Research Proposal

Design and Development of Zero-Knowledge Protocol for Collaborative Missions in Robotics

Roshan Singh
https://kalikho.github.io

1 Introduction:

In swarm robotics and multi-robot systems, a robot needs to collaborate with other robots to achieve mission goals. Robots exchange mission-specific messages with each other, often as a form of broadcast or P2P. This exchange of messages raise several security concerns about the broader objectives of the mission. A malicious robot or a subset of robots that have access to some intercepted message can attempt to learn about the mission goals individually or by colluding together.

Zero Knowledge(ZK) based protocols can help enhance security and increase the confidentiality of the mission. Limited works in the literature exist in the domains of application of ZK protocols in robotics. In[2] authors introduced a Merkle-Tree-based authenticated data structure that enables robots in a swarm to cooperate and carry out sequential tasks without having explicit knowledge about the mission's high-level objectives. However, the work has certain limitations:-

1. Only allows for sequential execution of tasks.
2. Although the work use hashes to preserve the privacy of each step in the mission. It is not difficult for an average adversary to reconstruct the message from the hash. Given the fact that the robot knows the custom hash function $\boldsymbol{H}$=H(h_a,h_s), and the base hash function h(eg. SHA256, MD5) which is used to construct $\boldsymbol{H}$.

   Consider the foraging scenario, where the robots need to sequentially arrange objects. Say, the objects come in 4 colors $\{Red, Green, Blue, White\}$ and there exists only 2 valid moves $\{move-left, move-right\}$. With this information, even a low-resource adversary can easily decode a hash in the leaf of the Merkle tree by brute force. In this particular scenario, there exists only 8 valid moves i.e $\{(Red, move-left), (Red, move-right), (Green, move-left), ...\}$.

2 Proposal:

We improve the concept introduced in[2] by applying Non-Interactive Zero Knowledge(NIZK) schemes such as Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKS). A NIZK-based approach will avoid any sort of brute force attack that was earlier possible in the Merkle-Tree-based approach in[2], further being non-interactive the communication overhead between the Prover and the Verifier is $O(1)$ for proving execution of a task t. The main objectives of the research is as follows:-

1. Allow parallel execution of non- mutually exclusive tasks in the mission. This can be achieved by segregating non- mutually exclusive or independent tasks in ranges. Further, a robot can provide a zero-knowledge range proof that the task is independent of the tasks in some other group.
2. For complex missions such as arranging LEGO blocks to form a 3D structure of a monument, the task Merkle tree can be quite large with millions of unit tasks possible. The traditional hash-based verification approach will not be scalable as the verifier needs to scan the entire records until it finds the correct hash and starts verifying the hash at the upper level of the tree to the root hash. A Merkle tree inclusion/non-inclusion proof along with recursive proofs can help avoid the search overhead[1].
3. Provide zero-knowledge proof of physical task done in the real world environment. Each task in the mission can be considered as a milestone. A robot completing the task t can provide a zk-proof of the change in the mission state $S_{t-1} \rightarrow S_t$. The robots can capture the physical properties of the change happened in the environment before and after the execution of task t and can use the information to create the proof.

3 Timeline:

We plan to execute the research project in 6 months. The project duration can be divided into 3 phases and each phase has a duration of 2 months. In Phase-I we do a thorough survey of the state of the art of zero knowledge technologies available in academia and industry. In Phase II we develop our zero-knowledge solution for robotics. Phase-III will involve testing and evaluating the proposed solution in simulation and in real-life deployments.

References

[1] Rasmus Dahlberg, Tobias Pulls, and Roel Peeters. Efficient sparse merkle trees: Caching strategies and secure (non-) membership proofs. In *Secure IT Systems: 21st Nordic Conference, NordSec 2016, Oulu, Finland, November 2-4, 2016. Proceedings 21*, pages 199–215. Springer, 2016.

[2] Eduardo Castelló Ferrer, Thomas Hardjono, Alex Pentland, and Marco Dorigo. Secure and secret cooperation in robot swarms. *Science Robotics*, 6(56):eabf1538, 2021.