Rosas *et al. Comput Soc Netw* (2018) 5:10
https://doi.org/10.1186/s40649-018-0057-7

Computational Social Networks

RESEARCH Open Access

Social learning for resilient data fusion against data falsification attacks

Fernando Rosas[1,2*], Kwang-Cheng Chen[3] and Deniz Gündüz[2]

*Correspondence:
f.rosas@imperial.ac.uk
[1] Centre of Complexity Science and Department of Mathematics, Imperial College London, Kensington, London SW72AZ, UK
Full list of author information is available at the end of the article

Abstract

Background: Internet of Things (IoT) suffers from vulnerable sensor nodes, which are likely to endure data falsification attacks following physical or cyber capture. Moreover, centralized decision-making and data fusion turn decision points into single points of failure, which are likely to be exploited by smart attackers.

Methods: To tackle this serious security threat, we propose a novel scheme for enabling distributed decision-making and data aggregation through the whole network. Sensor nodes in our scheme act following social learning principles, resembling agents within a social network.

Results: We analytically examine under which conditions local actions of individual agents can propagate through the network, clarifying the effect of Byzantine nodes that inject false information. Moreover, we show how our proposed algorithm can guarantee high network performance, even for cases when a significant portion of the nodes have been compromised by an adversary.

Conclusions: Our results suggest that social learning principles are well suited for designing robust IoT sensor networks and enabling resilience against data falsification attacks.

Keywords: Distributed decision-making, Data fusion, Sensor networks, Social networks, Data falsification attacks, Byzantine nodes, Collective behaviour, Multi-agent systems, Social learning, Information cascades

Background

Motivation

Internet of Things (IoT) is expected to play a central role in future digital society. However, to fully adopt this technology, it is crucial to guarantee its security, specially for public utilities whose safety is essential for the well-being of our society [1]. Recent cyber-attacks that created significant damage have been widely reported, e.g. the self-propagating malware *WannaCry* that caused a infamous worldwide network hack in May 2017 [2]. Developing technologies that can guarantee the safety of large information networks, such as IoT, is a challenging but urgent need. As information networks get more closely intertwined within our daily lives, ensuring their security and thus safety is becoming an even more challenging issue.

As the level of security is typically determined by the weakest link, a major dilemma of IoT security lies in the low-complexity sensor networks that are located at the network edge. These sensor networks are usually composed by a large number of autonomous

electronic devices, which collect critical information for the control and operation of IoT [3, 4]. By monitoring extensive geographical areas, these networks can enable a wide range of services to society, becoming a key element for the well-being of future smart cities [5, 6]. These networks may also perform sensitive tasks, including the surveillance over military or secure zones, intrusion detection to private property, monitoring of drinkable water tanks and protection from chemical attacks [7, 8].

Although the design of secure wireless sensor networks have been widely studied (e.g. [9–11] and references therein), there remain many open problems of both theoretical and engineering nature [12]. In particular, as the number of sensors is usually very large, precise management of them is challenging or even infeasible. A significant portion of the sensors might be deployed in unprotected areas, where it is impossible to ensure their physical or cyber security (e.g. war zones, or regions easily accessed by adversaries). Furthermore, sensor nodes are generally not tamper-proof due to cost restrictions, and have limited computing and networking capabilities. Therefore, they may not be capable of employing complex cryptographic or security protocols.

The vulnerability of sensor nodes makes them potential victims of cyber/physical attacks driven by intelligent adversaries. Attacks to information networks are usually categorized into *outsider attacks* and *insider attacks*. Outsider attacks include (distributed) denial of service (DoS) attacks, which use the broadcasting nature for wireless communications to disrupt the communications capabilities [10]. In contrast, in insider attacks the adversary "recruits" sensor nodes by malware through cyber/wireless means, or directly by physical substitution [13]. Following the classical *Byzantine generals problem* [14], these "Byzantine nodes" are authenticated, and recognized as valid members of the network. Byzantine nodes can hence generate false data, exhibit arbitrary behaviour, and collude with others to create network malfunctions. In general, insider attacks are considered to be more potentially harmful to information networks than outside attacks.

The effect of Byzantine nodes and data falsification over distributed sensor networks has been intensely studied; the impact over the network performance has been characterized, and various defense mechanisms has been proposed (c.f. [15] for an overview, and also [16–20] for some recent contributions). However, all these works focus on networks with star or tree topology, and rely on centralizing the decision-making in special nodes, called "fusion centers" (FCs), which gather all the sensed data. Therefore, a key element in these approaches is a strong division of labour: ordinary sensor nodes merely sense and forward data, while the processing is done exclusively at the FC corresponding to a *distributed-sensing/centralized-processing* approach. This literature implicitly assume that the FCs are capable of executing secure coding and protocols, and hence, are out of the reach of attackers. However, large information networks might require another kind of mediator devices, known as data aggregators (DAs), which have the capability to access the cloud through high-bandwidth communication links [21]. DAs are attractive targets for insider attacks, as they might also be located in unsafe locations due to the limited range of sensor node radios. Please note that a tampered DA can completely disable the sensing capabilities of all the nodes whose information has been aggregated, generating a single point of failure that is likely to be exploited by smart adversaries [22].

An attractive route to address this issue is to consider *distributed-sensing/distributed-processing* schemes, which avoid centralized decision-making by distributing processing

tasks throughout the network [23]. However, the design of practical distributed-sensing/distributed-processing schemes is a challenging task, as collective computation phenomena usually exhibit highly non-trivial features [24, 25]. In effect, even though the distributed-sensing literature is vast (for classic references c.f. [26–28], and more modern surveys see [3, 4, 29, 30]), the construction of optimal distributed schemes is in general NP-hard [31]. Moreover, although in many scenarios the optimal schemes can be characterized as a set of thresholds for likelihood functions, the determination of these thresholds is usually an intractable problem [26]. For example, homogeneous thresholds can be suboptimal even for networks with similar sensors arranged in star topology [32], being only asymptotically optimal in the network size [33]. Moreover, symmetric strategies are not suitable for more complicated network topologies, requiring heuristic methods.

Distributed decision-making and social learning

In parallel, significant research efforts have been dedicated to analysing *social learning*, which refers to the decision-making processes that take place within social networks [34]. In these scenarios, agents make decisions based on two elements: private information that represents agent's personal knowledge, and social information derived from previous decisions made by the agent's peers [35].

Social learning has been investigated in pioneering works that study sequential decision-making of Bayesian agents over simple social network structures [36, 37]. These models showed how, thanks to social interactions, individuals with weak private signals can harvest information from the decisions of other agents [38]. Interestingly, it was also found that aggregation of rational decisions through *information cascades* could generate suboptimal collective responses, degrading the "wisdom of the crowds" into mere herd behaviour. After these initial findings, researchers have aimed at developing a deeper understanding of information cascades extending the original models by considering more general cost metrics [39–41], and by studying the effects of the network topology on the aggregated behaviour [42–45]. Non-Bayesian learning models have also been explored, where agents use simple rule-of-thumb methods to exchange information [46–52].

Social learning plays a crucial role in many important social phenomena, e.g. in the adoption or rejection of new technology, or in the formation of political opinions [34]. Social learning models are particularly interesting for studying information cascades and herd dynamics, which arises when the social information pushes all the subsequent agents to ignore their own personal knowledge and adopt a homogeneous behaviour [37]. Moreover, there have been a renewed interest in understanding information cascades in the context of e-commerce and digital society [45]. For example, information cascades might have tremendous consequences in online stores where customers can see the opinions of previous customers before deciding to buy a product, or in the emergence of viral media contents based on sequential actions of "like" or "dislike". Therefore, developing a deep understanding of the mechanics behind information cascades, and how they impact social learning, is fundamental for our modern networked society.

The main motivation behind this article is to explore the connections between social learning and secure sensor networks, building a bridge between the research done separately by economists and sociologist on one side and electrical engineers and computer scientists on the other. A key insight for establishing this connection is to realize that

Table 1 Table of correspondances between distributed detection in sensor networks and social learning in social networks

Distributed detection	Social learning
Sensor node	Social agent
Communication range	Social neighbourhood
Environmental variables	State of the world
Noisy measurement	Private information
Local processing	Agent's decision
Bandwidth constraints	Decision sharing

each agent's decision corresponds to a compressed description of his/her private information. Therefore, the fact that agents cannot access the private information of others, but can only observe their decisions, can be understood as a constraint on the communication resources. In this way, social learning can be regarded as an information network that performs distributed inference under communication constraints (see Table 1). Moreover, it would be natural to use social learning principles in the design of distributed-sensing/distributed-processing schemes, with the hope that this might enable additional robustness to decision-making processes in sensor networks.

Contributions

In contrast to almost all the existing research, this work considers powerful topology-aware data falsification attacks, where the adversary knows the network topology and leverages this knowledge to take control of the most critical nodes of the network—either regular nodes, DAs or FCs. This represents a worst-case scenario where the network structure has been disclosed or inferred through network tomography via traffic analysis [53]. The reason why this adversary model has not been popular in the literature might be because traditional distributed-sensing schemes do not offer any resistance against this kind of attack.

This works presents a distributed-sensing/distributed-processing scheme for sensor networks that uses social learning principles in order to deal with a topology-aware adversary. The scheme is a threshold-based data fusion strategy, related to those considered in [26]. However, its relationship with social decision-making allows an intuitive understanding of its mechanisms. For avoiding security threats introduced by FCs, our scheme adopt tandem or serial decision sequencing [27, 54–57]. It is noted that, contrasting with some related literature, our analysis does not focus on optimality aspects of data fusion, but aims to illustrate how distributed decision-making can enable network resilience against powerful topology-aware data falsification attacks. We demonstrate how network resilience hold even when a significant number of nodes have been compromised.

Our work exploits a positive effect of information cascades that have been overlooked before: information cascades make a large number of agents/nodes to hold equally qualified estimators, generating many locations where a network operator can collect aggregated data. Therefore, information cascades are crucial in our solution for avoiding single points of failure. For enabling a better understanding of information cascades,

this work extends results presented in [58] providing a mathematical characterization of information cascades under data falsification attacks. In particular, our results clarify the conditions upon which local actions of individual agents can propagate across the network, compromising the collective performance. These results provide a first step towards the clarification of these non-trivial social dynamics, enriching our understanding of decision-making processes in biased social networks.

This paper expands the ideas presented in [59] by developing a formalism that allows considering incomplete or imperfect social information. This formalism is used to overcome the strongest limitation of the scheme presented in [59], namely the fact that each node was required to overhear and store all the previous transmissions in the network. Clearly this cannot take place in a large sensor network, due both to the storage constraints of the nodes, and to the large energy consumption required to transmit and receive across all pairs of nodes [60]. Therefore, this research presents an important step towards practical applications.

The rest of this article is structured as follows: "System model and problem statement" section introduces the system model, describing the network controller and the adversary behaviour. Our social learning data fusion scheme is then described in "Social learning as a data aggregation scheme" section, where some basic statistical properties are explored, and a practical algorithm for implementing the decision rule is derived. "Information cascade" section analyses the mathematical properties of the decision process, providing a geometrical description and a characterization of information cascades. All these ideas are then illustrated in a concrete scenario in "Proof of concept" section. Finally, "Conclusions" section summarizes our main conclusions.

Notation: uppercase letters are used to denote random variables, i.e. X, and lowercase letters their realizations, e.g. x. Boldface letters $\boldsymbol{X}$ and $\boldsymbol{x}$ represent random vectors and their realizations, respectively. Also, $\mathbb{P}_w\{X = x|Y = y\} = \mathbb{P}\{X = x|Y = y, W = w\}$ is used as a shorthand notation. A table summarizing the symbols and notation used through this article can be found in Appendix D.

System model and problem statement

System model

We consider a sensor network of N nodes, each corresponding to an information-processing device that has been deployed in an area of interest. Each node is equipped with sensory equipment to track variables of interest following a scheduled duty cycle. The measurement of the n-th sensor node is denoted by S_n, taking values over a set $\mathcal{S} \subset \mathbb{R}$ that can be discrete or continuous.[1] Based on these signals, the network needs to infer the value of an underlying binary variable W.

We consider networks where all the nodes have equal sensing capabilities, that is, the signals S_n are assumed to be identically distributed. Unfortunately, the general distributed detection problem for arbitrarily correlated signals is known to be NP-hard [31]. Hence,

[1] The generalization of our framework and results to vector-valued sensor outputs is straightforward.

for the sake of tractability, it is assumed that the variables $S_1, \ldots, S_N$ are conditionally independent given the event $\{W = w\}$, [2] following a probability distribution denoted by μ_w. It is also assumed that both μ_0 and μ_1 are absolutely continuous with respect to each other [67], i.e. no particular signal determines W unequivocally. This property guarantees that the log-likelihood ratio of these two distributions is always well defined, being given by the logarithm of the corresponding Radon–Nikodym derivative[3] $\Lambda_S(s) = \log \frac{d\mu_1}{d\mu_0}(s)$.

In addition to sensing hardware, each node is equipped with limited computing capability and a radio to wirelessly transit and receive data. Two nodes in the network are assumed to be connected if they can exchange information wirelessly. Note that, sensor nodes usually have a very limited battery budget, which imposes severe restrictions on their communication capabilities [68]. Therefore, it is assumed that each node forwards its data to others only by broadcasting a binary variable X_n. These simple signals do not impose an additional burden on the communication resources, as they could be appended to existent wireless control packages and viceversa, or could be shared by light, ultrasound or other alternative media.

We focus on the case in which the sensing capabilities of each sensor are limited, and hence, any inference about W made based only on the sensed data S_n cannot achieve a high accuracy. Interestingly, due to the nature of wireless broadcasting, nearby transmissions can be overheard and their information can be fused with what is extracted from the local sensor. The information that a node can extract from overhearing transmissions of other nodes is called "social information", contrasting with the "sensorial information" that is obtained from the sensed signal S_n.

Without loss of generality, nodes transmit their signals sequentially according to their indices (i.e. node 1 transmits first, then node 2, etc.).[4] It is assumed that this sequence is randomly chosen, and can be changed by the network operator at any time and be redistributed through the network (c.f. "The sensor network operator and the adversary" section). In general the broadcasted signals $X_1, \ldots, X_{n-1}$ might not be directly observable by the n-th agent because of various restrictions, including range limitations of the node's receiver radio [70], or the limited duty cycles imposed by battery restrictions [68]. Therefore, the social observations obtained by the n-th node are represented by $\boldsymbol{G}_n \in \mathcal{G}_n$, which can be a random scalar, vector, matrix or other mathematical object. Some cases of interest are as follows:

(i) The k previous decisions: $\boldsymbol{G}_n = (X_{n-k}, \ldots, X_{n-1})$.

(ii) The average value of all the previous decisions: $\boldsymbol{G}_n = \frac{1}{n-1}\sum_{k=1}^{n-1} X_k$.

(iii) The decisions of agents connected by an Erdös–Rényi random network with parameter $\xi \in [0, 1]$, i.e. $\boldsymbol{G}_n = (Z_1, \ldots, Z_{n-1}) \in \{0, 1, e\}^{n-1}$, where

$$Z_k = \begin{cases} X_k & \text{with probability } \xi, \\ e & \text{with probability } 1 - \xi. \end{cases} \tag{1}$$

[2] The conditional independence of sensor signals is satisfied when the sensor noise is due to local causes (e.g. thermal noise), but do not hold when there exist common noise sources (e.g. in the case of distributed acoustic sensors [61]). For works that consider sensor interdependence see [62–66].

[3] When S_n takes a finite number of values then $\frac{d\mu_1}{d\mu_0}(s) = \frac{\mathbb{P}\{S_n=s|W=1\}}{\mathbb{P}\{S_n=s|W=0\}}$, while if S_n is a continuous random variable with conditional p.d.f. $p(S_n|W = w)$ then $\frac{d\mu_1}{d\mu_0}(s) = \frac{p(s|W=1)}{p(s|W=0)}$.

[4] Note that the synchronization requirements of this procedure are low, so standard techniques can be used to keep the nodes' local clocks within the required synchronization constraints (see e.g. [69]).

Please note that the Erdös–Rényi model in (iii) has only been used as an illustrative example, and it can be easily generalized to consider the topology of any stochastic network of interest.

In this work, we study the social dynamics based on the properties of the transition probability from state $\boldsymbol{g'} \in \mathcal{G}_{n-1}$ to $\boldsymbol{g} \in \mathcal{G}_n$, as given by the conditional probabilities

$$\beta_w^n(\boldsymbol{g}|x_{n-1}, \boldsymbol{g'}) := \mathbb{P}_w\{\boldsymbol{G}_n = \boldsymbol{g}|X_{n-1} = x_{n-1}, \boldsymbol{G}_{n-1} = \boldsymbol{g'}\}, \tag{2}$$

where $x_{n-1} \in \{0, 1\}$. It is also assumed that the social dynamics are causal, meaning that $\boldsymbol{G}_n$ is conditionally independent of S_m given W for all $m \geq n$.

The sensor network operator and the adversary

The network is managed by a network operator, who is an external agent that uses the network as a tool to build an estimate of W. The network operator is opposed by an adversary, whose goal is to disrupt the inference capabilities of the network. For this aim, the adversary controls a group of authenticated Byzantine nodes without being noticed by the network operator, which have been captured by malware through cyber/wireless means, or by physical substitution.

The overall performance of a network of N nodes is defined by the accuracy of the inference of the last node in the decision sequence. As the decision sequence is generated randomly by the network operator, every node is equally likely to be at the end of the decision sequence. It is further assumed that the adversary has no knowledge of the decision sequence, as it can be chosen at run-time and changed regularly. Therefore, as the adversary has no reason to target any particular node in the network, hence, it is reasonable to assume that the adversary captures nodes randomly. Byzantine nodes are, hence, assumed to be uniformly distributed over the network.

For simplicity, we model the strength of the attack with a single parameter p_b, which corresponds to the probability of a node being compromised.[5] Moreover, we assume that the capture probability does not depend on W. Hence, the number of Byzantine nodes, denoted by N^*, is a Binomial random variable with $\mathbb{E}\{N^*\} = p_\mathrm{b}N$. Due to the law of large numbers, $N^* \approx p_\mathrm{b}N$ for a large network, and hence, p_b is also the ratio of expected Byzantine nodes in the network, which is the traditional metric for attack strength used in the literature.

For enabling data processing and forwarding, the network operator defines a *strategy*, i.e. a data fusion scheme given by a collection of (possibly stochastic) functions $\{\pi_n\}_{n=1}^{\infty}$, such that $\pi_n : \mathcal{S} \times \mathcal{G}_n \to \{0, 1\}$ for all $n \in \mathbb{N}$. On the other hand, the adversary can freely set the values of the binary signals transmitted by Byzantine nodes. This can be modelled as a random mapping $C\colon \{0, 1\} \to \{0, 1\}$ that corrupts broadcasted signals. Therefore, the signal broadcasted by the n-th node is given by

$$X_n = \begin{cases} C(\pi_n(S_n, \boldsymbol{G}_n)) & \text{with probability } p_\mathrm{b}, \text{ and} \\ \pi_n(S_n, \boldsymbol{G}_n) & \text{otherwise.} \end{cases} \tag{3}$$

Furthermore, as broadcasted signals are binary, the corruption mapping $C(\cdot)$ can be characterized by the conditional probabilities $c_{0|0}$ and $c_{0|1}$, where $c_{i|j} = \mathbb{P}\{C(\pi) = i|\pi = j\}$.

[5] This attack model assumes implicitly that the capture of each node is an independent event. Extensions considering cyber-infection propagation properties are possible (c.f. [71]), being left for future studies.

The rest of this work focuses on the case in which the network operator can deduce the corruption function and can estimate the capture risk p_{b}. Then, the average network miss-detection and false alarm rates for an attack of intensity p_{b} are defined as

$$\mathbb{P}\{\mathrm{MD}; p_{\mathrm{b}}\} := \mathbb{P}_1\{\pi_N(S_N, \boldsymbol{G}_N) = 0\}, \quad \text{and} \tag{4}$$

$$\mathbb{P}\big\{\mathrm{FA}; p_{\mathrm{b}}\big\} := \mathbb{P}_0\{\pi_N(S_N, \boldsymbol{G}_N) = 1\}, \tag{5}$$

respectively (note that p_{b} implicitly affects the distribution of $\boldsymbol{G}_N$). The case in which these quantities are unknown can be addressed using the current framework with a min-max analysis, which is left for future studies.

Problem statement

Our goal is to develop a resilient strategy, in order to provide a reliable estimation of W even under a significant number of unidentified Byzantine nodes. Note that in most surveillance applications, miss-detections are more important than false alarms, being difficult to estimate the cost of the worst-case scenario. Therefore, the average network performance is evaluated following the Neyman–Pearson criteria, by setting an allowable false alarm rate α and focusing on reducing the miss-detection rate [72]. By denoting by $\mathcal{P}$ the set of all strategies, we have the following optimization problem:

$$\begin{array}{ll} \underset{\{\pi_n\}_{n=1}^{\infty} \in \mathcal{P}}{\text{minimize}} & \mathbb{P}\{\mathrm{MD}; p_{\mathrm{b}}\} \\ \text{subject to} & \mathbb{P}\{\mathrm{FP}; p_{\mathrm{b}}\} \leq \alpha. \end{array} \tag{6}$$

Finding an optimal solution to (6) is a formidable challenge, even for the simple case of networks with start topology and no Byzantine attacks (see [30, 73] and references therein). Therefore, our aim is to develop a sub-optimal strategy that enables resilience, while being suitable for implementation in sensor nodes with limited computational power.

Social learning as a data aggregation scheme

This section describes our proposed data fusion scheme, and explains its function against topology-aware data falsification attacks. In the sequel, "Data fusion rule" section describes and analyses the data fusion rule, then "Decision statistics" section derives basic properties of its statistics, and finally "An algorithm for computing the social log-likelihood" section presents a practical algorithm for its implementation.

Data fusion rule

Let us assume that each sensor node is a rational agent that tries to maximizes the profit of an inference within a social network. Rational agents follow *Bayesian strategies*,[6] which can be elegantly described by the following threshold-based decision rule [72, Chapt. 2]:

$$\frac{\mathbb{P}\{W = 1 | S_n, \boldsymbol{G}_n\}}{\mathbb{P}\{W = 0 | S_n, \boldsymbol{G}_n\}} \underset{\pi_n=1}{\overset{\pi_n=0}{\lessgtr}} \frac{u(0,0) - u(1,0)}{u(1,1) - u(0,1)}. \tag{7}$$

[6] Although Bayesian models are elegant and tractable, they assume agents act always rationally [74] and make strong assumptions on the knowledge agents have about posterior probabilities [49]. However, Bayesian models provide an important benchmark, not necessarily due to their accuracy but because they give an important reference point with which other models can be compared [35].

Above, $u(\pi_n, w)$ is a cost assigned to the decision π_n when $W = w$, which can be engineered in order to match the relevance of miss-detections and false alarms [72].

Let us find a simpler expression for the decision rule (7). Due to the causality constraint (c.f. "System model" section), $\boldsymbol{G}_n$ can only be influenced by $S_1, \ldots, S_{n-1}$; and therefore, it is conditionally independent of S_n given W. Using this conditional independence condition, one can find that

$$\frac{\mathbb{P}\{W = 1|S_n, \boldsymbol{G}_n\}}{\mathbb{P}\{W = 0|S_n, \boldsymbol{G}_n\}} = e^{\Lambda_S(S_n)+\Lambda_{\boldsymbol{G}_n}(\boldsymbol{G}_n)}, \tag{8}$$

where $\Lambda_S(S_n)$ is the log-likelihood ratio of S_n (c.f. "System model" section) and $\Lambda_{\boldsymbol{G}_n}(\boldsymbol{G}_n)$ is the log-likelihood ratio of $\boldsymbol{G}_n$. Then, using (8) one can re-write (7) as

$$\Lambda_S(S_n) + \Lambda_{\boldsymbol{G}_n}(\boldsymbol{G}_n) \underset{\pi_n=1}{\overset{\pi_n=0}{\lesseqgtr}} \tau_0, \tag{9}$$

where $\tau_0 = \log \frac{\mathbb{P}\{W=0\}}{\mathbb{P}\{W=1\}} + \log \frac{u(0,0)-u(1,0)}{u(1,1)-u(0,1)}$. In simple words, (9) states how the n-th node should fuse the private and social knowledge: the evidence is provided by the corresponding log-likelihood terms, which are then simply added and then compared against a fixed threshold.[7]

Further understanding of the above decision rule can be attained by studying it from the point of view of communication theory [58]. We first note that the decision is made not over the raw signal S_n but over the "decision signal" $\Lambda_S(S_n)$. Interestingly, the processing done by the function $\Lambda_S(\cdot)$ might serve for dimensionality reduction, as $\Lambda_S(S_n)$ is always a single number even though S_n may be a matrix or a high-dimensional vector. Due to their construction and the underlying assumptions over S_n (c.f. "System model" section), the variables $\Lambda_S(S_n)$ are identically distributed and conditionally independent given $W = w$. Moreover, by introducing the shorthand notation $\tau_n(\boldsymbol{G}_n) = \tau_0 - \Lambda_{\boldsymbol{G}_n}(\boldsymbol{G}_n)$, one can re-write (9) as

$$\Lambda_S(S_n) \underset{\pi_n=1}{\overset{\pi_n=0}{\lesseqgtr}} \tau_n(\boldsymbol{G}_n). \tag{10}$$

Therefore, the decision is made by comparing the decision signal with a decision threshold $\tau_n(\boldsymbol{G}_n)$, which can be efficiently computed using the algorithm proposed in "An algorithm for computing the social log-likelihood" section. Note that this represents a comparison between the sensed data, summarized by $\Lambda_S(S_n)$, and the social information carried by $\tau_n(\boldsymbol{G}_n)$.

Decision statistics

Let us find expressions for the probabilities of the actions of the n-th agent, first focusing on the case $n = 1$. Note that

$$\mathbb{P}_w\{\pi_1(S_1) = 0\} = \mathbb{P}_w\{\Lambda_S(S_1) < \tau_0\} = F_w^{\Lambda}(\tau_0), \tag{11}$$

[7] As the prior distribution of W is usually unknown, τ_0 is a free parameter of the scheme. Following the discussion in "Problem statement" section, the network operator shall select the lowest value of τ_0 that satisfies the required false alarm rate specified by the Neyman–Pearson criteria.

where $F_w^{\Lambda}(\cdot)$ is the c.d.f. of Λ_S conditioned on $W = w$. Then, considering the possibility that the first node could be a Byzantine node, one can show that

$$\begin{aligned}\mathbb{P}_w\{X_1 = 0\} &= p_{\mathrm{b}}\mathbb{P}_w\big\{X_1 = 0|\text{ Byzantine}\big\} + (1-p_{\mathrm{b}})\mathbb{P}_w\big\{X_1 = 0|\text{not a Byzantine}\big\} \\ &= p_{\mathrm{b}}(c_{0|0}F_w^{\Lambda}(\tau_0) + c_{0|1}[1 - F_w^{\Lambda}(\tau_0)]) + (1-p_{\mathrm{b}})F_w^{\Lambda}(\tau_0) \qquad (12)\\ &= z_0 + z_1 F_w^{\Lambda}(\tau_0), \qquad (13)\end{aligned}$$

where we are introducing $z_0 := p_{\mathrm{b}}c_{0|1}$ and $z_1 := 1 - p_{\mathrm{b}}(1 - c_{0|0} + c_{0|1})$ as short-hand notation, which are non-negative constants that summarize the strength of the adversary. In particular, when the adversary is powerless then $z_0 = 0$ and $z_1 = 1$, and hence $\mathbb{P}_w\{\pi_1(S_1) = 0\} = \mathbb{P}_w\{X_1 = 0\}$.

By considering the n-th node, one can find that

$$\begin{aligned}\mathbb{P}_w\big\{\pi_n(S_n, \boldsymbol{G}_n) = 0|\boldsymbol{G}_n = \boldsymbol{g}_n\big\} &= \int_{\mathcal{S}} \mathbb{P}_w\big\{\pi_n(s_n, \boldsymbol{g}_n) = 0|S_n = s\big\}\mu_w(s)\mathrm{d}s \\ &= \int_{\mathcal{S}} \mathbb{1}\big\{\pi_n(\boldsymbol{g}_n, s) = 0\big\}\mu_w(s)\mathrm{d}s \qquad (14)\end{aligned}$$

$$= \mathbb{P}_w\big\{\Lambda_S(s) < \tau_n(\boldsymbol{g}_n)\big\} \qquad (15)$$

$$= F_w^{\Lambda}(\tau_n(\boldsymbol{g}_n)). \qquad (16)$$

The first equality is a consequence of the fact that S_n is conditionally independent of $\boldsymbol{G}_n$ given $W = w$, while the second equality is a consequence that X_n can be expressed as a deterministic function of $\boldsymbol{G}_n$ and S_n, and hence, becomes conditionally independent of W. Above, (16) shows that τ_n is a sufficient statistic for predicting X_n with respect to $\boldsymbol{G}_n$. Note that $F_w^{\Lambda}(x)$ can be directly computed from the statistics of the distribution of S_n (c.f. Appendix A). Moreover, using (16) and following a similar derivation as in (12), one can conclude that

$$\mathbb{P}_w\big\{X_n = 0|\boldsymbol{G}_n = \boldsymbol{g}_n\big\} = z_0 + z_1 F_w^{\Lambda}(\tau_n(\boldsymbol{g}_n)). \qquad (17)$$

Let us now study the statistics of $\boldsymbol{G}_n$. By using the definition of the transition coefficients $\beta_w^n(\boldsymbol{g}_{n+1}|x_n, \boldsymbol{g}_n)$, one can find that

$$\mathbb{P}_w\big\{\boldsymbol{G}_{n+1} = \boldsymbol{g}_{n+1}\big\} = \sum_{\boldsymbol{g}_n \in \mathcal{G}_n} \sum_{x_n \in \{0,1\}} \beta_w^n(\boldsymbol{g}_{n+1}|x_n, \boldsymbol{g}_n)\mathbb{P}_w\big\{X_n = x_n, \boldsymbol{G}_n = \boldsymbol{g}_n\big\}. \qquad (18)$$

Note that, using the above derivations, the terms $\mathbb{P}_w\big\{X_n = x_n, \boldsymbol{G}_n = \boldsymbol{g}_n\big\}$ can be further expressed as

$$\begin{aligned}\mathbb{P}_w\big\{X_n = x_n, \boldsymbol{G}_n = \boldsymbol{g}_n\big\} &= \mathbb{P}_w\big\{X_n = x_n|\boldsymbol{G}_n = \boldsymbol{g}_n\big\}\mathbb{P}_w\big\{\boldsymbol{G}_n = \boldsymbol{g}_n\big\} \qquad (19)\\ &= \lambda(z_0 + z_1 F_w^{\Lambda}(\tau_n(\boldsymbol{g}_n)), x_n)\mathbb{P}_w\big\{\boldsymbol{G}_n = \boldsymbol{g}_n\big\}, \qquad (20)\end{aligned}$$

where $\lambda(p, x) = x(1-p) + (1-x)p$. Therefore, a closed form expression can be found for (18) recursively over $\boldsymbol{G}_n$.

An algorithm for computing the social log-likelihood

The main challenge for implementing (9) as a data processing method in a sensor node is to have an efficient algorithm for computing $\tau_n(\boldsymbol{g}_n)$. Leveraging the above derivations, we develop Algorithm 1 as an iterative procedure for computing τ_n.

Algorithm 1 Computation of the decision threshold

function COMPUTE_TAU($N, F_0^\Lambda(\cdot), F_1^\Lambda(\cdot), \beta_w^n(\cdot|\cdot,\cdot), \tau_0, z_0, z_1$)
  $\tau_1 = \tau_0$
  for $x_1 \in \{0,1\}$ **do**
    $\mathbb{P}_0\{X_1 = x_1, \boldsymbol{G}_1 = 0\} = \lambda(z_0 + z_1 F_0^\Lambda(\tau_1), x_1)$
    $\mathbb{P}_1\{X_1 = x_1, \boldsymbol{G}_1 = 0\} = \lambda(z_0 + z_1 F_1^\Lambda(\tau_1), x_1)$
  for $n = 1, \ldots, N-1$ **do**
    for $\forall \boldsymbol{g} \in \mathcal{G}_{n+1}$ **do**
      $\mathbb{P}_0\{\boldsymbol{G}_{n+1} = \boldsymbol{g}\} = \sum_{\boldsymbol{g}_n \in \mathcal{G}_n} \sum_{x_n \in \{0,1\}} \beta_0^n(\boldsymbol{g}_{n+1}|x_n, \boldsymbol{g}_n) \mathbb{P}_0\{X_n = x_n, \boldsymbol{G}_n = \boldsymbol{g}_n\}$
      $\mathbb{P}_1\{\boldsymbol{G}_{n+1} = \boldsymbol{g}\} = \sum_{\boldsymbol{g}_n \in \mathcal{G}_n} \sum_{x_n \in \{0,1\}} \beta_1^n(\boldsymbol{g}_{n+1}|x_n, \boldsymbol{g}_n) \mathbb{P}_1\{X_n = x_n, \boldsymbol{G}_n = \boldsymbol{g}_n\}$
      $\Lambda_{\boldsymbol{G}_n}(\boldsymbol{g}) = \log \frac{\mathbb{P}_1\{\boldsymbol{G}_n = \boldsymbol{g}\}}{\mathbb{P}_0\{\boldsymbol{G}_n = \boldsymbol{g}\}}$
      $\tau_n(\boldsymbol{g}) = \tau_0 - \Lambda_{\boldsymbol{G}_n}(\boldsymbol{g})$
      for $x_{n+1} \in \{0,1\}$ **do**
        $\mathbb{P}_0\{X_{n+1} = x_{n+1}, \boldsymbol{G}_{n+1} = \boldsymbol{g}\} = \lambda(z_0 + z_1 F_0^\Lambda(\tau_n(\boldsymbol{g}_n)), x_{n+1}) \mathbb{P}_0\{\boldsymbol{G}_{n+1} = \boldsymbol{g}\}$
        $\mathbb{P}_1\{X_{n+1} = x_{n+1}, \boldsymbol{G}_{n+1} = \boldsymbol{g}\} = \lambda(z_0 + z_1 F_1^\Lambda(\tau_n(\boldsymbol{g}_n)), x_{n+1}) \mathbb{P}_1\{\boldsymbol{G}_{n+1} = \boldsymbol{g}\}$
  return $\tau_N(\cdot)$

The inputs of Algorithm 1 can be classified into two groups. First, the terms $N, F_0^\Lambda(\cdot), F_1^\Lambda(\cdot), \beta_w^n(\cdot|\cdot,\cdot)$ are properties of the network (position of the node within the decision sequence, sensor statistics and social observability, respectively) that the network operator could measure. On the other hand, τ_0, z_0, z_1 are properties of the adversary profile that depend on the prior statistics of W, the rate of compromised nodes p_b and the corruption function defined by $c_{0|0}$ and $c_{0|1}$ (c.f. "The sensor network operator and the adversary" section). In most scenarios, the knowledge of the network controller about these quantities is limited, as attacks are rare and might follow unpredictable patterns. Limited knowledge can still be exploited using e.g. Bayesian estimation techniques [75]. If no knowledge is available for the network controller, then these quantities can be considered free parameters of the strategy that span a range of alternative balances between miss-detections and false positives, i.e. a receiver operating characteristic (ROC) space.

Algorithm 1 initialises from the initial decision threshold τ_0, and explores all the relevant scenarios iteratively in order to build estimations of the likelihood functions that are required to compute τ_N. The computation of the terms $\mathbb{P}_w\{\boldsymbol{G}_n = \boldsymbol{g}\}$ is done following (18), while the ones involving $\mathbb{P}_w\{X_n = x_n, \boldsymbol{G}_n = \boldsymbol{g}\}$ follow (20). Please note that the algorithm's complexity scales gracefully for many cases of interest. For the particular case of nodes with memory of length k (i.e. $\boldsymbol{G}_n = (X_{n-k-1}, \ldots, X_{n-1})$), the complexity of Algorithm 1 is $\mathcal{O}(2^k N)$, and therefore grows linearly with the size of the network, while being limited in the values of k that one can consider. In general, the algorithm complexity scales linearly with N as long as the cardinality of $\mathcal{G}_n$ are bounded, or if a significant portion of the terms $\beta_w^n(\boldsymbol{g}_{n+1}|x_n, \boldsymbol{g}_n)$ are zero.

Information cascade

The term "social learning" refers to the fact that $\pi_n(S_n, \boldsymbol{G}_n)$ becomes a better predictor of W as n grows; and hence, larger networks tend to develop a more accurate inference. However, as the number of shared signals grows, the corresponding "social pressure" can make nodes to ignore their individual measurements to blindly follow the dominant choice, triggering a cascade of homogeneous behaviour. It is our interest to clarify the role of the social pressure in the decision-making of the agents involved in a social network, as information cascades can introduce severe limitations in the asymptotic performance of social learning [44].

Moreover, an adversary can leverage the information cascade phenomenon. In effect, if the number of Byzantine nodes N^* is large enough then a misleading information cascade can be triggered almost surely, making the learning process to fail. However, if N^* is not enough then the network may undo the pool of wrong opinions and end up triggering a correct cascade.

In the sequel, the effect of information cascades is first studied in individual nodes in "Local information cascades" section. Then, the propagation properties of cascades are explored in "Social information dynamics and global cascades" section.

Local information cascades

In general, the decision $\pi_n(S_n, \boldsymbol{G}_n)$ is made based on the evidence provided by both S_n and $\boldsymbol{G}_n$. A *local cascade* takes place in the n-th agent when the information conveyed by S_n is ignored in the decision-making process due to a dominant influence of $\boldsymbol{G}_n$. We use the term "local" to emphasize that this event is related to the data fusion of an individual agent. This idea is formalized in the following definition using the notion of conditional mutual information [76], denoted as $I(\cdot;\cdot|\cdot)$.

Definition 1 The social information $\boldsymbol{g}_n \in \mathcal{G}_n$ generates a *local information cascade* for the n-th agent if $I(\pi_n; S_n|\boldsymbol{G}_n = \boldsymbol{g}_n) = 0$.

The above condition summarizes two possibilities: either π_n is a deterministic function of $\boldsymbol{G}_n$, and hence there is no variability in π_n once $\boldsymbol{G}_n$ has been determined; or there is still variability (i.e. π_n is a stochastic strategy) but it is conditionally independent of S_n. In both cases, the above formulation highlights the fact that the decision π_n contains no information coming from S_n. [8]

Lemma 1 *The variables $\boldsymbol{G}_n \to \tau_n \to \pi_n$ form a Markov Chain (i.e. τ_n is a sufficient statistic of $\boldsymbol{G}_n$ for predicting the decision π_n)*

Proof Using (16) one can find that

$$\mathbb{P}_w\{\pi_n|\tau_n, \boldsymbol{G}_n\} = \lambda(F_w^{\Lambda}(\tau_n), X_n) = \mathbb{P}_w\{\pi_n|\tau_n\},$$

[8] Recall that S_n and $\boldsymbol{G}_n$ are conditionally independent given $W = w$ (c.f. "Data fusion rule" section), and hence there cannot be redundant information about W that is conveyed by S_n and also $\boldsymbol{G}_n$. For a more detailed discussion about redundant information c.f. [77].

and therefore the conditional independency of π_n and $\boldsymbol{G}_n$ given τ_n is clear. □

Let us now introduce the notation $U_s = \operatorname{ess\,sup}_{s\in\mathcal{S}} \Lambda_S(S_n = s)$ and $L_s = \operatorname{ess\,inf}_{s\in\mathcal{S}} \Lambda_S(S_n = s)$ for the essential supremum and infimum of $\Lambda_S(S_n)$, being the signals within $\mathcal{S}$ that most strongly support the hypothesis $\{W = 1\}$ over $\{W = 0\}$ and vice versa.[9] If one of these quantities diverge, this would imply that there are signals $s \in \mathcal{S}$ that provide overwhelming evidence in favour of one of the competing hypotheses. If both are finite then the agents are said to have *bounded beliefs* [44]. As sensory signals of electronic devices are ultimately processed digitally, the number of different signals that an agent can obtain are finite, and hence their supremum is always finite. Therefore, in the sequel we assume that both L_s and U_s are finite. Using these notions, the following proposition provides a characterization for local information cascades.

Proposition 1 *The social information $\boldsymbol{g}_n \in \mathcal{G}_n$ triggers a local information cascade if and only if the agents have bounded beliefs and $\tau_n(\boldsymbol{g}_n) \notin [L_s, U_s]$.*

Proof Let us assume that the agents have bounded beliefs. From the definition of F_w^Λ, which is a cumulative density function, it is clear that if $\tau_n < L_s$ then $F_0^\Lambda(\tau_n) = F_1^\Lambda(\tau_n) = 0$, while if $\tau_n > U_s$ then $F_0^\Lambda(\tau_n) = F_1^\Lambda(\tau_n) = 1$. Therefore, if $\tau_n(\boldsymbol{g}_n) \notin [L_s, U_s]$ then, according to (16), it determines π_n almost surely, making π_n and S_n conditionally independent.

To prove the converse by contrapositive, let us assume that $L_s < \tau_n(\boldsymbol{g}_n) < U_s$. Using again (16) and the definition of U_s and L_s, one can conclude that this implies that $0 < \mathbb{P}_w\{\pi_n = 0|\boldsymbol{G}_n\} < 1$ for both $w \in \{0, 1\}$. This, in turn, implies that the sets $\mathcal{S}^0(\tau) = \{s \in \mathcal{S}|\Lambda_S(s) < \tau_n(\boldsymbol{G}_n\}$ and $\mathcal{S}^1(\tau) = \mathcal{S} - \mathcal{S}^0$ both have positive probability under μ_0 and μ_1, which in turn implies the existence of conditional interdependency between π_n and S_n in this case. □

Intuitively, Proposition 1 shows that a local information cascade happens when the social information goes above the most informative signal that could be sensed. Some consequences of this result are explored in the next section.

Social information dynamics and global cascades

It is of great interest to predict when a local information cascade could propagate across the network, disrupting the collective behaviour and hence affecting the network performance. The following definition captures how, during a "global information cascade", the broadcasted signals X_n do not convey information about the corresponding sensor signals anymore.

Definition 2 The social information $\boldsymbol{g}_n \in \mathcal{G}_n$ triggers a *global information cascade* if $I(X_m; S_m|\boldsymbol{G}_n = \boldsymbol{g}_n) = 0$ holds for all $m \geq n$.

[9] The essential supremum is the smallest upper bound over $\Lambda_S(S_n)$ that holds almost surely, being the natural measure-theoretic extension of the notion of supremum [78].

A global information cascade is a succession of local information cascades. As Proposition 1 showed that agents are free from local cascades as long as $\tau_n \in [L_s, U_s]$, one can guess that global cascades are related to the dynamics of τ_n. These dynamics are determined by the transitions of $\boldsymbol{G}_n$, which follows the behaviour dictated by the transition coefficients $\beta_w^n(\cdot|\cdot,\cdot)$. To further study the social information dynamics, we introduce the following definitions.

Definition 3 The collection $\{\boldsymbol{G}_n\}_{n=1}^{\infty}$ is said to have:

1. Strongly consistent transitions if, for any $W = w$, $\boldsymbol{g} \in \mathcal{G}_n$ and $\boldsymbol{g'} \in \mathcal{G}_{n-1}$, $\beta_w^n(\boldsymbol{g}|1,\boldsymbol{g'}) > 0$ implies $\tau_n(\boldsymbol{g}) \leq \tau_{n-1}(\boldsymbol{g'})$, while if $\beta_w^n(\boldsymbol{g}|0,\boldsymbol{g'}) > 0$ implies $\tau_n(\boldsymbol{g}) \geq \tau_{n-1}(\boldsymbol{g'})$.
2. Weakly consistent transitions if, for all $\boldsymbol{g} \in \mathcal{G}_n$ and $\boldsymbol{g'} \in \mathcal{G}_{n-1}$, $\tau_{n-1}(\boldsymbol{g'}) \leq L_s$ and $\mathbb{P}_w\{\boldsymbol{G}_n = g|\boldsymbol{G}_{n-1} = \boldsymbol{g'}\} > 0$ implies $\tau_n(\boldsymbol{g}) \leq L_s$, while $\tau_{n-1}(\boldsymbol{g'}) \geq U_s$ and $\mathbb{P}_w\{\boldsymbol{G}_n = \boldsymbol{g}|\boldsymbol{G}_{n-1} = \boldsymbol{g'}\} > 0$ implies $\tau_n(\boldsymbol{g}) \geq U_s$. [10]

Intuitively, strong consistency means that the decision threshold evolves monotonically with respect to the broadcasted signals X_n. Correspondingly, weak consistency implies that τ_n cannot return to the interval $[L_S, U_S]$ once it goes out of it. Moreover, the adjectives "strong" and "weak" reflect the fact that weak consistency only takes place outside the boundaries of the signal likelihood, while the strong consistency affects all the decision space. Moreover, strongly consistent transitions imply weakly consistent transitions when there are no Byzantine nodes, as shown in the next lemma.[11]

Lemma 2 *Strongly consistent transitions satisfy the weak consistency condition if* $p_{\mathrm{b}} = 0$.

Proof See Appendix B. □

Next, it is shown that if the evolution of $\boldsymbol{G}_n$ becomes deterministic and 1–1 after leaving the interval $[L_s, U_s]$ (henceforth called *weakly invertible transitions*), then it satisfies the weak consistency condition.

Lemma 3 *Weakly invertible transitions imply weakly consistent transitions.*

Proof See Appendix C. □

Now we present the main result of this section, which is the characterization of information cascades for the case of social information that follows weakly consistent transitions.

[10] Note that the condition $\mathbb{P}_w\{\boldsymbol{G}_n = \boldsymbol{g}|\boldsymbol{G}_{n-1} = \boldsymbol{g'}\} > 0$ is equivalent to either $\beta_w^n(\boldsymbol{g},|0,\boldsymbol{g'})$ or $\beta_w^n(\boldsymbol{g},|1,\boldsymbol{g'})$ being strictly positive.

[11] It is possible to build examples where weak consistency does not follow from strong consistency when $p_{\mathrm{b}} > 0$.

Theorem 1 *If the social information have weakly consistent transitions, then every local information cascade triggers a global information cascade.*

Proof Let us consider $\boldsymbol{g}_0 \in \mathcal{G}_n$ such that it produces a local cascade in the n-th node. Then, due to Proposition 1, this implies that $\tau_n(\boldsymbol{g}) \notin [L_s, U_s]$ almost surely. This, combined with the weak consistency assumption, implies that $\tau_{n+1}(\boldsymbol{G}_{n+1}) \notin [L_s, U_s]$ almost surely. A second application of Proposition 1 shows that $\mathbb{P}_w\{\pi = 0|\boldsymbol{G}_{n+1}\}$ is equal to 0 o 1. This, in turn, guarantees that $I(\pi_{n+1} : S_{n+1}|\boldsymbol{G}_n = \boldsymbol{g}) = 0$ almost surely, showing that the $(n+1)$-th node experiences a local information cascade because of $\boldsymbol{G}_n = \boldsymbol{g}_0$.

A recursive application of the above argument allows one to prove that $I(\pi_{n+m}; S_{n+m}|\boldsymbol{G}_n = \boldsymbol{g}) = 0$ for all $m \geq 0$, proving the existence of a global cascade. □

This theorem has a number of important consequences. Firstly, it provides an intuitive geometrical description about the nature of global cascades for networks with weak consistency. One can imagine the evolution of $\tau_n(\boldsymbol{G}_n)$ as function of n as a random walk within the interval $[L_s, U_s]$. Because of the weak consistency condition, if the random walk step out of the interval, it will never come back. Moreover, as a consequence of this theorem, the stepping out of $[L_s, U_s]$ is a necessary and sufficient condition to trigger a global information cascade over the network.

Also, note that when $G_n = \boldsymbol{X}^n$ (i.e. each node overhears all previous decision) one can prove that G_n has weakly invertible transitions. Therefore, Theorem 1 is a generalization of Theorem 1 of [58] to the case of a network with Byzantine nodes.

Proof of concept

This section illustrates the main results obtained in "Social learning as a data aggregation scheme" and "Information cascade" sections in a simple scenario. In the following, the scenario is described in "Scenario description" section, and numerical simulations are discussed in "Discussion" section.

Scenario description

Let us consider a sensor network that has surveillance duties over a sensitive geographical area. The sensitive area could correspond to a factory, a drinkable water container or a warzone, whose key variables need to be supervised. The task of the sensor network is, through the observation of these variables, to detect the events $\{W = 1\}$ and $\{W = 0\}$ that correspond to the presence or absence of an attack to the surveilled area, respectively. No knowledge about of the prior distribution of W is assumed.

We consider nodes that have been deployed randomly over the sensitive area, and hence their locations follow a Poisson point process (PPP). The ratio of the area of interest that falls within the range of each sensor is denoted by r. If attacks occur uniformly over the surveilled area, then r is also the probability of an attack taking place under the coverage area of a particular sensor. Note that, due to the limited sensing range, the miss-detection rate of individual nodes is roughly equal to $1 - r$. As r is usually a small number (5% in our simulations), this implies that each node is extremely unreliable without cooperation.

Each node measures its environment using a digital sensor of m levels dynamical range (i.e. $S_n \in \{0, 1, \ldots, m-1\}$). Under the absence of an attack, the measured signal is assumed to be normally distributed with a particular mean value and variance. For simplicity of the analysis, we assume that when conditioned in $\{W = 0\}$ the signal S_n is distributed following a binomial distribution of parameters (m, q), i.e.

$$\mathbb{P}_0\{S_n = s_n\} = \binom{m}{s_n} q^{s_n}(1-q)^{m-s_n} := f(s_n; m, q) \tag{21}$$

which, due to the central limit theorem, approximates a Gaussian variable when m is relatively large. Moreover, it is assumed that the sensor dynamical range is adapted to match the mean value on the lower third of the sensor dynamical range, i.e. $\mathbb{E}\{S_n | W = 0\} = m/3$. This naturally imposes the requirement $q = 1/3$.

Following standard statistical approaches, it is further assumed that the sensors observe the environment looking for anomalous events, i.e. when the measurement is larger than the mean value in more than two standard deviations. This may correspond, for example, to when a specific chemical compound trespasses safe concentration values, or when too much movement has been detected over a given time window (see e.g. [79]). Using the fact that $\mathrm{Var}\{S_n\} = mq(1-q)$, this gives a threshold $T = \mathbb{E}\{S_n\} + 2\sqrt{\mathrm{Var}\{S_n\}} = np + 2\sqrt{nq(1-q)}$. Therefore, it is assumed that an attack is related to the event of S_n being uniformly distributed in $[T, m]$. Therefore, one finds that

$$\begin{aligned}\mathbb{P}_1\{S_n = s_n\} &= (1-r)\mathbb{P}_1\{S_n = s_n | \text{attack out of range}\} + r\mathbb{P}_1\{S_n = s_n | \text{attack in range}\} \\ &= (1-r) f(s_n; m, q) + r\frac{H(s_n - T)}{m - T},\end{aligned} \tag{22}$$

where $H(x)$ is the discrete Heaviside (step) function given by

$$H(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{in other case.} \end{cases} \tag{23}$$

In summary, S_n conditioned on $\{W = 1\}$ is modelled as a mixture model between a Binomial and a truncated uniform distribution, where the relative weight between them is determined by r (c.f. Fig. 1, top). Finally, using (21) and (22), the log-likelihood function of the signal S_n can be determined as (see Fig. 1, bottom)

$$\Lambda_{S_n}(s_n) = \log \frac{\mathbb{P}_1\{S_n = s_n\}}{\mathbb{P}_0\{S_n = s_n\}} = \log\left\{(1-r) + \frac{rH(s_n - T)}{(m-T) f(s_n; m, q)}\right\}. \tag{24}$$

We are interested in studying how a restricted listening period affects the network performance. Restricted listening periods are usually mandatory for energy-limited IoT devices.[12] For simplicity of the analysis, we focus on scenarios in which a node can overhear the transmissions of all the other nodes, and hence the social information gathered

[12] It is well known that the wireless radios of small sensor nodes consume a similar amount of energy while transmitting or receiving data, and hence reducing overhearing periods is key for attaining energy efficiency, and hence long network lifetime [60].

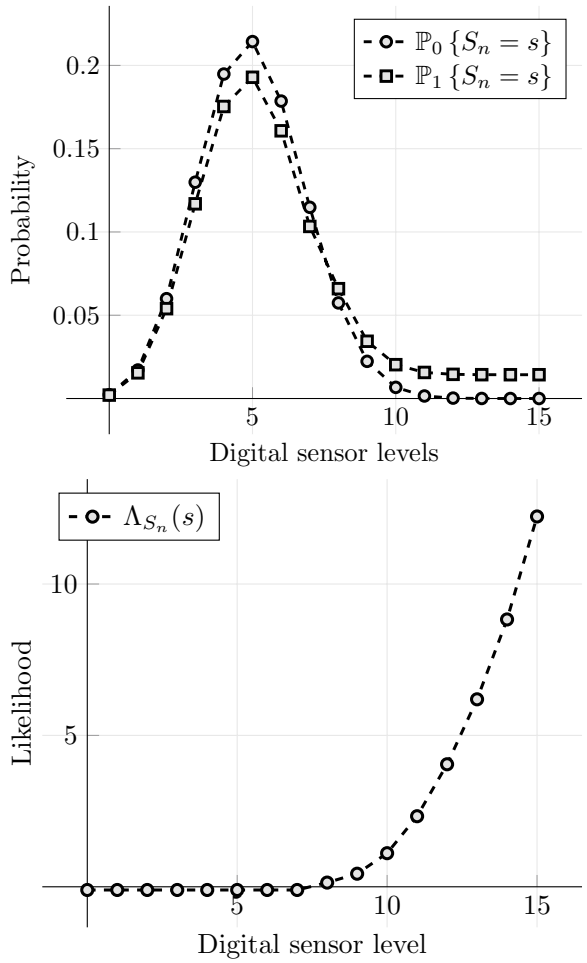

Fig. 1 Top: probability distribution for a digital sensor of $m = 16$ levels, conditioned on the events $\{W = 0\}$ and $\{W = 1\}$. Bottom: Log-likelihood of a digital signal of $m = 16$ levels with respect to the variable W

by the n-th node is $\boldsymbol{G}_n = (X_{n-k-1}, \ldots, X_{n-1})$ if $n > k$. Here k is a design parameter, whose impact on the network performance is studied in the next section.

Discussion

We analysed the performance of networks of $N = 300$ sensor nodes, each of which can monitor $r = 5\%$ of the target area. Using the definition given in (4) and (5), combined with (16), miss-detection and false alarm rates are computed as

$$\mathbb{P}\{\mathrm{MD}\} = \sum_{\boldsymbol{g}\in\mathcal{G}_n} F_1^{\Lambda}(\tau_n(\boldsymbol{g}))\mathbb{P}_1\{\boldsymbol{G}_n = \boldsymbol{g}\} \quad \text{and} \tag{25}$$

$$\mathbb{P}\{\mathrm{FA}\} = \sum_{\boldsymbol{g}\in\mathcal{G}_n} (1 - F_0^{\Lambda}(\tau_n(\boldsymbol{g})))\mathbb{P}_0\{\boldsymbol{G}_n = \boldsymbol{g}\}, \tag{26}$$

where the terms $\mathbb{P}_w\{\boldsymbol{G}_n = \boldsymbol{g}\}$ are computed using Algorithm 1 (c.f. "An algorithm for computing the social log-likelihood" section). In order to favour the reduction of miss-detections over false alarms $\tau_0 = 0$ is chosen, as it is the lowest value that still allows a

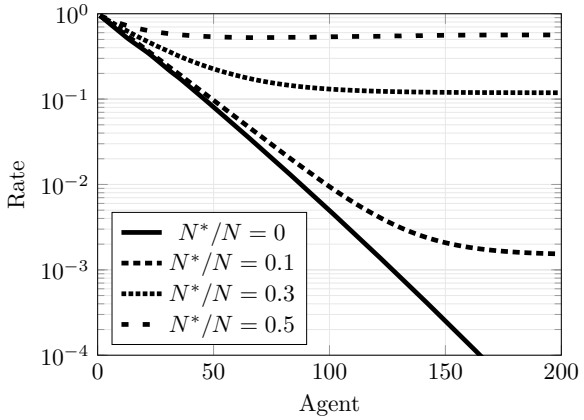

Fig. 2 Performance for the inference of each node for various attack intensities, given by the average ratio of Byzantine nodes $N^*/N = p_b$. Agents overhear the previous $k = 4$ broadcasted signals, and use sensors with dynamical range of $n = 64$

non-trivial inference process.[13] We consider an upper bound of 5% over the tolerable false alarm rate.

Simulations demonstrate that the proposed scheme enables strong network resilience in this scenario, allowing the sensor network to maintain a low miss-detection rate even in the presence of a large number of Byzantine nodes (see Fig. 2). Please recall that if a traditional distributed detection scheme based on centralized decision is used, a topology-aware attacker can cause a miss-detection rate of 100% by just compromising the few nodes that perform data aggregation [i.e. the FC(s)]. Figure 2 shows that nodes that individually would have a miss-detection rate of 95% can improve up to around 10% even when 30% of the nodes are under the control of the attacker. Therefore, by making all the nodes to aggregate data, the network can overcome the influence of Byzantine nodes, generating correct inferences even when a significant fraction of nodes have been compromised.

Please note that, for the case of data falsification attack illustrated by Fig. 2, the miss-detection rate improves until the network size reaches $N = 500$, achieving a performance of $\approx 10^{-12}$ (not shown in the Figure). This result has two important implications. First, this confirms the prediction of Theorem 1 that, if the signal log-likelihood is bounded, then information cascades are eventually dominant, hence stopping the learning process of the network (for a more detailed discussion about this issue please c.f. [58]). Secondly, this result stresses a key difference of our approach with respect to the existent literature about information cascades: *even if information cascades become dominant and perfect social learning cannot be achieved, the achieved performance can still be very high, and hence useful in a practical information-processing setup*.

The network resilience provided by our scheme is influenced by the sensor dynamical range, m, as a higher sensor resolution is likely to provide more discriminative power. Our results show three sharply distinct regimes (see Fig. 3). First, if m is too small ($m \leq 4$) the network performance is very poor, irrespective of the number of Byzantine

[13] Simulations showed that if $\tau < 0$ then $X_n = 1$ for all $n \in \mathbb{N}$ independently of the value of W, triggering a premature information cascade.

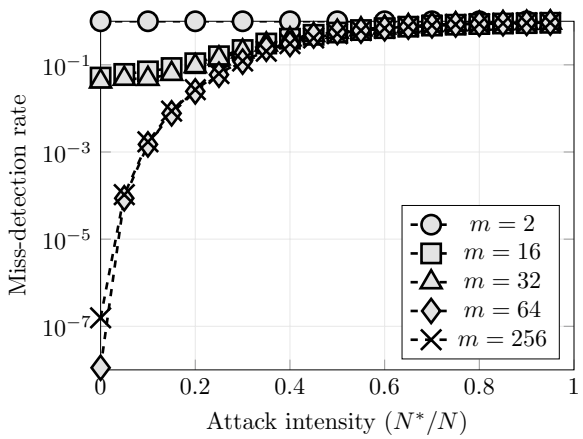

Fig. 3 Effect of the sensor dynamical range over the network resilience

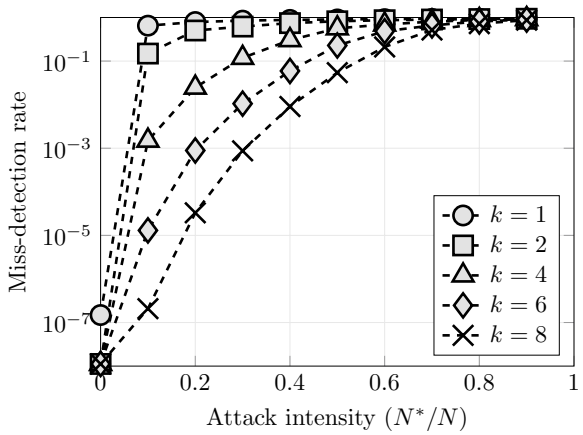

Fig. 4 A larger node memory, which allows incorporating more social signals into the inference process, greatly improves the network resilience

nodes. Secondly, if $8 \leq m \leq 32$ the miss-detection rate without Byzantine nodes is approx. 10% (cf. Fig. 3) and is exponentially degraded by the presence of Byzantine nodes. Finally, if $m \geq 64$ then the performance under no Byzantine nodes is very high, and is degraded super-exponentially by the presence of Byzantine nodes. Interestingly, the point at which the miss-detection rate of this regime goes above 10^{-1} is $N^*/N = 1/3$, having some resemblance with the well-known 1/3 threshold of the Byzantine generals problem [14]. Also, it is intriguing that variations between 8 and 32 levels in the dynamical range provide practically no performance benefits.

Our results also illustrate the effects of the memory size, k, showing that larger values of k provide great benefits for the network resilience (see Fig. 4). In effect, by performing an optimal Bayesian inference over 8 broadcasted signals the network miss-detection rate remains below 10% up to an attack intensity of 50% of Byzantine nodes. Unfortunately, the computation and storage requirements of Algorithm 1 grow exponentially with k, and hence using memories beyond $k = 10$ is not practical for resource-limited sensor networks. Overcoming this limitation is an interesting future line of investigation.

Conclusions

Traditional approaches to data aggregation over information networks are based on a strong division of labour, which discriminates between sensing nodes that merely sense and forward data, and FC that monopolize all the processing and inference capabilities. This generates a single point of failure that is likely to be exploited by smart adversaries, whose interest is the disruption of the network capabilities.

This serious security threat can be overcome by distributing the decision-making process across the network using social learning principles. This approach avoids single points of failure by generating a large number of nodes from where aggregated data can be accessed. In this paper, a social learning data fusion scheme has been proposed, which is suitable to be implemented in sensor networks consisting of devices with limited computational capabilities.

We showed that if the private signals are bounded then each local information cascade triggers a global cascade, extending previous results to the case where an adversary controls a number of Byzantine nodes. This result is highly relevant for sensor networks, as digital sensors are intrinsically bounded, and hence satisfy the assumptions of these results. However, contrasting with the literature, our approach does not focus on the conditions that guarantee perfect asymptotical social learning (i.e. miss-detection and false alarm rates converging to zero), but if their limits are small enough for practical applications. Our results show that this is indeed the case, even when the number of "overheard transmissions is limited.

Moreover, our results suggest that social learning principles can enable significant resilience of an information network against topology-aware data falsification attacks, which can totally disable the detection capabilities of traditional sensor networks. Furthermore, our results illustrate how the network resilience can persist even when the attacker has compromised an important number of nodes.

It is our hope that these results can motivate further explorations on the interface between distributed decision-making, statistical inference and signal processing over technological and social networks and multi-agent systems.

Authors' contributions

All the authors participated in the development of the concepts and the writing of the manuscript. All authors read and approved the final manuscript.

Author details

[1] Centre of Complexity Science and Department of Mathematics, Imperial College London, Kensington, London SW72AZ, UK. [2] Department of Electrical and Electronic Engineering, Imperial College London, Kensington, London SW72AZ, UK. [3] Department of Electrical Engineering, University of South Florida, 4202 E Fowler Ave, Tampa, FL 33620, USA.

Acknowledgements

Fernando Rosas is supported by the European Union's H2020 research and innovation programme, under the Marie Skłodowska-Curie Grant Agreement No. 702981.

Competing interests

The authors declare that they have no competing interests.

Appendix A: Properties of F_w^Λ

For simplicity let us consider the case of real-value signals, i.e. $S_n \in \mathbb{R}$. In this case, the c.d.f. of the signal likelihood is given by

$$F_w^\Lambda(y) = \int_{\mathcal{S}^y} \mathrm{d}\mu_w \tag{27}$$

where $\mathcal{S}^y = \{x \in \mathbb{R} | \Lambda_s(x) \leq y\}$. If Λ_s is an increasing function, then $\mathcal{S}^y = \{x \in \mathbb{R} | x \leq \Lambda_s^{-1}(y)\} = (-\infty, \Lambda_s^{-1}(y)]$ and hence

$$F_w^{\Lambda}(y) = \int_{-\infty}^{\Lambda_s^{-1}(y)} \mathrm{d}\mu_w = H_w(\Lambda_s^{-1}(y)), \tag{28}$$

where $H_w(s)$ is the cumulative density function (c.d.f.) of S_n for $W = w$. For the general case where Λ_s is an arbitrary (piece-wise continuous) function, then $\mathcal{S}^y$ can be expressed as the union of intervals. Then $\cup_{j=1}^{\infty}[a_j(y), b_j(y)] = \mathcal{S}^y$ (note that $\Lambda_s(a_j(y)) = \Lambda_s(b_k(y)) = y$) and hence from (27) is clear that

$$F_w^{\Lambda}(y) = \sum_{j=1}^{\infty} \int_{a_j(y)}^{b_j(y)} \mathrm{d}\mu_w = \sum_{j=1}^{\infty} \left[H_w(b_j(y)) - H_w(a_j(y))\right]. \tag{29}$$

Appendix B: Proof of Lemma 2

Proof Lets assume that the process $\boldsymbol{G}_n$ has strong consistent transitions and consider $\boldsymbol{g}' \in \mathcal{G}_{n-1}$ such that $\tau_{n-1}(\boldsymbol{g}') \leq L_s$. Note that, under these conditions $F_w^{\Lambda}(\tau_{n-1}(\boldsymbol{g}')) = 0$, and hence

$$\mathbb{P}_w\{X_{n-1} = 1 | \boldsymbol{G}_{n-1} = \boldsymbol{g}'\} = 1 - z_0 - z_1 F_w^{\Lambda}(\tau_{n-1}(\boldsymbol{g}')) = 1 - p_b c_{0|1} = 0 \tag{30}$$

holds for any $w \in \{0, 1\}$. Moreover, this allows to find that

$$\begin{aligned} \mathbb{P}_w\{\boldsymbol{G}_n = \boldsymbol{g} | \boldsymbol{G}_{n-1} = \boldsymbol{g}'\} &= \sum_{x_n \in \{0,1\}} \beta_w^n(\boldsymbol{g} | x_n, \boldsymbol{g}') \mathbb{P}_w\{X_{n-1} = x_n | \boldsymbol{G}_{n-1} = \boldsymbol{g}'\} \\ &= \beta_w^n(\boldsymbol{g} | 1, \boldsymbol{g}'). \end{aligned} \tag{31}$$

Therefore, due to the strongly consistent transition property, if $\mathbb{P}_w\{\boldsymbol{G}_n = \boldsymbol{g} | \boldsymbol{G}_{n-1} = \boldsymbol{g}'\} = \beta_w^n(\boldsymbol{g} | 1, \boldsymbol{g}') > 0$ then

$$L_s \geq \tau_{n-1}(\boldsymbol{g}') \geq \tau_n(\boldsymbol{g}), \tag{32}$$

proving the weak consistent transition property. The proof for the case of $\tau_{n-1}(\boldsymbol{g}') \geq U_s$ is analogous. □

Appendix C: Proof of Lemma 3

Proof Let us consider $\boldsymbol{g}_0 \in \mathcal{G}_n$ such that $\tau_n(\boldsymbol{g}_0) \notin [L_s, U_s]$. Then, due to the weakly invertible evolution, for each $x \in \{0, 1\}$ there exists $\boldsymbol{g}(x) \in \mathcal{G}_{n+1}$ such that

$$\beta_w^n(\boldsymbol{g} | x, \boldsymbol{g}_0) = \begin{cases} 1 & \text{if } \boldsymbol{g} = \boldsymbol{g}(x), \\ 0 & \text{in other case.} \end{cases} \tag{33}$$

Moreover, note that while the deterministic assumption implies that the event $\{\boldsymbol{G}_n = \boldsymbol{g}_0\}$ could be followed by either $\{\boldsymbol{G}_{n+1} = \boldsymbol{g}(0)\}$ or $\{\boldsymbol{G}_{n+1} = \boldsymbol{g}(1)\}$, the 1–1 assumption requires that $\boldsymbol{g}(0) = \boldsymbol{g}(1)$. With this, note that

$$\begin{aligned}\Lambda_{\boldsymbol{G}_{n+1}}(\boldsymbol{g}(0)) &= \log \frac{\mathbb{P}_1\{\boldsymbol{G}_{n+1} = \boldsymbol{g}(0)\}}{\mathbb{P}_0\{\boldsymbol{G}_{n+1} = \boldsymbol{g}(0)\}} \\ &= \log \frac{\sum_{\substack{\boldsymbol{g}' \in \mathcal{G}_n \\ x \in \{0,1\}}} \beta_w^n(\boldsymbol{g}(x)|x, \boldsymbol{g}')\mathbb{P}_1\{X_n = x, \boldsymbol{G}_n = \boldsymbol{g}'\}}{\sum_{\substack{\boldsymbol{g}' \in \mathcal{G}_n \\ x \in \{0,1\}}} \beta_w^n(\boldsymbol{g}(x)|x, \boldsymbol{g}')\mathbb{P}_0\{X_n = x, \boldsymbol{G}_n = \boldsymbol{g}'\}} \end{aligned} \tag{34}$$

$$= \log \frac{\sum_{x\in\{0,1\}} \mathbb{P}_1\{X_n = x|\boldsymbol{G}_n = \boldsymbol{g}_0\}\mathbb{P}_1\{\boldsymbol{G}_n = \boldsymbol{g}_0\}}{\sum_{x\in\{0,1\}} \mathbb{P}_0\{X_n = x|\boldsymbol{G}_n = \boldsymbol{g}_0\}\mathbb{P}_0\{\boldsymbol{G}_n = \boldsymbol{g}_0\}} \tag{35}$$

$$= \Lambda_{\boldsymbol{G}_{n-1}}(\boldsymbol{g}_0), \tag{36}$$

Above, (34) is a consequence of $\boldsymbol{g}(0) = \boldsymbol{g}(1)$, while (35) is because of the 1-1 condition over the dynamic. Finally, to justify (36) let us first consider

$$\mathbb{P}_w\{X_n = x|\boldsymbol{G}_n = \boldsymbol{g}_0\} = \lambda(z_0 + z_1 F_w^{\Lambda}(\tau_n(\boldsymbol{g}_0)), x). \tag{37}$$

Because $\tau_n(\boldsymbol{g}_0) \notin [L_s, U_s]$ then $F_w^{\Lambda}(\tau_n(\boldsymbol{g}_0))$ is either 0 or 1; in any case it does not depend on W. This, in turn means that $\mathbb{P}_1\{X_n = x|\boldsymbol{G}_n = \boldsymbol{g}_0\} = \mathbb{P}_0\{X_n = x|\boldsymbol{G}_n = \boldsymbol{g}_0\}$, which explains how (36) is obtained.

Please note that (36) shows that, once τ_n leaves $[L_s, U_s]$, it keeps a constant value. This, in turn, shows that weakly deterministic transitions satisfy the weakly consistency condition. □

Appendix D: List of symbols

Table2 presents a summary of the notation and symbols used in this work.

Table 2 List of symbols and notation

Network properties	
N	$\triangleq$ Size of the sensor network
N^*	$\triangleq$ Number of Byzantine nodes
p_b	$\triangleq$ Probability of a given node being compromised
Sensor and social signals	
S_n	$\triangleq$ Signal measured by the n-th node
$\mathcal{S}$	$\triangleq$ Set of values that S_n can take
μ_w	$\triangleq$ Distribution of S_n given $W = w$
$\Lambda_S(s)$	$\triangleq$ Log-likelihood of S_n with respect to W
$F_w^{\Lambda}(s)$	$\triangleq$ c.d.f. of $\Lambda_S(s)$ conditioned on $W = w$
$\boldsymbol{G}_n$	$\triangleq$ Social observations of the n-th node
$\mathcal{G}_n$	$\triangleq$ Set of values that $\boldsymbol{G}_n$ can take
$\Lambda_{\boldsymbol{G}_n}(\boldsymbol{g})$	$\triangleq$ Log-likelihood of $\boldsymbol{G}_n$ with respect to W
$\beta_w^n(\boldsymbol{g}\|x_n, \boldsymbol{g'})$	$\triangleq$ Transition probabilities from $\boldsymbol{G}_{n-1}$ to $\boldsymbol{G}_n$ given X_n and W
Data fusion variables	
W	$\triangleq$ Target of the networked inference
$u(\pi_n, w)$	$\triangleq$ Node's utility function for deciding π_n when $W = w$
τ_n	$\triangleq$ Decision threshold used by the n-th node
$\pi_n(s, \boldsymbol{g})$	$\triangleq$ Data fusion strategy of the n-th node given S_n and $\boldsymbol{G}_n$
X_n	$\triangleq$ Signal broadcasted by the n-th node
$C(\pi_n), c_{0\|0}, c_{0\|1}$	$\triangleq$ Corruption function, which links π_n and X_n
$\mathbb{P}\{\text{MD}; p_b\}$	$\triangleq$ Network miss-detection rate
$\mathbb{P}\{\text{FA}; p_b\}$	$\triangleq$ Network false alarm rate
Simulation parameters	
r	$\triangleq$ Ratio of the area of interest within the sensing range of a single node
m	$\triangleq$ Number of quantization levels of a node's sensor
k	$\triangleq$ Node's memory size

Publisher's Note

Received: 7 March 2018 Accepted: 21 September 2018
Published online: 25 October 2018

References

1. Kim K-D, Kumar PR. Cyber–physical systems: a perspective at the centennial. Proc IEEE. 2012;100(Special Centennial Issue):1287–308.
2. Response SS. What you need to know about the WannaCry Ransomware. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack
3. Veeravalli VV, Varshney PK. Distributed inference in wireless sensor networks. Philos Trans R Soc Lond A. 2012;370(1958):100–17.
4. Barbarossa S, Sardellitti S, Di Lorenzo P. Distributed detection and estimation in wireless. Academic Press library in signal processing: communications and radar signal processing. London: Academic Press; 2013. p. 329.
5. Hancke GP, Hancke GP Jr. The role of advanced sensing in smart cities. Sensors. 2012;13(1):393–425.
6. Difallah DE, Cudre-Mauroux P, McKenna SA. Scalable anomaly detection for smart city infrastructure networks. IEEE Internet Comput. 2013;17(6):39–47.
7. Lambrou TP, Panayiotou CG, Polycarpou MM. Contamination detection in drinking water distribution systems using sensor networks. In: Control Conference (ECC), 2015 European. New York: IEEE; 2015. p. 3298–303.
8. Lambrou TP, Anastasiou CC, Panayiotou CG, Polycarpou MM. A low-cost sensor network for real-time monitoring and contamination detection in drinking water distribution systems. IEEE Sens J. 2014;14(8):2765–72.
9. Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks. Commun ACM. 2004;47(6):53–7.
10. Shi E, Perrig A. Designing secure sensor networks. IEEE Wirel Commun. 2004;11(6):38–43.

11. Pathan A-SK, Lee H-W, Hong CS. Security in wireless sensor networks: issues and challenges. In: The 8th international conference of advanced communication technology, 2006. ICACT 2006, vol. 2. New York: IEEE; 2006. p. 6.
12. Trappe W, Howard R, Moore RS. Low-energy security: limits and opportunities in the internet of things. IEEE Secur Priv. 2015;13(1):14–21. https://doi.org/10.1109/MSP.2015.7.
13. Marano S, Matta V, Tong L. Distributed detection in the presence of Byzantine attacks. IEEE Trans Signal Process. 2009;57(1):16–29.
14. Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans Program Lang Syst (TOPLAS). 1982;4(3):382–401.
15. Vempaty A, Tong L, Varshney PK. Distributed inference with Byzantine data: state-of-the-art review on data falsification attack. IEEE Signal Process Mag. 2013;30(5):65–75.
16. Nadendla VSS, Han YS, Varshney PK. Distributed inference with M-Ary quantized data in the presence of Byzantine attacks. IEEE Trans Signal Process. 2014;62(10):2681–95. https://doi.org/10.1109/TSP.2014.2314072.
17. Zhang J, Blum RS, Lu X, Conus D. Asymptotically optimum distributed estimation in the presence of attacks. IEEE Trans Signal Process. 2015;63(5):1086–101. https://doi.org/10.1109/TSP.2014.2386281.
18. Kailkhura B, Han YS, Brahma S, Varshney PK. Distributed Bayesian detection in the presence of Byzantine data. IEEE Trans Signal Process. 2015;63(19):5250–63. https://doi.org/10.1109/TSP.2015.2450191.
19. Kailkhura B, Brahma S, Han YS, Varshney PK. Distributed detection in tree topologies with Byzantines. IEEE Trans Signal Process. 2014;62(12):3208–19.
20. Kailkhura B, Brahma S, Dulek B, Han YS, Varshney PK. Distributed detection in tree networks: Byzantines and mitigation techniques. IEEE Trans Inf Forensics Secur. 2015;10(7):1499–512. https://doi.org/10.1109/TIFS.2015.2415757.
21. Chen K-C, Lien S-Y. Machine-to-machine communications: technologies and challenges. Ad Hoc Netw. 2014;18:3–23.
22. Parno B, Perrig A, Gligor V. Distributed detection of node replication attacks in sensor networks. In: 2005 IEEE symposium on security and privacy (S&P'05). New York: IEEE; 2005. p. 49–63.
23. Lin S-C, Chen K-C. Improving spectrum efficiency via in-network computations in cognitive radio sensor networks. IEEE Trans Wirel Commun. 2014;13(3):1222–34.
24. Daniels BC, Ellison CJ, Krakauer DC, Flack JC. Quantifying collectivity. Curr Opin Neurobiol. 2016;37:106–13.
25. Brush ER, Krakauer DC, Flack JC. Conflicts of interest improve collective computation of adaptive social structures. Sci Adv. 2018;4(1):1603311.
26. Tsitsiklis JN. Decentralized detection. Adv Stat Signal Process. 1993;2(2):297–344.
27. Viswanathan R, Varshney PK. Distributed detection with multiple sensors I. Fundamentals. Proc IEEE. 1997;85(1):54–63.
28. Blum RS, Kassam SA, Poor HV. Distributed detection with multiple sensors I. Advanced topics. Proc IEEE. 1997;85(1):64–79.
29. Chen B, Tong L, Varshney PK. Channel aware distributed detection in wireless sensor networks. IEEE Signal Process Mag. 2006;23(4):16–26.
30. Chamberland J-F, Veeravalli VV. Wireless sensors in distributed detection applications. IEEE Signal Process Mag. 2007;24(3):16–25.
31. Tsitsiklis J, Athans M. On the complexity of decentralized decision making and detection problems. IEEE Trans Autom Control. 1985;30(5):440–6.
32. Warren D, Willett P. Optimum quantization for detector fusion: some proofs, examples, and pathology. J Franklin Inst. 1999;336(2):323–59.
33. Chamberland J-F, Veeravalli VV. Asymptotic results for decentralized detection in power constrained wireless sensor networks. IEEE J Sel Areas Commun. 2004;22(6):1007–15.
34. Easley D, Kleinberg J. Networks, crowds, and markets, vol. 1(2.1). Cambridge: Cambridge University Press; 2010. p. 2–1.
35. Acemoglu D, Ozdaglar A. Opinion dynamics and learning in social networks. Dyn Games Appl. 2011;1(1):3–49.
36. Banerjee AV. A simple model of herd behavior. Q J Econ. 1992;107:797–817.
37. Bikhchandani S, Hirshleifer D, Welch I. A theory of fads, fashion, custom, and cultural change as informational cascades. J Political Econ. 1992;100:992–1026.
38. Bikhchandani S, Hirshleifer D, Welch I. Learning from the behavior of others: conformity, fads, and informational cascades. J Econ Perspect. 1998;12(3):151–70.
39. Smith L, Sørensen P. Pathological outcomes of observational learning. Econometrica. 2000;68(2):371–98.
40. Bala V, Goyal S. Conformism and diversity under social learning. Econ Theory. 2001;17(1):101–20.
41. Banerjee A, Fudenberg D. Word-of-mouth learning. Games Econ Behav. 2004;46(1):1–22.
42. Gale D, Kariv S. Bayesian learning in social networks. Games Econ Behav. 2003;45(2):329–46.
43. Gill D, Sgroi D. Sequential decisions with tests. Games Econ Behav. 2008;63(2):663–78.
44. Acemoglu D, Dahleh MA, Lobel I, Ozdaglar A. Bayesian learning in social networks. Rev Econ Stud. 2011;78(4):1201–36.
45. Hsiao J, Chen KC. Steering information cascades in a social system by selective rewiring and incentive seeding. In: to Be included in 2016 IEEE international conference on communications (ICC) 2016.
46. DeMarzo PM, Zwiebel J, Vayanos D. Persuasion bias, social influence, and uni-dimensional opinions. In: Social Influence, and Uni-Dimensional Opinions (November 2001). MIT Sloan Working Paper (4339-01). 2001.
47. Golub B, Jackson MO. Naive learning in social networks and the wisdom of crowds. Am Econ J. 2010;2(1):112–49.
48. Acemoglu D, Ozdaglar A, ParandehGheibi A. Spread of (mis) information in social networks. Games Econ Behav. 2010;70(2):194–227.
49. Jadbabaie A, Molavi P, Sandroni A, Tahbaz-Salehi A. Non-Bayesian social learning. Games Econ Behav. 2012;76(1):210–25.
50. Lalitha A, Sarwate A, Javidi T. Social learning and distributed hypothesis testing. In: 2014 IEEE international symposium on information theory. New York: IEEE; 2014. p. 551–5.

51. Rhim JB, Goyal VK. Distributed hypothesis testing with social learning and symmetric fusion. IEEE Trans Signal Process. 2014;62(23):6298–308.
52. Huang SL, Chen KC. Information cascades in social networks via dynamic system analyses. In: 2015 IEEE international conference on communications (ICC); 2015. p. 1262–7. https://doi.org/10.1109/ICC.2015.7248496.
53. Castro R, Coates M, Liang G, Nowak R, Yu B. Network tomography: recent developments. Stat sci. 2004;19:499–517.
54. Viswanathan R, Thomopoulos SC, Tumuluri R. Optimal serial distributed decision fusion. IEEE Trans Aerospace Electron Syst. 1988;24(4):366–76.
55. Papastavrou JD, Athans M. Distributed detection by a large team of sensors in tandem. IEEE Trans Aerospace Electron Syst. 1992;28(3):639–53.
56. Swaszek PF. On the performance of serial networks in distributed detection. IEEE Trans Aerospace Electron Syst. 1993;29(1):254–60.
57. Bahceci I, Al-Regib G, Altunbasak Y. Serial distributed detection for wireless sensor networks. In: Proceedings. International symposium on information theory, ISIT 2005. New York: IEEE; 2005. p. 830–4.
58. Rosas F, Hsiao J-H, Chen K-C. A technological perspective on information cascades via social learning. IEEE Access. 2017;5:22605–33.
59. Rosas F, Chen K-C. Social learning against data falsification in sensor networks. In: International workshop on complex networks and their applications. New York: Springer; 2017. p. 704–16.
60. Rosas F, Oberli C. Modulation and SNR optimization for achieving energy-efficient communications over short-range fading channels. IEEE Trans Wirel Commun. 2012;11(12):4286–95.
61. Bertrand A. Applications and trends in wireless acoustic sensor networks: a signal processing perspective. In: 2011 18th IEEE symposium on communications and vehicular technology in the Benelux (SCVT); 2011. p. 1–6. https://doi.org/10.1109/SCVT.2011.6101302.
62. Kam M, Zhu Q, Gray WS. Optimal data fusion of correlated local decisions in multiple sensor detection systems. IEEE Trans Aerospace Electron Syst. 1992;28(3):916–20.
63. Chen J-G, Ansari N. Adaptive fusion of correlated local decisions. IEEE Trans Syst Man Cyberne Part C (Appl Rev). 1998;28(2):276–81.
64. Willett P, Swaszek PF, Blum RS. The good, bad and ugly: distributed detection of a known signal in dependent Gaussian noise. IEEE Trans Signal Process. 2000;48(12):3266–79.
65. Chamberland J-F, Veeravalli VV. How dense should a sensor network be for detection with correlated observations? IEEE Trans Inf Theory. 2006;52(11):5099–106.
66. Sundaresan A, Varshney PK, Rao NS. Copula-based fusion of correlated decisions. IEEE Trans Aerospace Electron Syst. 2011;47(1):454–71.
67. Loeve M. Probability theory, vol. 1. New York: Springer; 1978.
68. Karl H, Willig A. Protocols and architectures for wireless sensor networks. Chichester: Wiley; 2007.
69. Sundararaman B, Buy U, Kshemkalyani AD. Clock synchronization for wireless sensor networks: a survey. Ad hoc Netw. 2005;3(3):281–323.
70. Rosas F, Brante G, Souza RD, Oberli C. Optimizing the code rate for achieving energy-efficient wireless communications. In: Wireless communications and networking conference (WCNC), 2014 IEEE. New York: IEEE; 2014. p. 775–80.
71. Karyotis V, Khouzani M. Malware diffusion models for modern complex networks: theory and applications. Cambridge: Morgan Kaufmann; 2016.
72. Poor HV. An introduction to signal detection and estimation. Berlin-Heidelberg: Springer; 2013.
73. Smith P, Hutchison D, Sterbenz JP, Schöller M, Fessi A, Karaliopoulos M, Lac C, Plattner B. Network resilience: a systematic approach. IEEE Commun Mag. 2011;49(7):88–97.
74. Shiller RJ. Conversation, information, and herd behavior. Am Econ Rev. 1995;85(2):181–5.
75. Gelman A, Carlin JB, Stern HS, Dunson DB, Vehtari A, Rubin DB. Bayesian data analysis. Boca Raton: CRC Press; 2014.
76. Cover TM, Thomas JA. Elements of information theory. New Jersey: Wiley; 2012.
77. Rosas F, Ntranos V, Ellison CJ, Pollin S, Verhelst M. Understanding interdependency through complex information sharing. Entropy. 2016;18(2):38.
78. Dieudonne J. Treatise on analysis, vol. II. New York: Associated Press; 1976.
79. McKenna SA, Wilson M, Klise KA. Detecting changes in water quality data. J Am Water Works Assoc. 2008;100(1):74.