Privacy preserving Mean-square consensus for discrete-time heterogeneous multi-agent systems with Communication Noises

Tongqing Yang
School of Mathematics and Statistics, Beijing Technology and Business University, 11 Fucheng Road, Haidian District, Beijing, 100048, China

Lipo Mo
School of Computer and Artificial Intelligence, Beijing Technology and Business University, 11 Fucheng Road, Haidian District, Beijing, 100048, China

Yingmin Jia
The seventh Division, Beihang university, 37 Xueyuan Road, Haidian District, Beijing, 100191, China
Email: yangtongqing08@126.com, molipo@th.btbu.edu.cn, ymjia@buaa.edu.cn.
www.btbu.edu.cn

Abstract

This paper investigates privacy-preserving mean-square consensus in distributed heterogeneous multi-agent systems with communication noise on fixed undirected graphs. To mitigate the impact of communication noise, we introduce a stochastic approximation step rule in the control protocol. Utilizing graph theory, stochastic analysis, and Lyapunov theory, consensus conditions are derived. Subsequently, a cryptographic cryptosystem encrypts the designed protocol, safeguarding against eavesdropping and information privacy loss between agents during consensus. Numerical simulations confirm the efficacy of the proposed consensus protocol and privacy protection algorithm.

Keywords: Distributed, Heterogeneous multi-agent systems (HMAS), Consensus, Privacy preserving

1. Introduction

In recent years, research on multi-agent systems has profoundly impacted the development of engineering technology [1]. Consensus control stands out as a key issue in multi-agent system studies, aiming for the convergence of state and output values of each agent through a control protocol [2]. Extensive research results exist for consensus control in multi-agent systems comprising first or second-order agents [3]. However, the focus is expanding to include Heterogeneous Multi-Agent Systems (HMAS) consisting of both first-order and second-order agents. HMAS demonstrates superior load and task configuration capabilities, making it suitable for more complex environments [4].

In the above research, the consensus control protocol relies on the interaction of state information between adjacent nodes to achieve consensus. For instance, a group of agents aiming to converge at a specific location may wish to keep their initial locations confidential. In recent years, various privacy protection schemes have been explored. A commonly used method is differential privacy, where random noise is introduced to the interaction state to obscure the true state [5]. However, this approach is susceptible to eavesdropping, as the added noise compromises accuracy [6], [7]. Another approach involves a state decomposition mechanism introduced in literature. To address privacy concerns without sacrificing accuracy, the study delves into the homomorphic encryption scheme and extends the average consensus of first-order agent systems to second-order agent systems [7], [8]. Nevertheless, practical networks often operate in uncertain communication environments with random perturbations. Consequently, instead of assuming a deterministic form, literature considers the mean square consensus of communication noise [9], [10]. However, it overlooks privacy protection in the presence of communication noise, leaving the challenge of achieving privacy-preserving consensus for Heterogeneous Multi-Agent Systems (HMAS) with communication noises unresolved. This paper presents a distributed consensus algorithm for HMAS based on cryptography. The main contributions of this paper are as follows:

1) We propose a privacy consensus algorithm for HMAS with communication noises based on partial homomorphic cryptography;

2) The privacy protection for the initial state of the agent is analyzed in detail. In particular, compared with the existing approach in [7], [8], our algorithm can achieve higher privacy when there exists an agent connected with only one neighbor;

3) The effectiveness of our method is verified by simulation.

2. Preliminaries and problem description

The network of HAMS consisting of n agents is represented by an undirected connected graph G. For HMAS with first-order and second-order agents, the Laplacian matrix of the graph G can be described as

$$\mathrm{L}=\begin{bmatrix}\mathrm{L}_s+\mathrm{D}_{sf} & -\mathrm{A}_{sf}\\ -\mathrm{A}_{fs} & \mathrm{L}_f+\mathrm{D}_{fs}\end{bmatrix},$$

where L_s and L_f represent the Laplacian matrices of the graph comprising the second-order agents and first-order agents, respectively. A_{sf} and A_{fs} denote the adjacency matrix between the second-order agents (first-order agents) and first-order agents (second-order agents) respectively, D_{sf} and D_{fs} denote their row sums.

Paillier Cryptosystem: The Pailler crypto-system has key generation, encryption and decryption functions. The encryption operator E and the decryption operator D are usually used in the encryption and decryption process. Now, we introduce the additive homomorphism property of the Paillier cryptosystem:

$$\mathrm{E}(z)^k=\prod_{i=1}^{k}\mathrm{E}(z)=\mathrm{E}(\sum_{i=1}^{k}z)=\mathrm{E}(kz).$$

We assume that there are n agents in the HMAS, and the first group has m second-order agents, labeled $\mathrm{V}_m=\{1,2,\cdots,m\}$, while the rest are first-order agents, labeled $\mathrm{V}_{n-m}=\{m+1,m+2,\cdots,n\}$. The dynamic equation of the composed HMAS is as follows:

$$\begin{cases}x_i(k+1)=x_i(k)+v_i(t)T\\ v_i(k+1)=v_i(k)+u_i(t)T, & i\in\mathrm{V}_m,\\ x_i(k+1)=x_i(k)+u_i(t)T, & i\in\mathrm{V}_{n-m}.\end{cases}\tag{1}$$

where $x_i(k)\in\mathbb{R}$, $v_i(k)\in\mathbb{R}$ and $u_i(k)\in\mathbb{R}$ are the position, velocity and control input of agent i, respectively. The sample time is $0<T<1$. All results can obtained exist in $\mathbb{R}^n$ by using the Kronecker product.

Definition 1. The HMAS consisted of (1) is said to achieve mean-square consensus if for any initial condition, we have

$$\lim_{k\to\infty}E\|x_j(k)-x_i(k)\|^2=0\quad i,j=1,2,\cdots,n$$
$$\lim_{k\to\infty}E\|v_i(k)\|^2=0\quad i,j=1,2,\cdots,m$$

Lemma 1. Let $\{\tau(k)\},\{\beta(k)\}$ and $\{q(k)\},k=0,1,\cdots,$ be real sequences, satisfying $0<q(k)\le 1,\tau(k)\ge 0,$ $\beta(k)\ge 0$, $\sum_{k=0}^{\infty}q(k)=\infty,\frac{\beta(k)}{q(k)}\to 0,k\to\infty,$ and $\tau(k+1)\le(1-q(k))\tau(k)+\beta(k),$ then $\tau(k)\to 0,k\to\infty$.

3. Main contents

3.1. *Mean-square Consensus in Heterogeneous Multi-agent Systems*

We propose the following consensus protocol:

$$\begin{cases}u_i(k)=\alpha(k)\sum_{j=1}^{n}a_{ij}(x_j(k)+w_{ji}(k)-x_i(k))-k_1v_i(k), & i\in\mathrm{V}_m,\\ u_i(k)=\alpha(k)\sum_{j=1}^{n}a_{ij}(x_j(k)+w_{ji}(k)-x_i(k)), & i=\mathrm{V}_{n-m}.\end{cases}\tag{2}$$

where $\alpha(k)$ and k_1 are the control gains, $\{w_{ji}(k),$ $k\ge 0\}$ are communication noise sequences.

Let $y_i(k)=x_i(k)+v_i(k),\ i\in\mathrm{V}_m$, then derived from (1)
$x_i(k+1)=(1-T)x_i(k)+Ty_i(k)$.

Define $\xi(k)=[x_1(k),\cdots,x_m(k),y_1(k),\cdots,y_m(k),x_{m+1}(k),$ $\cdots,x_n(k)]^{\cdot}$, $W(k)=[W_1^T(k),\cdots,W_m^T(k),W_1^T(k),\cdots,W_n^T(k)]^T$, $\Lambda=diag\{0,\cdots,0,\Lambda_1,\cdots,\Lambda_n\},\Lambda_i=[a_{i1},a_{i2},\cdots,a_{in}],$ $W_i(k)=[w_{1i}(k),\cdots,w_{ni}(k)]^T$. Then the HMAS (1) can be rewritten as

$$\xi(k+1)=[I_{m+n}-\alpha(k)T\Psi_1-(1-\alpha(k))T\Psi_2]\xi(k)+\alpha(k)T\Lambda W(k)\tag{3}$$

where

$$\Psi_1=\begin{bmatrix}I_m & -I_m & \mathbf{0}\\ (1-k_1)I_m+(\mathrm{L}_s+\mathrm{D}_{sf}) & (k_1-1)I_m & -\mathrm{A}_{sf}T\\ -\mathrm{A}_{fs}T & \mathbf{0} & (\mathrm{L}_f+\mathrm{D}_{fs})T\end{bmatrix}$$
$$\Psi_2=\begin{bmatrix}I_m & -I_m & \mathbf{0}\\ (1-k_1)I_m & (k_1-1)I_m & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & \mathbf{0}\end{bmatrix}.$$

It is clear that $\theta=[(k_1-1)\mathbf{1}_m^{封},\mathbf{1}_m,\mathbf{1}_{n-m}^{\cdot}]$ and $\mathbf{1}_{n+m}$ are the left eigenvector and right eigenvector associated with zero eigenvalue of $\alpha(k)T\Psi_1+(1-\alpha(k))T\Psi_2$, respectively.

Assumption 1. The additive independent noise $\{w_{ji}(k),$ $k\ge 0\}$, $E(w_{ji}(k))=0$, $Var(\{w_{ji}(k))=\sigma_W$.

Assumption 2. Suppose that the control gains satisfy the following conditions

$$1)\sum_{k=0}^{\infty} a(k) = \infty, 0 < a(k) < 1, a(k+1) \le a(k), 2)\sum_{k=0}^{\infty} a^2(k) < \infty.$$

Lemma 2. If Assumptions 1-2 hold, $0 < T \le \min\{\max_{\lambda_i \ne 0} \frac{1}{\sqrt{\mathrm{Re}^2(\lambda_i)+\mathrm{Im}^2(\lambda_i)}}, \max_{\eta_i \ne 0} \frac{1}{\sqrt{\mathrm{Re}^2(\eta_i)+\mathrm{Im}^2(\eta_i)}}\}$ and $k_1 \ge 1+\max l_{ii}$, l_{ii}, $1,2,\cdots,n$, then $0 < \alpha(k)T\rho_1 < 1$, $0 < (1-\alpha(k))T\rho_2 < 1$,

where $\lambda_i, i = 1,2,\cdots,n+m$ and $\eta_i, i = 1,2,\cdots,n+m$ are the eigenvalues of Ψ_1 and Ψ_2 , ρ_1 and ρ_2 are the spectral radius of Ψ_2 and Ψ_2 , respectively. l_{ii} is the diagonal element of the Laplacian matrix.

Theorem 1. If Assumptions 1-2 hold, $0 < T \le \min\{\max_{\lambda_i \ne 0} \frac{1}{\sqrt{\mathrm{Re}^2(\lambda_i)+\mathrm{Im}^2(\lambda_i)}}, \max_{\eta_i \ne 0} \frac{1}{\sqrt{\mathrm{Re}^2(\eta_i)+\mathrm{Im}^2(\eta_i)}}\}$ and $k_1 \ge 1+\max l_{ii}$, $l_{ii}, i = 1,2,\cdots,n$, then the HMAS (3) reach mean-square consensus.

3.2. *Privacy protection*

In this paper, honest-but-curious and eavesdropper were considered.

Algorithm 1 Encrypted information exchange

Initialization: Each agent i initializes its state $x_i(0)$, the public key pk_i and private key sk_i are generated, and broadcasts pk_i to its neighbor(s) while keeps sk_i private. Each time a message is sent, a independent random variable $w_{j\to i}(k), \forall i, j \in \mathbb{V}_m, k = 0,1,\cdots$ is added.

Input: $x_i(k), k_1$ **; Output:** $u_i(k)$.

1: Agent i encrypts $x_i(k)$ with its public key pk_i :

$$-x_i(k) \to \mathrm{E}_i(-x_i(k))$$

then sends $\mathrm{E}_i(-x_i(k))$ to each neighbor $j \in N_i$, the equivalent of sending $\mathrm{E}_i(-x_i(k)+w_{i\to j}(k))$.

2: Each agent j encrypts $x_j(k)$, and $v_j(k)$ with its public key pk_i :

$$x_j(k) \to \mathrm{E}_i(x_j(k))$$

3: Each agent i generates the number $a_i(k)$ and agent $j \in N_i$ generates the number $a_j(k)$.

4: Each agent $j \in N_i$ computes the encrypted differences based on property of the Paillier cryptosystem:

$$\mathrm{E}_i(x_j(k))\mathrm{E}_i(-x_i(k)+w_{i\to j}(k)) = \mathrm{E}_i(x_j(k)-x_i(k)+w_{i\to j}(k)) \to (\mathrm{E}_i(x_j(k)-x_i(k)+w_{i\to j}(k)))^{a_j(k)} = \mathrm{E}_i(a_j(k)(x_j(k)-x_i(k)+w_{i\to j}(k)))$$

then sends encrypted differences back to agent i .

5: Agent i decrypts the received ciphertexts with private key sk_i and computes weighted differences:

$$\mathrm{E}_i(a_j(k)(x_j(k)-x_i(k)+w_{i\to j}(k)+w_{j\to i}(k))) \to a_j(k)(x_j(k)-x_i(k)+w_{ji}(k)) \xrightarrow{\times a_i(k)} a_{ij}(x_j(k)-x_i(k)+w_{ji}(k))$$

6: The values calculated in step 5 are taken into protocol (2) to update $x_i(k)$ and $v_i(k)$.

7: Set $k \leftarrow k+1$.

Definition 2 [7]: For a connected network of n nodes, the privacy of the initial value $x_i(0)$ of node i is preserved if an honest-but-curious adversary cannot estimate $x_i(0)$ with any accuracy.

Similar to [7], the fixed coupling weight can be decomposed, $a_{ij} = a_{ij} = a_i(k)a_j(k) > 0$, where $a_i(k)$ is generated when agent i transmits information and only known by itself. Similarly, we split the noise delivered by a communication link, i.e., $w_{ji}(k) = w_{i\to j}(k) + w_{j\to i}(k)$ in (2).

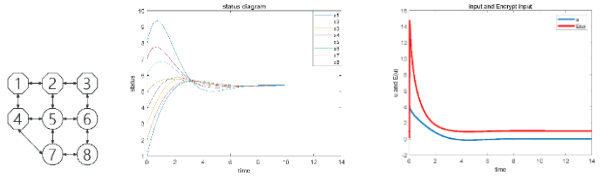
Theorem 2: In a connected network of nodes with system dynamics given by (1), each agent adheres to the consensus protocol (2) and Algorithm 1 for state updates. An honest-but-curious node, Eve, capable of receiving messages from a neighboring node, Alice, cannot ascertain Alice's initial state if Alice is also connected to another legitimate node, Bob. Furthermore, Alice's privacy remains undisclosed to external eavesdroppers.

Theorem 3: In a connected network of nodes governed by system dynamics as described in (1), each agent adheres to the consensus protocol (2) and Algorithm 1 for state updates. If a node, Alice, is solely connected to the rest of the network through an honest-but-curious node (or a colluding group of such nodes) Eve, and the noise introduced by the communication link is symmetrical, Eve can asymptotically deduce Alice's initial state. Conversely, in the case of asymmetric noise, while Eve can receive messages from its neighbor Alice, it lacks the means to ascertain Alice's initial state.

4. Numerical simulation

Consider the HMAS with eight agents, where nodes 1-4 represent first-order agents with input saturation and nodes 5-8 represent second-order agents. The network of the eight agents between communication topology shown

in Fig. 1 (a). We assume $k_1 = 5$, given the initial value $x(0) = [1,2,3,4,5,6,7,8]^{封}, v(0) = [1,2,3,4]$. Fig. 1 (b) represents the case where the state of the agent converges to 0. Fig. 1 (c) is the comparison between the real value of the input of agent 1 and the encrypted ciphertext.



a. Network b. Convergence c. Control input

Fig.1. Numerical simulation picture

5. Conclusion

This paper explores privacy-preserving consensus in distributed heterogeneous multi-agent systems with first-order and second-order agents, addressing communication noise using graph theory, stochastic analysis, Lyapunov theory, and cryptography. It proves that the closed-loop system attains consensus. The designed protocol is encrypted to prevent eavesdropping and information privacy loss. However, there are limitations when a secure agent connects with an adversary alone. Numerical simulations validate the consensus protocol's effectiveness and the privacy protection algorithm's ability to safeguard agent privacy.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (6197020462).

References

1. W. Yue, Y. Yang and W. Sun, "Resilient Consensus Control for Heterogeneous Multiagent Systems via Multiround Attack Detection and Isolation Algorithm," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2023.3327175.
2. A. Nedic, A. Ozdaglar and P. A. Parrilo, "Constrained Consensus and Optimization in Multi-Agent Networks," in IEEE Transactions on Automatic Control, vol. 55, no. 4, pp. 922-938, April 2010.
3. H. Du, S. Li, and P. Shi, “Robust consensus algorithm for second-order multi-agent systems with external disturbances,” International Journal of Control, vol. 85, no. 12, pp. 1913–1928, 2012.
4. Y. Liu, H.B. Min, S.C. Wang, Z.G. Liu, S.Y. Liao, Distributed consensus of a class of networked heterogeneous multi-agent systems, J. Frankl. Inst. 351 (2014) 1700–1716.
5. X. Li, H. Yan, Z. Cheng, W. Sun and H. Li, "Protecting Regression Models With Personalized Local Differential Privacy," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 960-974, 1 March-April 2023.
6. Zhang K, Li Z, and Wang Y, “Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control,” Automatica, vol. 139, May. 2022.
7. M. Ruan, H. Gao and Y. Wang, "Secure and Privacy-Preserving Consensus," in IEEE Transactions on Automatic Control, vol. 64, no. 10, pp. 4035-4049, Oct. 2019.
8. W. Fang, M. Zamani, and Z. Chen, “Secure and privacy preserving consensus for second-order systems based on paillier encryption,” Syst.Control Lett., vol. 148, p. 104869, 2021.
9. S. Guo, L. Mo, Y. Yu, Mean-square consensus of heterogeneous multi-agent systems with communication noises, Journal of the Franklin Institute 355 (8) (2018) 3717-3736.
10. T. Li, J.-F. Zhang, Consensus conditions of multi-agent systems with time-varying topologies and stochastic communication noises, IEEE Transactions on Automatic Control 55 (9) (2010) 2043-2057.

Authors Introduction

Mr. Tongqing Yang

He received his Bachelor degree in Engineering in 2022 from the School of Mechanical and Electrical Engineering, Guizhou Minzu University in China. He is currently a master student in Beijing Technology and Business University, China.

Dr. Lipo Mo

He received his B.S. degree in Department of Mathematics, Shihezi University, China, in 2003, and the Ph.D. degree in School of Mathematics and Systems Science from the Beihang University, Beijing, in 2010.

Yingmin Jia (Member, IEEE)

He received the B.S. degree in control theory from Shandong University, Jinan, China, in 1982, and the M.S. and Ph.D. degrees in control theory and applications from Beihang University, Beijing, China, in 1990 and 1993, respectively.