Privacy-Preserving Average Consensus in Multiagent Systems for Node Collusion

Yaqi Wang
Qufu Normal University
Engineering college
Rizhao, China
yqwang1118@qfnu.edu.cn

Jiabei Ye
Qufu Normal University
Engineering college
Rizhao, China
jiabeiye1207@163.com

Yue Lu
Qufu Normal University
Engineering college
Rizhao, China
1140037411@qq.com

I. Abstract

Average consensus problem of multiagent systems has always been an active topic, allowing multiple agents to interact with the average information of the initial values obtained locally. However, explicit sharing of state variables may lead to privacy disclosure. Many researchers have devoted to solving this problem and there have been several kinds of methods. In 1978, Rivest first proposed the concept of homomorphic encryption algorithms. Then, several proposals have emerged in academia to support partially homomorphic encryption, such as, RSA, the Elgamal Algorithm, and the Paillier Algorithm. Another method is adding noises or perturbation signals to the transmitted signals. The primary effect of this method is to obscure the initial values. Some researchers have added random noise and analyzed the privacy in this framework. In addition to the above two categories of approaches to achieving privacy preservation, there are some alternative approaches, such as state decomposition method and partial information transmission.

In this brief, we deal with the problem of privacy preserving average consensus and node collusion for multiagent systems. We propose a novel algorithm to achieve the privacy-preserving average consensus against node collusion. Each agent passes subinformation to other agents through state decomposition. We show that privacy can be guaranteed under our approach, even if there is more than one curious node and they collude with each other. Finally, an example is provided to illustrate the design process and practical applications of the proposed approach.

Through the above discussions and comparisons, the advantages of our method can be clearly observed. Now, we summarize the main contributions of this article as follows.

1) We propose a novel idea for the establishment of privacy protection method against node collusion.

2) We rigorously prove that the accuracy (convergence to the exact average of the initial values) and privacy (the initial state of agent can be protected against internal honest-but-curious nodes) can be achieved simultaneously under our method.

Suppose that each agent has an initial scalar state $x_i(0)$. At each iteration, agents will communicate with their neighbors and update their states according to the following protocol:

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in \mathcal{N}_i} a_{ij}(x_j(k) - x_i(k)). \quad (1)$$

For the types of agents in the network, we provide the following explanation.
1) A neutral agent is defined as an agent that faithfully follows the consensus agreement. It does not help other agents infer information, nor does it help them to hide information.
2) A honest-but-curious agent is an agent that is able to follow all protocol steps correctly, but tries to obtain some information about other agents based on the collected data.

We are now ready to describe the problem that will be addressed in this paper. Considering multiagent systems (1), our main research goal is to propose a suitable consensus protocol that meets the following two requirements
1) Average consensus is achieved.
2) Initial state $x(0)$ remains private for honest-but-curious agents, even if they are colluding.

Every agent updates its sub-information according to the decomposed topology , which can be formulated as

$$x_i^l(k+1) = x_i^l(k) + \epsilon \sum_{j \in \mathcal{N}_i^l} \tilde{a}_{ij}(x_j^l(k) - x_i^l(k)). \quad (2)$$

Theorem 1: Consider a discrete-time multiagent systems (1) with a connected undirected graph G, using the aforementioned privacy-preserving average consensus approach, the average consensus value can be obtained by averaging the sum of the convergence values of all the sub-states in the (2), i.e.,

$$\lim_{k \to \infty} x_i(k) = \frac{1}{N} \sum_{l=1}^{N} c_l = \frac{1}{N} \sum_{i=1}^{N} x_i(0). \quad (3)$$

Theorem 2: Consider the discrete-time multiagent systems (1) with a connected undirected graph G, using the aforementioned privacy-preserving average consensus approach, it is not possible for the honest-but-curious node to accurately deduce the initial state $x_i(0)$ with certainty if its has at least one neutral neighbor.