Consensus Algorithm with Censored Data for Distributed Detection with Corrupted Measurements: A Game-Theoretic Approach

Kassem Kallas(✉), Benedetta Tondi, Riccardo Lazzeretti, and Mauro Barni

Department of Information Engineering and Mathematics,
University of Siena, Via Roma 56, 53100 Siena, Italy
kassem.kallas@unisi.it, benedettatondi@gmail.com,
riccardo.lazzeretti@gmail.com, barni@dii.unisi.it

Abstract. In distributed detection based on consensus algorithm, all nodes reach the same decision by locally exchanging information with their neighbors. Due to the distributed nature of the consensus algorithm, an attacker can induce a wrong decision by corrupting just a few measurements. As a countermeasure, we propose a modified algorithm wherein the nodes discard the corrupted measurements by comparing them to the expected statistics under the two hypothesis. Although the nodes with corrupted measurements are not considered in the protocol, under proper assumptions on network topology, the convergence of the distributed algorithm can be preserved. On his hand, the attacker may try to corrupt the measurements up to a level which is not detectable to avoid that the corrupted measurements are discarded. We describe the interplay between the nodes and the attacker in a game-theoretic setting and use simulations to derive the equilibrium point of the game and evaluate the performance of the proposed scheme.

Keywords: Adversarial signal processing · Consensus algorithm · Distributed detection with corrupted measurements · Data fusion in malicious settings · Game theory

1 Introduction

In distributed detection applications a group of nodes in a network collect measurements about a certain phenomenon [1]. In centralized architectures, the measurements are sent to a central processor, called fusion center (FC), which is responsible of making a global decision. If needed, the result of the decision is then transmitted to all the nodes. Though attractive for the possibility of adopting an optimum decision strategy based on the entire set of measurements collected by the network, centralized solutions present a number of drawbacks, most of which related to the security of the network. For instance, the FC represents a single point of failure or a bottleneck for the network, and its failure may compromise the correct behavior of the whole network. In addition, due to

Q. Zhu et al. (Eds.): GameSec 2016, LNCS 9996, pp. 455–466, 2016.
DOI: 10.1007/978-3-319-47413-7_26

privacy considerations or power constraints, the nodes may prefer not to share the gathered information with a remote device. For the above reasons, decentralized solutions have attracted an increasing interest. Consensus Algorithm is a fusion decentralized algorithm in which the nodes locally exchange information to reach a final agreement about the phenomenon of interest [2,3]. Consensus algorithm have been proven to provide good performance in many applications like cognitive radio [4], social networks or experimental sociology [5], and many others like flocking, formation control, load-balancing network, wireless sensor networks, etc. [2].

Despite the benefits of decentralized solutions using consensus algorithm, their nature makes them vulnerable to many security threats: for instance, attacks that emulate the phenomenon of interest to have an exclusive benefit from the resource, i.e., the Primary User Emulation Attack (PUEA) in cognitive radio applications [6], or data (measurements) falsification attacks [7], in which the attacker tries to induce a wrong decision by injecting forged measurements. This kind of attack can be launched in one of two ways: either the attacker can directly access the programmable device or, more simply, attack the physical link between the phenomenon and the nodes. In the first case, the attacker has full control over the nodes, and many effective solutions are proposed [8–11] whereas in the second case, the attacker cannot control the node and then he is not part of the network. In this paper, we focus on this second case.

In this attack scenario, when centralized systems are considered, by relying on the observation of the entire set of measurements, the fusion center can easily 'detect' the corrupted values and discard them, as long as their number remains limited. In this way, a reliable decision can still be done, see [12–15]. Attempts have been made to defend against those attacks in decentralized networks that employ a consensus algorithm to make a decision [16–18], when the attacker is assumed to control the nodes. Other solutions based on network control theory are proposed in [8–11]. However, all these methods do not consider the possibility that the attackers are aware of the defense mechanism adopted by the network and hence have their own countermeasures.

In this paper, by focusing on the measurement falsification attack with corruption of the physical link, we propose a game theoretical framework to distributed detection based on consensus algorithm. Specifically, we propose to include a preliminary isolation step in which each node may discard its own measurement based on the available a priori knowledge of the measurements statistics under the tho hypotheses. Then, the algorithm proceeds as usual, with the nodes that continue to receive and dispatch messages from their neighbors. Under some assumptions on network topology, that prevents that isolation step causes the network to disconnect, the convergence of the consensus algorithm is preserved. By following the principles of adversarial signal processing [19], we assume that in turn the attacker may adjust the strength of the falsification attack to avoid that the fake measurements are discarded. We then formalise the interplay between the network designed and the attacker as a zero-sum competitive game and use simulations to derive equilibrium point of the game.

The rest of this paper is organized as follows. In Sect. 2, we introduce the network model and describe the consensus algorithm. In Sect. 3, we introduce the measurement falsification attack against the detection based on consensus showing its powerfulness. In Sect. 4, we propose a refinement of the consensus algorithm to make it robust to the measurement falsification attack. Then, the interplay between the attacker and the network designer is casted into a game-theoretic framework in Sect. 5. The equilibrium point is found numerically in Sect. 6. Then, we conclude the paper in Sect. 7 with some final remarks.

2 Distributed Detection Based on Consensus Algorithm

In this section, we describe the distributed detection system considered in this paper, when no adversary is present and introduce the consensus algorithm the detection system relies on.

2.1 The Network Model

The network is modeled as an undirected graph $\mathcal{G}$ where the information can be exchanged in both directions between the nodes. A graph $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ consists of the set of nodes $\mathcal{N} = \{n_1, ..., n_N\}$ and the set of edges $\mathcal{E}$ where $(n_i, n_j) \in \mathcal{E}$ if and only if there is a common communication link between n_i and n_j, i.e., they are neighbors. The neighborhood of a node n_i is indicated as $\mathcal{N}_i = \{n_j \in \mathcal{N} : (n_i, n_j) \in \mathcal{E}\}$. For task of simplicity, we sometimes refer to $\mathcal{N}_i$ as the set of indexes j instead than directly of nodes. The graph $\mathcal{G}$ can be represented by its adjacency matrix $A = \{a_{ij}\}$ where $a_{ij} = 1$, if $(n_i, n_j) \in \mathcal{E}$, 0 otherwise.

The degree matrix D of $\mathcal{G}$ is a diagonal matrix with $d_{ii} = a_{i1} + a_{i2} + ... + a_{in}$, $d_{ij} = 0$, $\forall i, j \neq i$ [20].

2.2 The Measurement Model

Let S be the status of the system under observation: we have $S = 0$, under hypothesis H_0 and $S = 1$ under hypothesis H_1. We use the capital letter X_i to denote the random variable describing the measurement at node n_i, and the lower-case letter x_i for a specific instantiation. By adopting a Gaussian model, the probability distribution of each measurement x_i under the two hypothesis is given by:[1]

$$P_X(x) = \begin{cases} \mathcal{N}(-\mu, \sigma), \text{ under } H_0, \\ \mathcal{N}(\mu, \sigma), \text{under } H_1, \end{cases} \tag{1}$$

where, $\mathcal{N}(\mu, \sigma)$ is the Normal Distribution with mean μ and variance σ^2.

Let us denote with U the result of the final (binary) decision. An error occurs if $u \neq s$. By assuming that the measurements are conditionally independent, that

[1] We are assuming that the statistical characterization of the measurement at all the nodes is the same.

is that are independent conditioned to the status of the system, the optimum decision strategy consists in computing the mean of the measurements, $\bar{x} = \sum_i x_i/N$ and comparing it with a threshold λ which is set based on the a-priori probability ($\lambda = 0$ in the case of equiprobable system states). In a distributed architecture based on consensus, the value of $\bar{x}$ is computed iteratively by means of a proper message exchanging procedure between neighboring nodes, the final decision is made at each single node by comparing $\bar{x}$ with λ.

In this paper we consider the case of equiprobable system states. It is worth observing that our analysis, included the game formulation in Sect. 5, can be extended to the general case in which this assumption does not hold.

2.3 The Consensus Algorithm

Consensus algorithm for distributed detection is a protocol where the nodes locally exchange information with their neighbors in order to converge to an agreement about an event or a physical phenomenon [2], e.g. the existence of a transmission signal in cognitive radio applications [4]. It consists of three phases: the initial phase, the state update phase and the decision phase.

1. Initial phase: the nodes collect their initial measurement $x_i(0)$ about the phenomenon they are monitoring, and exchange the measurement with their neighbors.
2. State update phase: at each time step k, each node updates its state based on the information received from its neighbors. Then, at step $k+1$ we have:

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in \mathcal{N}_i} (x_j(k) - x_i(k)) \tag{2}$$

   where, $0 < \epsilon < (\max_i \mathcal{N}_i)^{-1}$ is the update step parameter. This phase is iterated until they reach the consensus value $\bar{x}(\mathcal{N}) = \frac{1}{N} \sum_{i \in \mathcal{N}} x_i(0)$, which corresponds to the mean of the initial measurements. It is proven that, with the above choice for ϵ, the consensus algorithm converges to $\bar{x}$ regardless of the network topology [3].
3. The final decision phase: this is the last phase in which all nodes compare the consensus value $\bar{x}$ to a threshold λ to make the final decision u:

$$u = \begin{cases} 1, & \text{if } \bar{x} > \lambda. \\ 0, & \text{otherwise,} \end{cases} \tag{3}$$

   In the symmetric setup considered in this paper $\lambda = 0$.

3 Measurement Falsification Attack Against Consensus-Based Detection

In this section, we consider an adversarial setup of the setting described in the previous section and show that even a single false measurement can result in a wrong decision.

3.1 Consensus Algorithm with Corrupted Measurements

In the binary decision setup we are considering, the objective of the attacker is inducing one of the two decision errors (or both of them): decide that $S = 0$ when H_1 holds (False Alarm), decide that $S = 1$ when H_0 holds (Missed Detection). For simplicity, we optimistically make the worst case assumption that the attacker knows the true system state. In this case, he can try to push the network toward a wrong decision by replacing one or more measurements so to bias the average computed by using the consensus algorithm. Specifically, for any corrupted node, the attacker forces the measurement to a positive value Δ_0 under H_0 and to a negative value Δ_1 under H_1. For the symmetric setup, reasonably, $\Delta_1 = -\Delta_0 = \Delta > 0$. In the following we assume that the attacker corrupts a fraction α of the nodes, that is the number of attacked nodes is $N_A = \alpha N$.

Given the initial vector of measurements, the consensus value the network converge to because of the attack is:

$$\tilde{x} = \frac{1}{N} \sum_{i \in \mathcal{N}_H} x_i(0) + \frac{N_A \Delta}{N}, \tag{4}$$

where $\mathcal{N}_H$ is the set of the uncorrupted nodes ($|\mathcal{N}_H| = N - N_A$).

By referring to the model described in Sect. 2.2, it is easy to draw a relation between Δ, α and the probability p that the attacker induces a decision error. By exploiting the symmetry of the considered setup we can compute p by considering the behavior under one hypothesis only, that is we have $p = P(U = 1|H_0) = P(\tilde{X} > 0|H_0)$.

In the following we indicate with $\bar{X}(\mathcal{N})$ the average of the measurements made by the nodes in a set $\mathcal{N}$.

The error probability p for a given N_A can be written as:

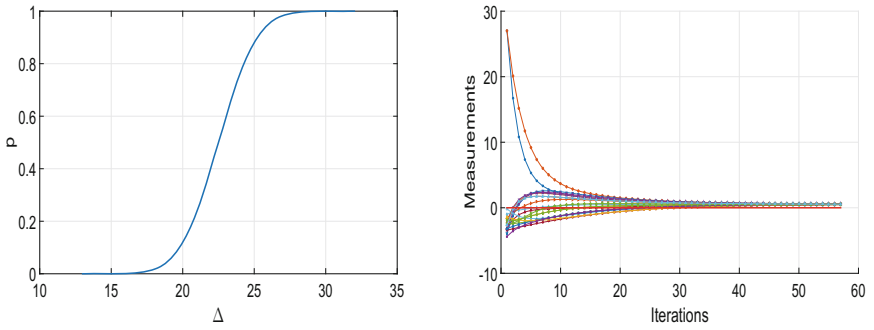
$$\begin{aligned} p =& P(\tilde{X} > 0|H_0) = P\left(\frac{N - N_A}{N} \bar{X}(\mathcal{N}_H) > -\frac{N_A \Delta}{N} \middle| H_0\right) \\ =& P\left(\bar{X}(\mathcal{N}_H) > \frac{N}{N - N_A}\left(-\frac{N_A \Delta}{N}\right) \middle| H_0\right) = \int_{-\frac{N_A \Delta}{N - N_A}}^{\infty} \mathcal{N}(-\mu, \sigma/\sqrt{N - N_A}). \end{aligned} \tag{5}$$

Clearly, if there is no limit to the value of Δ, the attacker will always succeed in inducing a wrong decision (see for example Fig. 1).

This shows how harmful the attack can be against distributed detection based on consensus algorithm. Therefore, the issue of securing distributed detection with consensus algorithm must be studied, at the purpose to increase the robustness of the consensus algorithm to intentional attacks.

4 Consensus Algorithm with Censored Data

With centralized fusion is quite easy to detect false measurements, since they assume outlier values with respect to the majority of the measurements. In a



(a) (b)

Fig. 1. (a): Success probability of the attack versus Δ in the adversarial setup $N = 20$, $\mu = 2.5$, $\sigma = 1$, $N_A = 2(\alpha = 0.1)$. (b): Effect of the attack on the convergence of the consensus algorithm for $\Delta = 27$, the network decides for H_1 even if H_0 is true.

distributed setting, however, this is not easy since, at least in the initial phase (see Sect. 2.3), each node sees only its measurement and has no other clue about the system status.

In contrary with most of proposed solutions in the literature [8,18], in this paper we propose to tackle with the problem of the measurement falsifications at the initial phase of the consensus algorithm (see for instance [2]), by letting each node discard its measurement if it does not fall within a predefined interval containing most of the probability mass associated to both H_0 and H_1, being then a suspect measurement. In the subsequent phase the remaining nodes continue exchanging messages as usual according to the algorithm, whereas the nodes which discarded their measurements only act as receivers and do not take part in the protocol. Due to the removal, the measurements exchanged by the nodes follows a censored gaussian distribution, i.e. the distribution which results by constraining the (initial) gaussian variable to stay within an interval [21]. Specifically, the nodes discards all the measurements whose absolute values are large than a removal threshold η. By considering the results shown in Fig. 1a, we see that, in the setup considered, if we let by letting $\eta = 17.5$ the error probability drops to nearly zero since the attacker must confine the choice of Δ to values lower than 17.5. The proposed strategy is simple, yet effective, and allow us to use a game theoretical approach to set the parameters (see Sect. 5).

For our analysis, we consider conditions on the network topology, such that the connectivity of the network is preserved and then the algorithm converges to the average of measurements which have not been discarded. For a given graph, this fact is characterized by the node connectivity, namely, the maximum number of nodes whose removal does not cause a disconnection [22]. Convergence is guaranteed for instance in the following cases (see [23] for an extensive analysis of the connectivity properties for the various topologies): Fully-connected graph; Random Graph [24], when the probability of having a connection between two

nodes is large enough; Small-World Graph [25] when the neighbour list in ring formation is large and the rewiring probability is large as well; Scale-Free Graph [26], for sufficiently large degree of the non-fully meshed nodes.

We now give a more precise formulation of the consensus algorithm based on censored data. Let us denote with $\mathcal{R}$ the set of all the remaining nodes after the removal, that is

$$\mathcal{R} = \{n_j \in \mathcal{N} : -\eta < x_j < \eta\}, \tag{6}$$

and let $\mathcal{R}_i$ be the 'active' neighborhood of node i after the isolation, $i \in \mathcal{R}$ (i.e. the set of the nodes in the neighborhood of i which take part in the protocol). The update rule for node $i \in \mathcal{R}$ can be written as:

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in \mathcal{R}_i} (x_j(k) - x_i(k)), \tag{7}$$

where $0 < \epsilon < (\max_i \mathcal{N}_i)^{-1}$, and the degree refers to the network after the removal of the suspect nodes, that is to the graph $(\mathcal{R}, \mathcal{E})$ (instead of $(\mathcal{N}, \mathcal{E})$).

Under the above conditions on the network topologies, the consensus algorithm converges to the average value computed over the measurements made by the nodes in $\mathcal{R}$, namely $\bar{x}(\mathcal{R})$. Otherwise, disconnection may occur and then it is possible that different parts of the network (connected components) converge to possibly different values.

5 Game-Theoretic Formulation

The consensus based on censored data is expected to be robust in the presence of corrupted measurements. On the other hand, we should assume that the attacker is aware that the network takes countermeasures and removes suspect measurements in the initial phase, hence he will adjust the attack strength Δ to avoid that the false measurement is removed. We model the interplay between the attacker and the network as a two-player zero sum game where each player will try to maximize its own payoff. Specifically, we assume that the network designer, hereafter referred as the defender (D), does not know the attack strength Δ, while the attacker (A) does not know the value of the removal threshold η adopted by the defender.

With these ideas in mind, the Consensus-based Distributed Detection game $\mathcal{CDD}(\mathcal{S}_\mathcal{A}, \mathcal{S}_\mathcal{D}, v)$ is a two-player, strategic game played by the attacker and the defender, defined by the following strategies and payoff.

- The space strategies of the defender and the attacker are respectively

$$\begin{aligned} \mathcal{S}_\mathcal{D} &= \{\eta \in [0, \infty)\} \\ \mathcal{S}_\mathcal{A} &= \{\Delta \in [0, \infty)\}; \end{aligned} \tag{8}$$

The reason to limit the strategies of D to values larger than by λ is to avoid removing correct measurements at the defender side and to prevent to vote for the correct hypothesis at the attacker side.

- The payoff function is defined as the final error probability,

$$v = P_e = P(U \neq S) = P(\bar{X} > 0/H_0), \tag{9}$$

where $\bar{X} = \bar{X}(\mathcal{R})$, that is the mean computed over the nodes that remain after the removal. The attacker wishes to maximize v, whereas the defender wants to minimize it.

Note that according to the definition of the $\mathcal{CDD}$ game, the sets of strategies of the attacker and the defender are continuous sets. We remind that, in this paper, we consider situations in which the network remains connected after the isolation and then convergence of the algorithm is preserved. Notice that, with general topologies, when disconnection may occur, the payoff function should be redefined in terms of error probability at the node level.

In the next section, we use numerical simulations to derive the equilibrium point of the game under different settings and to evaluate the payoff at the equilibrium.

6 Simulation Results

We run numerical simulations in order to investigate the behavior of the $\mathcal{CDD}$ game for different setups and analyze the achievable performance when the attacker and the defender adopt their best strategies with parameters tuned following a game-theoretic formalization. Specifically, the first goal of the simulations is to study the existence of an equilibrium point for the $\mathcal{CDD}$ game and analyze the expected behavior of the attacker as well as the defender at the equilibrium. The second goal is to evaluate the payoff at the equilibrium as a measure of the best achievable performance of distributed detection with the consensus algorithm based on censored data.

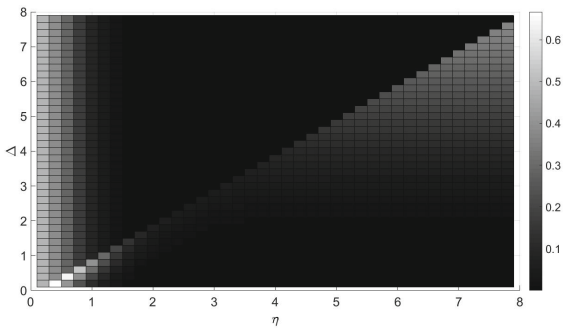
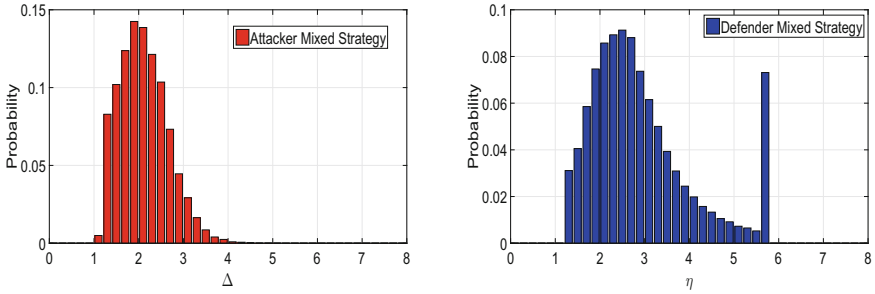


Fig. 2. Payoff matrix of the game with $N = 20$, $\alpha = 0.1$ and $\mu = 1$ (SNR = 4).



(a) The Attacker Mixed Strategy. (b) The Defender Mixed Strategy.

Fig. 3. Equilibrium strategies in the following setup: $N = 20$, $\alpha = 0.1$, $\mu = 1$, (SNR = 4). Payoff at the equilibrium: $v = 0.0176$.

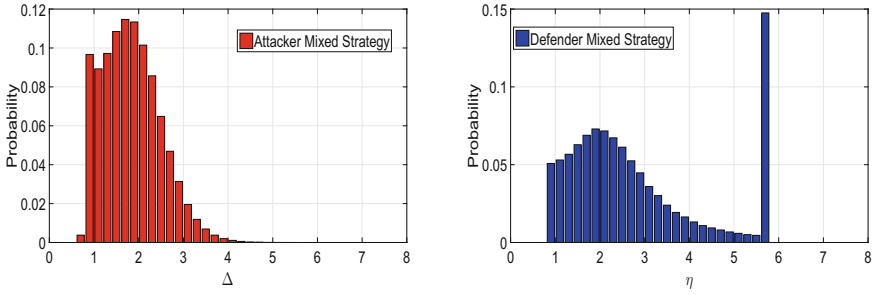


Fig. 4. Equilibrium strategies in the following setup: $N = 20$, $\alpha = 0.2$, $\mu = 1$ (SNR = 4). Payoff at the equilibrium: $v = 0.1097$.

To perform our experiments, we quantize the values of η and Δ with step 0.2 and then we consider the following sets: $\mathcal{S}_D = \{\eta \in \{0, 0.2, ...\}\}$ and $\mathcal{S}_A = \{\Delta \in \{0, 0.2, ...\}\}$. Simulations were carried out according to the following setup. We considered a network with $N = \{20, 50\}$ nodes where the measurement of each node is corrupted with probability $\alpha \in \{0.1, 0.2\}$. We assume that the probability that the measurement of a node is corrupted does not depend on the other nodes (independent node corruption). According to the model introduced in Sect. 2.2, the measurements are drawn according to Gaussian distribution with variance $\sigma^2 = 1$ and mean $-\mu$ and μ under H_0 and H_1 respectively. In our tests, we take $\mu = \{1, 2\}$. For each setting, we estimated the error probability of the decision based on the censored data over 10^5 trials. Then, we find the mixed strategies Nash equilibrium by relying on the minimax theorem [27] and then solving two separate linear programming problems.

Figure 2 shows the payoff matrix in gray levels for the game with $\alpha = 0.1$ and $\mu = 1$ (i.e., $SNR = 4$). Notice that the stepwise behavior of the values of the payoff in correspondence of the diagonal, which is due to the hard isolation (for each Δ, when $\eta < \Delta$ all the corrupted measurements are kept, while they are removed for $\eta \geq \Delta$). When very low values of η are considered, the error

probability increases because many 'honest' (good) measurements are removed from the network and the decision is based on very few measurements (in the limit case, when all measurements are removed, the network decides at random, leading to $P_e = 0.5$). Figure 3 shows the player's mixed strategies at the equilibrium. By focusing on the distribution of the defense strategy, D seems to follow the choice of A by choosing the value η which is one step ahead of Δ, a part for the presence of a peak, that is a probability mass (of about 0.075) assigned to the value $\eta = 5.6$, which is the last non-zero value. Interestingly, a closer inspection of the payoff matrix shows that all the strategies above this values are dominated strategies; hence, reasonably, the defender never plays them (assigning them a 0 probability). This is quite expected since for larger η it is unlikely that an observation falls outside the range $[-\eta, \eta]$ and then the 'censoring' does not significantly affect the 'honest' measurements (i.e. $\mathcal{R} = \mathcal{N}$ with very high probability). When this is the case, it is clear that it is better for D to choose η small, thus increasing the probability of removing the corrupted measurements.

A possible explanation for the peaked behavior is the following. When η decreases, D starts removing good measurements which fall in the tail of the Gaussian under the corresponding hypothesis, whose values are not limited to Δ, but can take arbitrarily large values. Depending also on the setup considered, it may happen that the positive contribution they give to the correct decision is more relevant than the negative contribution given by the values introduced by A. When this is the case, it is better for the defender to use all the measurements. Therefore, the behavior of the defender at the equilibrium has a twofold purpose: trying to remove the corrupted measurements on one side (by choosing η one step ahead of Δ) and avoiding to rule out the large good measurements on the other (by selecting the critical η). The error probability at the equilibrium is 0.0176 thus showing that the proposed scheme allows to get correct detection with high probability despite the data corruption performed by A.

Figure 4 shows the equilibrium strategies for $\alpha = 0.2$. Since the removal of the large good measurements has more impact when α is large, a bit higher weight is associated in this case to the peak. The error probability at the equilibrium is

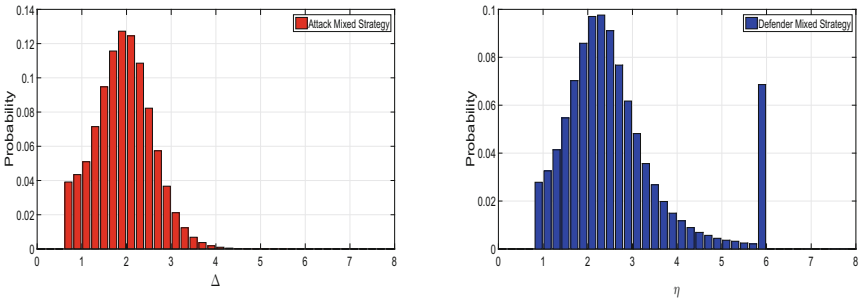


Fig. 5. Equilibrium strategies in the following setup: $N = 50$, $\alpha = 0.2$, $\mu = 2$ (SNR = 4). Payoff at the equilibrium $v = 0.0556$.

$v = 0.1097$. Finally, Fig. 5 shows the equilibrium mixed strategies for D and A when $N = 50$, $\alpha = 0.2$ and $\mu = 2$.

7 Conclusion

We proposed a consensus algorithm based on censored data which is robust to measurement falsification attacks. Besides, we formalized the interplay between the attacker and the network in a game-theoretic sense, and we numerically derive the optimal strategies for both players and the achievable performance in terms of error probability in different setups. Simulation results show that, by adopting the proposed scheme, the network can still achieve correct detection through consensus, despite the presence of corrupted measurements.

As a future work, we would like to extend the game-theoretic approach to include the graph disconnection as a part of the defender payoff and then apply our analysis to general topologies. In addition, we would like to extend the analysis to more complicated statistical models for the measurements, e.g. the case of the chi-square distribution, and to consider more complicated versions of the game, e.g. by allowing the players to adopt randomized strategies.

References

1. Varshney, P.K., Burrus, C.S.: Distributed Detection and Data Fusion. Springer, New York (1997)
2. Olfati-Saber, R., Fax, J.A., Murray, R.M.: Consensus and cooperation in networked multi-agent systems. Proc. IEEE **95**, 215–233 (2007)
3. Sardellitti, S., Barbarossa, S., Swami, A.: Optimal topology control and power allocation for minimum energy consumption in consensus networks. IEEE Trans. Signal Process. **60**, 383–399 (2012)
4. Li, Z., Yu, F., Huang, M.: A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios. IEEE Trans. Veh. Technol. **59**, 383–393 (2010)
5. Mossel, E., Schoenebeck, G.: Reaching consensus on social networks. In: Innovations in Computer Science, pp. 214–229 (2010)
6. Chen, R., Park, J.-M., Reed, J.: Defense against primary user emulation attacks in cognitive radio networks. IEEE J. Sel. Areas Commun. **26**, 25–37 (2008)
7. Chen, R., Park, J.-M., Bian, K.: Robust distributed spectrum sensing in cognitive radio networks. In: 2008 IEEE Proceedings INFOCOM - The 27th Conference on Computer Communications (2008). doi:10.1109/infocom.2007.251
8. Sundaram, S., Hadjicostis, C.N.: Distributed function calculation via linear iterative strategies in the presence of malicious agents. IEEE Trans. Autom. control **56**, 1495–1508 (2011)
9. Pasqualetti, F., Dorfler, F., Bullo, F.: Attack detection and identification in cyber-physical systems. IEEE Trans. Autom. Control **58**, 2715–2729 (2013)
10. Leblanc, H.J., Zhang, H., Koutsoukos, X., Sundaram, S.: Resilient asymptotic consensus in robust networks. IEEE J. Sel. Areas Commun. **31**, 766–781 (2013)
11. Vaidya, N.H., Tseng, L., Liang, G.: Iterative approximate Byzantine consensus in arbitrary directed graphs. In: Proceedings of the 2012 ACM Symposium on Principles of Distributed Computing - PODC 2012 (2012). doi:10.1145/2332432.2332505

12. Barni, M., Tondi, B.: Multiple-observation hypothesis testing under adversarial conditions (2013). doi:10.1109/wifs.2013.6707800
13. Abrardo, A., Barni, M., Kallas, K., Tondi, B.: A game-theoretic framework for optimum decision fusion in the presence of Byzantines. IEEE Trans. Inf. Forensics Secur. **11**, 1333–1345 (2016)
14. Abrardo, A., Barni, M., Kallas, K., Tondi, B.: A game-theoretic approach. In: 53rd IEEE Conference on Decision and Control. doi:10.1109/cdc.2014.7039431
15. Rawat, A.S., Anand, P., Chen, H., Varshney, P.K.: Collaborative Spectrum sensing in the presence of Byzantine attacks in cognitive radio networks. IEEE Trans. Signal Process. **59**, 774–786 (2011)
16. Yu, F.R., Tang, H., Huang, M., Li, Z., Mason, P.C.: Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios. In: 2009 IEEE Military Communications Conference (MILCOM) (2009). doi:10.1109/milcom.2009.5379832
17. Liu, S., Zhu, H., Li, S., Li, X., Chen, C., Guan, X.: An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum sensing. In: 2012 IEEE Global Communications Conference (GLOBECOM) (2012). doi:10.1109/glocom.2012.6503179
18. Yan, Q., Li, M., Jiang, T., Lou, W., Hou, Y.T.: Vulnerability, protection for distributed consensus-based spectrum sensing in cognitive radio networks. In: 2012 Proceedings of IEEE International Conference on Computer Communications (INFOCOM) (2012). doi:10.1109/infcom.2012.6195839
19. Barni, M., Pérez-González, F.: Advances in adversary-aware signal processing. In: 2013 IEEE International Conference on Acoustics, Speech and Signal Processing (2013). doi:10.1109/icassp.6639361
20. Godsil, C.D., Royle, G.: Algebraic Graph Theory. Springer, New York (2001)
21. Helsel, D.R., et al.: Nondetects and Data Analysis. Statistics for Censored Environmental Data. Wiley-Interscience, Hoboken (2005)
22. Bollobás, B.: Modern Graph Theory. Springer, New York (2013)
23. Jamakovic, A., Uhlig, S.: On the relationship between the algebraic connectivity and graph's robustness to node and link failures. In: 3rd EuroNGI Conference on Next Generation Internet Networks, Trondheim, pp. 96–102 (2007). doi:10.1109/NGI.2007.371203
24. Bollobás, B.: Random Graphs. Cambridge University Press, Cambridge (2001)
25. Watts, D.J., Strogatz, S.H.: Collective dynamics of 'small-world' networks. Nature **393**(1998), 440–442 (1998)
26. Barabási, A.: Emergence of scaling in random networks. Science **286**, 509512 (1999)
27. Osborne, M.J., Rubinstein, A.: A Course in Game Theory. MIT Press, Cambridge (1994)