

Tree Proof-of-Position Algorithms

Aida Manzano Kharman, Pietro Ferraro, Homayoun Hamedmoghadam, Robert Shorten

Abstract—We present a novel class of proof-of-position algorithms: **Tree-Proof-of-Position (T-PoP)**. This algorithm is decentralised, collaborative and can be computed in a privacy preserving manner, such that agents do not need to reveal their position publicly. We make no assumptions of honest behaviour in the system, and consider varying ways in which agents may misbehave. Our algorithm is therefore resilient to highly adversarial scenarios. This makes it suitable for a wide class of applications, namely those in which trust in a centralised infrastructure may not be assumed, or high security risk scenarios. Our algorithm has a worst case quadratic runtime, making it suitable for hardware constrained IoT applications. We also provide a mathematical model that summarises T-PoP’s performance for varying operating conditions. We then simulate T-PoP’s behaviour with a large number of agent-based simulations, which are in complete agreement with our mathematical model, thus demonstrating its validity. T-PoP can achieve high levels of reliability and security by tuning its operating conditions, both in high and low density environments. Finally, we also present a mathematical model to probabilistically detect platooning attacks.

Index Terms—location, position, proof, tree, algorithms, privacy, decentralisation.

I. INTRODUCTION

An emerging problem in many domains concerns the verification that an individual, or an object, is in the location that it claims to be in. Examples of situations where such a need arises range from images in conflict zones to vehicles who need to prove their location in order to access services. Proof-of-position algorithms refer to a suite of algorithmic tools that are designed to enable such objects to prove their location.

The question of proving one’s position is trivial to answer when a centralised and trustworthy infrastructure exists. An example such an infrastructure of this could, for example, be a network of surveillance cameras that are operated by a trusted government agency. In such situations it is relatively straightforward for an agent to verify their claimed location. However, such architectures impose a very strong trust assumption, and should the centralised network be compromised or malicious, one can no longer ensure that the location proof is trustworthy. Consequently, making such a trust assumption greatly restricts the practicality of any solution relying on it.

Hence we advocate for the need for a proof-of-position algorithm that is *decentralised*. However, decentralisation alone does not suffice. Information on an individual’s position is sensitive. Revealing it may incur safety risks to the user. Thus, the proof-of-position algorithms must also be privacy preserving. More concisely: one should be able to provide a verifiable proof of their position, without having to publicly reveal their position. In addition, for any solution to be applicable to real-world use cases, it must be designed to

withstand adversarial environments and account for individuals that lie and misbehave. In the context of proof-of-position, there are many ways an agent could lie: they may lie about their own position, but also about the position of others. With these considerations in mind, our objective in this paper is to provide a proof-of-position algorithm that is decentralised; private; and robust to adversarial attacks.

II. RELATED WORK

A preliminary version of our work was presented at [1]. The following *Related Work* section closely resembles the related work in [1], given that, to the best of our knowledge, since the publication [1], the only new proof-of-position protocol published in the literature is [2].

A number of works have appeared in the literature addressing the problem of proving one’s position; see for example [3], [4], [5], [6], [7]. These proposals are unsuitable for high risk scenarios we consider because they introduce trust assumptions that may not hold in adversarial environments. They also *de facto* re-introduce a degree of centralisation in their systems. We proceed by outlining some of this prior work.

An early example of a decentralized proof-of-location scheme, known as APPLAUS, was introduced in [8]. APPLAUS addressed collusion attacks through graph clustering and computing a ‘betweenness’ metric to evaluate node trustworthiness. In [9], nodes weakly connected in the graph are considered less reliable. They propose a time-decayed weight function and determine node trustworthiness based on the ratio of approvals to neighbours. This latter contribution serves as a starting point for our work. Whilst offering a number of valuable contributions, this work relies on a central server that stores information on the number of agents at particular time and location to detect fraudulent proof generation. This information can be used to estimate whether a prover lies about not finding enough peers or always finding the same peer based on some statistical techniques. Conversely, the security and integrity of our algorithm does not rely assuming access to a trusted central server that stores said information.

Another scheme, SHARP, presents a private proximity test without revealing actual locations to a server [10]. They introduce a secure handshake method without needing pre-shared secrets, ensuring a witness¹ can only extract the session key if in they are indeed in the vicinity of the prover². Security is ensured by requiring that location tags are unforgeable. However, a coerced user could generate a valid location proof and relay it to a malicious user in a different location. This means the location proof is not non-repudiable [11].

¹An agent that verifies that they see another agent wishing to prove their position.

²An agent that wishes to prove their position.

Vouch+ [12], another decentralized approach, addresses high-speed and platooning scenarios. However, its security relies on the assumption that the selected proof provider is honest. We consider this assumption to be too strong. Indeed, our algorithm provides probabilistic guarantees of detecting that a prover is lying about their position. SPARSE [3] makes collusion difficult by preventing provers from choosing their own witnesses. Their solution provides integrity, unforgeability and non-transferability. However, this is achieved through the use of a trusted verifier, and it is assumed that they will not publish users' identity and their data. We again consider this assumption too strong.

The authors in [2] propose a proof-of-position protocol using blockchain agnostic smart contracts. A number of proposals have emerged to design proof-of-position schemes leveraging blockchain technologies, see: [7], [6], [13], [14]. Blockchain is known to centralise over time [15], and is highly resource intensive [16]. Our protocol does not rely on blockchain, thus avoiding the drawbacks inherent to its design.

Contributions with respect to prior-art: In this paper we present a decentralised proof-of-position algorithm, T-PoP. It is decentralised because it does not rely on a trusted central server or authority to ensure the position proof is valid. It is privacy preserving, because the position proof may be computed without revealing the position of an agent publicly, and other participants may verify that the position proof is indeed valid. Indeed, we provide a proof of concept using Zama's fully homomorphic encryption library [17], where agents provide their encrypted position, and run T-PoP without having to decrypt it. It is available on our GitHub repository. Our algorithm is also robust to highly adversarial scenarios: we consider that agents may not only lie about their own position, but also about the position of other agents. We take this consideration into account to provide a probabilistic guarantee of an agent's position. We provide a mathematical model that summarises the behaviour of our algorithm, and validate that the model does indeed represent our algorithm through the use of agent-based simulations. This model provides designers with security and reliability guarantees of T-PoP's performance, given an expected distribution of malicious agents in the network. Thus, designers may use this model as opposed to conducting resource intensive agent based simulations to determine what operating conditions of our algorithm best suit their needs. Our algorithm runs in quadratic time and thus can be implemented in a wide range of IoT applications. T-PoP is a solution to prove one's location in a highly adversarial and mutually distrusting environment, where a central authority and trusted infrastructure cannot be relied upon. We demonstrate it performs well in both high and low density applications, given that its operating conditions may be tuned to provide increased security or reliability.

III. COMPONENTS

We proceed by introducing the components necessary to understand the functioning of T-PoP.

Agents: Any participant in the proof-of-position protocol is considered an agent, a_i , where $a_i \in A$, $|A| = N$ and N is the

total number of agents operating in the protocol. All agents are in a given *state*, that determines if they are honest, and coerced, or not. For brevity, we omit the agent's index where unnecessary.

Environment: We assume that agents willing to participate in the protocol are situated in an environment, E , where $E \subseteq \mathbb{R}^2$. We note that this does not represent a limitation of the protocol and that any space with a suitable distance metric can be employed for the T-PoP protocol.

Position: All agents have a *real* position, p , and a *claimed* position, \hat{p} . Each agent can lie about their claimed position by committing to \hat{p} such that $\hat{p} \neq p$.

$$\hat{p} \in \{p, p'\} \tag{1a}$$

$$\hat{p} = p \vee \hat{p} = p' \tag{1b}$$

$$p' \neq p \tag{1c}$$

In other words, the *claimed* position may or may not be equal to the *real* position. We say that $\{\hat{p}, p, p'\} \in E$.

Agent states: All agents are in a given *state*, which is comprised of three attributes: honesty, coercion and position.

- An agent is considered *honest* if they claim to be in their real position. i.e.: $\hat{p} = p$, and *dishonest* otherwise, where $\hat{p} \neq p$.
- All agents are in a real position. *Honest* agents will claim to be in their real position, and *dishonest* agents will claim to be elsewhere.
- An agent is considered *coerced* if they attest to seeing a *dishonest* agent in their claimed (fake) position. In other words: a *coerced* agent will claim to see agents that are not actually in its vicinity, if the latter are dishonest. *Non-coerced* agents will only attest to seeing other nearby agents in their *real* position.

Prover: An agent initiating the proof-of-position protocol, wishing to prove that they are in their *claimed* position, is called a *prover*.

Range of sight: Agents have a fixed, positive range of sight, r_i with $r_i \geq 0$.

Field of view: Agent a_i 's field of view, \overline{D}_i , is defined as the closed disk area with centre $\hat{p}_i = (x_i, y_i)$ and radius r_i .

$$\overline{D}_i = \{(x, y) \in \mathbb{R}^2 : (x - x_i)^2 + (y - y_i)^2 \leq r_i^2\} \tag{2}$$

We say agent a_j with position $\hat{p}_j = (x_j, y_j)$, is in a_i 's field of view if:

$$(x_j - x_i)^2 + (y_j - y_i)^2 \leq r_i^2$$

In other words, if the position of a_j falls inside \overline{D}_i .

Note: this field of view is not restrictive of physical obstacles blocking immediate range of sight, rather, it is intended as a model for connectivity range.

Witness: Provided a_j is in a_i 's field of view, a_j may be named as a *witness* of a_i , depending on the *states* of both

agents.

Approvals: If a witness a_j attests to seeing the agent that named it, a_i , the witness is said to *approve* a_i . Approvals are always computed from both the agents' *claimed* position.

IV. OVERVIEW OF OUR PROTOCOL

In this section, we outline a brief, high-level description of the protocol we propose. It is structured around three stages: **Commit**, **Tree Building**, and **Verification**. This protocol is initiated by an agent wishing to prove they are in a claimed position. In the initial stage, **Commit**, each agent constructs a cryptographic commitment of their claimed position, using a cryptographic commitment scheme³. This commitment ensures the position claim cannot be changed *a posteriori*, i.e., it is binding, and is also hiding, meaning the position need not be publicly revealed. Upon constructing the commitment, each agent then uploads their commitment onto a decentralised network. This can be a transaction in a DLT or uploaded to IPFS, a peer to peer file sharing network [21]. In this manner, immutability and verifiability are assured.

Subsequently, the Tree Building stage follows. It may only be computed by an agent that has already committed to a position in the **Commit** stage. Said agent is considered the prover. The prover constructs a tree by naming other nearby agents, which are considered the prover's witnesses. Each node in the tree is an agent, where the prover is the root of the tree, and the witnesses are the leaves. The tree's dimensions are predetermined *a priori*, namely the height and the branching factor. The protocol imposes strict constraints to prevent the naming the same witness twice in the same tree, aiming to mitigate deceitful practices (e.g., agents cyclically validating each other).

The final stage of the protocol is the Verification stage. In it, the prover's tree of witnesses is assessed to verify the prover's position. The witnesses may attest to seeing the agent that named them, or not. If a witness does so, this is considered an approval. If sufficient approvals in the tree are amassed, the prover's position claim is considered valid, provided other necessary criteria are also met in the tree.

V. IMPLEMENTATION DETAILS OF T-POP

We proceed by giving a more detailed description of the novel components we present in the T-PoP protocol.

- **Tree Building:** Each agent who has already committed their position, then constructs a tree of depth $h \in \mathbb{N}^+$, incorporating the committed positions of agents, called *witnesses*, at levels $d \in \{0, \dots, h\}$. A specific agent — which we denote as g —is the root of the resulting tree. For every *prover*, g , the tree is constructed as follows:
 - g is the root node at level 0.

³Many options are available: KZG commitment schemes [18], Pedersen commitments, Merkle trees or Hashing [19]. Some schemes also offer the desirable property of being additively and/or multiplicatively homomorphic [20]. The choice of commitment scheme will be driven by application specific needs.

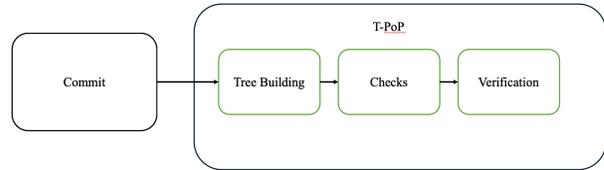


Fig. 1: High-level Overview of the Proof of Position protocol.

- For each $d \in \{1, \dots, h\}$, each node at level $d - 1$ will name w_d other agents. An agent at level d is an agent, a_j , that is in the range of sight of agent, a_i at level $l - 1$ (note that, if $\hat{p}_i \neq p_i$, and a_i is lying about their position, it is possible that a_j is not in the range of sight of a_i). a_i is called the *parent* of the *child* a_j .

In practice, the root node, g , names w_1 witnesses who in turn name w_2 witnesses and so on, until we reach depth h . The number of witnesses per level, n_l , can therefore be computed recursively:

$$n_d = w_d n_{d-1}, \quad d = 1, \dots, h, \quad (3)$$

with $n_0 \equiv 1$.

- **Checks and Verification:** The Checks and Verification stages start by considering level $d = h - 1$ of the tree:
 - 1 Each witness at level $d+1$ states whether their parent at level d is their neighbour or not (the child *approves* the parent). If the answer is yes, and the child has not yet been named in the tree, this witness becomes a confirmed level d witness. The total number of confirmed level d witnesses is denoted as $D_d \leq n_d$, and the total number of witnesses that confirm a parent b is denoted by $K_b \leq w_l$.
 - 2 If a witness has already been named before, this witness is removed, regardless of whether they confirm their parent or not.
 - 3 If $K_b < tw_d$, $t \in (0, 1]$, parent b is pruned from the tree. Here, t is a parameter of T-PoP, called the *threshold*, which is used to regulate the security and reliability properties of the algorithm.
 - 4 If $D_d < tn_d$ then the algorithm interrupts and outputs that root g is lying about their position. Otherwise, we move on to level $d - 1$ and we repeat this process. Note that any parent removed by the previous step will not be included in this next iteration of T-PoP.

T-PoP is therefore an algorithm depending on a set of parameters, $\theta \equiv \{t, h, w_1, \dots, w_h\}$. The influence of these parameters on the performance of the algorithm will be explored in Section IX.

Example: Consider the T-PoP example in Figures 3 and 4, in which $\theta = \{t = 0.5, d = 2, w_1 = 2, w_2 = 2\}$, and so $n_1 = 2$ and $n_2 = 4$ (3). Solid arrows mean that a witness approves their parent and dotted lines mean that a witness does not approve their parent. Agents a_5 and a_6 are dishonest agents,

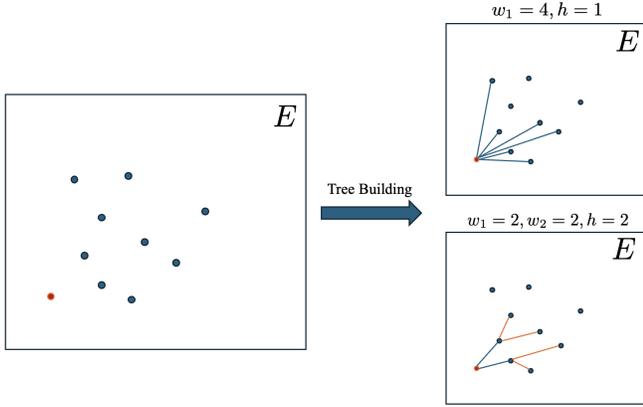


Fig. 2: Tree building examples. Agent a commits their alleged position. The panel on the top right shows the construction of a tree for $h = 1$ and $w_1 = 4$, while the panel on the bottom right shows the construction of a tree for $h = 2, w_1 = 2, w_2 = 2$.

so that their committed positions, \hat{p}_5 and \hat{p}_6 , are different from their true positions. However, agent a_2 does not know this, it saw those cars next to it and it picked a_5 and a_6 as witnesses. So, a_5 and a_6 do not confirm that a_2 is a neighbour of theirs, whereas a_3 and a_4 confirm that a_1 is a neighbour of theirs. In line with point 3 of *Checks and Verification* (above), agent a_1 has enough confirmed witnesses ($K_{a_1} = 2 \geq t \times w_2 = 0.5 \times 2$) and stays in the tree, while agent a_2 does not have enough confirmed witnesses ($K_{a_2} = 0 < 0.5 \times 2$), and so a_2 is removed from the tree. However, since the total number of confirmed witnesses at level 2 is $D_2 = 2 \geq t \times n_2 = 0.5 \times 4$, T-PoP does not stop for g , and we move to level 1. At level 1, a_2 has been removed but a_1 confirms that g is its neighbour. As per points 2 and 3 of *Checks and Verification*, the final output of T-PoP is that g is *truthful* about their position. As can be seen in the example above, t is critical in determining the output of T-PoP. For instance, if $t = 1$, then $M_2 = 2 < t \times n_2 = 1 \times 4 = 4$, causing T-PoP to stop at point 4 of *Checks and Verification*, and returning an output of *untruthful* for g .

T-PoP's practical implementations will vary depending on the application. It may be used in by vehicles to prove their position within a city, or it could be implemented in a smartphone, operated by individuals wishing to prove their location. It is also worth noting that T-PoP is not a highly resource intensive algorithm to execute, and thus the hardware constraints are not a critical concern. It is comprised of two algorithms: **Verification** and **Checks**. These are further defined in 3 and 2 accordingly. **Verification** is a (reverse) breadth-first-search algorithm, meaning its runtime in the worst case scenario is $O(|V| + |E|)$, where V is the number of nodes and E the number of edges in the tree data structure [22]. The **Verification** algorithm calls the **Checks** algorithm at each node, and the **Checks** algorithm has a time complexity of $O(|V|)$. So T-PoP's time complexity is $O(|V|^2 + |E|)$.

Of significant importance are the identity management solution, the commitment scheme selected, the communication security protocol and the notarising of the position proofs.

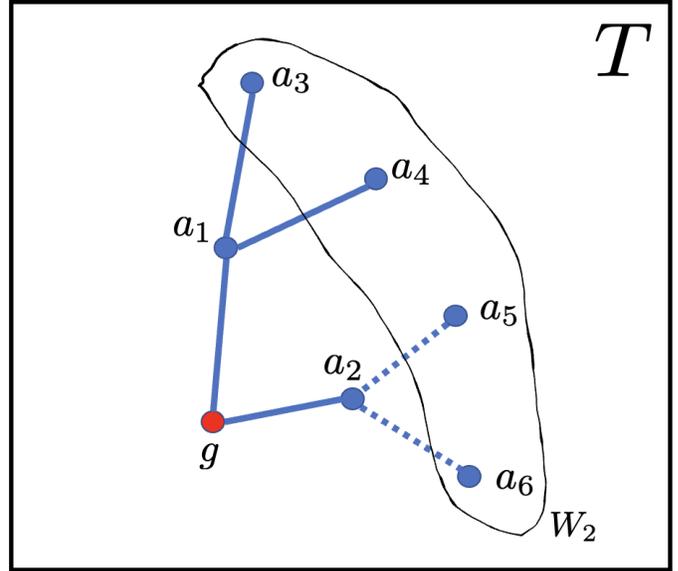


Fig. 3: We start by evaluating the outer level of the tree and we evaluate the witnesses in W_2 (the circled set). Agents a_5 and a_6 do not confirm that they see agent a_2 , even though a_2 is an honest agent. This leads to agent a_2 being eliminated from the tree.

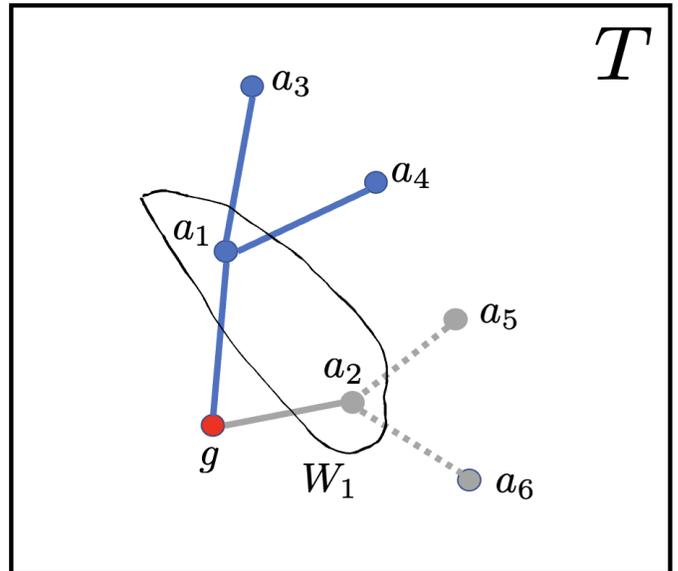


Fig. 4: We go down one level, and now evaluate the witnesses in W_1 (the circled set). a_2 has been eliminated by the tree (shown in grey) and so only agent a_1 is left.

Subsequently, we proceed with providing some possible options, but we note that the final decision must be made considering the context specific needs: conflict-zones will have different security and privacy needs to smart cities.

Identity management is trivial using a centralised solution. T-PoP is a decentralised, peer to peer algorithm, so should a centralised trust assumption not be desirable, we suggest other alternatives: Proof of Humanity (PoH) is a decentralised project ‘to provide a social identity verification system for humans on Ethereum’ [23]. Users cannot submit duplicate identities, fake or deceased identities may be challenged and removed and identities are verified by other verified and registered users. The drawback of this mechanism is that the identity is (naturally) public. For reporting purposes this is not an issue: paired with a commitment scheme, the reporter’s position remains hidden, but the proof of humanity shows the reporter (prover) is a real and verified individual. PoH is built on the Ethereum blockchain, thus incurring transaction costs to the user wishing to obtain a proof of humanity, however, this is a one time cost, as users will not obtain more than one proof of humanity.

Regarding securing communication between agents in T-PoP, we advise using established protocols such as TLS 1.3. The protocol used should guarantee the following properties are met:

- 1) Confidentiality: Information is kept secret from all but authorized parties.
- 2) Integrity: Messages have not been modified in transit.
- 3) Message Authentication: The sender of the message is authentic.
- 4) Non-repudiation: The sender of the message cannot deny the creation of the message. [11]

Finally, upon gaining a proof-of-position, this may be easily notarised in a DLT or IPFS, along with the prover’s position commitment and prover’s tree, such that all other agents may verify that with the same inputs, they obtain the same T-PoP result. This must be accompanied with the prover and the witnesses’ unique signature to prevent forgery.

VI. TPOP PROTOCOL

In this section we provide an overview of T-PoP from an algorithmic perspective and we introduce some notation that is used in the remainder of the paper.

Accordingly, there are three main algorithms that T-PoP calls:

- *Tree Building*: the process of building the tree of witnesses.
- *Checks*: the process of verifying that the tree that has been built satisfies certain criteria, listed below.
- *Verification*: the process of assessing the tree and deciding whether or not to confirm the prover’s position.

A. Tree Building

A *prover’s* aim is to amass sufficient *approvals* to support their position claim. Indeed, the prover provides a tree data structure that summarises their received approvals and the

dependencies between them. The number of nodes and edges present in the tree are evaluated to determine the likelihood of the prover’s claim being true. We proceed by outlining the algorithm the prover follows when constructing the tree structure of approvals.

Terminology: Each node in the tree represents an agent. The root of the tree is the prover. In a pair of nodes connected by a directed edge, the node where the edge originates is the *parent*, and the node where the edge terminates is the *child*. Each edge represents an *approval*. Namely, an edge from parent a_i to child a_j encodes a_j ’s approval of a_i . The tree must be of a specific dimension. Precisely, the variables are:

- **height**: the size of the longest path from the root to the leaves of the tree, h .
- **branching factor**: the number of children, w_d , that a parent must have at a given depth level, d . For brevity, if the branching factor is constant across levels, we omit the index and simply denote it as w .

Algorithm 1 Tree Construction

Require: Prover a_i , Height h , Branching Factor w_1, \dots, w_d

- 1: Initialise a_i as the root of the tree g and as a parent of depth level 1
- 2: **for** $d = 1, \dots, h - 1$ **do**
- 3: **for** each parent a_i at depth level d **do**
- 4: a_i names w_{d+1} children among its neighbours
- 5: All the named children are added as nodes of G at depth level $d + 1$, with a_j as their parent node.
- 6: **end for**
- 7: **end for**
- 8: **return** G

B. Checks Algorithm

This algorithm is called within the **Verification** algorithm, and its purpose is to assess, for each parent’s sub-tree, whether it satisfies certain criteria. If so, the parent node is considered honest and therefore remains in the prover’s tree. Otherwise, it and its branch are pruned from the prover’s tree. The criteria being checked for each sub-tree defined in algorithm 2, and are the following:

- 1) each child *approves* their parent (Line 1),
- 2) the parent has named sufficient children (Line 2),
- 3) no child has been already named in the tree by another parent (Line 3),
- 4) no parent names the same child twice (Line 4).

Indeed, criterion 3 and 4 can be summarised by ensuring each agent in the tree is unique. The threshold parameter, t , is a percentage that determines the minimum number of children that a parent must have. A parent remains in the tree iff $|parent's\ children| \geq w_d \cdot t$.

C. Verification

Starting at the lowest depth level, for each parent in that level, **Verification** calls the **Checks** algorithm for all of its children. If successful, the parent and its branch remains in

Algorithm 2 Checks

Require: Child a_j , Parent a_i , Named Agents A , Branching Factor w_d , threshold t

- 1: **if** a_j approves a_i
- 2: **and** $\#[a_i$'s children] $\geq w_d \cdot t$
- 3: **and** a_i not in A
- 4: **and** $\#set([a_i$'s children]) = $\#[a_i$'s children] **then**
- 5: **Add** a_j to A
- 6: **return** True
- 7: **else**
- 8: **return** False
- 9: **end if**

the tree, otherwise, it is pruned. It then moves up a level, and performs the same operations, only considering the non-pruned nodes. The algorithm terminates at the root of the tree, where it evaluates if the tree has sufficient nodes after pruning. If so, the *prover* is considered honest, otherwise it is considered dishonest. Using the prover's tree and the **Checks** function, **Verification** calls **Checks** in a reverse breadth-first-search manner. The algorithm returns True if the *prover* meets the required criteria and False otherwise.

Algorithm 3 Verification

Require: Tree G , threshold t , Height h , Branching Factor w_1, \dots, w_d , threshold t

- 1: Initialise Named Agents to $A = []$
- 2: Initialise G 's nodes to *not pruned*
- 3: Initialise Depth Level Approvals to D_1, \dots, D_{d-1}
- 4: **for** $d = 1, \dots, h - 1$ **do**
- 5: Depth Level Approval: $D_d = 0$
- 6: **for** each parent in at depth level d **do**
- 7: *Parent Approvals* = 0
- 8: **for** each parent's child **do**
- 9: **if** child is *not pruned* **then**
- 10: **if** **Checks**(child, parent, A , w_d , t) is True
- 11: *Parent Approvals* + = 1
- 12: **end if**
- 13: **end if**
- 14: **end for**
- 15: **if** *Parent Approvals* < $w_d \cdot t$ **then**
- 16: parent is *pruned*
- 17: **else**
- 18: D_d + = 1
- 19: **end if**
- 20: **end for**
- 21: **if** $D_d < w_d \cdot t$ **then**
- 22: **return** False
- 23: **else**
- 24: **return** True
- 25: **end if**
- 26: **end for**

VII. MATHEMATICAL MODELLING OF T-POP

We proceed with mathematically characterising the functioning of T-PoP. This mathematical model can be used to select the most suitable operating conditions of T-PoP, $\theta = (h, w, t)$, provided the designers select a desired performance level they wish to achieve in their application.

As discussed in Section VI, the heart of T-PoP is the **Checks** algorithm, which is recursively called in the **Verification** algorithm. The **Checks** algorithm assesses whether the criteria necessary to confirm an agent's position claim are satisfied. These criteria are the following:

- 1) each child *approves* their parent,
- 2) each parent has named sufficient children,
- 3) all agents are unique in the tree

We hypothesize that it suffices to compute the probability that each of the criterion above are met to determine the probability that an agent will receive a valid proof-of-position. We proceed by computing the individual probabilities of each criterion and finally we combine them into one model. Consequently, the probability that an agent a_i with state s_u will receive a proof-of-position through T-PoP with operating conditions θ , is equal to the product of the probability of each criterion above being satisfied:

$$P(\text{TPoP}(a) = \text{True} | s_u, \theta) = \prod_{j=1}^3 P(\text{Criteria } j = \text{True} | s_u, \theta)$$

Finally, in order to analyse T-PoP's performance, we consider two metrics: Security and Reliability.

- **True Negatives or Security**, TN , is a conditional probability quantifying the ability of the algorithm to detect malicious agents. Specifically, it is the true-negative conditional probability, which, under stationarity assumptions, is independent of $i \in \{1, \dots, |A|\}$:

$$TN \equiv \Pr[\text{TPoP}(a) = \text{False} | a \in \overline{H}]$$

- **True Positives or Reliability**, TP , is a conditional probability quantifying the ability for the algorithm to detect honest agents. Specifically, it is the true-positive conditional probability. Once again, under stationarity assumptions:

$$TP \equiv \Pr[\text{TPoP}(a) = \text{True} | a \in H]$$

In what follows, we derive a mathematical expression for $P(\text{Criteria } j = \text{True} | s_u, \theta)$, $j \in \{1, 2, 3\}$, and subsequently demonstrate that our model faithfully represents T-PoP's behaviour. We do so by conducting extensive agent-based simulations, and find that the results obtained are in complete agreement with those of the mathematical model we provide.

The rationale behind our analysis is to understand the performance of the algorithm when multiple agents collude together to try and, either fake their own position (dishonest agents) or attest that they see another agent in their fake position (coherced agents). We first begin by formalising the agent states mathematically. This allows us to construct a probability model to determine the likelihood that a prover will obtain sufficient approvals in their tree.

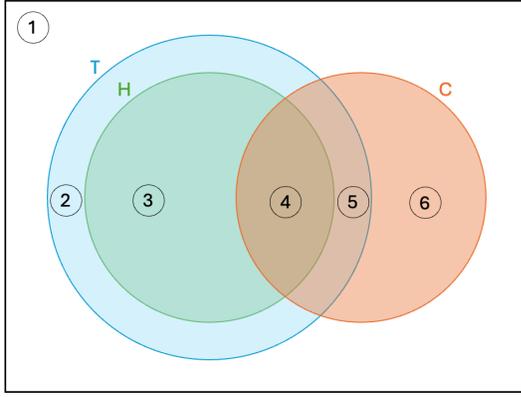


Fig. 5: Venn Diagram Representing Possible Agent State Combinations

A. Agent States

All agents have three attributes: honesty, α , coercion, β and a claimed position, γ . These attributes are binary, taking either a **True** or **False** value. We say an agent a_i has an honesty attribute α_i , coercion attribute β_i and claimed position γ_i , where $a_i \in A$, recalling that A is the set of all agents.

- *Honesty*: An agent a_i is either *honest*, $\alpha_i = h$ or *dishonest*, $\alpha_i = \bar{h}$. An *honest* agent claims to be in their *real* position, whereas a *dishonest* agent claims to be in a position that is different to their *real* position. We call the set of *honest* agents $H = \{a_i \in A : \hat{p}_i = p_i\}$ and the set of *dishonest* agents $\bar{H} = \{a_i \in A : \hat{p}_i \neq p_i\}$.
- *Coercion*: An agent a_i is either *coerced*, $\gamma_i = c$ or *non-coerced*, $\gamma_i = \bar{c}$. When approving other agents, a *coerced* agent will approve other agents in their *claimed* position (regardless of whether this *claimed* position is equal to their *real* position or not). A *non-coerced* agent will only approve agents in their *real* position. We call the set of *coerced* agents $C = \{a_i \in A : \beta_i = c\}$ and the set of *non-coerced* agents $\bar{C} = \{a_i \in A : \beta_i = \bar{c}\}$.
- *Position*: An agent a_i claim to be in a position. If the agent is *honest*, their *claimed* position is equal to their *real* position p . As such, we say, $\gamma_i = t$. If the agent is *dishonest*, their *claimed* position \hat{p} is different to their *real* position, p , and therefore, $\gamma_i = \bar{t}$. We call the set of agents that claim to be in their *real* position $T = \{a_i \in A : \gamma_i = t\}$ and the set of agents that claim to be elsewhere $\bar{T} = \{a_i \in A : \gamma_i = \bar{t}\}$.

We denote all three attributes of an agent a_i as follows:

$$\alpha_i \in \{h, \bar{h}\} \quad (4a)$$

$$\beta_i \in \{c, \bar{c}\} \quad (4b)$$

$$\gamma_i \in \{t, \bar{t}\} \quad (4c)$$

We depict the agents having each attribute (honesty, coercion and position) as a set in Figure 5. Each numbered region in Figure 5, u , where $u \in \{1, 2, 3, 4, 5, 6\}$ corresponds to a

possible set of attribute combinations, S_u , that an agent may possess. For example, if $a_i \in S_2$ then a_i belongs to the set of all agents that are dishonest, \bar{H} , the set of all agents that are not coerced, \bar{C} , and the set of all agents that claim to be in their true position, T . For ease of exposition, we define the *state* of an agent a_i , $x(a_i)$, to be the set of attributes an agent has:

$$x(a_i) = \{\alpha_i, \beta_i, \gamma_i\} \quad (5)$$

where $x(a_i)$ may be any of the following permutations:

$$s_1 = \{\bar{h}, \bar{c}, \bar{t}\} \quad (6a)$$

$$s_2 = \{\bar{h}, \bar{c}, t\} \quad (6b)$$

$$s_3 = \{h, \bar{c}, t\} \quad (6c)$$

$$s_4 = \{h, c, t\} \quad (6d)$$

$$s_5 = \{\bar{h}, c, \bar{t}\} \quad (6e)$$

$$s_6 = \{\bar{h}, c, t\} \quad (6f)$$

In short, we say that an agent a_i has a state $x(a_i)$, and that it belongs to the set of agents S_u , ($a_i \in S_u$), where $i \in |A|$, $u \in \{1, 2, 3, 4, 5, 6\}$ and

$$S_1 = \{\bar{H} \cap \bar{C} \cap \bar{T}\} \quad (7a)$$

$$S_2 = \{\bar{H} \cap \bar{C} \cap T\} \quad (7b)$$

$$S_3 = \{H \cap \bar{C} \cap T\} \quad (7c)$$

$$S_4 = \{H \cap C \cap T\} \quad (7d)$$

$$S_5 = \{\bar{H} \cap C \cap \bar{T}\} \quad (7e)$$

$$S_6 = \{\bar{H} \cap C \cap T\} \quad (7f)$$

$$P(a_i \in S_u) = P(x(a_i) = s_u) \quad (8a)$$

$$P(x(a_i) = s_u) = P(\alpha_i)P(\beta_i)P(\gamma_i|\alpha_i) \quad (8b)$$

Formally, we assume that variables α and β are binary random variables, independent of each other. These attributes represent the probability of an agent being honest and coerced respectively. We can therefore define the probability of an agent being honest (i.e.: $P(\alpha_i = h)$) as p_h , and being coerced (i.e.: $P(\beta_i = c)$) as p_c , where $p_h, p_c \in [0, 1]$. Similarly, $1 - p_h$ and $1 - p_c$ are the probabilities of an agent being dishonest and non-coerced respectively. Formally

$$p_h = P(x(a_i) = s_u, \forall u \in \{3, 4\}) \quad (9a)$$

$$p_c = P(x(a_i) = s_u, \forall u \in \{4, 5, 6\}) \quad (9b)$$

where $p_h, p_c \in [0, 1]$.

$$p_h = P(\alpha_i = h) \quad (10a)$$

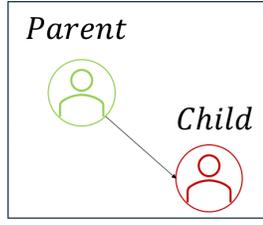
$$p_c = P(\beta_i = c) \quad (10b)$$

$$1 - p_h = P(\alpha_i = \bar{h}) \quad (10c)$$

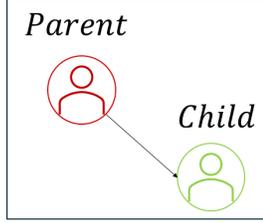
$$1 - p_c = P(\beta_i = \bar{c}) \quad (10d)$$

Next, we wish to compute the following probabilities: $P(\alpha_i = h)$, $P(\beta_i = c)$ and $P(\gamma_i = t)$ where:

$$P(\alpha_i = h) = 1 - P(\alpha_i = \bar{h})$$



(a) Dishonest parent



(b) Dishonest child

Fig. 6: Possible scenarios in which a dishonest agent may appear in a prover tree.

$$P(\beta_i = c) = 1 - P(\beta_i = \bar{c})$$

$$P(\gamma_i = t) = 1 - P(\gamma_i = \bar{t})$$

This is not the case with γ . Attributes γ and α are not independent. Indeed, by definition:

$$P(\gamma_i = t | \alpha_i = h) = 1 \quad (11a)$$

$$P(\gamma_i = \bar{t} | \alpha_i = h) = 0 \quad (11b)$$

. In practical terms: an honest agent will always claim to be in their real position. If $P(\alpha_i = \bar{h})$, finding $P(\gamma_i = t)$ is slightly more convoluted. This is because when a dishonest agent is sampled in a tree, one cannot, in theory, distinguish if its claimed position is its real position or not. Indeed, that is the purpose of T-PoP: to determine whether an agent is claiming to be in their real position.

Remark: When a dishonest agent is named in a tree, it could be that the dishonest agent is being observed in their real position, or that it has somehow tricked other nearby agents into pretending it is in their vicinity, when in fact it is elsewhere (by sending a fake signal or through any other possible attack vector). Because of this, we consider dishonest agents to effectively exist in two places: their real position, and their claimed position, which is fake.

To determine $P(\gamma_i = t)$, we must therefore consider the two possible cases in which a dishonest agent may appear in a tree: as a parent or as a child. This is depicted in Figure 6.

Let us begin with the first case, shown in Figure 6a. If the dishonest agent a_i , is the parent in the tree:

$$P(\gamma_i = t | \alpha_i = \bar{h}) = 0 \quad (12a)$$

$$P(\gamma_i = \bar{t} | \alpha_i = \bar{h}) = 1 \quad (12b)$$

This is because the dishonest agent would never construct a tree for their real position: doing so would expose their lie.

In the second case, as depicted in Figure 6b, if the dishonest agent is a child in the tree, then $P(\gamma_i = t) = 1$ if their parent

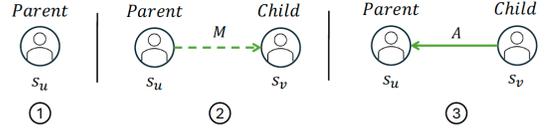


Fig. 7: Process of Parent to Child Approval

is *non-coerced*, and $P(\gamma_i = t) = 0$ if their parent is *coerced*. Formally, for a dishonest child a_i , with a parent a_j :

$$P(\gamma_i = t | \alpha_i = \bar{h}, \beta_j = c) = 0 \quad (13a)$$

$$P(\gamma_i = \bar{t} | \alpha_i = \bar{h}, \beta_j = c) = 1 \quad (13b)$$

$$P(\gamma_i = t | \alpha_i = \bar{h}, \beta_j = \bar{c}) = 1 \quad (13c)$$

$$P(\gamma_i = \bar{t} | \alpha_i = \bar{h}, \beta_j = \bar{c}) = 0 \quad (13d)$$

Remark: Recall that a *coerced* agent is one that covers up for other agents that lie about their position. This means that if they happen to name a dishonest agent as their child, they will name the dishonest agent in their fake position. The reader may consider the state of coercion as an agent being bribed, attacked or threatened to co-operate with another agent that is lying about their own position.

B. Condition 1: does a child approve their parent

Let us proceed by formalising the most crucial criterion: whether a child will approve the parent that named them. There are three stages in the process of an approval, as depicted in Figure 7.

1) *Initial Parent State:* First, consider the probability of the parent being in state s_u in equation 8. The vector in equation 14 summarises the probability of the parent being in any of the initial states.

$$I_1 = [P(s_1), P(s_2), P(s_3), P(s_4), P(s_5), P(s_6)]^T \quad (14)$$

where $P(s_u)$ is short for $P(\text{parent} \in S_u)$ with $\sum_{k=1}^6 P(s_k) = 1$.

2) *Picking a child, given a parent:* In the next step, we determine the probability of picking a child in a given state, provided the parent is in another state. Let us denote the child as agent \mathbf{c} and the parent as agent \mathbf{p} . We then summarise the probability that a parent \mathbf{p} in a state s_u will select a child \mathbf{c} in state s_v in Table I.

Note: Certain parent to child combinations are not possible by definition. This is shown by the entries of the Table I that are 0. For example, a *non-coerced* parent will never name a *dishonest* child in their *claimed* (fake) position. This is because *non-coerced* agents do not ‘see’ agents in a their fake positions.

We summarise the information in Table I as a matrix:

$$M = \begin{bmatrix} m_{1,1} & m_{1,2} & m_{1,3} & m_{1,4} & m_{1,5} & m_{1,6} \\ m_{2,1} & m_{2,2} & m_{2,3} & m_{2,4} & m_{2,5} & m_{2,6} \\ m_{3,1} & m_{3,2} & m_{3,3} & m_{3,4} & m_{3,5} & m_{3,6} \\ m_{4,1} & m_{4,2} & m_{4,3} & m_{4,4} & m_{4,5} & m_{4,6} \\ m_{5,1} & m_{5,2} & m_{5,3} & m_{5,4} & m_{5,5} & m_{5,6} \\ m_{6,1} & m_{6,2} & m_{6,3} & m_{6,4} & m_{6,5} & m_{6,6} \end{bmatrix} \quad (15)$$

Parent \ Child	$\bar{H} \cap \bar{C} \cap \bar{T}$	$\bar{H} \cap \bar{C} \cap T$	$H \cap \bar{C} \cap T$	$H \cap C \cap T$	$\bar{H} \cap C \cap \bar{T}$	$\bar{H} \cap C \cap T$
$\bar{H} \cap \bar{C} \cap \bar{T}$	0	$m_{1,2}$	$m_{1,3}$	$m_{1,4}$	0	$m_{1,5}$
$\bar{H} \cap \bar{C} \cap T$	0	0	0	0	0	0
$H \cap \bar{C} \cap T$	0	$m_{3,2}$	$m_{3,3}$	$m_{3,4}$	0	$m_{3,6}$
$H \cap C \cap T$	$m_{4,1}$	0	$m_{4,3}$	$m_{4,4}$	$m_{4,5}$	0
$\bar{H} \cap C \cap \bar{T}$	$m_{5,1}$	0	$m_{5,3}$	$m_{5,4}$	$m_{5,5}$	0
$\bar{H} \cap C \cap T$	0	0	0	0	0	0

TABLE I: Parent to Child Witness Selections

where the entry $m_{u,v}$ is defined as:

$$m_{u,v} = P[x(\mathbf{c}) = s_j | (x(\mathbf{p}) = s_i)] \quad (16)$$

and

$$x(\mathbf{c}) = s_j = \{\alpha_{\mathbf{c}}, \beta_{\mathbf{c}}, \gamma_{\mathbf{c}}\}$$

$$x(\mathbf{p}) = s_i = \{\alpha_{\mathbf{p}}, \beta_{\mathbf{p}}, \gamma_{\mathbf{p}}\}$$

To compute $m_{i,j}$ it suffices to evaluate:

$$m_{u,v} = P(\alpha_{\mathbf{c}})P(\beta_{\mathbf{c}})P(\gamma_{\mathbf{c}}) \quad (17)$$

$P(\alpha_{\mathbf{c}})$ and $P(\beta_{\mathbf{c}})$ are known through equations 10a and 10b respectively. To evaluate $P(\gamma_{\mathbf{c}})$ we begin with the prover agent, which has no parents by definition. In this case, $P(\gamma_{\mathbf{p}}) = P(\gamma_{\mathbf{p}} | \alpha_{\mathbf{p}})$, and we simply refer to equations 12 or 11 and pick the correct case. We then consider that parent's child agent, and to compute $P(\gamma_{\mathbf{c}})$, we evaluate

$$P(\gamma_{\mathbf{c}}) = P(\gamma_{\mathbf{c}} | \alpha_{\mathbf{c}})P(\beta_{\mathbf{p}})$$

using equations 13 or 11 accordingly. If the tree architecture has more than one depth level, the child agent then becomes the parent, and the process is repeated for its children until the leaves of the tree are reached.

It can be observed that $P(\gamma_{\mathbf{c}})$ is therefore a binary coefficient in Equation 17. We evaluate this coefficient for every possible parent to child state combinations in equations 18.

$$P[\text{child} \in \bar{H} \cap T | \text{parent} \in H \cap C \cap T] = 0 \quad (18a)$$

$$P[\text{child} \in \bar{H} \cap \bar{T} | \text{parent} \in H \cap C \cap T] = 1 \quad (18b)$$

$$P[\text{child} \in \bar{H} \cap T | \text{parent} \in H \cap \bar{C} \cap T] = 1 \quad (18c)$$

$$P[\text{child} \in \bar{H} \cap \bar{T} | \text{parent} \in H \cap \bar{C} \cap T] = 0 \quad (18d)$$

$$P[\text{child} \in \bar{H} \cap T | (\text{parent} \in \bar{H} \cap C \cap T)] = 0 \quad (18e)$$

$$P[\text{child} \in \bar{H} \cap \bar{T} | \text{parent} \in \bar{H} \cap C \cap T] = 1 \quad (18f)$$

$$P[\text{child} \in \bar{H} \cap T | \text{parent} \in \bar{H} \cap C \cap \bar{T}] = 0 \quad (18g)$$

$$P[\text{child} \in \bar{H} \cap \bar{T} | \text{parent} \in \bar{H} \cap C \cap \bar{T}] = 1 \quad (18h)$$

$$P[\text{child} \in \bar{H} \cap T | \text{parent} \in \bar{H} \cap \bar{C} \cap T] = 0 \quad (18i)$$

$$P[\text{child} \in \bar{H} \cap \bar{T} | \text{parent} \in \bar{H} \cap \bar{C} \cap T] = 0 \quad (18j)$$

$$P[\text{child} \in \bar{H} \cap T | \text{parent} \in \bar{H} \cap \bar{C} \cap \bar{T}] = 1 \quad (18k)$$

$$P[\text{child} \in \bar{H} \cap \bar{T} | \text{parent} \in \bar{H} \cap \bar{C} \cap \bar{T}] = 0 \quad (18l)$$

Remark: We adopt a different notation in equations 18 to aid with readability. For example, equation 18a is equivalent to expressing said probability as:

$$P[\gamma_{\mathbf{c}} = t, \alpha_{\mathbf{c}} = \bar{h} | \beta_{\mathbf{p}} = c] = 0$$

. Note that only the coercion attribute of the parent affects the result of equations 18. We include all three attributes to ease exposition, to show all possible state combinations.

3) *Child to parent approval:* The final stage shown in Figure 7 is whether the child will approve the parent. This approval is also entirely dependent on the state of both the parent and the child, and is summarised in Table II. This table can be expressed as a matrix:

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (19)$$

Thus, all components necessary to characterise whether a parent will receive an approval from their child have been mathematically formalised. We define $\mathcal{P}_{u,d}$ as the probability that a prover \mathbf{p} , with state $x(\mathbf{p}) = s_u$ will receive an approval from a witness at depth level d of the witness tree. It is easy to verify that $\mathcal{P}_{u,d}$ can be expressed as follows:

$$\mathcal{P}_{u,d} = e_u^T (M \odot A)^d \mathbf{1} \quad (20)$$

where e_u is the u -th element of the canonical base of \mathbb{R}^6 and \odot represents the element-wise matrix multiplication (Hadamard product) and $\mathbf{1} = [1, 1, 1, 1, 1, 1]^T$. Then, the probability that a prover \mathbf{p} , with state $x(\mathbf{p}) = s_u$ will have enough approvals is equivalent to the probability that, for each level d of the tree, $D_d \geq t \cdot n_d$, where D_d is the number of depth level approvals at a given depth level d . The number of approval D_d can be modeled as a Binomial distribution with parameter $\mathcal{P}_{u,d}$. Therefore, we can formalize the probability of satisfying criterion 1 as

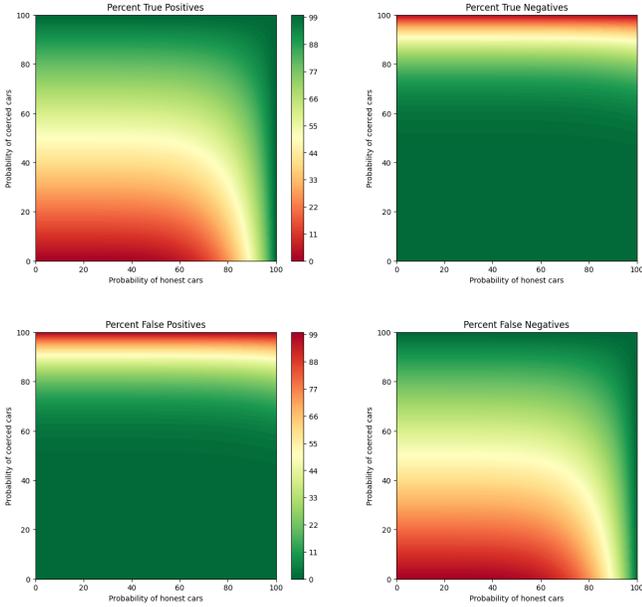
$$P(\text{Criteria 1} = \text{True} | s_u, \theta) = P(D_d \geq t \cdot n_d, \forall d \in \{1, \dots, h\})$$

Which in turn can be expressed as:

$$\prod_{d=1}^h \sum_{k=\lceil tn_d \rceil}^{n_d} \binom{n_d}{k} \mathcal{P}_{u,d}^k (1 - \mathcal{P}_{u,d})^{n_d - k}. \quad (21)$$

Child \ Parent	Parent					
	$\bar{H} \cap \bar{C} \cap \bar{T}$	$\bar{H} \cap \bar{C} \cap T$	$H \cap \bar{C} \cap T$	$H \cap C \cap T$	$\bar{H} \cap C \cap \bar{T}$	$\bar{H} \cap C \cap T$
$\bar{H} \cap \bar{C} \cap \bar{T}$	0	0	0	1	0	0
$\bar{H} \cap \bar{C} \cap T$	0	0	0	0	0	0
$H \cap \bar{C} \cap T$	0	0	1	1	0	0
$H \cap C \cap T$	1	0	1	1	1	0
$\bar{H} \cap C \cap \bar{T}$	0	0	0	1	1	0
$\bar{H} \cap C \cap T$	0	0	0	0	0	0

TABLE II: Approvals of a child to a parent.

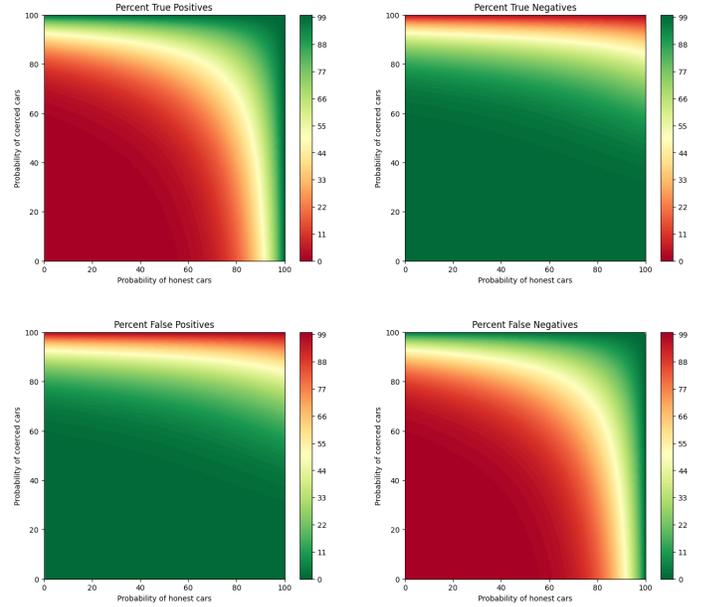

 Fig. 8: Theoretical performance of TPoP with $\theta = \{t = 1, h = 1, w_1 = 6\}$.

Equation 21 allows us to quickly simulate the behaviour of T-PoP for different values of θ (under the assumption of an infinite density of agents). As an example, consider Figures 8 and 9 which show, for values of p_h and p_c ranging in the interval $[0, 1]$, the performance of the T-PoP for two set of parameters, respectively: $\theta = \{t = 1, h = 1, w_1 = 6\}$ and $\theta = \{t = 1, h = 2, w_1 = 2, w_2 = 2\}$. Later, in Section IX we show that the theoretical behavior matches perfectly the behaviour of a detailed agent-based simulator of TPoP.

Furthermore, we can define the probability that a child will confirm that they see the parent that selected them (i.e., that an edge exists between a parent and child). This probability can be expressed as follows:

$$I_{d+1} = I_d(M \odot A) \quad (22)$$

where I_d is the probability vector of a parent being in any given state, at depth level d of the tree. Using the initial starting state in equation 14, we can then compute the expected number of edges, $\mathbb{E}(e)$, in a tree of any given height, h , and branching


 Fig. 9: Theoretical performance of TPoP with $\theta = \{t = 1, h = 2, w_1 = 2, w_2 = 2\}$.

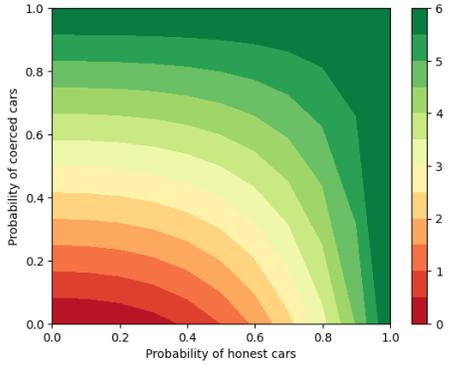
factor, w_d :

$$\vec{v} = \sum_{d=1}^h d \cdot n_d (I_{d-1} (M \odot A)^d) \quad (23)$$

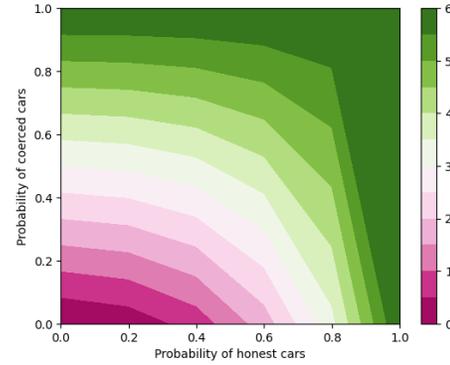
$$\mathbb{E}(e) = \mathbf{1}^T \vec{v} \quad (24)$$

Using equations 21 and 23, we can compute the expected number of edges in a prover's tree as the values of p_h and p_c range from 0 to 1. Figure 10 shows the results of equation 24.

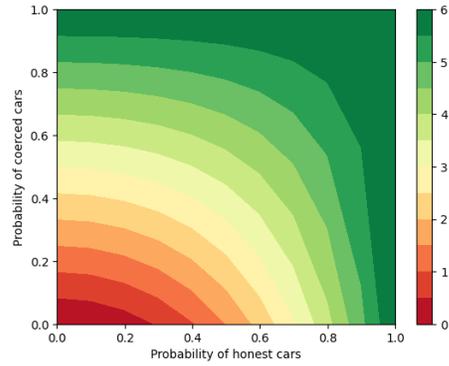
We then conduct 423,500 Monte-Carlo agent-based simulations, shown in Figure 11, that count the number of edges in each agent's tree after running T-PoP. In them, we create a uniform grid of 5 by 5 square units, and a total of 3500 agents, meaning the density is 140 agents per unit square. Each agent is set to have a range of sight equivalent to the size of the unit square, meaning there are 140 agents within their range of sight. If the density of agents is not sufficiently high, an agent will not have enough edges in their tree because it does not have sufficient agents in its vicinity to name as children. We therefore purposefully select a high value of agents, to ensure that the probability of a tree not having sufficient edges is not due to a lack of nearby agents being available, but rather



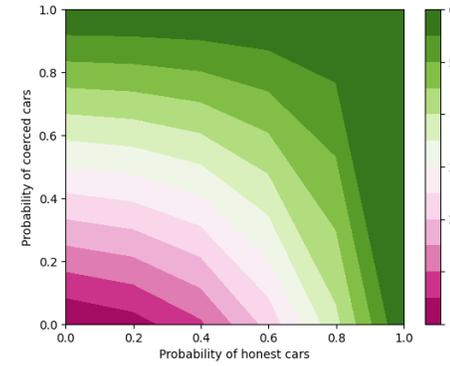
(a) Tree of height 2 and branching factor 2, with threshold = 100%.



(a) Tree of height 2 and branching factor 2, with threshold = 100%.



(b) Tree of height 1 and branching factor 6, with threshold = 100%.



(b) Tree of height 1 and branching factor 6, with threshold = 100%.

Fig. 10: Expected number of edges in the tree.

Fig. 11: Number of edges in agent's trees after running T-PoP.

because the agents do not approve each other. This is precisely what we are modelling in equation 24. These simulations are conducted with a threshold 100%. The results obtained are in complete agreement with the mathematical model presented, thereby demonstrating its validity.

C. Condition 2: The tree has sufficient nodes

The second condition is modeled by considering the following assumptions:

- We assume a constant average density of agents μ ;
- We assume that agents are scattered uniformly across the environment.

Accordingly, let N_a be the amount of neighbours of agent a . This random variable can be approximated by a Poisson Point Process [24] of parameter $\lambda = \mu \cdot \pi r^2$, where r is the range of sight of the agent. It follows then that the probability that there are at least n_d neighbours around agent a can be immediately computed as

$$P(N_a > n_d) = 1 - P(N_a \leq n_d) = 1 - \sum_{k=0}^{n_d-1} e^{-\lambda} \frac{\lambda^k}{k!} \quad (25)$$

D. Condition 3: all the nodes in the tree are unique

In this subsection we analyze the probability of constructing a tree with distinct nodes given a certain density of agents.

Specifically we focus on the two structures that are presented in Section IX:

- A tree with height $h = 1$ and branching factor $w = 6$.
- A tree with height $h = 2$ and branching factor $w = 2$.

We denote this probability as $P(h, w)$. In the remainder of this section we make the assumption that each agent selects witnesses among its neighbours without replacement. Although it may be an unrealistic assumption (as in practice each prover would select distinct witnesses and they would not deliberately try to hinder their own proof), it allows us to provide a lower bound on the probability of selecting a tree made of unique nodes.

Let us now assume that a population of N agents are distributed uniformly at random on a plane of size $l \times l$, with every agent's range of sight set to constant r . We can view agents as nodes in a graph, where there exists a link between two nodes if and only if the distance between corresponding agents is less than or equal to r . This graph structure is called a Random Geometric Graph and it has a known mean node-degree $\langle k \rangle \simeq \pi N r^2 / l^2$ [25]. The mean node-degree $\langle k \rangle$ of the graph is equivalent to the expected number of neighbours in the population of agents.

For our calculations we make use of a function $\kappa_{n,y}$ defined

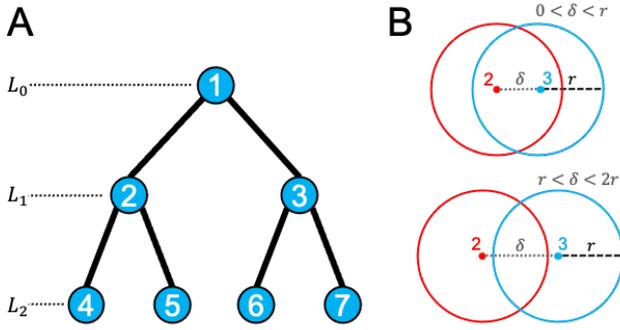


Fig. 12: A) A tree of height $h = 2$ and branching factor $w = 2$, with agents and levels labeled. B) Two separated scenarios visualized, when agents a_2 and a_3 selected at random in the field of view of a_1 are $\delta < r$ nearby (top) versus $\delta > r$ far apart (bottom).

as:

$$\kappa_{n,y} = \frac{\binom{\langle k \rangle - n}{y}}{\langle k \rangle^y / y}, \quad (26)$$

representing the probability of picking $n + y$ unique agents from a set of $\langle k \rangle$ neighbours, given that n options are picked beforehand (eliminated) and y new agents are to be picked.

For the case of $h = 1$ and $w = 6$, $P(h, w)$ is straightforward to compute and it is equal to $P(1, 6) = \kappa_{0,6}$.

For the tree of $h = 2$ and $w = 2$, finding the probability that all nodes are unique is more complex. Let us consider a tree started by a *prover* a_1 at the root, tree height of $h = 2$, and branching factor of $w = 2$, i.e., each parent choosing two of its neighbours at random (with replacement) as its children (i.e., the nodes at level 1 will not choose themselves).

Let a_2 and a_3 (at depth level 1 in the tree) be the children of a_1 (which is at level 0) in the tree, selected at random within a_1 's field view; $a_2, a_3 \in \overline{D}_1$. Agents a_4, \dots, a_7 are the leaves of the tree (forming level 2); see Fig. 12A. We denote the probability of 7 distinct agents forming the three levels of the tree (L_0, L_1, L_2) as $P(L_0, L_1, L_2)$, which can be written as:

$$P(L_0, L_1, L_2) = P(L_0)P(L_1|L_0)P(L_2|L_0, L_1), \quad (27)$$

with $P(L_0) = 1$, $P(L_1|L_0)$ denoting the probability that $a_1 \neq a_2 \neq a_3$, and $P(L_2|L_0, L_1)$ being the probability that a_1, \dots, a_7 are different agents given that a_1, a_2, a_3 are distinct.

The probability of having $a_1 \neq a_2 \neq a_3$ can be calculated in a straightforward manner, since a_1 has an expected number of $\langle k \rangle$ neighbours with none of them eliminated as options. Thus, using Eq. (26), we get the probability of picking two different agents at random from a set of size $\langle k \rangle$, i.e., $P(L_1|L_0) = \kappa_{0,2}$. Now, with a_2 and a_3 picked at random within the field of view of a_1 , which is a disk of radius r , we use the probability density function for the distance between the two agents $\delta = \|p_2 - p_3\|_2$. This is simply the probability density function for the distance between two random points in a disk:

$$f(\delta) = \frac{4\delta}{\pi r^2} \cos^{-1}\left(\frac{\delta}{2r}\right) - \frac{2\delta^2}{\pi r^3} \sqrt{1 - \frac{\delta^2}{4r^2}}. \quad (28)$$

If $\delta < r$ then a_1 is a neighbour of a_2 and vice versa, thus for each agent, one neighbour out of the expected number of neighbours is eliminated (in order to have distinct agents in the tree). See Fig. 12B (top panel). Also, for all possible values of δ , i.e., $0 < \delta < 2r$, the probability of selecting a common neighbour by either a_1 or a_2 equals the fraction of their field of view that is overlapping. This can be calculated by \mathcal{A}_δ , a function of δ , defined as below:

$$\mathcal{A}_\delta = \left[2r^2 \cos^{-1}\left(\frac{\delta}{2r}\right) - \frac{\delta}{2} \sqrt{4r^2 - \delta^2} \right] / \pi r^2, \quad (29)$$

where the numerator of the RHS is the overlapping area of two circles with radius r with centers δ far apart, and the denominator is the area of the circle with radius r .

Without loss of generality, assume that a_2 picks two random neighbours a_4 and a_5 as its children (starting with $a_1 \neq a_2 \neq a_3$). The Prover agent a_1 is certainly a neighbor of a_2 , and if $\delta < r$ ($\delta > r$) then a_3 is (is not) a neighbor of a_2 , and a_1, \dots, a_5 are distinct with probability κ_2 (κ_1). Also, with probability \mathcal{A}_δ , a_4 is in the intersection between the fields of view of a_2 and a_3 and thus reducing the number neighbours from which a_3 can pick (for its children to be distinct from the agents already appearing in the tree). With probability \mathcal{A}_δ^2 , both a_4 and a_5 are neighbours of a_3 and reducing a_3 's options by two, and with probability $\mathcal{A}_\delta(1 - \mathcal{A}_\delta)$, a_4 is a neighbour of a_3 and a_5 is not. Using the above logic we can approximate the probability of having 7 distinct agents in the tree, given that $a_1 \neq a_2 \neq a_3$, i.e.:

$$\begin{aligned} P(L_2|L_0, L_1) = & \int_0^r f(\delta) \kappa_{2,2} \\ & \cdot [(1 - \mathcal{A}_\delta)^2 \kappa_{2,2} + 2(1 - \mathcal{A}_\delta) \mathcal{A}_\delta \kappa_{3,2} + \mathcal{A}_\delta^2 \kappa_{4,2}] d\delta \\ & + \int_r^{2r} f(\delta) \kappa_{1,2} \\ & \cdot [(1 - \mathcal{A}_\delta)^2 \kappa_{1,2} + 2(1 - \mathcal{A}_\delta) \mathcal{A}_\delta \kappa_{2,2} + \mathcal{A}_\delta^2 \kappa_{3,2}] d\delta. \end{aligned} \quad (30)$$

Finally, inserting equation (30) into equation (27), we have the theoretical approximation for the probability of the tree ($h = w = 2$) being comprised of strictly distinct agents, i.e., $P(2, 2) = P(L_0, L_1, L_2) = \kappa_{0,2} \cdot P(L_2|L_0, L_1)$. This value of $P(L_0, L_1, L_2)$, given a constant range of sight r , is only dependent on the density of agents N/l^2 and can be calculated numerically.

The theoretical approximation of $P(L_0, L_1, L_2)$ can be validated via a numerical experiment. To do so, we uniformly scatter N agents on a unit 2-dimensional square, at random. A tree is then sampled, by randomly drawing a prover from the population, which then picks draws two agents at random (with replacement) within its field of view (here, r is set to 0.1). We vary N from 200 to 10,000, and for each N sample 10,000 trees at random and count those made up of 7 distinct agents. Figure 13, compares the fraction of sampled trees with all distinct agents (red curve) with the theoretical approximation given by equations (27)-(30). As demonstrated by the results, the approximation performs well, converging

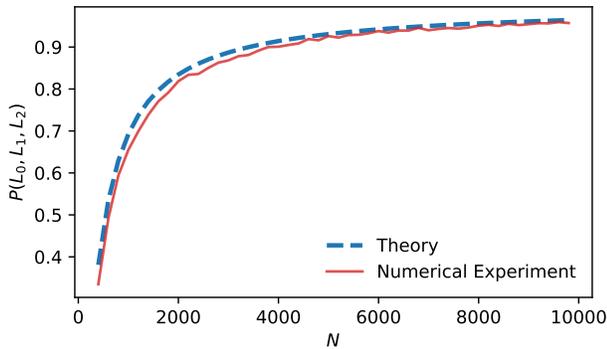


Fig. 13: Validation of theoretical approximation for probability of a randomly sampled tree ($h = w = 2$) containing 7 distinct agents. The results show the probability as a function of the number of agents N uniformly distributed at random over a unit square plane. The red curve shows the probability calculated through a numerical experiment, where a tree is generated following the tree-building algorithm 1, starting with a randomly selected prover. The dashed curve shows the value of the theoretical approximation denoted $P(L_0, L_1, L_2)$ calculated by equations (27)-(30).

fast to the numerical observation as the density of agents increases.

As a final remark we note that while it may be possible to obtain a recursive formula to compute the probability of finding distinct agents in a tree with depth h and branching factor w , this might prove very complicated and it is quite straightforward to approximate $P(h, w)$, for a given $\langle k \rangle$ and a given r , by making use of a large number of Monte-Carlo simulations.

VIII. DETECTING PLATOON ATTACKS

Given T-Pop's collaborative nature, it is susceptible to a platooning attack. In it, one *dishonest* agent coerces a subset of agents to *approve* their (fake) *claimed* position. This cluster of agents cruise together and because the *dishonest* agent has sufficient approvals, T-Pop will consistently fail in detecting that this claim is dishonest. To address this attack vector, we construct an alternative mathematical model that defines the behaviour of these agents. With this model, it is possible to determine the likelihood that a prover tree is formed by a group of malicious platooning agents. We follow the same steps outlined in VII.

A. Initial Agent State

Given that a platoon is always initiated by an *dishonest* agent in their *claimed* position, and not their *real* position, the probability of an agent being in a given state is:

$$\tilde{I}_1 = [P(s_1), P(s_4), P(s_5)] \quad (31a)$$

$$P(s_4) = 0 \quad (31b)$$

Remark: We include state s_4 in the set of possible agent states, since the agent is *coerced*, so it may be part of the set of

agents approving the platoon *prover*, however, it may never be the *prover*, since it is *honest*.

$$\tilde{M} = \begin{bmatrix} m_{1,1} & m_{1,4} & m_{1,5} \\ m_{4,1} & m_{4,1} & m_{4,5} \\ m_{5,1} & m_{5,4} & m_{5,5} \end{bmatrix} \quad (32)$$

where the entries of \tilde{M} are computed following equation 17, but we only consider parent to child combinations where the agents are in states $\{s_1, s_4, s_5\}$, so $u, v \in \{1, 4, 5\}$.

Similarly, to create the platoon approvals matrix, \tilde{A} , we sample the entries $a_{i,j}$, of A that correspond to the approvals of all the possible agent pair combinations in states $\{s_1, s_4, s_5\}$.

$$\tilde{A} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad (33)$$

With these components, we can proceed to compute the expected number of edges in a platoon tree by substituting \tilde{I}_d , \tilde{M} and \tilde{A} into the corresponding terms in equation 23 and 24.

We then show the model behaviour in Figures 14 and 15.

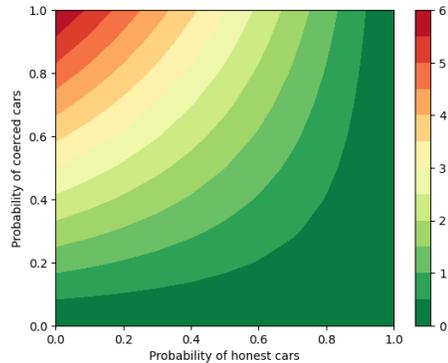


Fig. 14: Expected number of edges in a platoon tree of height 1 and branching factor 6, with threshold = 100%.

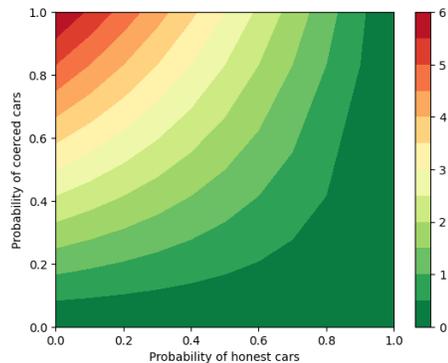


Fig. 15: Expected number of edges in a platoon tree of height 2 and branching factor 2, with threshold = 100%.

We highlight that to detect honest trees, it does not suffice with simply counting the number of edges. These edges must be connecting nodes that are honest, i.e., agents in states s_3 and s_4 . The challenge is that the state of a node is not known

$m_{i,j}$	Parent	Child	Optimal Point
$m_{3,3}$	s_3	s_3	$P(H) = 1, P(C) = 0$
$m_{3,4}$	s_3	s_4	$P(H) = 1, P(C) = 0.5$
$m_{4,3}$	s_4	s_3	$P(H) = 1, P(C) = 0.5$
$m_{4,4}$	s_4	s_4	$P(H) = 1, P(C) = 1$

or observable when a tree is assessed. However, we may find the optimal conditions such that the probability of an edge connection between agents in states s_3 and s_4 are maximised. The elements of the matrix M that encode child to parent approvals that are honest are entries $m_{3,3}, m_{3,4}, m_{4,3}, m_{4,4}$. The optimal values of p_h and p_c that maximise the probability of these edges existing is denoted in Table VIII-A.

IX. AGENT BASED SIMULATIONS

We simulate the performance of T-PoP in both high density and low density cases, under varying operating conditions. Our purpose is to determine the security and reliability guarantees that T-PoP provides in both scenarios.

We construct an agent-based simulator, coded in Python, which is available in our GitHub Repository. In it, we create an environment of a given size, and instantiate a fixed number of agents with a fixed value for their range of sight. Agents are assigned an honesty, α_i , and a coercion, β_i , attribute independently and at random, following equations 10a and 10b. All agents are given a real position, within the bounds of the defined environment, and dishonest agents also have a claimed position that is different to their real position. These positions are uniformly and randomly distributed across the environment. We first simulate a low-density scenario, as shown in Figures 17, 16, 19 and 18. We initialise an environment of size 10 by 10 arbitrary square units, and instantiate 350 agents, such that each has a range of sight of 1 unit. Thus, agents have an average of 3.5 agents within their field of view. Each agent constructs a tree, and then runs the T-PoP algorithms to obtain a proof-of-position. These simulations are carried out across the ranging values of p_h and p_c , starting from 0 to 100% in intervals of 10%. At each combination of p_h and p_c , 5 Monte Carlo simulations are run for every agent. In total, that is 211,750 T-PoP simulations⁴. We test the performance of T-PoP for the following operating conditions:

$$threshold = 100\%, w_d = 2, h = 2$$

$$threshold = 100\%, w_d = 6, h = 1$$

$$threshold = 40\%, w_d = 2, h = 2$$

$$threshold = 40\%, w_d = 6, h = 1$$

We measure the recall rate of true positives, true negatives, false positives and false negatives. Each classification instance is described below:

⁴There are 121 possible combinations of p_h and p_c when varying the values at intervals of 10%. 350 agents and 5 simulations per possible combination of p_h and p_c yields $5 * 121 * 350$.

- A true positive (TP) instance means TPoP correctly labelled an agent as honest.
- A true negative (TN) means TPoP correctly labelled an agent as dishonest.
- A false positive (FP) means TPoP incorrectly classified a dishonest agent as honest.
- A false negative (FN) means TPoP incorrectly classified an honest agent as dishonest.

$$TP\% = \frac{TP}{TP + FN} \times 100 \quad (34a)$$

$$FN\% = 100 - (TP\%) \quad (34b)$$

$$TN\% = \frac{TN}{TN + FP} \times 100 \quad (34c)$$

$$FP\% = 100 - (TN\%) \quad (34d)$$

We consider recall over precision, since we are particularly interested in the sensitivity of the algorithm. Namely, it is of utmost importance that the number of False Positives is low, as this is the most dangerous possible outcome.

We then consider a high-density scenario, as shown in Figures 21, 20, 23 and 22. We run these simulations with the density at which the probability of selecting all unique agents in the tree tends to 1. From Figure 13, this density is found to be 50 agents per unit squared, when each agent has a range of sight of 1 square unit. In these simulations we create a grid of 5 by 5 arbitrary square units, with 1250 agents in total, each with a range of sight of 1 square unit. We again run simulations for each possible combination of p_h and p_c values, at intervals of 10%. In each combination of p_h and p_c values, we run T-PoP for each of the 1250 agents and repeat this process 5 times. In total, the number of simulations is 756,250. We do so for the same operating conditions previously outlined.

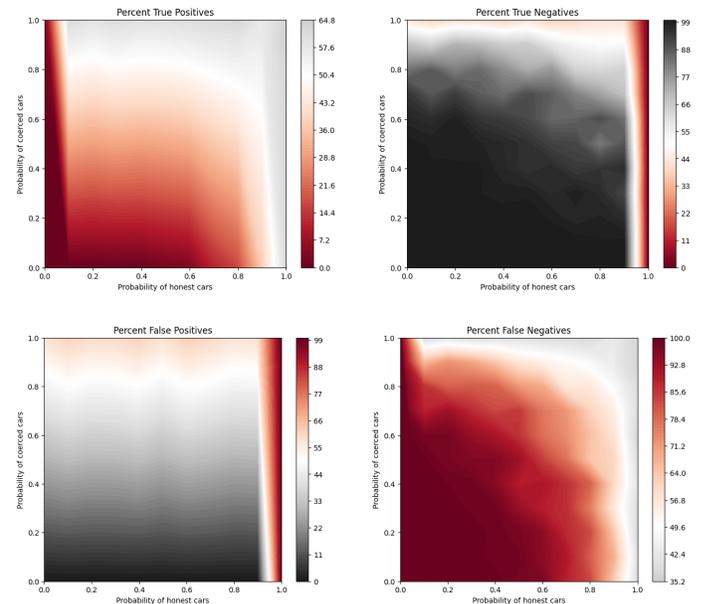


Fig. 16: Performance of TPoP with a tree of height 2 and branching factor 2, and a threshold = 100%.

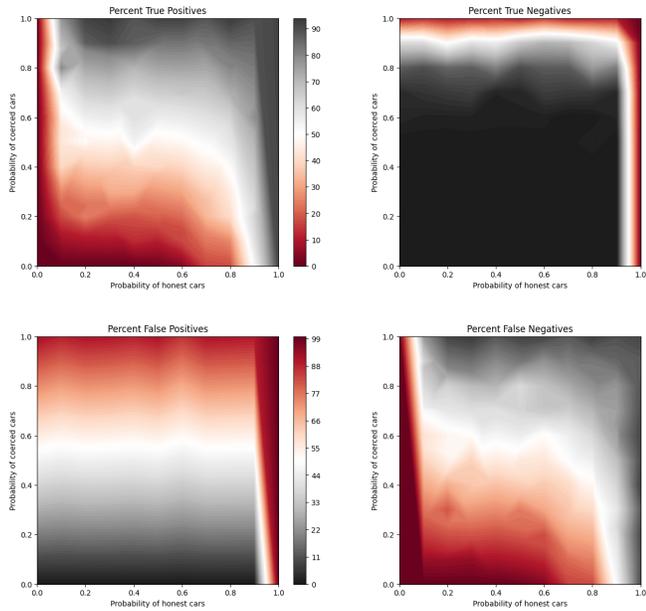


Fig. 17: Performance of T-PoP with a tree of height 1 and branching factor 6, and a threshold = 100%.

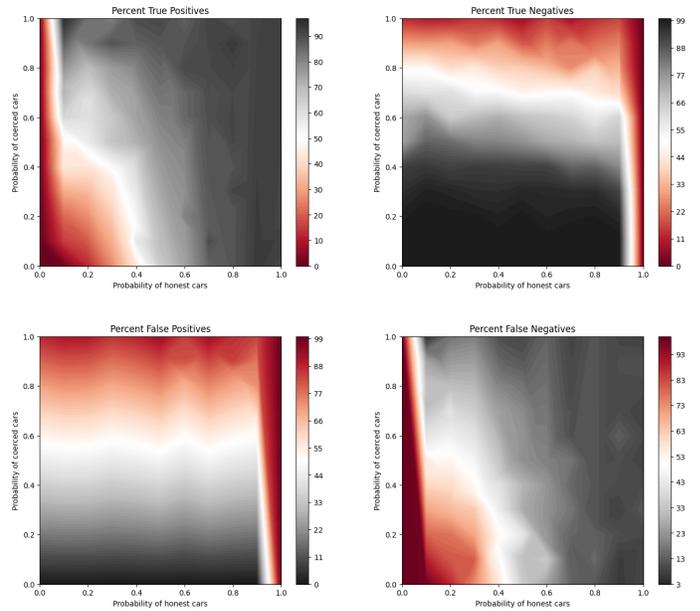


Fig. 19: Performance of T-PoP with a tree of height 1 and branching factor 6, and a threshold = 40%.

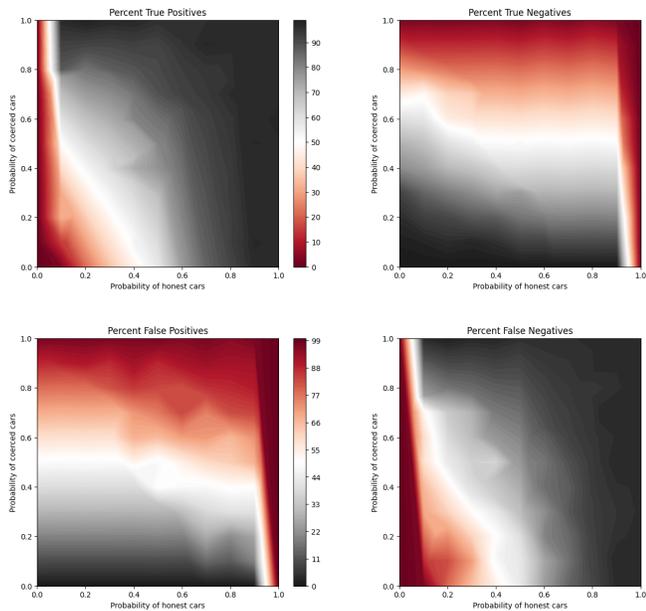


Fig. 18: Performance of T-PoP with a tree of height 2 and branching factor 2, and a threshold = 40%.

X. PERFORMANCE OF T-PoP

From the results obtained, it can be observed that the performance of T-PoP does not vary greatly when using a tree of $h = 1, w = 6$ versus $h = 2, w = 2$. The prior slightly outperforms the latter in both thresholds tested. This is consistent with the results shown in Figures 10. The main difference in performance is observed when varying the threshold parameter, and when varying the density. Increasing density increases the number of True Positives, given that honest agents will not be classified as dishonest for not having sufficient nodes in their tree. Decreasing the threshold improves the rate of True

Positives (Reliability) of T-PoP in very low density scenarios, but this comes at the expense of Security. A lower threshold makes it easier for dishonest agents to submit a valid tree. As such, users may tune the threshold parameters to obtain a desired level of Security or Reliability, depending on the expected density of their system.

XI. CONCLUSION

In summary, we provide an algorithm for agents to prove their position in a decentralised, collaborative and privacy preserving manner. Our algorithm is robust to powerful adversaries, and we make no assumption of honest behaviour in the system. We provide a simple mathematical model to aid users to select the most suitable operating conditions of T-PoP, provided the security and reliability guarantees they wish to achieve, and the expected agent density in their system. We validate the model through the use of extensive Monte-Carlo agent-based simulations, and find these are in complete agreement with our model. Our code base is open-source, and the results along with the mathematical model and the agent-based simulator can be found in our GitHub Repository. For future work, we consider implementing this protocol in useful applications.

REFERENCES

- [1] A. M. Kharman, P. Ferraro, A. Quinn, and R. Shorten, "Robust decentralised proof-of-position algorithms for smart city applications," in *2023 62nd IEEE Conference on Decision and Control (CDC)*, pp. 112–119, 2023.
- [2] M. Bonini, M. Zichichi, S. Ferretiv, and G. D'Angelo, "Proof of location through a blockchain agnostic smart contract language," in *2023 IEEE 43rd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 55–60, 2023.
- [3] M. R. Nosouhi, S. Yu, M. Grobler, Y. Xiang, and Z. Zhu, "SPARSE: privacy-aware and collusion resistant location proof generation and verification," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2018.

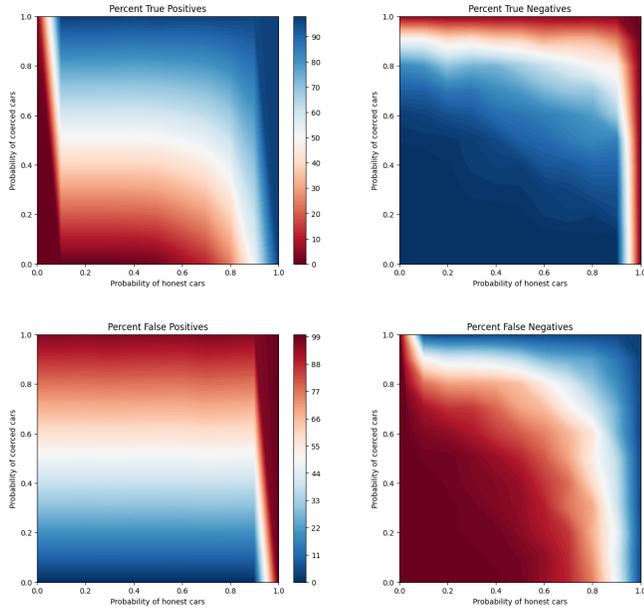


Fig. 20: Performance of TPOp with a tree of height 2 and branching factor 2, and a threshold = 100%.

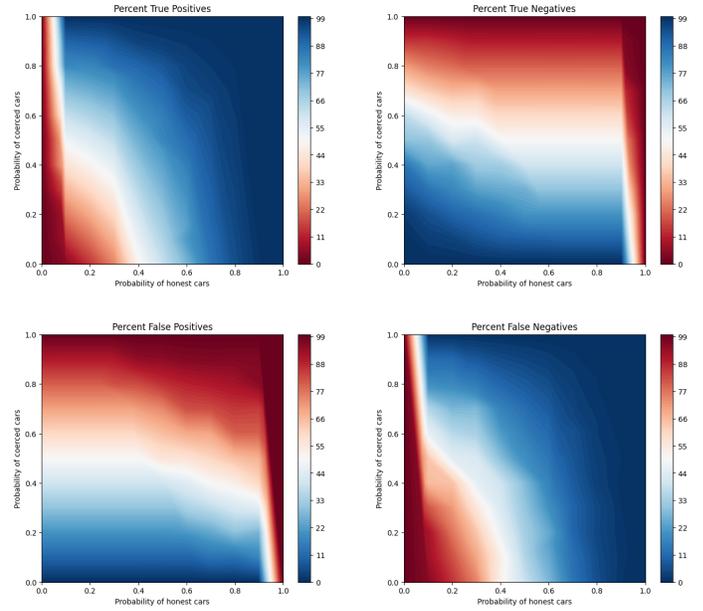


Fig. 22: Performance of TPOp with a tree of height 2 and branching factor 2, and a threshold = 40%.

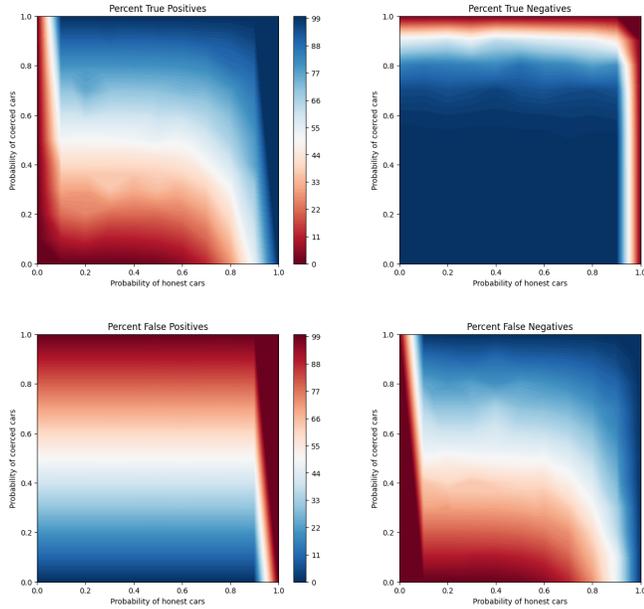


Fig. 21: Performance of TPOp with a tree of height 1 and branching factor 6, and a threshold = 100%.

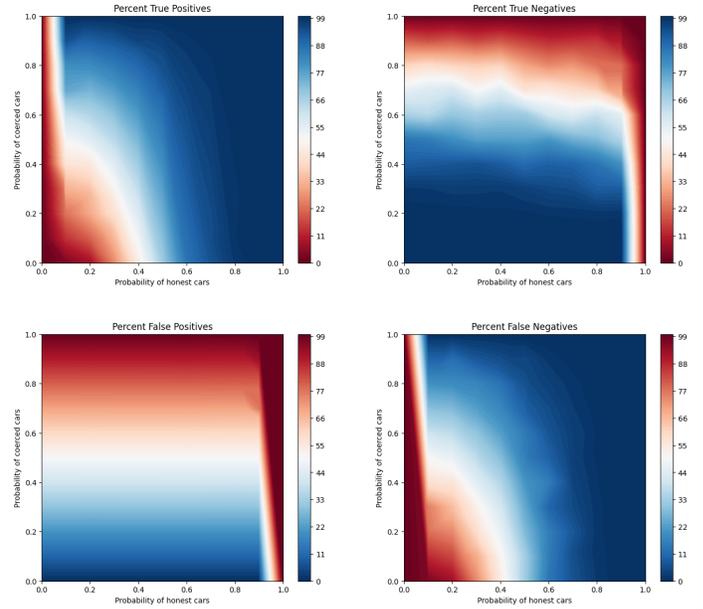


Fig. 23: Performance of TPOp with a tree of height 1 and branching factor 6, and a threshold = 40%.

[4] H. Alamlah and A. A. S. al-Qahtani, “A cheat-proof system to validate GPS location data,” in *2020 IEEE International Conference on Electro Information Technology (EIT)*, pp. 190–193, IEEE, 2020.

[5] C. Javali, G. Revadigar, K. B. Rasmussen, W. Hu, and S. Jha, “I am Alice, I was in wonderland: secure location proof generation and verification protocol,” in *2016 IEEE 41st conference on local computer networks (LCN)*, pp. 477–485, IEEE, 2016.

[6] W. Wu, E. Liu, X. Gong, and R. Wang, “Blockchain based zero-knowledge proof of location in IOT,” in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, IEEE, 2020.

[7] M. Amoretti, G. Brambilla, F. Medioli, and F. Zanichelli, “Blockchain-based proof of location,” in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 146–153, IEEE, 2018.

[8] Z. Zhu and G. Cao, “Toward privacy preserving and collusion resistance in a location proof updating system,” *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 51–64, 2011.

[9] Z. Zhu and G. Cao, “APPLAUS: A privacy-preserving location proof updating system for location-based services,” in *2011 Proceedings IEEE INFOCOM*, pp. 1889–1897, IEEE, 2011.

[10] Y. Zheng, M. Li, W. Lou, and Y. T. Hou, “SHARP: Private proximity test and secure handshake with cheat-proof location tags,” in *ESORICS*, pp. 361–378, Springer, 2012.

[11] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[12] F. Boeira, M. Asplund, and M. Barcellos, “Decentralized proof of location in vehicular ad hoc networks,” *Computer Communications*, vol. 147, pp. 98–110, 2019.

- [13] M. R. Nosouhi, S. Yu, W. Zhou, M. Grobler, and H. Keshtiar, "Blockchain for secure location verification," *Journal of Parallel and Distributed Computing*, vol. 136, pp. 40–51, 2020.
- [14] F. Victor and S. Zickau, "Geofences on the blockchain: Enabling decentralized location-based services," in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, pp. 97–104, IEEE, 2018.
- [15] A. Beikverdi and J. Song, "Trend of centralization in bitcoin's distributed network," in *2015 IEEE/ACIS 16th international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD)*, pp. 1–6, IEEE, 2015.
- [16] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The energy consumption of blockchain technology: Beyond myth," *Business & Information Systems Engineering*, vol. 62, no. 6, pp. 599–608, 2020.
- [17] I. Chillotti, M. Joye, D. Ligier, J.-B. Orfila, and S. Tap, "Concrete: Concrete operates on ciphertexts rapidly by extending tthe," in *WAHC 2020-8th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, 2020.
- [18] A. Kate, G. M. Zaverucha, and I. Goldberg, "Polynomial commitments," 2010.
- [19] I. Damgård, "Commitment schemes and zero-knowledge protocols," in *School organized by the European Educational Forum*, pp. 63–86, Springer, 1998.
- [20] T. K. Frederiksen, T. P. Jakobsen, J. B. Nielsen, and R. Trifiletti, "On the complexity of additively homomorphic uc commitments," in *Theory of Cryptography Conference*, pp. 542–565, Springer, 2015.
- [21] J. Benet, "Ipfes-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.
- [22] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2022.
- [23] S. James, "Proof of Humanity - An Explainer," 2021. <https://blog.kleros.io/proof-of-humanity-an-explainer/>, Last accessed on 2024-04-10.
- [24] R. L. Streit and R. L. Streit, *The poisson point process*. Springer, 2010.
- [25] M. Penrose, *Random geometric graphs*, vol. 5. OUP Oxford, 2003.