured by the helper with the acceleration maxima. Let $\mathbf{t}_{acc} = \{t_{acc}(1), t_{acc}(2), \ldots, t_{acc}(\ell)\}$ be the times where H records its maximum acceleration (at the ends of each sweep motion) and let $\mathbf{t}_{RSS}^{M} = \{t_{RSS}^{M}(1), t_{RSS}^{M}(2), \ldots, t_{RSS}^{M}(\ell)\}$ by the times where M induces the RSS ratio minima at H via directional transmissions and power control. The adversary M must select $\mathbf{t}_{RSS}^{M}$ such that it matches the periodicity of $\mathbf{t}_{acc}$. However, there are two sources of error that make this matching difficult. First, the period of the helper's motion is not fixed due to the variation induced by the user's hand motion. Second, the start time of the motion is not known unless it is directly observed with a high accuracy camera system. The latter is a very strong requirement that would reveal the presence of an adversary. We capture the two sources of error between $\mathbf{t}_{acc}$ and $\mathbf{t}_{RSS}^{M}$ in the following relationship:

$$|t_{acc}(i) - t_{RSS}^{(M)}(i)| = i\mathbf{\Delta} + \mathbf{E}_M$$

where $\mathbf{\Delta}$ is a random variable denoting the estimation error for the period of each sweep and $\mathbf{E}_M$ is a random variable denoting the misalignment between the acceleration peaks and RSS ratio valleys due to the unknown motion start time. Note that the error for the sweep period is cumulative with every sweep, whereas the start time error is only at the beginning of the motion. For Test 4, the RMSE achieved by the adversary becomes,

$$\begin{aligned} RMSE_M &= \sqrt{\frac{\sum_{i=1}^{\ell}(t_{acc}(i) - t_{RSS}^{(M)}(i))^2}{\ell}} \\ &= \sqrt{\frac{\sum_{i=1}^{\ell}(i\mathbf{\Delta} + \mathbf{E}_M)^2}{\ell}}, \end{aligned} \tag{9}$$

where ℓ is the number of sweeps. We now show that even if the the adversary knows the motion starting time ($\mathbf{E}_M = 0$), the error in the sweep period estimation will make him fail the test, given sufficient number of sweeps. For this worst case ($\mathbf{E}_M = 0$),

$$\begin{aligned} RMSE_M &= \sqrt{\frac{\sum_{i=1}^{\ell}(i\mathbf{\Delta})^2}{\ell}} \\ &= |\mathbf{\Delta}|\sqrt{\frac{\sum_{i=1}^{\ell} i^2}{\ell}} \\ &= |\mathbf{\Delta}|\sqrt{\frac{(\ell+1)(2\ell+1)}{6}}. \end{aligned} \tag{10}$$

Without loss of generality, let $\mathbf{\Delta}$ by uniformly distributed in $[-\delta, \delta]$. We analyze this case here because of the simple form of the distribution for $|\mathbf{\Delta}|$, but the latter is computable for any distribution. For a uniformly distributed $\mathbf{\Delta}$, the PDF of the $RMSE_M$ is uniformly distributed in $[0, \delta\sqrt{\frac{(\ell+1)(2\ell+1)}{6}}]$. This easily follows from eq. (10) and the fact the $|\mathbf{\Delta}|$ is uniformly distributed in $[0, \delta]$. Test 4 detects an adversary if $RMSE_M$ exceeds ϵ. Given that $RMSE_M$ is a random variable, we calculate the probability that it exceeds ϵ using the CDF.

$$\Pr[RMSE_M > \epsilon] = 1 - \frac{\epsilon}{\delta\sqrt{\frac{(\ell+1)(2\ell+1)}{6}}}. \tag{11}$$

We calculate the minimum number of sweeps ℓ^* required such that $RMSE_M$ exceeds ϵ with probability at least p_0.

$$\Pr[RMSE_M > \epsilon] \geq p_0, \tag{12a}$$

$$1 - \frac{\epsilon}{\delta\sqrt{\frac{(\ell+1)(2\ell+1)}{6}}} \geq p_0, \tag{12b}$$

$$2\ell^2 + 3\ell + 1 \geq \frac{6\epsilon^2}{\delta^2(1-p_0)^2}, \tag{12c}$$

$$2\ell^2 + 3\ell + 1 - \frac{6\epsilon^2}{\delta^2(1-p_0)^2} \geq 0, \tag{12d}$$

$$\ell \geq \frac{\sqrt{1 + \frac{48\epsilon^2}{\delta^2(1-p_0)^2}} - 3}{4}, \tag{12e}$$

$$\ell^* \geq \max\left[1, \left\lceil \frac{\sqrt{1 + \frac{48\epsilon^2}{\delta^2(1-p_0)^2}} - 3}{4} \right\rceil\right]. \tag{12f}$$

In (12e), we have kept the root of the quadratic equation that can be positive. In (12f), we have ensured that at least one sweep is needed for the test, because the root ℓ in (12e) can still be negative for large δ. Finally, we have taken the ceiling function on ℓ because the number of sweeps is an integer. This concludes the proof.

□