SAFE: Secure Symbiotic Positioning, Navigation, and Timing

Md Sadman Siraj*, Eirini Eleni Tsiropoulou*, Symeon Papavassiliou†, and Jim Plusquellic *
{mdsadmansiraj96@unm.edu, eirini@unm.edu, papavass@mail.ntua.gr, jplusq@unm.edu}
* Dept. of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM, USA
† School of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece

GLOBECOM 2023 - 2023 IEEE Global Communications Conference | 979-8-3503-1090-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/GLOBECOM54140.2023.10437205

Abstract—**Increasing the security and robustness of Positioning, Navigation, and Timing (PNT) systems is a critical issue towards exploiting the PNT service at its full capacity. In this paper, we treat the joint problem of designing a secure and robust alternative PNT solution that supports the targets' PNT services, while simultaneously detecting and ejecting malicious nodes from the system that aim at deteriorating the proposed PNT solution's accuracy. The overall problem is formulated as a non-cooperative game among the targets and other collaborator nodes in order to jointly minimize their personal experienced positioning and timing error, as well as the overall system's error. The theory of potential games is adopted to prove the existence of at least one Pure Nash Equilibrium (PNE), while a log-linear-based reinforcement learning (RL) algorithm is proposed to enable the targets and collaborators to determine such a PNE. A detailed analysis for attack detection is presented considering both single-attack and distributed denial of service (DDoS) attack scenarios, where the malicious collaborators can fake their coordinates and their transmission power, while an overall PNT methodology including their ejection from the system is outlined. The performance evaluation of the proposed approach is achieved via modeling and simulation.**

Index Terms—**Positioning, Navigation, and Timing, Game Theory, Reinforcement Learning, Security.**

I. Introduction

Positioning, navigation, and timing (PNT) services play a critical role in many domains given the wide variety of application that they support. However, not only urban canyons and indoor environments suffer from limited availability of Global Positioning System (GPS) services, but GPS is also vulnerable to spoofing, jamming, and unintentional or man-made interference to the satellite signals due to long propagation distances [1]. Thus, the development of an alternative secure and robust PNT solution is a real need. In this paper, a secure PNT solution, named SAFE, is introduced, exploiting the symbiotic relationship among the various involved entities (i.e., anchor nodes, targets, and collaborator nodes, who have known, unknown, and a rough estimate of their position and timing, respectively) in order to accurately determine the positioning and timing of the two latter ones, while incorporating a defense mechanism to detect and eject malicious nodes from the symbiotic system.

A. Related Work

In the last decade, several PNT solutions have been proposed to detect malicious actions in adversarial environments. Two different types of attacks are studied in [2] considering the knowledge of the targets' positions and either exploiting beacon nodes aligned in a line or strategically placing malicious nodes in locations to maximize the error in the localization process. A geometric-based approach is followed in [3] to detect attackers, who manipulate their distance measurements, by applying the generalized likelihood ratio test, considering an initial estimate of the targets' positions. The correlation of the Doppler shift measurements stemming from multiple vehicles is performed in [4] to detect spoofing attacks from malicious nodes by exploiting the GPS signals from the vehicles' commercial GPS receivers. A trust-based solution is introduced in [5] to detect distance outliers by implementing a message passing algorithm that combines the belief propagation and the variational message passing to detect abnormal nodes' distance reports.

The problem of detecting a jammer of the localization signals has also attracted the interest of the research community. A machine learning-based anti-jamming protocol is introduced in [6] to discriminate jamming vehicles' signals and determine the precise location of the jamming vehicles in order to eject them from the system. A location privacy protection mechanism is proposed in [7] to protect the location privacy of drones in the presence of jammers by exploiting drones' topology characteristics, while reducing the use of the jammed wireless communication channel. The problem of identifying malfunctioning nodes, who are not necessarily jamming nodes, is analyzed in [8] by exploiting the exclusive characteristics revealed by the correct and erroneous locations of the malfunctioning nodes and implementing a corresponding detection algorithm of the nodes with wrong locations.

B. Contributions & Outline

While there has been extensive literature on the design of alternative PNT solutions and on the detection of malicious nodes in PNT systems, in their overwhelming majority they remain fragmented, mainly addressing separately each problem, i.e., PNT solution and malicious nodes' detection. However, the corresponding problems are highly interleaved, and therefore the joint problem becomes even more complicated

The research of Dr. Tsiropoulou was partially supported by the NSF Awards #2219617 and #2319994.

978-1-6654-3540-6/22 © 2023 IEEE

in cases of GPS-denial or poor GPS signals. This paper aims exactly at filling this gap, and to the best of our knowledge, it is the first effort in the literature to examine the joint problem of designing a secure and robust alternative PNT solution that supports the targets' PNT services while simultaneously detecting and ejecting malicious nodes from the system that aim at deteriorating the proposed PNT solution's accuracy. Our primary contributions are summarized as follows.

1) A symbiotic PNT solution is introduced by exploiting the relationships among the anchor nodes, targets, and collaborators, who have known, unknown, and rough estimate of their positioning and timing. Under the proposed symbiotic PNT solution, a non-cooperative game is formulated among the targets and collaborators in order to jointly minimize their personal experienced positioning and timing error, as well as the error of the overall system.
2) The non-cooperative game is addressed as a potential game and the existence of at least one Pure Nash Equilibrium (PNE) is shown, determining the targets' and collaborators' accurate positioning and timing. A log-linear-based reinforcement learning (RL) algorithm is proposed in order to enable the targets and collaborators to determine their PNE strategies.
3) A detailed analysis of attacks detection is presented considering a single-attack or a distributed denial of service (DDoS) attack, where the malicious collaborators can fake their coordinates and their transmission power. A defense scheme, named SAFE, is introduced that is capable of jointly providing PNT services, detecting, and ejecting malicious collaborators.
4) A thorough evaluation of the SAFE scheme is performed, via modeling and simulation, showing its effectiveness and robustness in providing accurate PNT services, while securing the overall system by detecting and ejecting malicious nodes.

The remainder of the paper is organized as follows. Section II presents the symbiotic PNT solution based on a game theoretic approach and Section III analyzes the different types of attacks' detection along with the ejection mechanism of the malicious nodes. Section IV introduces the SAFE scheme, while Section V contains its performance evaluation. Finally, Section VI concludes the paper.

II. Symbiotic Positioning, Navigation, and Timing

A symbiotic PNT system is considered consisting of a set of anchor nodes $\mathcal{A} = \{1, \dots, a, \dots, A\}$, collaborator nodes $\mathcal{C} = \{1, \dots, c, \dots, C\}$, and targets $\mathcal{U} = \{1, \dots, u, \dots, U\}$. The collaborator nodes, anchor nodes, and targets are assumed to have a rough estimate, known, and unknown positioning and timing information, respectively, denoted as $\hat{\mathbf{X}}_c = (\hat{x}_c, \hat{y}_c, \hat{z}_c, \hat{\Delta t}_c), \forall c \in \mathcal{C}$, $\mathbf{X}_a = (x_a, y_a, z_a, \Delta t_a), \forall a \in \mathcal{A}$, and $\hat{\mathbf{X}}_u = (\hat{x}_u, \hat{y}_u, \hat{z}_u, \hat{\Delta t}_u), \forall u \in \mathcal{U}$, respectively.

Consider a target, e.g., Alice, aims at determining her positioning and timing $\hat{\mathbf{X}}_u$ following the proposed symbiotic PNT model. Alice will perform the following actions to identify her symbionts, i.e., anchor nodes and collaborators that can help her determine her positioning and timing. Alice broadcasts a ranging request beacon signal, which is received by the sets of neighboring anchor nodes $\mathcal{A}_u$ and collaborators $\mathcal{C}_u$. All nodes in $\mathcal{A}_u$ and $\mathcal{C}_u$ send a ranging reply beacon signal with transmission power $P_a = P_c = P$ [W], $\forall a \in \mathcal{A}_u, \forall c \in \mathcal{C}_u$, including digital information of their positioning and timing, i.e., $\mathbf{X}_a, \forall a \in \mathcal{A}_u, \hat{\mathbf{X}}_c, \forall c \in \mathcal{C}_u$. Alice measures the pseudoranges $d_{u,a}, \forall a \in \mathcal{A}_u, d_{u,c}, \forall c \in \mathcal{C}_u$ [m] based on the received power: $P^{rec}_{u,j} = P \frac{G^{tran}_j G^{rec}_u}{L_{u,j}}, \forall j \in \mathcal{A}_u \cup \mathcal{C}_u$, where G^{tran}_j [dB] and G^{rec}_u [dB] are the gains of the transmitting and receiving antennas, respectively. $L_{u,j}$ captures the signal propagation following the Okumura/Hata radio propagation model, that is $L_{u,j} = 69.55 + 26.16 \log f + (44.9 - 6.55 \log h_j) \log d_{u,j} - 13.82 \log h_j - 3.2[log(11.75 h_u)]^2 - 4.97$ [dB] with h_j, h_u [m] denoting the height of the transmitting nodes and receiving node, respectively, and f [Hz] is the carrier frequency $(f \geq 400MHz)$ [9].

Based on the above process, Alice knows the pseudoranges $d_{u,a}, \forall a \in \mathcal{A}_u, d_{u,c}, \forall c \in \mathcal{C}_u$ and neighboring nodes' positioning and timing, i.e., $\mathbf{X}_a, \forall a \in \mathcal{A}_u, \hat{\mathbf{X}}_c, \forall c \in \mathcal{C}_u$. Assuming that all her neighboring nodes are honest (this assumption will be relaxed in Section III), Alice will rely on all of them in order to determine her positioning and timing $\hat{P}_u$, as the more measured pseudoranges, the better her positioning and timing estimation. Our goal is to design a symbiotic PNT model that accurately determines Alice's positioning and timing $\hat{\mathbf{X}}_u, \forall u \in \mathcal{U}$, while jointly minimizing the positioning and timing estimation error of each target and collaborator, as well as the overall estimation error in the system.

Let us denote as $\hat{D}_{u,j}$ the Euclidean distance between the estimated positioning and timing and the corresponding accurate value, which is given as follows.

$$\hat{D}_{u,j}(\hat{\mathbf{X}}_u, \hat{\mathbf{X}}_j) = \begin{cases} ||\hat{\mathbf{X}}_u - \mathbf{X}_j||, \text{ if } j = a, \forall a \in \mathcal{A}_u \\ ||\hat{\mathbf{X}}_u - \hat{\mathbf{X}}_j||, \text{ if } j = c, \forall c \in \mathcal{C}_u \end{cases} \quad (1)$$

Thus, the corresponding positioning and timing error is $\epsilon(\hat{\mathbf{X}}_u, \hat{\mathbf{X}}_j) = [D_{u,j} - \hat{D}_{u,j}(\hat{\mathbf{X}}_u, \hat{\mathbf{X}}_j)]^2$ where $D_{u,j}$ was previously determined via the neighborhood identification process. Obviously, if $\hat{\mathbf{X}}_u, \hat{\mathbf{X}}_j, \forall j = c \in \mathcal{C}_u, \forall u \in \mathcal{U}$ are accurately determined, then $\epsilon(\hat{\mathbf{X}}_u, \hat{\mathbf{X}}_j) \to 0$. The goal of each target and collaborator $k = u, j, \forall u \in \mathcal{U}, \forall j \in \mathcal{C}$ is to minimize its own experienced estimated error:

$$\min_{\{\hat{\mathbf{X}}_k\}_{k \in \mathcal{U} \cup \mathcal{C}}} \sum_{\forall j \in \mathcal{A}_k \cup \mathcal{C}_k} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j) \quad (2)$$

and the overall goal of the system is to minimize the overall estimation error in the system.

$$\min_{\{\hat{\mathbf{X}}_k\}_{k \in \mathcal{U} \cup \mathcal{C}}} E(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j) = \sum_{\forall k \in \mathcal{U} \cup \mathcal{C}} \sum_{\forall j \in \mathcal{A}_k \cup \mathcal{C}_k} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j) \quad (3)$$

Towards solving the optimization problems (2) and (3), we formulate a non-cooperative game $G = [\mathcal{N}, \{S_n\}_{\forall n \in \mathcal{N}}, \{U_n\}_{\forall n \in \mathcal{N}}]$, where $\mathcal{N} = \mathcal{U} \cup \mathcal{C}$ is the set of players, i.e., targets and collaborators, $S_n = \{s_n\} = \{\hat{\mathbf{X}}_n\}$

is the strategy set of each player in terms of positioning and timing decision, and $U_n(s_n, \mathbf{s}_{-n}) = \sum_{\forall j \in \mathcal{A}_n \cup \mathcal{C}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j)$ is the player's n payoff function.

Definition 1: **(Pure Nash Equilibrium – NE)** A strategy vector $\mathbf{s}^*$ is a Pure Nash Equilibrium (PNE) of the non-cooperative game G, iff $U_n(s_n^*, \mathbf{s}_{-n}^*) \leq U_n({s_n}', \mathbf{s}_{-n}^*), \forall {s_n}' \in S_n, \forall n \in \mathcal{N}$.

Definition 2: **(Exact Potential Game)** The non-cooperative game G is an exact potential game, iff $\Phi(s_n, \mathbf{s}_{-n}) - \Phi({s_n}', \mathbf{s}_{-n}) = U_n(s_n, \mathbf{s}_{-n}) - U_n({s_n}', \mathbf{s}_{-n}), \forall {s_n}' \in S_n, \forall n \in \mathcal{N}$, where $\Phi(s_n, \mathbf{s}_{-n})$ is the potential function.

Theorem 1: **(Existence of PNE)** The non-cooperative game $G = [\mathcal{N}, \{S_n\}_{\forall n \in \mathcal{N}}, \{U_n\}_{\forall n \in \mathcal{N}}]$ is an exact potential game, with potential function $\Phi(s_n, \mathbf{s}_{-n}) = \frac{E(s_n, \mathbf{s}_{-n})}{2}$ and has at least one PNE.

Proof: For any ${s_n}' \neq s_n, \forall n \in \mathcal{N}$, we have: $U_n(s_n, \mathbf{s}_{-n}) - U_n({s_n}', \mathbf{s}_{-n}) = \sum_{\forall j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) - \sum_{\forall j \in \mathcal{N}_n} \epsilon({\hat{\mathbf{X}}_n}', \hat{\mathbf{X}}_j)$, with $\mathcal{N}_n = \mathcal{A}_n \cup \mathcal{C}_n$. Also, we have: $\Phi(s_n, \mathbf{s}_{-n}) = \frac{1}{2} \sum_{\forall n \in \mathcal{N}} \sum_{\forall j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) = \frac{1}{2}[\sum_{\forall j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) + \sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} \sum_{\forall j \in \mathcal{N}_k} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j)] = \frac{1}{2}[\sum_{\forall j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) + \sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} [(\sum_{\substack{\forall j \in \mathcal{N}_k \\ j \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j)) + \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_n)]] = \frac{1}{2}[\sum_{j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) + \sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} \sum_{\substack{\forall j \in \mathcal{N}_k \\ j \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j) + \sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_n)]$. If two nodes k, n are not neighbors, then, they cannot measure their pseudoranges, thus: $\epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_n) = 0, k, n \notin \mathcal{N}_n$. Thus, the last term of the potential function written as: $\sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_n) = \sum_{\forall k \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_n) + \underbrace{\sum_{\substack{\forall k \notin \mathcal{N}_n \\ k \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_n)}_{= 0} = \sum_{\forall k \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_n)$. Thus, the potential function is written as follows: $\Phi(s_n, \mathbf{s}_{-n}) = \frac{1}{2}[\sum_{\forall j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) + \sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} \sum_{\substack{\forall j \in \mathcal{N}_k \\ j \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j) + \sum_{\forall k \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_n)] = \frac{1}{2}[2 \sum_{\forall j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) + \sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} \sum_{\substack{\forall j \in \mathcal{N}_k \\ j \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j)] = \sum_{\forall j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) + \frac{1}{2} \sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} \sum_{\substack{\forall j \in \mathcal{N}_k \\ j \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j)$. Then, we calculate the difference of the potential function for two different strategies $s_n, {s_n}' \in S_n$, as follows: $\Phi(s_n, \mathbf{s}_{-n}) - \Phi(s_n', \mathbf{s}_{-n}) = \sum_{\forall j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) + \frac{1}{2} \sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} \sum_{\substack{\forall j \in \mathcal{N}_k \\ j \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j) - [\sum_{\forall j \in \mathcal{N}_n} \epsilon({\hat{\mathbf{X}}_n}', \hat{\mathbf{X}}_j) + \frac{1}{2} \sum_{\substack{\forall k \in \mathcal{N} \\ k \neq n}} \sum_{\substack{\forall j \in \mathcal{N}_k \\ j \neq n}} \epsilon(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j)] = \sum_{\forall j \in \mathcal{N}_n} \epsilon(\hat{\mathbf{X}}_n, \hat{\mathbf{X}}_j) - \sum_{\forall j \in \mathcal{N}_n} \epsilon({\hat{\mathbf{X}}_n}', \hat{\mathbf{X}}_j) = U_n(s_n, \mathbf{s}_{-n}) - U_n({s_n}', \mathbf{s}_{-n}), \forall n \in \mathcal{N}$. Thus, the non-cooperative game G is an exact potential game and has at least one PNE [10]. ■

III. Attacks Detection & Malicious Nodes Ejection

In this section, a detailed attacks detection analysis is provided considering that the malicious collaborators can fake their PNT signals' transmission power ${P_c}'$ [W] and their positioning and timing information $\hat{\mathbf{X}}_c$. The scenarios of single-attack and DDoS attack are considered and the ejection mechanism of the malicious collaborators is also presented.

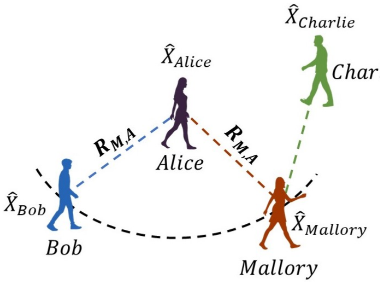

Fig. 1: Fake positioning and timing attack.

A. *Fixed Transmit Power & Fake Positioning and Timing*

Initially, we analyze the scenario where all the collaborators transmit their ranging reply beacon signal with fixed power $P_c = P, \forall c \in \mathcal{C}$ and one malicious collaborator M fakes its positioning and timing $\hat{\mathbf{X}}_M$. As presented in Fig. 1, the malicious collaborator M can pretend that it belongs to any position of the dotted circle line. In that case, Alice cannot detect the malicious collaborator M. However, an anchor node a, e.g., Charlie, that belongs to the same neighborhood, who accurately knows its own positioning and timing $\mathbf{X}_a$, by receiving the malicious collaborators' digital information $\hat{\mathbf{X}}_M$ and by measuring the received power, it determines the pseudorange $d_{a,M}$. Then, by calculating the pseudorange ${d_{a,M}}' = ||(x_a, y_a, z_a) - (\hat{x}_M, \hat{y}_M, \hat{z}_M)||$, it identifies that $d_{a,M} \neq {d_{a,M}}'$, and raises a "red flag" that M is a malicious collaborator. Then, this "red flag" information is broadcasted to all the targets in the anchor node's neighborhood, and Alice excludes the malicious node M from her collaborators, i.e., $\mathcal{C}_{Alice} = \mathcal{C}_{Alice} \setminus \{M\}$. A similar analysis can be derived for the case of DDoS attack, where multiple malicious collaborators $\mathcal{M} = \{1, \ldots, M, \ldots, |\mathcal{M}|\}$ fake their positioning and timing information in order to damage the accuracy of the proposed symbiotic PNT model. The neighboring anchor nodes will detect them, inform the targets via broadcasting the red flag information, and ultimately the targets will eject them from the system. It is noted that in the probabilistically rare case that the anchor node a (Charlie in Fig. 1) belongs at the same circle line with Alice, with center the malicious collaborator M and radius $R_{M,A}$ [m], then it cannot detect the malicious collaborator M. In that case, either another neighbor anchor node will contribute to the accurate detection of the malicious collaborator, or a neighbor legitimate collaborator will detect the malicious nodes with an approximate attack detection given its own positioning and timing estimation error.

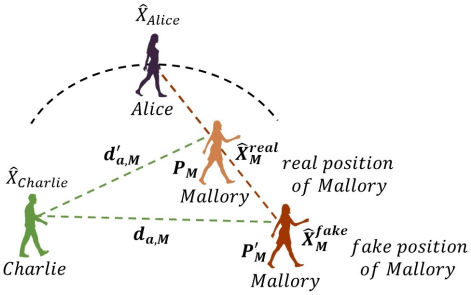

Fig. 2: Variable transmit power & fake positioning and timing attack

B. Variable Transmit Power & Fake Positioning and Timing

We extend our study by considering that a malicious collaborator M fakes both its positioning and timing information $\hat{\mathbf{X}}_M$ and its transmission power $P_M{}'$ [W] of its ranging reply beacon signal. In this case, Alice cannot detect the malicious collaborator M. However, a neighbor anchor node a receives the malicious collaborator's positioning and timing information $\hat{\mathbf{X}}_M$ and determines its corresponding pseudorange $d_{a,M}$ based on the received power of the malicious collaborator's ranging reply beacon signal $P_M{}'$. Given that the anchor node a has perfect knowledge of its positioning and timing $\mathbf{X}_a$, it calculates the pseudorange $d_{a,M}{}' = ||(x_a, y_a, z_a) - (\hat{x}_M, \hat{y}_M, \hat{z}_M)||$. Evidently, the anchor node identifies that $d_{a,M} \neq d_{a,M}{}'$ and categorizes the collaborator M as malicious, and informs all the targets in its neighborhood via broadcasting the list of malicious collaborators. Similar analysis can be derived in the case of a DDoS attack, where multiple malicious collaborators fake both their transmission power and their positioning and timing. Also, the same ejection policy of the malicious collaborators can be followed as in Section III-A, if the anchor node belongs to the same circle line with Alice, with center the malicious collaborator M.

IV. SAFE: A Defense Scheme

By combining the analysis presented in Sections II and III, in this section, we introduce the SAFE secure symbiotic PNT that is capable of jointly providing accurate estimates of the targets' positioning and timing in the cases of GPS-denial or poor GPS signals, and detecting and ejecting the malicious nodes from the system. Towards determining the PNE, as presented in Theorem 1, the log-linear Max-logit algorithm is adopted where each target $u \in \mathcal{U}$ and each collaborator $c \in \mathcal{C}$ perform the exploration and learning processes in order to determine their optimal positioning and timing $\mathbf{s}^*$ that minimizes their own estimation error (Eq. 2), as well as the one of the overall system (Eq. 3). Initially, each node selects a strategy $s_n{}'$ with equal probability $Pr(s_n{}') = \frac{1}{|S_n|}$ and explores its experienced payoff $U_n(s_n{}', \mathbf{s}_{-n})$ given the strategies of the rest of the nodes. Then, each node $n \in \mathcal{N} = \mathcal{U} \cup \mathcal{C}$ updates its strategy based on the following probabilistic rules:

$$Pr(\mathbf{s}_n^{ite} = \mathbf{s}_n^{ite-1}) = \frac{e^{\beta U_n(\mathbf{s}_n^{ite-1})}}{\max\{e^{\beta U_n(\mathbf{s}_n^{ite-1})}, e^{\beta U_n(\mathbf{s}_n^{ite'})}\}} \quad (4a)$$

$$Pr(\mathbf{s}_n^{ite} = \mathbf{s}_n^{ite'}) = \frac{e^{\beta U_n(\mathbf{s}_n^{ite'})}}{\max\{e^{\beta U_n(\mathbf{s}_n^{ite-1})}, e^{\beta U_n(\mathbf{s}_n^{ite'})}\}} \quad (4b)$$

where $\beta \in \mathbb{R}^+$ denotes the learning rate. The SAFE secure symbiotic PNT algorithm is presented in Algorithm 1 and its complexity is $O(Ite)$, where Ite is the number of iterations required for convergence to the PNE. Detailed results of the SAFE algorithm's execution time are presented in Section V.

Algorithm 1 SAFE: Secure Symbiotic PNT Algorithm

```
Input: $\mathbf{X}_a, \forall a \in \mathcal{A}$, $\hat{\mathbf{X}}_c, \forall c \in \mathcal{C}$, $P$, $P_M, \forall M \in \mathcal{M}$, $\hat{\mathbf{X}}_M, \forall M \in \mathcal{M}$
Output: $s^*$
Initialization: $ite = 0$, $Convergence = 0$, $\mathbf{s}_n^{ite=0}$, $\forall n \in \mathcal{N} = \mathcal{U} \cup \mathcal{C}$.
for all $c \in \mathcal{C}$ do
    for all $a \in \mathcal{A}$ do
        Determine $d_{a,c}$ based on the received power of the ranging reply beacon signal.
        Determine $d_{a,c}{}' = ||(x_a, y_a, z_a) - (\hat{x}_c, \hat{y}_c, \hat{z}_c)||$
        if $d_{a,c}{}' \neq d_{a,c}$ then
            Eject the malicious collaborator node $c = M$ by broadcasting a "red flag" signal.
        end if
    end for
end for
while $Convergence == 0$ do
    $ite = ite + 1$;
    A node $n \in \mathcal{N} = U \cup C \setminus \{M\}_{\forall M \in \mathcal{M}}$ selects $s_n^{ite'}$ with equal probability $\frac{1}{|S_n|}$, receives a payoff $U_n^{ite}(s_n^{ite'})$ and updates $\mathbf{s}_n^{ite}$ based on Eq. 4a, 4b, while the rest of the nodes keep their previous strategies, i.e., $\mathbf{s}_{-n}^{ite} = \mathbf{s}_{-n}^{ite-1}$.
    if $\left|\frac{\sum_{ite=0}^{Ite} \sum_{\forall n \in \mathcal{N}} U_n^{ite}}{ite} - \sum_{\forall n \in \mathcal{N}} U_n^{ite}\right| \leq \delta$, $\delta$: small positive number then
        $Convergence = 1$;
    end if
end while
```

V. Numerical Results

In this section, a simulation-based evaluation is introduced to demonstrate the operational characteristics of the SAFE: Secure Symbiotic PNT scheme, as well as its benefits in terms of providing an accurate estimation of the nodes' positioning and timing, in an effective and robust manner. Specifically, Section V-A discusses the pure performance and operation of the SAFE scheme, and Section V-B quantifies its efficiency and robustness against malicious attacks. Also, Section V-C provides a scalability analysis of the SAFE scheme to demonstrate its superiority in addressing DDoS attacks. A topology of $U = 5$ targets, $C = 10$ collaborators and $A = 20$ anchor nodes is considered. The rest of the simulation parameters are:

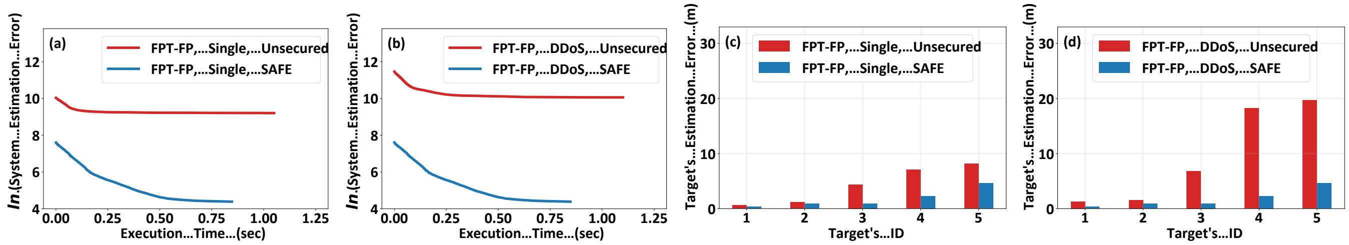

Fig. 3: SAFE scheme's operation under attacks of fake positioning and timing.

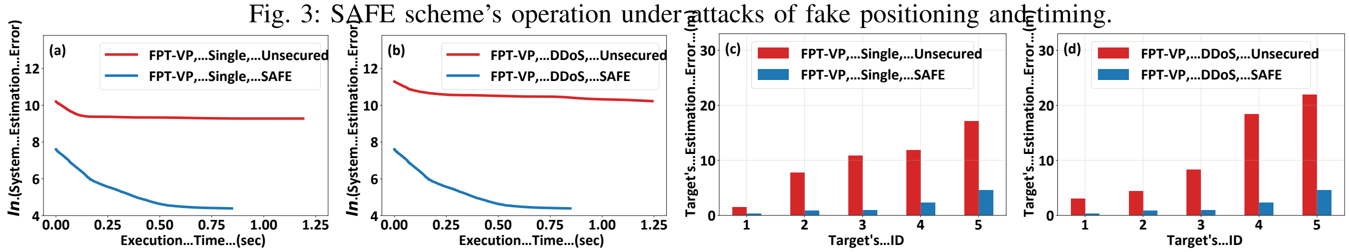

Fig. 4: SAFE scheme's operation under attacks of variable transmission power and fake positioning and timing.

$P = 2$ [W], $G_j^{tran} = 0$ [dB], $G_u^{rec} = 0$ [dB], $f = 400$ [MHz], $h_j = 1.5$ [m], $h_u = 1.5$ [m], unless otherwise explicitly stated.

A. Pure Performance and Operation of the SAFE Model

The operational characteristics of the SAFE scheme are initially presented and compared to the corresponding ones for the unsecured symbiotic PNT solution, where the malicious collaborators are not detected and ejected from the system. The scenarios of a single-attack, i.e., 1 malicious collaborator, and a DDoS attack with 5 malicious collaborators are examined, considering the cases that: (i) they only fake their positioning and timing (FPT) with fixed transmission power (FP), and (ii) they fake both their positioning, timing (FPT) and transmission power by transmitting at variable power (VP) levels. The corresponding acronyms are: FPT-FP and FPT-VP.

Figs. 3a-3b present the system's estimation error $E(\hat{\mathbf{X}}_k, \hat{\mathbf{X}}_j)$ (logarithmic axis) as a function of the execution time to determine the optimal positioning and time, under the unsecured FPT-FP and the SAFE schemes, considering the single-attack and DDoS attack, respectively. Similar results are presented in Figs. 4a-4b for the FPT-VP case. Moreover, Figs. 3c-3d (Figs. 4c-4d) illustrate each target's estimation error for the single-attack and DDoS attack scenarios, respectively, under the FPT-FP (FPT-FP) case. It is noted that the targets with higher ID are placed in worse positions in the system with respect to their localization perspective, e.g., more physical obstacles in their communication with the neighbor nodes.

The results reveal that the SAFE scheme substantially safeguards the overall system in terms of achieving low system's estimation error under single-attacks (Fig. 3a and Fig. 4a) and DDoS attack scenarios (Fig. 3b and Fig. 4b) compared to the unsecured FPT-FP (Figs. 3a-3b) and FPT-VP (Figs. 4a-4b) counterparts, which are not capable of detecting and ejecting the malicious collaborators. Also, the results show the real-time applicability of the proposed SAFE scheme, as less than 1 sec is needed to accurately determine the nodes' positioning and timing, and detect and eject the malicious collaborators. The results also indicate that the DDoS attack (Fig. 3b and Fig. 4b) can deteriorate more the system's estimation error compared to the single-attack scenario (Fig. 3a and Fig. 4a).

Focusing on the target's estimation error, we observe that the SAFE scheme achieves the lowest one for all the targets both under the single-attack (Fig. 3c and Fig. 4c) and the DDoS attack (Fig. 3d and Fig. 4d). The targets with higher ID experience higher estimation error under all the examined attack scenarios and PNT cases, given their a priori disadvantaged position in the system. The DDoS attack deteriorates the targets' estimation error (Fig. 3d and Fig. 4d) substantially more than the single-attack scenario (Fig. 3c and Fig. 4c) under both the FPT-FP and FPT-VP cases. Under the FPT-VP case, the targets' estimation error (Figs. 4c-4d) is worse compared to the FPT-FP case (Figs. 3c-3d), as the malicious collaborators can fake their positioning, timing and transmission power.

B. Efficiency & Robustness of the SAFE Scheme

In this section, we demonstrate the efficiency and robustness of the proposed SAFE scheme to safeguard the system from malicious attacks in a real-time manner. For the evaluation purposes, the efficiency metric is defined as $\frac{1}{(\sum_{\forall u \in \mathcal{U}} Target'sEstimationError_u) \cdot TotalExecutionTime}$, capturing both the PNT solution's accuracy and time efficiency. Fig. 5 presents the efficiency and the system's estimation error under the single-attack and DDoS attacks scenarios for both the FPT-FP and FPT-VP cases, while considering the unsecured schemes and the SAFE scheme. It is noted that the SAFE scheme detects and ejects the malicious collaborators under all comparative cases. The results reveal that the SAFE scheme achieves the highest efficiency and the lowest system's estimation error under all the examined attacks scenarios and FPT-FP, FPT-VP cases. Also, the results demonstrate that the DDoS attack can substantially decrease the efficiency and increase the system's estimation error compared to the single-attack scenario under both the FPT-FP and FPT-VP cases. Furthermore, when the malicious collaborators fake both their transmission power and their positioning and timing information, i.e., FPT-VP case, they can harm the system more

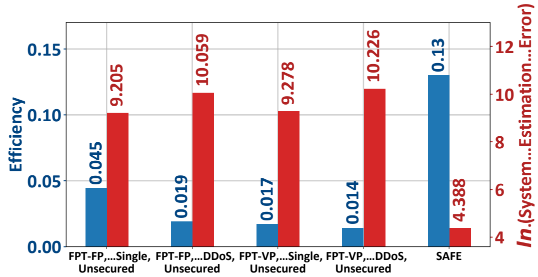

Fig. 5: Comparative evaluation.

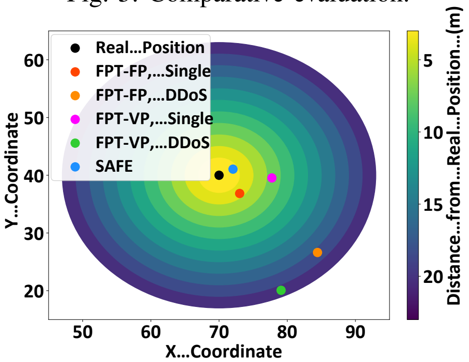

Fig. 6: Efficiency and robustness of the SAFE scheme.

in terms of its efficiency and estimation error compared to the case of faking only their transmission power, i.e., FPT-FP case.

Fig. 6 illustrates via a heatmap the estimated position of an indicative target under the FPT-FP and FPT-VP cases both under the single-attack and DDoS attacks scenarios compared to the SAFE scheme. The results clearly demonstrate the accuracy of the proposed SAFE scheme in terms of determining the target's position, while the worst impact is imposed by the DDoS attack of multiple malicious collaborators, when they fake both their transmission power and positioning and timing information (FPT-VP DDoS).

C. Scalability Analysis to DDoS Attacks

In this section, a scalability analysis of the proposed SAFE scheme is provided for an increasing number of malicious collaborators in order to capture its success in defending against DDoS attacks. Figs. 7a-7b present the system's estimation error and the targets' total estimation error as a function of the number of malicious collaborators, respectively, considering the FPT-FP, FPT-VP unsecured cases, and the SAFE scheme. It is noted that as the number of malicious collaborators increases, an equivalent increase is performed to the number of legitimate collaborators for fairness in the comparison. The results reveal that the two factors of attack (FPT-VP) can result in the largest damage in the system (Fig. 7a) and the targets' total estimation error (Fig. 7b). On the other hand, the SAFE scheme can successfully detect and eject the malicious collaborators from the system, resulting in decreasing targets' total estimation error (Fig. 7b), as more legitimate collaborators remain in the system to support the targets' PNT services. Also, the increasing number of legitimate collaborators that remain in the system under the SAFE scheme contribute to the slow-rate increase of the system's estimation error.

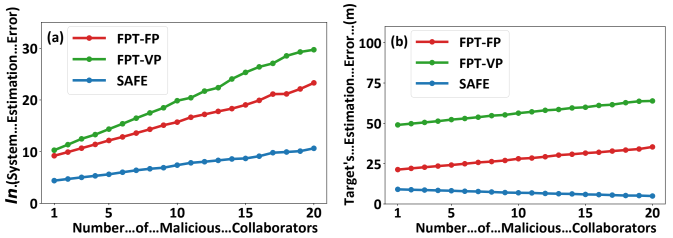

Fig. 7: Robustness to DDoS attacks.

VI. Conclusion

In this paper, a secure and robust symbiotic PNT model is introduced, named SAFE, exploiting the symbiotic relationship among the anchor nodes, collaborators, and targets, who have known, a rough estimate, and unknown positioning and timing information, respectively. The SAFE scheme jointly determines the targets' and collaborators' positioning and timing following a game-theoretic approach, and detects and ejects malicious collaborators from the system. Different scenarios of malicious nodes faking their transmission power and their positioning and timing information are analyzed. Part of our current and future work focuses on the extension of the SAFE scheme considering the involved nodes' mobility [11], [12].

References

[1] M. S. Siraj, A. B. Rahman, M. Diamanti, E. E. Tsiropoulou, and S. Papavassiliou, "Alternative positioning, navigation, and timing enabled by games in satisfaction form and reconfigurable intelligent surfaces," *IEEE Systems Journal*, 2023.

[2] J. Won and E. Bertino, "Robust sensor localization against known sensor position attacks," *IEEE Transactions on Mobile Computing*, vol. 18, no. 12, pp. 2954–2967, 2019.

[3] S. Tomic and M. Beko, "Detecting distance-spoofing attacks in arbitrarily-deployed wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 4383–4395, 2022.

[4] C. Sanders and Y. Wang, "Localizing spoofing attacks on vehicular gps using vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 656–15 667, 2020.

[5] Z. Wang, S. Wang, M. Z. A. Bhuiyan, J. Xu, and Y. Hu, "Cooperative location-sensing network based on vehicular communication security against attacks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 942–952, 2023.

[6] S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao, and H. Zhou, "Delimitated anti jammer scheme for internet of vehicle: Machine learning based security approach," *IEEE Access*, vol. 7, pp. 113 311–113 323, 2019.

[7] A. R. Svaigen, A. Boukerche, L. B. Ruiz, and A. A. F. Loureiro, "A topological dummy-based location privacy protection mechanism for the internet of drones," in *IEEE ICC*, 2022, pp. 1–6.

[8] Z. Li, Z. Tian, Z. Wang, and Y. Wang, "Multipath-assisted indoor localization: Turning multipath signal from enemy to friend," in *IEEE GLOBECOM*, 2019, pp. 1–6.

[9] V. Garg, "Radio propagation and propagation path-loss models," *Wireless Communications & Networking*, pp. 47–84, 2007.

[10] D. Monderer and L. S. Shapley, "Potential games," *Games and economic behavior*, vol. 14, no. 1, pp. 124–143, 1996.

[11] M. S. Siraj, A. B. Rahman, M. Diamanti, E. E. Tsiropoulou, S. Papavassiliou, and J. Plusquellic, "Orchestration of reconfigurable intelligent surfaces for positioning, navigation, and timing," in *IEEE Military Communications Conference*. IEEE, 2022, pp. 148–153.

[12] M. S. Hossain, N. Irtija, E. E. Tsiropoulou, J. Plusquellic, and S. Papavassiliou, "Reconfigurable intelligent surfaces enabling positioning, navigation, and timing services," in *IEEE ICC*. IEEE, 2022, pp. 4625–4630.