Optimal Privacy-Preserving Distributed Median Consensus

Wenrui Yu
Aalborg University
Denmark
wenyu@es.aau.dk

Qiongxiu Li*
Aalborg University
Denmark
qili@es.aau.dk

Richard Heusdens
Netherlands Defence Academy
Delft University of Technology
the Netherlands
r.heusdens@tudelft.nl

Sokol Kosta
Aalborg University
Denmark
sok@es.aau.dk

***Abstract*—Distributed median consensus has emerged as a critical paradigm in multi-agent systems due to the inherent robustness of the median against outliers and anomalies in measurement. Despite the sensitivity of the data involved, the development of privacy-preserving mechanisms for median consensus remains underexplored. In this work, we present the first rigorous analysis of privacy in distributed median consensus, focusing on an L_1-norm minimization framework. We establish necessary and sufficient conditions under which exact consensus and perfect privacy - defined as zero information leakage - can be achieved simultaneously. Our information-theoretic analysis provides provable guarantees against passive and eavesdropping adversaries, ensuring that private data remain concealed. Extensive numerical experiments validate our theoretical results, demonstrating the practical feasibility of achieving both accuracy and privacy in distributed median consensus.**

***Index Terms*—median consensus, distributed optimization, privacy, information-theoretical analysis, adversary**

I. Introduction

Consensus algorithms facilitate agreement in distributed systems through localized computations and information exchange among neighboring nodes. Common examples include averaging [1], [2], maximum/minimum [3], and median consensus [3]–[5]. These algorithms form the backbone of distributed optimization and have been extensively applied in sensor networks, multi-agent systems, and high-performance computing [6]. Among them, median consensus stands out due to its inherent robustness to outliers—a critical advantage in large-scale sensor and multi-agent networks where noisy and unreliable data are common. By mitigating the influence of extreme values, median consensus is particularly well-suited for environments such as distributed computing clusters and parallel processing frameworks. However, despite its robustness, prior research has largely overlooked the issue of *privacy preservation* in median consensus algorithms.

Several privacy-preserving frameworks have been proposed for consensus problems more broadly. A widely applicable framework for ensuring privacy in consensus problems involves the use of differential privacy (DP) techniques [7]–[11]. However, these methods often involve a trade-off between privacy preservation and the accuracy of the consensus output. Another approach to protecting privacy is the secure multiparty computation (SMPC) [12]–[19], which enables distributed computation while keeping individual inputs private. Despite its potential, SMPC often introduces significant communication overhead due to the need to split and distribute messages for secure transmission. Moreover, existing SMPC techniques primarily focus on consensus problems involving linear operations, such as averaging consensus, and their applicability to non-linear operations remains limited. Another notable framework for addressing privacy concerns in distributed systems is subspace perturbation (SP) [20]–[22], along with its variants [23]–[25]. SP is grounded in distributed optimization techniques, such as the Alternating Direction Method of Multipliers (ADMM) [26] and the Primal-Dual Method of Multipliers (PDMM) [27], [28]. The core idea involves injecting noise into the non-convergent subspace of the optimization process. This approach ensures privacy preservation by obfuscating sensitive information while simultaneously preserving the accuracy and integrity of sensitive information in the convergent subspace. Recent work [29] has extended SP to maximum consensus, but its applicability to median consensus remains unexplored.

Although median consensus algorithms have demonstrated exceptional robustness against outliers, their privacy implications remain critically underexplored. This leaves a significant gap in understanding how to protect sensitive information while maintaining robustness and efficiency. In this work, we take the first step toward bridging this gap by investigating whether perfect privacy (zero information leakage) can be achieved while maintaining consensus correctness. In particular, we establish a sufficient and necessary condition for achieving perfect privacy preservation in an L_1-norm formulation of the median consensus problem. Rooted in an information-theoretic framework, our methodology derives conditions that guarantee zero leakage of private inputs for honest nodes. Experimental results confirm the practical feasibility of our derived conditions and illustrate how network density and convergence parameters impact privacy. To the best of our knowledge, this work presents the first rigorously analyzed privacy-preserving median consensus algorithm, supported by a comprehensive information-theoretic foundation. Our study bridges a critical gap between robustness and privacy in distributed consensus systems.

* Corresponding author.

II. Preliminaries

A. Problem formulation

We model the network as an undirected graph $G = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{1, \dots, n\}$ represents the set of nodes/participants in the network and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ represents the set of edges, indicating the communication links between nodes. For each node i, its neighbor is defined as $\mathcal{N}_i = \{j \in \mathcal{V} \,|\, (i,j) \in \mathcal{E}\}$ and its degree is given by $d_i = |\mathcal{N}_i|$. Each node $i \in \mathcal{V}$ holds a local data value[1] $s_i \in \mathbb{R}$. When we consider s_i as a realization of a random variable, the corresponding random variable will be denoted by S_i (corresponding capital).

The privacy-preserving median consensus problem involves determining the median value s_{med} without revealing the private data s_i. This problem can be formulated [3] as an L_1-norm minimization problem:

$$\begin{aligned} \min_{\{x_i \,:\, i \in \mathcal{V}\}} \quad & \sum_{i \in \mathcal{V}} |x_i - s_i|, \\ \text{subject to} \quad & x_i - x_j = 0, \quad (i,j) \in \mathcal{E}. \end{aligned} \tag{1}$$

B. A/PDMM framework

Building on the work of [27], we can address the problem of minimizing a separable convex function under a set of equality constraints. The optimization problem is formulated as follows

$$\begin{aligned} \min_{\{x_i \,:\, i \in \mathcal{V}\}} \quad & \sum_{i \in \mathcal{V}} f_i\left(x_i\right), \\ \text{subject to} \quad & A_{ij} x_i + A_{ji} x_j = b_{ij}, \quad (i,j) \in \mathcal{E}, \end{aligned} \tag{2}$$

where f_i are convex, closed and proper (CCP) functions, $A_{ij} = -A_{ji} = 1$ for $i < j$, and $b_{ij} = 0$ for consensus problem. To solve (2), the update equations for node $i \in \mathcal{V}$ are given by

$$\begin{aligned} x_i^{(t)} &= \arg\min_{x_i} \left(f_i(x) + \sum_{j \in \mathcal{N}_i} (z_{i|j}^{(t)} A_{ij} x_i + \frac{c}{2} \|x_i\|^2) \right), \quad (3) \\ y_{i|j}^{(t)} &= z_{i|j}^{(t)} + 2cA_{ij} x_i^{(t)}, \\ z_{i|j}^{(t+1)} &= (1-\theta) z_{i|j}^{(t)} + \theta y_{j|i}^{(t)}, \end{aligned}$$

where y and z are auxiliary variables, $\theta \in (0, 1]$ is an avaraging constant and $c > 0$ is a convergence parameter that influences the convergence rate. When $\theta = 1$, the algorithm corresponds to standard PDMM, while $\theta = \frac{1}{2}$ represents the $\frac{1}{2}$-averaged version of PDMM, which is equivalent to ADMM [30]. In this work, since the L_1-norm lacks uniform convexity, standard PDMM will fail to converge. For this reason, we will focus our analysis on the case where $\theta = \frac{1}{2}$.

C. Adversary model and evaluation metrics

Adversary model: We examine two commonly studied adversary models in the context of privacy-preserving algorithms. The first is the passive adversary model, which involves corrupt nodes within the network. These nodes adhere to the protocol, but they collide to collect and exchange information in an attempt to infer private data. We denote the set of corrupt nodes as $\mathcal{V}_c$ and the set of honest nodes as $\mathcal{V}_h$. Hence, $\mathcal{V}_h \cup \mathcal{V}_c = \mathcal{V}$ and $\mathcal{V}_h \cap \mathcal{V}_c = \emptyset$. The second model is the eavesdropping adversary, which intercepts all messages transmitted over unencrypted communication channels. These adversaries are assumed to collaborate, combining their knowledge to infer the private data of honest nodes.

Individual privacy: In this work, we employ mutual information as a privacy metric due to its demonstrated effectiveness in prior research [31]–[33]. Let S_i be the random variable that represents the private data at node i, and $\mathcal{O}$ represent the total information observable by the adversary. The mutual information $I(S_i; \mathcal{O})$ [34] quantifies the amount of information about S_i that can be inferred from $\mathcal{O}$. It is defined as

$$I(S_i; \mathcal{O}) = h(S_i) - h(S_i \mid \mathcal{O}),$$

where $h(\cdot)$ denotes differential entropy, assuming it exists. When $I(S_i; \mathcal{O}) = I(S_i; S_i)$, the adversary can fully reconstruct s_i. When $I(S_i; \mathcal{O}) = 0$, the adversary does not gain any information about S_i by observing $\mathcal{O}$.

III. Algorithm and Privacy Analysis

In this section, we first present the detailed A/PDMM algorithm designed to address the L_1-norm formulation introduced in Section II-A. Then, we analyze the privacy leakage in the corresponding distributed median consensus problem.

To address problem (1), we can employ the regular equality constraint A/PDMM framework [27]. Specifically, we define $f_i(x_i) = |x_i - s_i|$. This formulation aligns with the framework required for applying ADMM/PDMM. The detailed steps of this approach are outlined in Algorithm 1.

Algorithm 1 Median consensus

for all $i \in \mathcal{V}, j \in \mathcal{N}_i$, **do**
  Randomly initialize $z_{i|j}^{(0)}$ ▷ Initialization
  $\text{Node}_j \leftarrow \text{Node}_i(z_{i|j}^{(0)})$

for $t = 0, 1, \dots$ **do**
  for all $i \in \mathcal{V}$ **do**

$$x_i^{(t)} = \begin{cases} \frac{-1 - \sum_{j \in \mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{c d_i}, & \text{if } \frac{-1 - \sum_{j \in \mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{c d_i} > s_i, \\ \frac{1 - \sum_{j \in \mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{c d_i}, & \text{if } \frac{1 - \sum_{j \in \mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{c d_i} < s_i, \\ s_i, & \text{otherwise.} \end{cases} \tag{4}$$

$$\forall j \in \mathcal{N}_i : z_{j|i}^{(t+1)} = \frac{1}{2} z_{j|i}^{(t)} + \frac{1}{2}(z_{i|j}^{(t)} + 2cA_{ij} x_i^{(t)}) \tag{5}$$

  $\text{Node}_{j \in \mathcal{N}_i} \leftarrow \text{Node}_i(x_i^{(t)})$ ▷ Broadcast
  for all $j \in \mathcal{N}_i$ **do**

$$z_{j|i}^{(t+1)} = \frac{1}{2} z_{j|i}^{(t)} + \frac{1}{2}(z_{i|j}^{(t)} + 2cA_{ij} x_i^{(t)})$$

As defined in Section II-C, we evaluate privacy preservation for node $i \in \mathcal{V}$ using the mutual information between S_i and the total information observed by the adversary. The information observed throughout the iterations is given by $\{S_j, X_j^{(t)}, Z_{j|k}^{(t)}, Z_{j|k}^{(t)}\}_{j \in \mathcal{V}_c, k \in \mathcal{N}_j, t \in \mathcal{T}}$, where

[1]For simplicity, s_i is assumed to be a scalar, though the results can be easily generalized to vectors.

$\mathcal{T} = \{0, \ldots, t_{\max}\}$ and $t_{\max}$ is the maximum number of iterations. For the eavesdropping adversary, the information accessible in the communication channels includes $\{Z_{j|k}^{(0)}, X_j^{(t)}\}_{j\in\mathcal{V},(j,k)\in\mathcal{E},t\in\mathcal{T}}$. By eliminating redundant information that both types of adversaries can access, individual privacy can be expressed as

$$I(S_i;\mathcal{O}) = I(S_i;\{S_j\}_{j\in\mathcal{V}_c},\{X_j^{(t)}\}_{j\in\mathcal{V},t\in\mathcal{T}},\{Z_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E},t\in\mathcal{T}})$$

We have the following result.

Theorem 1. *Let $i \in \mathcal{V}_h$. We have*

$$I(S_i;\mathcal{O}) = 0,$$

if and only if for all $t \in \mathcal{T}$,

$$s_i \notin [\frac{-1-\sum_{j\in\mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{cd_i}, \frac{1-\sum_{j\in\mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{cd_i}]. \quad (6)$$

Proof. Replacing $z_{j|i}^{(t)}$ and $z_{i|j}^{(t)}$ in (5) we obtain

$$\begin{aligned} z_{j|i}^{(t+1)} - z_{j|i}^{(t)} &= cA_{ij}x_i^{(t)} - \frac{1}{2}cA_{ij}x_i^{(t-1)} + \frac{1}{2}cA_{ji}x_j^{(t-1)} \\ &= cA_{ij}\left(x_i^{(t)} - \frac{1}{2}x_i^{(t-1)} - \frac{1}{2}x_j^{(t-1)}\right). \end{aligned} \quad (7)$$

Assume condition (6) holds. Considering the difference $x_j^{(t+1)} - x_j^{(t)}$ using (4) and combining with (7) we obtain

$$\begin{aligned} x_j^{(t+1)} - x_j^{(t)} &= \frac{-\sum_{k\in\mathcal{N}_j} A_{jk}(z_{j|k}^{(t+1)} - z_{j|k}^{(t)})}{cd_j} + r_j^{(t)} \\ &= \frac{\sum_{k\in\mathcal{N}_j}(x_k^{(t)} - \frac{1}{2}x_k^{(t-1)} - \frac{1}{2}x_j^{(t-1)})}{d_j} + r_j^{(t)}, \end{aligned} \quad (8)$$

where $r_j^{(t)} \in \{0, \pm\frac{2}{cd_j}\}$ is a constant depending on the range of $x_j^{(t+1)}$ and $x_j^{(t)}$. Hence, assume a set of nodes $\mathcal{V}_s \subset \mathcal{V}$ satisfy the condition, we have

$$\begin{aligned} I(S_i;\mathcal{O}) &= I(S_i;\{S_j\}_{j\in\mathcal{V}_c},\{X_j^{(t)}\}_{j\in\mathcal{V},t\in\mathcal{T}},\{Z_{j|k}^{(t)}\}_{(j,k)\in\mathcal{E},t\in\mathcal{T}}) \\ &\overset{(a)}{=} I(S_i;\{S_j\}_{j\in\mathcal{V}_c},\{X_j^{(t)}\}_{j\in\mathcal{V},t\in\mathcal{T}},\{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}}) \\ &\overset{(b)}{\leq} I(S_i;\{S_j\}_{j\in\mathcal{V}_c},\{X_j^{(0)},X_j^{(1)}\}_{j\in\mathcal{V}},\{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}},\{S_l\}_{l\in\mathcal{V}\backslash\mathcal{V}_s}) \\ &\overset{(c)}{=} I(S_i;\{S_j\}_{j\in\mathcal{V}_c},\{S_l\}_{l\in\mathcal{V}\backslash\mathcal{V}_s},\{Z_{j|k}^{(0)}\}_{(j,k)\in\mathcal{E}}) \\ &\overset{(d)}{=} \begin{cases} 0, & \text{if } i \in \mathcal{V}_h \cap \mathcal{V}_s, \\ I(S_i;S_i), & \text{if } i \in \mathcal{V}_c \cup (\mathcal{V}\backslash\mathcal{V}_s) \end{cases} \end{aligned} \quad (9)$$

where (a) follows from (5), (b) follows from (8) for the nodes that satisfy the condition, while introducing $\{s_l\}_{l\in\mathcal{V}\backslash\mathcal{V}_s}$ simplifies the expression of $x^{(t)}$ for the nodes that do not satisfy the condition, (c) holds since $\{x_j^{(0)}, x_j^{(1)}\}_{j\in\mathcal{V}}$ can be computed from $z_{j|k}^{(0)}$ and $z_{k|j}^{(0)}$, while (d) holds since all $Z^{(0)}$s are independent of S_i.

For node $i \notin \mathcal{V}_s$, its s_i can be derived from exist $x_i^{(t)}$, thus we have

$$I(S_i;\mathcal{O}) \geq I(S_i;\{S_j\}_{j\in\mathcal{V}_c},\{S_l\}_{l\in\mathcal{V}\backslash\mathcal{V}_s}). \quad (10)$$

Hence, with two inequalities in (9) and (10), we thus have this following equality

$$I(S_i;\mathcal{O}) = \begin{cases} 0, & \text{if } i \in \mathcal{V}_h \cap \mathcal{V}_s, \\ I(S_i;S_i), & \text{if } i \in \mathcal{V}_c \cup (\mathcal{V}\backslash\mathcal{V}_s). \end{cases}$$

□

Two remarks are placed here:

1) Theorem 1 states that if node i never transmits s_i to its neighboring nodes, no information about s_i will be disclosed. The fundamental principle of privacy preservation is thus to ensure that s_i remains outside the interval $\left[\frac{-1-\sum_{j\in\mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{cd_i}, \frac{1-\sum_{j\in\mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{cd_i}\right]$, which is of length $\frac{2}{cd_i}$. This length is solely determined by the degree of node i and the convergence parameter c. The impact of d_i and c on privacy preservation will be further discussed in Sections IV-C and IV-D, respectively.

2) The condition in equation (6) is equivalent to requiring that $x_i^{(t)} \neq s_i$ for all $t \in \mathcal{T}$. Therefore, by monitoring whether the updated value $x_i^{(t)}$ ever equals the private value s_i, we can directly determine whether perfect privacy is maintained.

IV. Simulation Results

In this section we present numerical results to validate our theoretical claims and discuss the factors that influence privacy leakage.

Initialization: We generate a random geometric graph (RGG) [35] with $n = 5$ nodes. The private data are randomly drawn from a standard normal distribution $\mathcal{N}(0,1)$. For the purpose of comparison, we fixed the values of s_i throughout the experiments. However, it is important to emphasize that s_i can, in fact, be randomized arbitrarily without affecting the validity of the analysis or the results. The auxiliary variables $z_{i|j}^{(0)}$ are sampled from a normal distribution $\mathcal{N}(\mu A_{ij}, \sigma^2)$. The choice of μ plays a critical role in determining the initialization of x.

A. Feasibility of derived conditions

We investigate whether the derived condition in Theorem 1 is satisfied in real-world scenarios. We first set $\mu = 0$ and $\sigma^2 = 10^{-2}$, ensuring that each node starts its iterations from a point near the median value. Figure 1 illustrates the convergence of the entire network (left plot) and individual nodes (right plot). Note that the actual private data values s_i are indicated in the legend. As shown in Figure 1(b), the optimization variables of all nodes, except for the one holding the median value, satisfy $x_i^{(t)} \neq s_i$ for all $t \in \mathcal{T}$. Consequently, the condition in equation (6) is automatically satisfied for these nodes, implying that perfect privacy is maintained throughout the optimization process.

B. The case when the conditions are not satisfied

Although we demonstrated above that the derived conditions can be satisfied, there are scenarios in which they are not. For example, it is not always feasible to identify an initial point that lies sufficiently close to the median value without prior knowledge. Figure 2(a) illustrates a scenario where $\mu = -10$ and $\sigma^2 = 1$. Under these conditions, the initialization of x

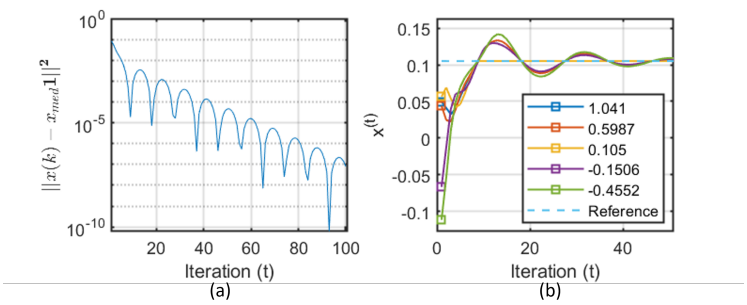

Fig. 1. (a) Overall convergence error of the whole network; (b) Convergence of the optimization variable $x^{(t)}$ for each node, as a function of iteration (t).

tends to be significantly larger than the actual data distribution. As shown, nodes holding values above the median (represented by the blue and red lines) may encounter a plateau during the process, where $s_i \in [\frac{-1-\sum_{j\in\mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{cd_i}, \frac{1-\sum_{j\in\mathcal{N}_i} A_{ij} z_{i|j}^{(t)}}{cd_i}]$. Consequently, privacy guarantees are only achievable for half of the nodes whose values lie below the median. In this case, only half of the nodes satisfy the privacy condition. To further enhance the privacy of nodes lacking guarantees, we can apply differential privacy techniques [36], [37]. Adding differential private noise to our approach will result in the following information leakage:

$$I(S_i; \mathcal{O}) = I(S_i; S_i + N_i) < I(S_i; S_i),$$

where the random variable N represents the introduced random noise. In Figure 2(b), we illustrate the same scenario as in Figure 1 and 2(b), but with the inclusion of a random offset drawn from a normal distribution $\mathcal{N}(0, 10^{-2})$. It is evident that the plateau still exists, however, noise offsets are introduced in the private value, thereby providing a certain level of privacy protection. This improvement in privacy comes at a cost: a reduction in accuracy, illustrating the inherent trade-off between privacy and precision.

C. The impact of topology density

As discussed in Section III, the number of neighbors (degree d_i) influences the length of the decision interval, which affects individual privacy. To examine this effect, we generate three types of graphs with $n = 15$ nodes: a ring graph (where each node has degree $d_i = 2$), a complete graph (where each node has degree $d_i = |\mathcal{V}| - 1$), and a random geometric graph (RGG). For each graph, we run 100 simulations and compute the average proportion of nodes that preserve their privacy. The results are presented in Figure 3. Our analysis shows that a denser topology, with a higher degree d, reduces the window width, allowing more nodes to securely preserve their values.

D. The impact of convergence parameter c

In addition to the degree, the convergence parameter c also plays a critical role in determining the convergence rate and the length of the decision interval. As illustrated in our analysis,

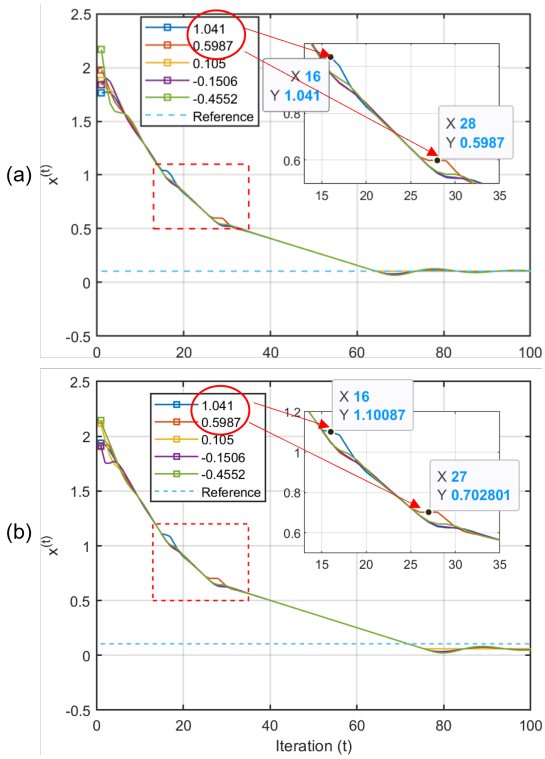

Fig. 2. Information leakage with specific initialization: (a) without differential privacy and (b) with differential privacy.

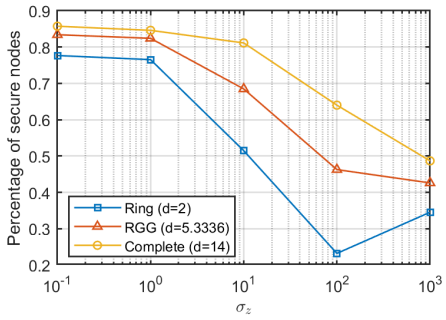

Fig. 3. Proportion of secure nodes under different topologies (ring graph, random geometric graph and complete graph)

the impact of this parameter on privacy mirrors the influence of node degree in Figure 4: as expected, a larger value of c results in a smaller window, thus enhancing the ability of more nodes to securely preserve their values. This relationship highlights the need to carefully choose the convergence parameter to balance efficiency and privacy.

V. Conclusion

In this study, we established sufficient and necessary conditions for achieving privacy-preserving median consensus under the ADMM/PDMM framework. Our results demonstrate that it is possible to achieve both perfect privacy and optimal accuracy simultaneously. In addition, we analyzed the influence of network density and convergence parameters on the robustness

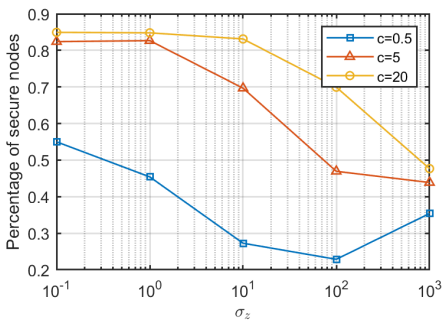

Fig. 4. Proportion of secure nodes with different choices of c

of privacy guarantees. Finally, we showed that incorporating differential privacy can provide additional protection when the derived conditions are not entirely met, albeit at the cost of reduced accuracy.

ACKNOWLEDGMENT

This research is partially supported by the EU ChipsJU and the Innovation Fund Denmark through the project CLEVER (no. 101097560).

REFERENCES

[1] G. França and J. Bento, "Distributed optimization, averaging via admm, and network topology," *Proceed. IEEE*, vol. 108, no. 11, pp. 1939–1952, 2020.

[2] R. Zhang and J. Kwok, "Asynchronous distributed admm for consensus optimization," in *Int. Conf. Mach. Learn.* PMLR, pp. 1701–1709, 2014.

[3] D. Deplano, N. Bastianello, M. Franceschelli, and K. H. Johansson, "A unified approach to solve the dynamic consensus on the average, maximum, and median values with linear convergence," in *2023 62nd IEEE Conf. Decis. Control (CDC)*, pp. 6442–6448, 2023.

[4] M. Franceschelli, A. Giua, and A. Pisano, "Finite-time consensus on the median value with robustness properties," *IEEE Trans. Automatic. Control*, vol. 62, no. 4, pp. 1652–1667, 2016.

[5] Z. Al Z. S. Dashti, C. Seatzu, and M. Franceschelli, "Dynamic consensus on the median value in open multi-agent systems," in *IEEE 58th Conf. Decis. Control (CDC)*. IEEE, pp. 3691–3697, 2019.

[6] L.e Singhal, M. A Iyer, and S. Adya, "Lsc: A large-scale consensus-based clustering algorithm for high-performance fpgas," in *Proc. 54th Annual Design Auto. Conf.*, pp. 1–6, 2017.

[7] Z. Huang, S. Mitra, and N. Vaidya, "Differentially private distributed optimization.," in *Proc. Int. Conf. Distrib. Comput. Netw*, pp. 1–10, 2015.

[8] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private distributed convex optimization via functional perturbation," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 395–408, 2018.

[9] T. Zhang and Q. Zhu, "Dynamic differential privacy for ADMM-based distributed classification learning," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 172–187, 2016.

[10] X. Zhang, M. M. Khalili, and M. Liu, "Improving the privacy and accuracy of ADMM-based distributed algorithms," *Proc. Int. Conf. Mach. Learn.*, pp. 5796–5805, 2018.

[11] Y. Xiong, J. Xu, K. You, J. Liu and L. Wu, "Privacy preserving distributed online optimization over unbalanced digraphs via subgradient rescaling," *IEEE Trans. Control Netw. Syst.*, 2020.

[12] N. Gupta, J. Katz, N. Chopra, "Privacy in distributed average consensus," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 9515–9520, 2017.

[13] Q. Li, I. Cascudo, and M. G. Christensen, "Privacy-preserving distributed average consensus based on additive secret sharing," in *Proc. Eur. Signal Process. Conf.*, pp. 1–5, 2019.

[14] K. Tjell and R. Wisniewski, "Privacy preservation in distributed optimization via dual decomposition and ADMM," in *Proc. IEEE 58th Conf. Decis. Control.*, pp. 7203–7208, 2020.

[15] K. Tjell, I. Cascudo and R. Wisniewski, "Privacy preserving recursive least squares solutions," in *Proc. Eur. Control Conf.*, pp. 3490–3495, 2019.

[16] Z. Xu and Q. Zhu, "Secure and resilient control design for cloud enabled networked control systems," in *Proc. 1st ACM Workshop Cyber-Phys. Syst.-Secur. Privacy.*, pp. 31–42, 2015.

[17] Q. Li and M. G. Christensen, "A privacy-preserving asynchronous averaging algorithm based on shamir's secret sharing," in *Proc. Eur. Signal Process. Conf.*, pp. 1–5, 2019.

[18] Y. Shoukry et al., "Privacy-aware quadratic optimization using partially homomorphic encryption," in *IEEE 55th Conf. Decis. Control.*, pp. 5053–5058, 2016.

[19] C. Zhang, M. Ahmad, and Y. Wang, "ADMM based privacy-preserving decentralized optimization," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 565–580, 2019.

[20] Q. Li, R. Heusdens and M. G. Christensen, "Convex optimisation-based privacy-preserving distributed average consensus in wireless sensor networks," in *Proc. Int. Conf. Acoust., Speech, Signal Process.*, pp. 5895–5899, 2020.

[21] Q. Li, R. Heusdens and M. G. Christensen, "Convex optimization-based privacy-preserving distributed least squares via subspace perturbation," in *Proc. Eur. Signal Process. Conf.*, 2020.

[22] Q. Li, R. Heusdens, and M. G. Christensen, "Privacy-preserving distributed optimization via subspace perturbation: A general framework," *IEEE Trans. Signal Process.*, vol. 68, pp. 5983–5996, 2020.

[23] S. O. Jordan, Q. Li, and R. Heusdens, "Privacy-preserving distributed optimisation using stochastic PDMM," in *Proc. Int. Conf. Acoust., Speech, Signal Process.*, pp. 8571–8575, 2024.

[24] Q. Li, R. Heusdens, and M. G. Christensen, "Communication efficient privacy-preserving distributed optimization using adaptive differential quantization," *Signal Process.*, vol. 194, pp. 108456, 2022.

[25] Q. Li, J. S. Gundersen, M. Lopuhaä-Zwakenberg, and R. Heusdens, "Adaptive differentially quantized subspace perturbation (ADQSP): A unified framework for privacy-preserving distributed average consensus," *IEEE Trans. Inf. Forensics Security.*, 2023.

[26] S. Boyd, N. Parikh, E. Chu, B. Peleato, J. Eckstein, et al., "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Found. Trends Mach. Learn.*, vol. 3, no. 1, pp. 1–122, 2011.

[27] G. Zhang and R. Heusdens, "Distributed optimization using the primal-dual method of multipliers," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 173–187, 2017.

[28] R. Heusdens and G. Zhang, "Distributed optimisation with linear equality and inequality constraints using pdmm," *IEEE Trans. Signal Inf. Process. Netw.*, 2024.

[29] W. Yu, R. Heusdens, J. Pang, and Q. Li, "Privacy-preserving distributed maximum consensus without accuracy loss," in *Proc. Int. Conf. Acoust., Speech, Signal Process.*, 2025.

[30] Thomas William Sherson, Richard Heusdens, and W. Bastiaan Kleijn, "Derivation and Analysis of the Primal-Dual Method of Multipliers Based on Monotone Operator Theory," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 5, no. 2, pp. 334–347, June 2019.

[31] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *Proc. IEEE Annu. Symp. Found. Comput. Sci.*, pp. 429–438, 2013.

[32] P. Kairouz, S. Oh, and P. Viswanath, "Extremal mechanisms for local differential privacy," in *Adv. Neural Inf. Process. Syst.*, pp. 2879–2887, 2014.

[33] Q. Li, J. S. Gundersen, K. Tjell, R. Wisniewski, and M. G. Christensen, "Privacy-preserving distributed expectation maximization for gaussian mixture model using subspace perturbation," in *IEEE Proc. Int. Conf. Acoust., Speech, Signal Process.*, pp. 4263–4267, 2022.

[34] T. M. Cover and J. A. Tomas, *Elements of information theory*, John Wiley & Sons, 2012.

[35] M. Penrose, *Random geometric graphs*, vol. 5, OUP Oxford, 2003.

[36] M. Kefayati, M. S. Talebi, B. H. Khalajand H. R. Rabiee , "Secure consensus averaging in sensor networks using random offsets," in *Proc. IEEE Int. Conf. Telec., Malaysia Int. Conf. Commun., pp. 556–560*, 2007.

[37] X. Wang, J. He, P. Cheng, and J. Chen, "Differentially private maximum consensus: Design, analysis and impossibility result," *IEEE Trans. Netw. Sci. Eng.*, vol. 6, no. 4, pp. 928–939, 2018.