Distributed Hypothesis Testing

in PEPR Réseaux du Futur
PC9 : Foundations of future communication networks

Mireille Sarkiss and Michèle Wigger

In the future, billions of IoT devices and sensors will be connected and cooperate together to detect events in distributed monitoring and alert systems in applications like intrusion detection, target tracking, smart grids and smart homes, industry 4.0, e-Health or intelligent transportation (connected cars or drones). Many of these applications have system-critical security requirements, in the sense that eavesdroppers and intruders should not learn or influence decisions or data and measurements. The objective of this thesis is to characterize the fundamental limits and devise new strategies of distributed detection systems with security constraints against external and internal eavesdroppers that should not be able to learn the data and measurements performed at the sensors. In this goal we shall propose an information-theoretic analysis as well as learning-assisted detection strategies.
In our previous works, we have derived fundamental limits of multi-hop and multi-sensor detection systems without secrecy constraints [1, 2, 3, 4] and of single-hop systems with a security constraint against an external eavesdropper [5]. All these works focused on binary hypotheses and asymmetric scenarios where the error probability under the null hypothesis (false-alarm probability) needs to be kept below a certain threshold while the error probability under the alternative hypothesis (miss-detection probability) should decay exponentially fast in the blocklength with largest possible exponent. In addition, in the secrecy setup with an external eavesdropper [5], the uncertainty (equivocation) about the sensor measurements should stay above pre-defined security thresholds given the two hypothesis. In particular, our work in [5] generalised the previous works in [6] and [7] to allow for positive asymptotic false-alarm probabilities.

The goal of this thesis is to extend the single-hop scenario with external eavesdropper in [5] to multiple hypotheses with either symmetric or asymmetric requirements on the probabilities of error under the various hypotheses. The focus is also on multi-hop scenarios where the security constraints are not only with respect to external eavesdroppers but also against system-internal intermediate relaying terminals. In such systems, the exchange of private sensitive information is undesirable with other terminals or decision centers, or even infeasible due to communication and resource constraints. Therefore, it is particularly important to analyze smart device selection strategies to identify which relays should be included in the distributed decision task, in particular in view of the internal security requirements, the overall energy-consumption and the various communication requirements of the system.
To derive the fundamental limits of the described systems, we shall rely on a recent converse strategy that we pioneered in [8] by using a change-of-measure argument and by proving asymptotic Markov chains, combined with the tools that we already used in our previous works [5, 4]. Leveraging on these limits and with the aid of deep learning and reinforcement learning techniques, smart device selection strategies and practical secure distributed detection systems will be proposed.

The project consists of three parts : i) characterize the fundamental limits of distributed detection systems in general multi-hop scenarios considering multiple hypotheses with different constraints on the error probabilities and the equivocations measured at external eavesdroppers, ii) extend these fundamental limits to scenarios where the conveyed information (data and/or decisions) need to be kept secret from other system terminals, and iii) design efficient distributed learning strategies to perform selection of devices participating collaboratively in the distributed decision. Distributed secure learning and distributed decision techniques will be designed taking into account the communication rate and security requirements, and the energy and device constraints of future networks.

The thesis will be co-supervised by Mireille Sarkiss from Telecom SudParis, and Michèle Wigger from Telecom Paris. Both have significant experience in information-theoretic analysis of distributed

detection systems, e.g., [9, 10, 1, 2, 3, 4]. M. Sarkiss has also various previous results on learning strategies for joint resource allocation and computation offloading in future networks [11, 12].

References

[1] M. Hamad, M. Wigger, and M. Sarkiss, "Cooperative multi-sensor detection under variable-length coding," in *2020 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2020.

[2] M. Hamad, M. Wigger, and M. Sarkiss, "Optimal exponents in cascaded hypothesis testing under expected rate constraints," in *2021 IEEE Information Theory Workshop (ITW)*, pp. 1–6, 2021.

[3] M. Hamad, M. Sarkiss, and M. Wigger, "Benefits of rate-sharing for distributed hypothesis testing," in *2022 IEEE International Symposium on Information Theory (ISIT)*, pp. 2714–2719, 2022.

[4] M. Hamad, M. Wigger, and M. Sarkiss, "Multi-hop network with multiple decision centers under expected-rate constraints," *IEEE Transactions on Information Theory*, 2023. `https://arxiv.org/abs/2208.14243`.

[5] S. Faour, M. Hamad, M. Sarkiss, and M. Wigger, "Testing against independence with an eavesdropper," in *2023 IEEE Information Theory Workshop (ITW)*, 2023. `https://arxiv.org/abs/2211.03475`.

[6] S. Sreekumar, A. Cohen, and D. Gündüz, "Privacy-aware distributed hypothesis testing," *Entropy*, vol. 22, 2020.

[7] M. Mhanna and P. Piantanida, "On secure distributed hypothesis testing," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 1605–1609, 2015.

[8] M. Hamad, M. Wigger, and M. Sarkiss, "Strong converses using change of measure and asymptotic markov chains," in *2022 IEEE Information Theory Workshop (ITW)*, pp. 535–540, 2022.

[9] S. Salehkalaibar and M. Wigger, "Distributed hypothesis testing based on unequal-error protection codes," *IEEE Transactions on Information Theory*, vol. 66, no. 7, pp. 4150–4182, 2020.

[10] S. Salehkalaibar and M. Wigger, "Distributed hypothesis testing with variable-length coding," *IEEE Journal on Selected Areas in Information Theory*, vol. 1, no. 3, pp. 681–694, 2020.

[11] I. Fawaz, M. Sarkiss, and P. Ciblat, "Delay-optimal resource scheduling of energy harvesting-based devices," *IEEE Transactions on Green Communications and Networking*, vol. 3, no. 4, pp. 1023–1034, 2019.

[12] I. Djemai, M. Sarkiss, and P. Ciblat, "Joint scheduling-offloading policies in noma-based mobile edge computing systems," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2023.