INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

Proof of Identity—a Blockchain Consensus Algorithm to Improve Byzantine Fault Tolerance in Swarm Robotics

A dissertation by

Mr. Theviyanthan Krishnamohan

Supervised by

Mr. Ragu Sivaraman

Submitted in partial fulfillment of the requirements for the MSc in Advanced Software Engineering degree at the University of Westminster.

August 2022

Abstract

Swarm robotics applies concepts of swarm intelligence to robotics. Discrete consensus achievement is one of the major behaviors found in swarm robotics. Various algorithms have been developed for discrete consensus achievement. However, existing discrete consensus-achievement algorithms, referred to henceforth as classical solutions, are vulnerable to Byzantine robots. Blockchain has been successfully used to mitigate the negative effect of Byzantine robots in discrete consensus achievement. Blockchain is the technology behind cryptocurrencies that allows the creation of immutable, decentralized, and distributed ledgers. Nevertheless, since the blockchain solution uses the Proof-of-Work blockchain consensus algorithm, it is vulnerable to the 51% attack. Besides, the swarm also takes longer to achieve consensus.

This research proposes a novel blockchain consensus algorithm called Proof-of-Identity—which uses a private-public key pair and a swarm controller—to create a dynamically permissioned blockchain that would negate the 51%-attack problem associated with the Proof-of-Work algorithm while also reducing the consensus time.

This proposed solution was tested against the classical solution and the existing blockchain solution using the collective perception scenario. The collective perception scenario is used to benchmark different discrete consensus achievement algorithms. Test results show that the Proof-of-Identity algorithm prevents the 51%-attack problem while improving the consensus time in comparison to the existing blockchain solution without affecting the exit probability.

Keywords—Swarm robotics, blockchain, Proof of Work, consensus algorithm, consensus achievement, collective perception scenario.