Distributed Coordination Based on Quantum Entanglement (Work in Progress)

Yotam Ashkenazi  
Dept. of Computer Science  
Ben-Gurion University of the Negev  
yotamash@cs.bgu.ac.il

Shlomi Dolev, IEEE Fellow  
Dept. of Computer Science  
Ben-Gurion University of the Negev  
dolev@cs.bgu.ac.il

Abstract—This paper demonstrates and proves that the coordination of actions in a distributed swarm can be enhanced by using quantum entanglement. In particular, we focus on

- Global and local simultaneous random walks, using entangled qubits that collapse into the same (or opposite) direction, either random direction or totally controlled simultaneous movements.
- Identifying eavesdropping from malicious eavesdroppers aimed at disturbing the simultaneous random walks by using entangled qubits that were sent at random or with predefined bases.

Index Terms—Mobile robots, Byzantine faults, Self-stabilization, Quantum entanglement

I. INTRODUCTION

This paper presents methods to achieve distributed coordination in a swarm of robots using quantum entanglement. We demonstrate a new benefit of quantum mechanics (using the entanglement capabilities) in the scope of distributed secure computing. Many applications use quantum entanglement to enhance the classical algorithm capabilities. In order to achieve coordination between the robots, we use similar methods used in quantum key distribution. This short version excludes many details. More details can be found in [1].

II. SIMULTANEOUS RANDOM WALKS

Definition 1 Simultaneous random walk. A path $P_r$ is defined as a sequence of positions of a robot $r$. $P_r = p_1, p_2, \ldots$, if for every $i \geq 1$, $p_{r_i+1}$ is reached from $p_r$, by a step of the robot $r$. A path of random steps defines a random walk. Each participant has a random path that is not affected by other participants. A simultaneous random walk occurs when every robot’s random walks are coordinated. For every $P_r$ and every $i \geq 1$, if $p_{r_i+1}$ is reached from $p_r$, by a step up, down, left, or right. All other $P_r' \neq P_r$ move up, down, left, or right at the same step $i$ respectively.

Coordinate a random walk problem. Develop an algorithm where the participants can coordinate a random walk. If robot $r_1$ moves up, meaning $P_1 = (i, j), (i, j+1)$, then robot $r_2$ will move up as well, meaning $P_2 = (k, l), (k, l+1)$. The idea is to share a random sequence between the participants, and then the participants can move in a coordinated random fashion.

A classic (no quantum) solution. There are several ways to share a random sequence. One of them, and the obvious one, is based on physical meetings, where every two participants can share a secret.

This scenario has significant drawbacks. A robot needs to predict upfront the robots that it will need to communicate with and establish a shared key in a pre-processing stage. Another drawback is the possibility of using the knowledge of the sequence and the risk of its leakage prior to the actual use of the sequence.

A standard method to receive a random share sequence is to use random noises from the environment. For example, in our solution, we can identify when a Byzantine or an attacker is eavesdropping and act accordingly.

The quantum solution. In the sequel, we propose and detail a new method to achieve distributed coordination between a swarm of robots. This can be based on one robot producing an entangled state and sending part of the state to another robot. Another option is based on a global entity (a satellite, for example) that sends entanglement photons to several robots. Our solution suggests several ways of using quantum capabilities in the case of two robots, to obtain a stream of an infinite number of random (qu)bits, while ensuring that no entity can clone or manipulate transmitted bits on their way.

- The first option is to use predetermined bases. Using this method, the robots (and the satellite, when used) decide on the predetermined bases for each measurement and measure them accordingly. This option has the same drawbacks as the classical physical meeting solution.
- The second method uses random bases, just as done in Quantum Key Distribution (QKD). Each robot chooses a random base for each measurement. The robots then send/broadcast their information on randomly chosen bases over another secure channel, where attackers can listen to the communication but cannot modify it.

When using the method of distributing entangled particles from a satellite, each robot receives a part of the entangled particle infinitely often. This can also be done by one participant sending entangled qubits to another robot, and both of them measure the states.

We consider two cases of random walks. In the first one, we would like to achieve a global coordinated random walk, where the robots are located very far from each other. In this scenario, the robots may not be able to sense a common random noise from the environment and can not observe the movements of
Fig. 1. When the distance between the robots is 1, the robots measure their particles from $|\Phi_1\rangle$ and $|\Phi_2\rangle$ and get $|11\rangle$, ... the left qubit from the second pair $|\Phi_2\rangle$, such that $\text{r}_1$ observes 00 and $\text{r}_2$ observes 01. $\text{r}_1$ moves up, and $\text{r}_2$ moves right.

In the second step, robots measure $|01\rangle$, and they both move right.

each other. Note that it is possible that the robots were close to each other in the past but later moved apart.

In the second scenario, we would like to achieve a local coordinated random walk to prevent a collision of two robots executing random walks $P_1$ and $P_2$. Consider the simple procedure in which a robot performs a simple random walk algorithm. The robot chooses its next move randomly with the same probability.

In one of the scenarios, we consider that there are two robots, $\text{r}_1$, and $\text{r}_2$, which are located very close to each other. There is a chance that $\text{r}_1$ randomly chooses to move toward $\text{r}_2$ and, at the same time, $\text{r}_2$ moves toward $\text{r}_1$, e.g., $\text{r}_1$ move right $P_1 = (i, j), (i+1, j)$ and $\text{r}_2$ moves down $P_2 = (i, j+1), (i+1, j)$ In this scenario, they may crash into each other.

We can address both cases by the use of entangled qubits. The robots measure the entanglement state and act simultaneously, even if they are (possibly) very far from each other.

The robots can move in four directions. Each robot needs two qubits to decide on the next move, meaning two entangled states $|\Phi_1\rangle$ and $|\Phi_2\rangle$ with a total of four qubits for each step.

The robots $\text{r}_1$ and $\text{r}_2$ measure the states, and each robot interpenetrates the measured values to a command to be executed, e.g., $|00\rangle$ up, $|11\rangle$ down, $|01\rangle$ right, and $|10\rangle$ left, where the $|xy\rangle$ represents the value measured. $\text{r}_1$ receives the first qubit of $|\Phi_1\rangle$ and the first qubit of $|\Phi_2\rangle$, and $\text{r}_2$ receives the second qubit of $|\Phi_1\rangle$ and the second qubit of $|\Phi_2\rangle$.

We can assume that the entangled qubits are Einstein–Podolsky–Rosen (EPR) pairs [2], so without loss of generality, the states are both $|\Phi^+\rangle$ and the robots measure on a normal basis. The robots measure their qubits and move accordingly to the result. Using this simple algorithm, assuming $\text{r}_1$ observes $|01\rangle$, $\text{r}_2$ observes the same result with a high probability and the robots move left. In case the distance between the robots is below the threshold or they want to coordinate their random walk, they can execute the algorithm above, see Fig. 1. Therefore, they continue to move together in a random fashion and do not collide.

When using this algorithm, the robots move together forever. The rest of the paper is organized as follows. In Section III, we demonstrate how the centralized entity can control the robots’ movements using quantum entanglement. Additionally, we consider the case where the robots can move together in a random fashion. However, a Byzantine robot or an attacker can eavesdrop on the states and predict the robots’ movements. Section V presents a method for preventing the eavesdropping attack.

Previously, we used pairs of EPR entangled particles in the case of two robots. In the case of three or more robots, we can expand the $|\Phi\rangle$ state to consist of more than two qubits. e.g. for three robots, $\text{r}_1$, $\text{r}_2$, and $\text{r}_3$, we can use the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, and the robots need two states to create the mapping between the results and the directions.

III. CONTROLLING THE ROBOT’S MOVEMENTS

The previous sections considered the case in which robots move together and execute simultaneous random walks. This section presents how a centralized entity can control the robots’ movements.

The robot swarm control problem. In some cases, we would like a centralized entity (a satellite, for example) to control the robots’ movements in a deterministic fashion. Say one wants to direct a swarm of drones in a specific direction.

A classic (no quantum) solution. Controlling the robots’ movements can be achieved using the same classical algorithm as in the previous section. Instead of sending a random sequence, the satellite can send specific bits which map the exact path of the robots.

The quantum solution. Controlling the robots’ movements can be achieved using the same simultaneous random walks quantum algorithm. However, instead of sending a random EPR state, the satellite can send an entangled state in the form of $|00\rangle$ or $|11\rangle$. In this case, using the same conditions as above, the centralized entity can decide on the complete path of the robots.

IV. AVOID ROBOTS COLLIDING IN A RANDOM FASHION

The collision avoidance problem. The previous section considered the case to avoid collision in a deterministic way. In this section, the robots avoid colliding and still move in a random fashion.

A classic (no quantum) solution. It is not trivial to solve the problem using a classical algorithm. The centralized entity can use one of the methods to share random sequence as demonstrated in Section II. However, if the centralized entity sends the same sequence to the robots, the robots keep moving together forever. One solution for the problem is when the centralized entity sends a different sequence to each of the robots.

The quantum solution. The centralized entity creates a random state with fewer options, so the robots continue to move in a random fashion without the probability of colliding. This can be done by sending two different EPR states where the robots move in a random direction but not toward each other. For example, if two robots are located at a distance one from each other, then the centralized entity can send the first pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ as the second pair.

In this case, the options for robot $\text{r}_1$ and robot $\text{r}_2$ are:

- $\text{r}_1$ and $\text{r}_2$ measure the left qubit from the first pair $|\Phi_1\rangle$ and the left qubit from the second pair $|\Phi_2\rangle$, such that $\text{r}_1$ observes 00 and $\text{r}_2$ observes 01. $\text{r}_1$ moves up, and $\text{r}_2$ moves right.
• $r_1$ and $r_2$ measure the left qubit from the first pair $|\Phi_1\rangle$ and the right qubit from the second pair $|\Phi_2\rangle$, such that $r_1$ observes 01 and $r_2$ observes 00. $r_1$ moves right, and $r_2$ moves up.
• $r_1$ and $r_2$ measure the right qubit from the first pair $|\Phi_1\rangle$ and the left qubit from the second pair $|\Phi_2\rangle$, such that $r_1$ observes 10 and $r_2$ observes 11. $r_1$ moves left, and $r_2$ moves down.
• $r_1$ and $r_2$ measure the right qubit from the first pair $|\Phi_1\rangle$ and the right qubit from the second pair $|\Phi_2\rangle$, such that $r_1$ observes 11 and $r_2$ observes 10. $r_1$ moves down, and $r_2$ moves left.

In the cases above, the distance between the robots can increase or remain identical with a positive probability.

V. EAVESDROPPING PREVENTION

The eavesdropping prevention problem. In the previous sections, we presented a method of distributed coordination. An eavesdropper can easily attack this method by measuring the random sequence before/together with the robots. If we have four identities; the centralized entity $c$ sending the random sequence, $r_1$ and $r_2$ receiving the sequence, and an attacker $eve$ trying to gain information about the random sequence or about the next robot’s movements.

A classic (no quantum) solution. In case the entities share a secret or have a Public Key Infrastructure (PKI), the obvious and most straightforward method to avoid eavesdropping is to use encryption. Consider the case where all of the information is encrypted and $eve$ does not have the secret, no eavesdropping can be done.

The quantum solution. We extend the quantum algorithm to be resilient to eavesdropping attacks by sending the quantum states in one of several bases. We obtain very high security using our solutions, the same as the secure method for quantum key distribution, e.g., [4].

The first and easy option is to use predefined bases. This solution has the same drawbacks as the physically meeting solution.

Another case is to use randomized bases. $c$ chooses a random base, $z$ basis or $x$ basis and creates the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ or $\frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$ respectively. For each received qubit, each robot $r_1$ and $r_2$ choose a random basis, $z$ basis or $x$ basis and measures the qubit state using the selected basis. After several measurements, $c$, $r_1$, and $r_2$ publish their selected bases in an authenticated secure channel. A valid measurement is when $c$, $r_1$, and $r_2$ choose the same basis for each measurement. If the basis is selected in a random fashion, the probability of the same basis is $\frac{1}{4}$.

In the case of $eve$ being active, we would like to prevent $eve$ from eavesdropping on the states. Without loss of generality, for all the valid measurements, consider the case where $eve$ measures the state before $r_1$ (or $r_2$) and returns the state after the measurement to $r_1$. If $eve$ measures the state with the same basis as $r_1$, $eve$ and $r_1$ (and $c$, and $r_2$) measure an identical value. If $eve$ measures the state with another basis and then sends the state to $r_1$, $r_1$ might measure a different result from $r_2$. In order to identify $eve$, $r_1$ and $r_2$ can publish several valid measurement results. If the measurement results are not identical (more than an error rate), $c$, $r_1$, and $r_2$ can assume $eve$ eavesdropped on several states, and the measurements are invalid. Using this method, honest participants can identify if an eavesdropping attack was executed with a high probability.

VI. CONCLUSIONS AND FUTURE WORK

We demonstrated the usage and benefits of using quantum entanglement to achieve simultaneous random walks between robots. In addition, we presented several methods to identify Byzantine robots. We propose to use entanglement to cope with possible eavesdropping and disturbing behaviors of the Byzantine robots. When the number of robots grows, the use of the global identical random base solution yields many useless measurements. The probability that all the robots will measure the same base decreases exponentially with the number of robots, i.e., the probability that all $c$, $r_1$, ..., $r_n$ choose the same basis from the two options, $z$ basis or $x$ basis, is $(\frac{1}{2})^n$. Thus, this method is doomed to yield many non useful measurements. This problem can be solved by sharing the bases before the measurements, using the same authenticated secure channels among the robots. However, we assumed the attacker can listen to the communication, so the attacker can measure the agreed upon bases and gain access to the secret sequence. We are currently working on the details and proofs for a solution of simultaneous random walks for multi robots. This solution can be extended to a QKD for multi participants. The idea, in a high level is that for every $i \geq 1$, $r_i$ and $r_{i+1}$ share sequence $s_i$ using the same process presented in this paper. For every $i \geq 2$, every $r_i$ update (using authenticated channels), the next participant $r_{i+1}$, which bits of the share sequence need to be flipped to get the same sequence as $r_{i-1}$ and $r_i$. So that eventually all use the key of $r_1$, while $eve$ does not reveal information about the global key. Note that a scheme in which $r_1$ randomly selects a sequence and sends the sequence/key to all other robots, may be vulnerable to eavesdropping as the channels are only authenticated (as encryption is based on the key exchange).

VII. ACKNOWLEDGMENT

This research was supported in part by the Helmsley Charitable Trust through the Agricultural, Biological and Cognitive Robotics Initiative, the Marcus Endowment Fund both at Ben-Gurion University of the Negev, and the Rita Altura Trust Chair in Computer Science.

REFERENCES

[1] Y. Ashkenazi and S. Dolev. Distributed coordination based on quantum entanglement. arXiv, 2210.10551, 2022.
[2] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.
[3] D. M. Greenberger, M. A. Horne, and A. Zeilinger. Going Beyond Bell’s Theorem, pages 69–72. Springer Netherlands, Dordrecht, 1989.
[4] J. et al. Yin. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, 582(7813):501–505, 2020.