E-bots vs. P-bots: Cooperative Eavesdropping in (partial) Silence Technichal Report

Mai Ben-Adar Bessos[1], Simon Birnbach[2] Amir Herzberg[1], and Ivan Martinovic[2]

[1] Bar-Ilan University, Israel
[2] University of Oxford, United Kingdom

1 Data leakage proofs

Notations. $r_e \in \mathbb{N}$ is the eavesdropping distance of an E-bot; we refer to the area within r_e around the target as the *sensitive area.* Let $dist_G(v, w)$ denote the length of the shortest path between $v, w \in V$; we assume G is an undirected 4-connected grid; therefore, $dist_G$ is simply Manhattan distance. $Ring_G(p, k)$ denotes points with distance $k \in \mathbb{N}$ from point $p \in G$. p_a, p_c, p_p are the capture probabilities by P-bots that are allocated to the roles *Area Patrol* , *Circumference Patrol* and *Pursuit* respectively, and we assume $0 < p_a \leq p_c$. P-bots focus on protecting the target point t. We strictly assume all data is flushed immediately to the sink after the E-bot escapes from the sensitive area. η is the amount of E-bots, p_d is the transmission-detection probability and $R : \mathbb{N} \to (0, 1]$ is a nonincreasing function which is the reward given to E-bots for a data item which reaches the sink x rounds after it was eavesdropped. We use $R_n = \sum_{i=1}^{n} R(i)$ to denote the reward given for the n latest consecutively-eavesdropped units. For an E-bot that uses the crawling E-bot strategy, and spends l rounds within the sensitive area each time it enters, we denote with $u(l)$ the expected reward it gains before being captured. $C(l)$ denotes the probability that it will be captured before exiting the sensitive area. We use $l_{escape} = \arg\max_{l\in\mathbb{N}} u(l)$. Let x be the reward given for data that reached the sink exclusively by flush. $E_{escape}(x, p_a, p_c, R)$, abbreviated to $E_{escape}(x)$), is the lower bound on the expected captured E-bots before then. Let k be the reward given for leaked data units that reached the sink exclusively from inside the sensitive area (by transmission). $E_{stay}(k, p_a, p_p, p_d, R)$, abbreviated to $E_{stay}(k)$, denotes the lower bound on the expected captured E-bots by the time they received the reward. If in all the transmissions the E-bots transmitted n units simultaneously, $E^n_{stay}(k, p_a, p_p, p_d, R)$, abbreviated to $E^n_{stay}(k)$, denotes the same.

Lemma 1. *1. $C(x)$ may be bounded as follows:*

$$C(x) \geq \begin{cases} p_c & x = 1 \\ (1 - (1 - p_c)^2 (1 - p_a)^{x-2}) & o.w. \end{cases}$$

2. $u(l)$ has a single extremum point in $[3, \infty)$

3. $E_{escape}(x, p_a, p_c, R) \geq \frac{x}{R_{l_{escape}}} \cdot \frac{C(l_{escape})}{1-C(l_{escape})}$

Proof. 1. Consider an E-bot that uses the crawling strategy exclusively. Let l be the length of a particular visit in the sensitive area, which is also the number of data items collected - if the E-bot is not captured. The accumulated data units are necessarily unique, since that E-bot collects data only when no other E-bot is active. Hence, the $\frac{1}{C(l)}$ is the expected number of rounds the E-bot repeats the process until it is captured (Binomial distribution), and the expected reward is: $u(l) \equiv \frac{R_l}{C(l)} - R_l = \frac{cl}{C(l)} - cl$.

   - For $l = 1$: the E-bot necessarily visited and immediately escaped a point in $Ring_G(t, r_e)$. Upon escaping, flushing the data do not increase capture probability, and therefore $C(1) = p_c$. Note that if an E-bot remains in $Ring_G(t, r_e)$ for $l = 2$, it risks losing the data it accumulated in the first round, and therefore such a strategy provides no benefit.
   - For $l > 2$: the E-bot has the opportunity to occupy points in $Ring_G(t, 0 < i < r_e)$ (excluding the first and last rounds), thus reducing the capture probability for some of the rounds. Therefore: $C(l) = 1 - (1 - p_c)^2(1 - p_a)^{l-2}$.

2. For any reward function R, the first point after the extremum is the first point for which it holds that: $\frac{R_{x+1}}{(1-(1-\gamma)^2(1-\alpha)^{x-1})} - R_{x+1} > \frac{R_x}{(1-(1-\gamma)^2(1-\alpha)^{x-2})} - R_x \xrightarrow{0<\alpha<\gamma<1} R(x+1) < R_x \frac{(-1+\alpha)\alpha}{((1-\alpha)^x\gamma^2-2(1-\alpha)^x\gamma-\alpha^2+(1-\alpha)^x+2\alpha-1)}$ (or the opposite, where $R(x+1) >$ for the first time). R_x is monotonically increasing since $R(x) > 0$. Additionally, it is multiplied by a monotonic term, since: $\frac{\Delta}{\Delta x}\frac{(-1+\alpha)\alpha}{((1-\alpha)^x\gamma^2-2(1-\alpha)^x\gamma-\alpha^2+(1-\alpha)^x+2\alpha-1)} = 0 \longleftrightarrow (-1+\alpha)\alpha((1-\alpha)^x ln(1-\alpha)\gamma^2 - 2(1-\alpha)^x ln(1-\alpha)\gamma + (1-\alpha)^x ln(1-\alpha)) = 0$ is never satisfied. If the right-hand side is < 0, it will be $< 0 < R(x)$ for any x. If the right-hand side is > 0, then $R(x)$ is nonincreasing and the left-hand is monotonically increasing, and therefore may meet only once.
3. An E-bot that transmits from within the sensitive area does not increase the amount of unique accumulated data (and potentially only decreases it), and does not contribute to transmissions from outside the sensitive area. Additionally, by design of the P-bots in this strategy transmissions may not decrease the probability of the E-bot for being captured. The expected number of transmitted data from outside the sensitive area until an E-bot gets captured $u(l) = R_l(\frac{1}{C(l)} - 1)$ is maximized for $l = l_{escape}$. That is, $E_{escape}(\frac{R_{l_{escape}}}{C(l_{escape})} - R_{l_{escape}}) \geq 1$ holds, and due to the linearity of expected value $E_{escape}(l) \geq l\frac{1}{\frac{R_{l_{escape}}}{C(l_{escape})} - R_{l_{escape}}} = l\frac{C(l_{escape})}{R_{l_{escape}}(1-C(l_{escape})}$ follows.

□

Lemma 2. $E^n_{stay}(l) \geq (n - \frac{(-1+p_a)((1-p_a)^n-1)}{p_a} + p_p)(\frac{l}{nR_n})$.

Proof. Consider an E-bot that exclusively uses the transmitting strategy. Since only one unique data unit is generated in each round, the E-bot that transmitted the oldest data unit had stayed for at least n rounds, at least one other E-bot had stayed for $n-1$, another for $n-2$ and so forth. Accordingly, the independent risk each E-bot takes is at least $1-(1-p_a)^n$, $1-(1-p_a)^{n-1}$,$\ldots$, $1-(1-p_a)$, which is summed up to $n-(1-p_a)\frac{(1-p_a)^n-1}{(1-p_a)-1} = n-\frac{(-1+p_a)((1-p_a)^n-1)}{p_a}$. After the transmission of the n units, the pursuit algorithm was invoked and targeted one of the transmitting E-bots that was not yet captured. That is, after any transmission an additional risk of p_p follows for some agent. Therefore, for a reward of R_n, $n-\frac{(-1+p_a)((1-p_a)^n-1)}{p_a}$ E-bots are expected to be captured before the transmissions begin, and additional p_p immediately in the next round. Similarly to the previous lemma, due to the linearity of expected value, $E^n_{stay}(n) = \frac{(n-\frac{(-1+p_a)((1-p_a)^n-1)}{p_a}+p_p)}{R_n}$ and $E^n_{stay}(l) = (n-\frac{(-1+p_a)((1-p_a)^n-1)}{p_a}+p_p)(\frac{l}{nR_n})$

(note that we disregard the option of leaving the sensitive area while transmitting, since this is considered flushing the data). □

Theorem 2. *The expected reward of the E-bots is bounded from above by:* $\frac{\eta}{\min(E_{escape}(1),E_{stay}(1))}$.

Proof. This follows directly from the previous lemmas since P-bots use a stateless strategy (i.e. the probability of capturing E-bots in each round does not depend on the state of P-bots in the previous round) and since in every round only a single new unique data unit is generated. We denote $k = \arg\max_{n\in[1,\ldots,\eta]} E^n_{stay}$. Consider any data unit that was eventually collected by E-bot$e$. Before the data unit is accumulated by e , e has a probability of at least $p = p_a$ or $= p_c$ for being captured (or $p + (1-p)\cdot\frac{p_p}{k}$ if it transmitted data at the previous round). This minimal risk is independent of the method used to eventually collect this data. That is, the expected risk for all E-bots in the sensitive area in that round was at least $E_{escape}(1)$ or at least $E_{stay}(1)$, and no additional data units were accumulated in that round (even if additional E-bots accumulated the same data unit, it wasn't unique upon collection). Additionally, accumulating the data and staying within the sensitive area may not reduce the minimal risk taken by any other E-bot or increase the reward given for other accumulated data units (and potentially only worsen the situation). Therefore, combining the two strategies is not preferable to using any one of them, and E-bots may repeat the preferable one. □

Since the bounds are lenient (it is assumed all simultaneous transmissions are done with optimal conditions for E-bots), it may appear that the combination of transmitting and crawling together may not be useful for E-bots, but in practice the combination may be beneficial e.g. letting by an E-bot participate in several simultaneous transmission, until most other E-bots were captured, then crawl back to the sink and flush the remaining untransmitted data.

2 Patrol and pursuit details

Assume P-bots have a velocity of r_p. In order to calculate how many P-bots are needed for *Area Patrol* , *Circumference Patrol* and *Pursuit* methods, we use the following lemma.

Lemma 3. *For graph $G = (V, E)$ and any two points $v_1, v_2 \in Ring_G(V, \{0 \leq i \leq r\})$ it holds that:*

1. *$dist_G(v_1, v_2) \leq 2r$.*
2. *Given distance $r > 1$ and a point $v \in V$ in the graph center, if G is a 4-connected grid graph then $|Ring_G(v, r)| = 4r$ and $|Ring_G(v, 0 \leq i \leq r)| = 2r(r+1)+1$ hold (the equations hold iff the numerated points do not intersect the edges of the grid graph).*

Proof:

1. By induction: For $r = 1$, trivial. We assume for $r > 1$. Given $v_1, v_2 \in Ring_G(V, r+1)$, let $v_1', v_2' \in Ring_G(V, r), dist_G(v_1, v_1') = dist_G(v_2, v_2') = 1$. By assumption, $dist_G(v_1', v_2')$. By concatenating the paths that correspond to the distances we create a path of length $2r + 1 + 1 = 2(r +_1)$.
2. By induction: For $r = 2$, trivial. We assume for $r > 2$. Let $v = V[x_0, y_0] \in V$ be the graph center, and $v_t = V[x_0, y_0 + r + 1] \in Ring_G(v, r + 1), v_b = V[x_0, y_0 - r - 1] \in Ring_G(v, r + 1)$. Except for v_t, v_b, for each $V[x, y] \in Ring_G(v, r+1)$: if $x \leq x_0$ then $V[x+1, y] \in Ring_G(v, r+1)$, and if $x \geq x_0$ then $V[x-1, y] \in Ring_G(v, r+1)$ since the vertex is closer by 1 edge to v. Clearly, only $V[x_0, y_0 + r], V[x_0, y_0 + -r]$ are matched in both connditions, and we get $|Ring_G(v, r)| + 2 + 2$ distinct vertices in $Ring_G(v, r+1)$. By summation, $\sum_{0 \leq i \leq r} 4i = 4\frac{r(r+1)}{2}$. Including the graph center gives $2r(r+1)+1$.

Area Patrol: For an area $Ring_G(t, 0 \leq i \leq r_p)$, denoted by A_{t,r_p}, a P-bot in point $(x_f, y_f) \in A_{t,r_p}$, if $x \leq y$ ($x \geq y$), every point $(x_d, y_d) \in A_{t,r_p}, x_d \leq y_d$ (respectively $x_d \geq y_d$) is reachable. Therefore, the 2 P-bots used by the area patrol algorithm are enough to insure that an area with radius r_p is reachable by at least one of them i.e. two P-bots are designated to an area of size $\left|A_{t,r_p}\right| = 2r_p(r_p + 1) + 1$.

An alternative method for the previously presented area patrol is assigning the area $A_{t,\frac{r_p}{2}}$ to a single P-bot. Since for every two points $p_1, p_2 \in A_{t,\frac{r_p}{2}}$ it holds that $dist_G(p_1, p_2) \leq r_p$, every point in the area will be reachable. Even though twice as many P-bots are required for covering an area using this method, if the area to cover is smaller (e.g. when a large area cannot be divided exactly to A_{x,r_p}-sized areas) as illustrated in Figure 1.

Circumference Patrol: $|Ring_G(t, d)| = 4d$, and each P-botmay reach $\frac{r_p}{2}$ points to every direction (and in particular, two directions are in $Ring_G(t, d)$), at least $\lceil \frac{4d}{r_p+1} \rceil$ P-bots are required to cover the area, where each P-bot may reach r_p points other than its current one.

Pursuit: In a single round, a P-bot may reach any point in distance r_p i.e. $2r_p(r_p + 1)$ different points other than its current one. Since another round is needed before the P-bot returns to the center of that area, at least two P-bots are needed for any area $A_{x,r_p}, x \in G$, and therefore its average designated points per P-bot is similar to that of the area patrol.

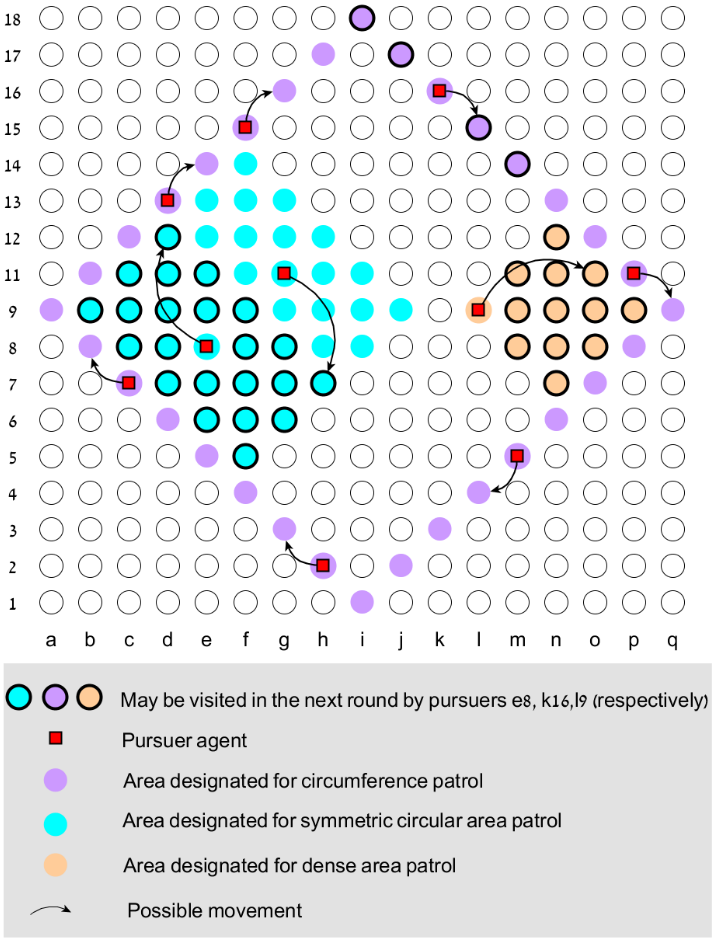
18
17
16
15
14
13
12
11
9
8
7
6
5
4
3
2
1
a b c d e f g h i j k l m n o p q
May be visited in the next round by pursuers e8, k16,l9 (respectively)
Pursuer agent
Area designated for circumference patrol
Area designated for symmetric circular area patrol
Area designated for dense area patrol
Possible movement

Fig. 1: Comparison of patrolling methods

3 Impact of not knowing E-bots' limitations

Figure 3 is similar to Figure 2, but in this case the P-bots may not assume that E-bots are limited to any specific strategy, even though they are. Since P-bots are optimized for the most difficult case, the E-bots gain only a small advantage.

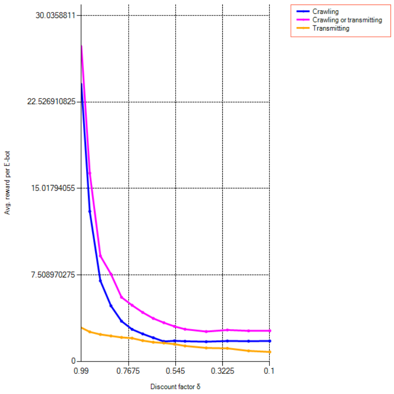

Fig. 2: Compare E-bot strategies, for different discount factor values, and P-bots are aware of E-bots strategy (as usual)

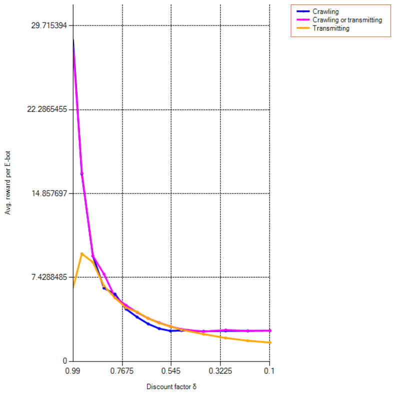

Fig. 3: Compare E-bot strategies, for different discount factor values, and P-bots are oblivious to E-bots strategy