Privacy consensus in distributed network ⋆

ZHOU Han * **YANG Wen** * **YANG Chao** * **Xiaofan Wang** **

* *School of information Science and Engineering, East China University of Science and Technology,Shanghai 200237, China(e-mail: weny@ecust.edu.cn).*
** *Department of Automation, Shanghai Jiaotong University, Shanghai, China, 200240.(e-mail: xfwang@sjtu.edu.cn)*

Abstract: There are plenty of reality issue can be formulated into consensus problem, on the same time of the researches care the result of consensus, the leakage of the initial state of each node catch their attention. In order to preserve the privacy of each node, some algorithm are proposed to achieve this goal. However, a attacker can infer the privacy of the network by utilize the defect of the algorithm. In this article, we analysis an consensus algorithm which can add offset in each node under some exact rule, and prove an quantitative result that can characterization the performance of the attack, furthermore, we provide the optimal attack strategy under some assumption and some numerical example to show the result.

Keywords: privacy; consensus; attack.

1. INTRODUCTION

Wireless network has gained much interest in the past decades which is a result of the recent advances in fabrication, modern sensor and communication technologies. The application of WSN include intelligent transportation, environment monitoring, health care, etc.

Consensus problem is a conventional point in network, the nodes in the network has to receive and send their state value to their neighbors, and finally reach to a same value. In Olfati-Saber et al. (2007), the author discuss consensus problems for networks of dynamic agents with fixed and switching topologies. The application of distributed consensus including distributed estimation, source location and compression, see Dimakis et al. (2010). Many researches focus on the consensus under some complicated network, such as switching topology and a network with time-delays in Olfatisaber and Murray (2015).

However, In the original consensus algorithm, each node exchange their state value with their neighbors, if the malicious node obtain the information of network topology and update rule, then it can track the initial state changes of other nodes see Mo and Murray (2016), Kolesnikov (2009) point it is still an important security problem. For instance, the node in the network is a closed-loop control system, the leakage of the initial state of each node is unexpected. Besides, in some decision-making scene, we must keep secrete the participant's information. So some researchers are trying to propose an consensus algorithm with privacy preserving. In centralized network, Katewa et al. (2015) present a mechanism that every node purposely adds noise to its measurements before transmission to the estimator. In distributed network, Dwork (2006) do some work which are based on differentially privacy in Dwork (2008), which is introduce in Huang et al. (2012) and Nozari et al. (2015). In Pequito et al. (2014), the author utilize structural systems theory, and achieve weighted average consensus that permitting nodes obtain only a small subset of the initial information of their non-neighbors. Mo and Murray (2016) propose an privacy preserving algorithm which add well-designed noise to each node, then the author prove the convergence rate of this consensus algorithm, what's more, a lower and an upper bound of is provided in this literature. In Manitara and Hadjicostis (2013), the article present a privacy preserving consensus algorithm that each node adds an arbitrary offset value to the result of iteration, where the total offsets cancel themselves out in the end. The common point in Pequito et al. (2014) and Manitara and Hadjicostis (2013) is that the algorithm in both article has some restrictions on the network structure, if a node and all of it's neighbor are belongs to the malicious node's neighbor node set, the privacy of that node can be speculated by the malicious node, but both two article didn't have profound study on this point.

This article review the similar algorithm in Manitara and Hadjicostis (2013), and transform the constrain on network structure into mathematical expression which is consisted of system matrix A and observation matrix, Then we focus on the attack problem under such a privacy algorithm, where the attack can obtain the information flow in the edges with constraint energy, and we demonstrate an indicator that show the degree of privacy leakage. Under a special network topology, we consider the problem from the view of attacker, and find preferable strategy to reach better attack performance. As we all know, there are plenty works on attack problem in network Kefayati et al. (2007); Zhang et al. (2014); Qi et al. (2015) and some researchers concern the privacy preserving in consensus,

⋆ This work was supported in part by the National Natural Science Foundation of China under Grant(61573143,61503139), the Innovation Program of Shanghai Municipal Education Commission under Grant No.14zz55, China Postdoctoral Science Funding 2015M570337

the most contribute of this literature is combine two parts together, considering the attack in network with privacy preserving.

The rest of paper is organized as follow: in Section 2, we review the consensus and privacy preserving problem, in Section 3, we show our main result which divided into two parts, privacy and attack analysis. In Section 4, we present examples to illustrate our result, and conclude this paper and show the future work in Section 5.

2. PROBLEM FORMULATION

In this paper, we model a sensor network as an undirected graph $G = (V, E)$ with the nodes $V = 1, 2, ..., n$ being the sensors and the edges $E \subset V \times V$ representing the communication links. Denote the set of neighbors of node i by $N(i) = \{j \in V : (i, j) \in E, j \neq i\}$. Each node can communicate with its neighbors. The interconnection topology of the network is described by Laplacian matrix $L = [l_{ij}]$, where $l_{ii} = -\sum_{j \in N_i} l_{ij}$ and $l_{ij} = 1$ if $(i,\ j) \in E$; otherwise, $l_{ij} = 0$. Assume that G is connected, and let the initial state of each node is $x_i(0)$. In the network, each node updates its state according to the following equation,

$$x_i(k+1) = x_i(k) + \varepsilon \sum_{j \in N(i)} a_{ij}(x_j(k) - x_i(k)). \tag{1}$$

By collecting all the states of the nodes, we define $x(k) \triangleq [x_1(k), \ldots, x_n(k)]'$. The single node dynamics (1) can be represented as the following vector form

$$x(k+1) = P_\varepsilon x(k), \tag{2}$$

where $P_\varepsilon = [a_{ij}]$ (called as *Perron matrix*) is satisfied with

$$P_\varepsilon = I - \varepsilon L. \tag{3}$$

we can denote the node with maximum number of neighbors of in G as $d_{max} = max\{l_{ii}\}$, then ε satisfied $\varepsilon \in (0, 1/d_{max})$.

Based on the existing results in Olfatisaber and Murray (2015), the node dynamics (2) asymptotically solves the average consensus problem if and only if G is balanced.

In this paper, we consider the privacy protection for consensus problem. First, we consider a problem that node n wants to infer the initial states of all the other nodes in the network. We denote the neighboring set of node n as $N(n) = \{j_1, \ldots, j_m\}$, and define an observation matrix C as $C = [e_{j_1}, ..., e_{j_m}\ e_n]^T \in \mathbb{R}^{(m+1)\times n}$, where e_i denotes the ith canonical basis in $\mathbb{R}^n$ with a 1 in the ith entry and zeros elsewhere. The output equation of the whole network can be rewritten as the following,

$$y(k) = Cx(k). \tag{4}$$

At time step k, node n's information set is

$$I(k) = \{x_n(0), y(0), ...y(k)\}. \tag{5}$$

Lemma 1. Mo and Murray (2016) Assume node n knows the A and C matrices and all variables in $I(k)$ at time step k, the consensus algorithm is deterministic and node n can perfectly infer $\zeta' x(0)$, given that $\zeta \in \mathbb{R}^n$ lies in the observable space of (A, C).

To protect the privacy of the initial states of nodes while enforcing that $x(k)$ converges to $\bar{x}$, Manitara and Hadjicostis (2013) propose a protocol in weighted and directed network, we simplify it into unweighted and undirected network as follow:

1) Each node i generate a random number m_i, which satisfied with $2 \leq m_i \leq M$, M is a positive real.
2) Each node generates m_i random number $r_i(1), r_i(2), ..., r_i(m_i)$, with average value is $x_i(0)$.
3) Clear the initial state of each node to $x_i(0) = 0$, we can mark the real initial state as $x_i^r(0)$.
4) At time step k, inject the number $d_i(k)$ into the state of each node, where

$$d_i(k) = \begin{cases} r_i(k)/n, & if\ 1 \leq k \leq m_i \\ 0, & otherwise, \end{cases}$$

According to the above steps, each node updates its state by

$$x_i(k+1) = x_i(k) + \varepsilon \sum_{j \in N_i} a_{ij}(x_j(k) - x_i(k)) + d_i(k+1), \tag{6}$$

Define $d(k) = [d_1(k), ...d_n(k)]^T \in \mathbb{R}^n$. The vector form of (6) and (4) in conjunction with Eq. (4) can be rewritten as

$$\begin{cases} x(k+1) = P_\varepsilon(x(k)) + d(k+1), \\ y(k) = Cx(k). \end{cases} \tag{7}$$

Instant of transmit each node's initial state to their neighbor, their real value are hidden in several parts. As a result, the privacy of $x(0)$ can be guaranteed by this method.

3. MAIN RESULT

3.1 Privacy Analysis

With a standard consensus algorithm, the initial states of nodes can be easily speculated by any other nodes. With the proposed privacy preserving algorithm (6), as we know in Manitara and Hadjicostis (2013), this algorithm can reach to an fixed average value finally, and the real initial states of nodes hide in $d(k)$. Hence, the problem of deducting $x_r(0)$ can be transformed into computing $d(k), k \in [1, M]$, and the solution of (7) as follows:

$$\begin{aligned} x(k) =& P_\varepsilon^k x(0) + \sum_{i=0}^{k-1} P_\varepsilon^{k-1-i} d(i+1), \\ y(k) =& CP_\varepsilon^k x(0) + C\sum_{i=0}^{k-1} P_\varepsilon^{k-1-i} d(i+1). \end{aligned} \tag{8}$$

Recalling that $x(0) = 0$, we obtain:

$$Y = FD \tag{9}$$

where,

$$F = \begin{bmatrix} C & 0 & \ldots & 0 \\ CP_\varepsilon & C & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ CP_\varepsilon^{M-1} & CP_\varepsilon^{M-2} & \ldots & C \end{bmatrix} \in \mathbb{R}^{((m+1)M)\times(nM)}$$

$$Y = \begin{bmatrix} y(1) \\ y(2) \\ \vdots \\ y(M) \end{bmatrix}, D = \begin{bmatrix} d(1) \\ d(2) \\ \vdots \\ d(M) \end{bmatrix} \in \mathbb{R}^{nM\times 1}.$$

For a fixed network topology G, F is a constant matrix. In order to derive the the real initial state $x_r(0)$ from D, we need to utilize the information Y to solve the function (9). Let us define

$$s_i = \begin{cases} e_i, & if\ i \in N(n) \\ \mathbf{0}, & else \end{cases}$$

where $\mathbf{0} \in \mathbb{R}^n$ is zero vector, e_i denotes the ith canonical basis in $\mathbb{R}^n$ with a 1 in the ith entry and zeros elsewhere. We further define:

$$\tilde{C} = [s_1, s_2, ...s_n]^T \in \mathbb{R}^{n\times n},$$
$$\tilde{y}(k) = \tilde{C}x(k) \in \mathbb{R}^{n\times 1},$$

where $\tilde{y}(k)$ is easily obtained from $y(k)$ for a given C.

Theorem 2. If the ith line of P_ε noted as P_{ε_i} satisfies $P_{\varepsilon_i}\tilde{C} = P_{\varepsilon_i}$, then node n can speculate the initial state of node i successfully.

Proof 1. For any $k \in [1, M-1]$, we have

$$\tilde{y}(k) = \tilde{C}\sum_{i=0}^{k-1} P_\varepsilon^{k-1-i} d(i+1).$$

Note that $P_{\varepsilon_i}\tilde{C} = P_{\varepsilon_i}$. We know that node i is one neighbor of node n, thus $x_i(k)$ lies in the ith line of $y(k)$, then

$$\begin{aligned} P_{\varepsilon_i}\tilde{y}(k) &= P_{\varepsilon_i}\sum_{i=0}^{k-1} P_\varepsilon^{k-1-i} d(i+1) \\ &= P_{\varepsilon_i} x_i(k). \end{aligned} \tag{10}$$

At time step $k+1$, we can derive $x_i(k+1)$ from $y(k+1)$. Hence,

$$d_i(k+1) = x_i(k+1) - P_{\varepsilon_i} x_i(k). \tag{11}$$

By this way, we can also obtain $(d_i(2), d_i(3)...d_i(M)$. Furthermore, $d_i(1)$ lies in $y(1) = Cd(1)$. Finally, we can obtain the initial state of node i.

As mentioned above, there still exist the possibility that node i's initial state can be speculated under a special structure of network $N(i)\bigcup i \subseteq N(n)\bigcup n$. If there exists an attacker with limited power in the network, it has the ability to intercept the information flow between the nodes. It is of practical meaning to design an optimized strategy to allocate power to attack nodes according to its position in the network.

3.2 Attack Analysis

In this subsection, we consider the case when an attacker with limited power exists in the network. Suppose that probability of attacker intercepting the information transmitted on the edge between node i and node j as $\lambda_{i,j}$. Due to our research is based on undirected graph, it's unnecessary to distinguish $\lambda_{i,j}$ and$\lambda_{j,i}$. To make the statement clear, we use (i,j) to present the edge in network. we assume $\lambda_{i,j}$ is proportional to the power $\mu_{i,j}$ distributed for this edge's attack, where $\lambda_{i,j} = k\cdot\mu_{i,j}$. Define the power constraint of the attacker as $\sum_{(i,j)\in E}\mu_{i,j} = T$. It can be restated as $\sum_{(i,j)\in E}\lambda_{i,j} = 1$ when $k = T$.

As discussed above, we know that the privacy of node i can be exposed in some situations. We define $g_{i,j}$ as the edge between i and j. In Fig. (1), let $i = 1$.

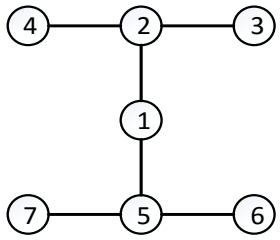

Fig. 1. wireless network

1) When the information passed by edge $g_{1,2}$ and $g_{1,5}$ have been exposed, at time step k, the attacker can easily utilize the obtained knowledge to predict the state of node 1 in step $k+1$ as $\overline{V}_{1,k+1}$, which don't contain the adding of offset $d_1(k+1)$. According to the information transmitted from node 1 to node 5 at time step $k+1$, $V_{1,k+1}$, we can further obtain the injected value which equals to$V_{1,k+1} - \overline{V}_{1,k+1}$. Due to the randomness of k, we can derive the injection value of each step, then the initial state of node 1 will be exposed.
2) When the information passed by edge $g_{1,2}$ and $g_{5,6}$ have been exposed, at time step k, because of the information sent from node 5 to it's neighbors are identical, the attacker can speculate all the messages sent to node 1, then it can complete the spy mission in the similar way.

As discussed above, once the network is under the situation which is similar to the situation 2), then the privacy states will be divulged. For example, edge $g_{1,5}$ and $g_{2,4}$'s information flow are exposed.

Remark 1. We conclude that for each node j in N_i, at least one edge connected to j has been exposed, and we should also guarantee there is at least one edge connected to i has been exposed.

In a random network, we suppose each edge is under attack with fixed energy. Notice that when the energy is zero, we can think the edge isn't suffer any attack. We can write down the adjacency matrix of the network as A_d, $A_d[i,j] = 1$ represent there is a connected edge between node i and j, then we can define attack matrix A_t, which satisfied

$$A_t[i,j] = \begin{cases} \lambda_{i,j}, & if\ A_d[i,j] = 1 \\ 0, & otherwise, \end{cases}$$

Notice $\lambda_{i,j} = \lambda_{j,i}$, so $A_t = A_t^T$.

Theorem 3. In order to investigate the influence of the existence of the attacker, we have to calculate the possibility of the privacy leakage P_i for each node.

$$\begin{aligned} P_i &= W_i - W_i^{'}, \\ W_i &= \prod_{m\in N(i)}[1 - \prod_{t=1}^{n}(1 - e_t^T A_t e_m)], \\ W_i^{'} &= \prod_{m\in N(i)}[1 - \prod_{t=1,t\neq i}^{n}(1 - e_t^T A_t e_m)] \end{aligned} \tag{12}$$

where e_i denotes the ith canonical basis in $\mathbb{R}^n$ with a 1 in the ith entry and zeros elsewhere.

Proof 2. $A_t(i,j)$ has the special structure that the element of $A_t(i,j)$ denotes the probability of edge between i and j been attacked, actually, $e_i^T A_t e_j$ is equal to $A_t(i,j)$. To gain

the degree of the leakage of node i, which is fully depend on the network topology, so we can use adjacency matrix A_d to fix this problem. Combined with the above Remark (1), we focus on the i's line in A_d, once the element in it is not zero, that means there is a connected edge in that place.

The meaning of $1-\prod_{t=1}^{n}(1-e_t^T A_t e_m)$ is at least one edge connected to node m has been exposed, and $1-\prod_{t=1,t\neq i}^{n}(1-e_t^T A_t e_m)$ represent there is at least one edge between m and it's neighbor except node i has been exposed. so it becomes easy to understand W_i and $W_i^{'}$, the former is represent each node in $N(i)$ has at least one leaked edge, and $W_t^{'}$ has a quite similar format with W_t, but it is worth noticing that in $W_t^{'}$ only consider the neighbor node's edge except $g_{i,m}$. Finally, the differential between them can totally represent the situation which can lead to the leakage of node i's privacy.

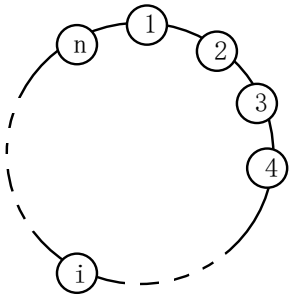

Fig. 2. Ring network

We consider a ring form network structure in Fig (2), which is quite special that the position of each node is same, and there are two edges connected to a node. Utilize Theorem 3, we can speculate P_i as follow:

$$\begin{aligned} P_i &= W_i - W_i^{'} \\ W_i &= H_{i-2}\cdot H_i \\ H_i &= 1-(1-\lambda_{i,i+1})(1-\lambda_{i+1,i+2}) \\ W_i^{'} &= \lambda_{i-2,i-1}\cdot(1-\lambda_{i-1,i})\cdot(1-\lambda_{i,i+1})\cdot\lambda_{i+1,i+2} \end{aligned} \tag{13}$$

The equation (13) can be written as

$$\begin{aligned} P_i = {} & \lambda_{i-1,i}\cdot\lambda_{i,i+1}+\lambda_{i-1,i}\cdot\lambda_{i+1,i+2}+\lambda_{i-2,i-1}\cdot\lambda_{i,i+1} \\ & -\lambda_{i-2,i-1}\cdot\lambda_{i-1,i}\cdot\lambda_{i,i+1}-\lambda_{i-1,i}\cdot\lambda_{i,i+1}\cdot\lambda_{i+1,i+2} \end{aligned} \tag{14}$$

In order to simplify the notation, we use λ_i to replace $\lambda_{i,i+1}$, specially, λ_n represent $\lambda_{n,1}$. Then we can denote the degree of the network's privacy being exposed as $P=\sum_{i=1}^{n}P_i$, In a ring network, because of the position of each node is same, we can write down P as follow,

$$\begin{aligned} P &= P_1+P_2+P_3...+P_n \\ &= \sum_{i=1}^{n}\lambda_i\cdot\lambda_{i+1}+2\sum_{i=1}^{n}\lambda_i\cdot\lambda_{i+2}-2\sum_{i=1}^{n}\lambda_i\cdot\lambda_{i+1}\cdot\lambda_{i+2} \end{aligned} \tag{15}$$

Assumption 1. The attacker only focus on sequential edges, and the energy allocated on each chosen edge is same, that means we can only consider the number of edge being chosen, once the number is determined, then the strategy also become the fixed one.

Remark 2. According to the conclusion in Eq. (15), when the chosen edge is m, we can calculate the P. As m sequential edges are allocated with energy T/m, the other edges are not under attack. Hence,

$$\begin{aligned} P &= (m-1)/m^2+2(m-2)/m^2-2(m-2)/m^3 \\ &= (m-1)(3m-4)/m^3 \end{aligned}$$

If we want to protect the safety of the network, sometimes we have to consider the problem in the view of a attacker. For attacker, it is necessary to point out the best attack strategy, which can lead to the furthest leakage of the network with constraint energy .

Due to P can be obtained by function with one parameter $m\in[1,n]$, we can calculate the biggest value of P is 0.375 when $m=4$.

Assumption 2. The attacker only choose edges with the following way, when it attack on an edge, then it will not attack this edge's next neighbor, but the next neighbor of it's neighbor will be chosen, and the energy allocated on each chosen edge is same.

Be similar to the analysis in assumption (1), we can write down the P when the number of chosen edge is $m\in[1,floor(n/2)]$ where we suppose n is a quite big number, and $floor()$ is the function of get integer. Hence

$$P=2(m-1)/m^2$$

The biggest value of P is 0.5 when $m=2$.

4. NUMERICAL EXAMPLES

we consider a network with 5 nodes in Fig 3, and set their initial state are $2,3,4,7,9$ respectively. Then use the consensus strategy introduced in this article, we can simulate the process of the system's update. The network can reach the average value finally. As mentioned in above article, we hide the initial state of each node in the random offset $r_i(1),r_i(2),...,r_i(m_i)$, the distribution of $r_i(k)$ can influence the convergence time. We set $M=20$, and m_i

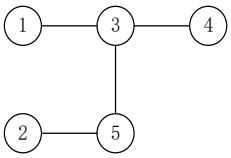

Fig. 3. Network Structure

subject to uniform distribution between $[2,M]$. Then we simulate the consensus process when $r_i(k)$ obey uniform, Gaussion and exponential distribution respectively. As shown in fig 4, the uniform distribution with average value equals to initial state of each node $x_i(0)$, and the range of random number is $[-100+x_i(0),100+x_i(0)]$.

In fig 5, we simulate the convergence process when $r_i(k)$ subject to Gaussian distribution $X\sim N(x_i(0),1000)$.

In fig 6, we simulate the convergence process when $r_i(k)$ subject to exponential distribution $X\sim E(1/x_i(0))$.

Then we treat the network reach the average consensus when each node's value is between $[4.9,5.1]$. When $r_i(k)$ is

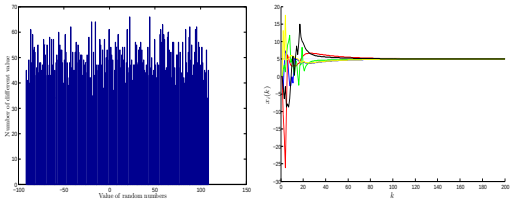

Fig. 4. Uniform distribution and consensus process

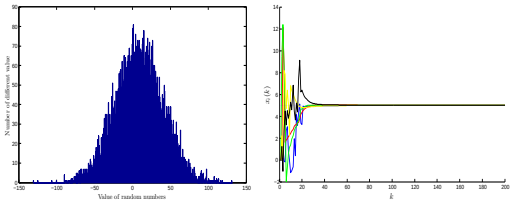

Fig. 5. Gaussian distribution and consensus process

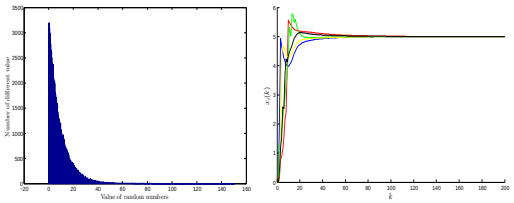

Fig. 6. Exponential distribution and consensus process

under above distribution, we can get the average convergence steps of 2000 simulations, which is shown in Table 1

Table 1. Convergence step

Distribution	Convergence steps
Uniform	70
Gaussian	61
Exponential	56

When a network with ring structure under the attack in assumption (1) and assumption (2), we can get the relationship between the extend of network's privacy leakage and number of chosen edges in fig 7. It is quite easy to cite the result in this article.

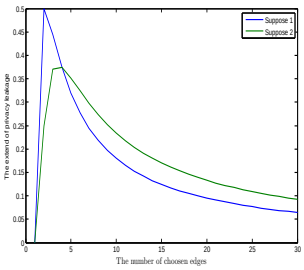

Fig. 7. Ring network under attack

5. CONCLUSION

In this article, we research the consensus algorithm which can protect the privacy when the network's structure satisfy some condition. Then we express this special condition into mathematical expression. What's more, we do some research in the performance of privacy preserving when the network is under the attack, and point out the best attack strategy under some suppose, then we can make a better decision when defend attack. The future work will spread in finding the optimal or sub-optimal attack strategy in a random network.

REFERENCES

Dimakis, A.G., Kar, S., Moura, J.M.F., Rabbat, M.G., and Scaglione, A. (2010). Gossip algorithms for distributed signal processing. *Proceedings of the IEEE*, 98(11), 1847 – 1864.

Dwork, C. (2006). *Differential Privacy*. Springer Berlin Heidelberg.

Dwork, C. (2008). *Differential Privacy: A Survey of Results*. Springer Berlin Heidelberg.

Huang, Z., Mitra, S., and Dullerud, G. (2012). Differentially private iterative synchronous consensus. 81–90.

Katewa, V., Chakrabortty, A., and Gupta, V. (2015). Protecting privacy of topology in consensus networks. In *American Control Conference*, 2476–2481.

Kefayati, M., Talebi, M.S., Khalaj, B.H., and Rabiee, H.R. (2007). Secure consensus averaging in sensor networks using random offsets. In *IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 2007. Ict-Micc*, 556–560.

Kolesnikov, V. (2009). Advances and impact of secure function evaluation. *Bell Labs Technical Journal*, 14(3), 187–192.

Manitara, N.E. and Hadjicostis, C.N. (2013). Privacy-preserving asymptotic average consensus. In *Control Conference*, 760–765.

Mo, Y. and Murray, R.M. (2016). Privacy preserving average consensus. *IEEE Transactions on Automatic Control*, 1–1.

Nozari, E., Tallapragada, P., and Cortĺęs, J. (2015). Differentially private average consensus with optimal noise selection. *Ifac Papersonline*, 48(22), 203–208.

Olfati-Saber, R., Fax, A., and Murray, R.M. (2007). Consensus and cooperation in networked multi-agent systems. *Proceedings of the IEEE*, 95(1), 215–233.

Olfatisaber, R. and Murray, R.M. (2015). Consensus problems in networks of agents with switching topology and time-delays. *IEEE Transactions on Automatic Control*, 49(9), 1520–1533.

Pequito, S., Kar, S., Sundaram, S., and Aguiar, A.P. (2014). Design of communication networks for distributed computation with privacy guarantees. In *Decision and Control*, 1370–1376.

Qi, Y., Cheng, P., Shi, L., and Chen, J. (2015). Event-based attack against remote state estimation. In *2015 54th IEEE Conference on Decision and Control (CDC)*, 6844–6849. doi:10.1109/CDC.2015.7403297.

Zhang, H., Cheng, P., Wu, J., Shi, L., and Chen, J. (2014). Online deception attack against remote state estimation. 47(3), 128–133.