Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
Pending assignment.	N/A	N/A

4. Title and Subtitle	5. Report Date
Secure Integrated Sensing and Communication with Transmitter Actions for Vehicular Communication	September 30, 2024
	6. Performing Organization Code N/A

7. Author(s)	8. Performing Organization Report No.
Truman Welling; Aylin Yener, Ph.D. https://orcid.org/0000-0003-0820-3390.	N/A

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
The Ohio State University Address: 281 W Lane Ave, Columbus, OH 43210	N/A
	11. Contract or Grant No. 69A3552348327

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
The Ohio State University Address: 281 W Lane Ave, Columbus, OH 43210	Final (June 2023 to Aug. 2024)
	14. Sponsoring Agency Code N/A

15. Supplementary Notes

Conducted in cooperation with the U.S. Department of Transportation, Federal Highway Administration.

16. Abstract

We have addressed securing communication in a joint communication and sensing model with autonomous cooperative routing over a vehicular communication network as a use case in mind. Joint communication and sensing is a new technology that aims to design signals that perform both functionalities simultaneously. Integrating sensing into communication signal design helps improve resource efficiency and is expected to be a pillar of the next generation connectivity.

In this first year project, we have identified a mathematical model that utilizes sensing signals towards designing communication signals that are unconditionally secure against external adversaries. We have derived asymptotic and non-asymptotic information theoretic bounds on the (strongly) secure communication rate. The former contributes to the Shannon limit in these systems, the latter fundamental limits in systems with low latency requirements as one would find in autonomous vehicular networks where ultra quick and ultra reliable decisions that are secure against attacks are essential for safe operation

17. Key Words	18. Distribution Statement
Secure communication, integrated sensing and communication	No restrictions. This document is available to the public through NTIS: National Technical Information Service Springfield, Virginia 22161

19. Security Classif.(of this report)	20. Security Classif.(of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	17 pages	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

CARMEN+ UTC

Center for Automated Vehicle Research with Multimodal AssurEd Navigation

University Transportation Centers Program

Final Report: Secure Integrated Sensing and Communication with Transmitter Actions for Vehicular Communication

P.I.	Project Info:
Aylin Yener The Ohio State University Department of Electrical and Computer Engineering	Grant No. 69A3552348327
	DUNS: 832127323
	EIN #: 31-6025986
	Project Effective: June 1, 2023 Project End: August 30, 2024 Submission: September 30, 2024

Consortium Members:

The Ohio State University College of Engineering

UCI University of California, Irvine

TEXAS The University of Texas at Austin

North Carolina Agricultural and Technical State University

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and accuracy of the information presented herein. This document is disseminated in the interest of information exchange. The report is funded, partially or entirely, under grant number 69A3552348327 from the U.S. Department of Transportation's University Transportation Centers Program. The U.S. Government assumes no liability for the contents or use thereof.

Abstract

We have addressed securing communication in a joint communication and sensing model with autonomous cooperative routing over a vehicular communication network as a use case in mind. Joint communication and sensing is a new technology that aims to design signals that perform both functionalities simultaneously. Integrating sensing into communication signal design helps improve resource efficiency and is expected to be a pillar of the next generation connectivity.

In this first year project, we have identified a mathematical model that utilizes sensing signals towards designing communication signals that are unconditionally secure against external adversaries. We have derived asymptotic and non-asymptotic information theoretic bounds on the (strongly) secure communication rate. The former contributes to the Shannon limit in these systems, the latter fundamental limits in systems with low latency requirements as one would find in autonomous vehicular networks where ultra quick and ultra reliable decisions that are secure against attacks are essential for safe operation.

Acknowledgements

This work was supported in part by the by the U.S. Department of Transportation under Grant 69A3552348327 for the CARMEN+ University Transportation Center.

Executive Summary

Next generation connected transportation networks will require extensive communication capabilities with low-latency and high-reliability. Further, these systems rely on significant sensing capabilities in order to function, for example for autonomous routing. Joint communications and sensing is clearly going to be a pillar of 6G in order to facilitate such use cases. Often termed integrated sensing and communication (ISAC), this paradigm foresees designing waveforms and transceivers simultaneously for communications and sensing. The main motivation is efficient (wireless) resource utilization, as the next generation systems will need to be low latency and high reliability and are radio resource heavy. It is important to note that, while great for bandwidth efficiency, these dual function systems open new attack surfaces to spoofing, eavesdropping and jamming alike, and present greater security risks that are unseen in today's separate sensing and communication paradigm. The goal of this project is to address information confidentiality on the communicated information, while ensuring reliable joint communication and sensing using the same signals.

As a concrete use case addressed by our work, consider autonomous cooperative routing over a vehicular communication network. Each vehicle needs to communicate with nearby vehicles to coordinate routing while simultaneously sensing the environment to localize pedestrians, other vehicles, and other obstacles. This communication needs to be secure to prevent malicious adversaries from learning private information or interfering with cooperative routing based on information obtained from observing the sensing/communication waveform. Similarly, the information needs to be protected from any object (e.g. out of network vehicles) even if they are not malicious entities. These are the cases we addressed in this year's effort. Because these systems open up new foundational problems that were unseen before, we targeted solving them in first asymptotic (traditional) information theoretic fundamental limits and then considered the finite block length regime in which we are able to assess the precise penalty for ultra-low latency.

Table of Contents

Introduction

Next generation connected transportation networks will require extensive communication capabilities with low-latency and high-reliability. Further, these systems rely on significant sensing capabilities in order to function, for example for routing. Joint communications and sensing is clearly going to be in 6G in order to facilitate such use cases. Often termed integrated sensing and communication (ISAC), this paradigm foresees designing waveforms and transceivers simultaneously for communications and sensing. The main motivation is efficient (wireless) resource utilization, as mentioned these systems will need to be low latency and high reliability and thus are radio resource heavy. While great for bandwidth efficiency, these dual function systems open new attack surfaces to spoofing and jamming alike and present greater security risks that are unseen in today's separate sensing and communication paradigm.

Figure 1: A depiction of vehicle-to-everything (V2X) communication including vehicle-to-pedestrian (V2P), vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) communication. Integrated sensing and communication (ISAC) in this environment, the vehicle observes reflections of the transmitted waveform caused by objects in the environment and uses those observations to map the environment.

The need for security in vehicle-to-everything (V2X) communication systems has received much attention in the literature, see [1] and [2]. There are many adversarial attacks that need to be mitigated including message modification, denial of service, and impersonation attacks. In this work we specifically consider an adversary that is a passive eavesdropper, meaning the adversary does not affect the fidelity of the communication between the transmitter and legitimate receiver, but attempts to decode the information sent from a transmitter to its legitimate receiver. Such an attack, if successful, can jeopardize not only the integrity of information transfer, but opens pathways for an intelligent adversary to design further attacks for substitution and impersonation. This could lead to collapsing autonomous operations as well as endangering them. The approach used in [1] and [2] to secure against an eavesdropper is encryption which is the state of the art in information security. However, such

approaches rely on the adversaries being computationally limited and thus unable to encrypt the information. We take a fundamentally different approach that provide unconditional security even if the adversary has complete knowledge of the system.

In particular, our work addresses the problem from an information theoretic security perspective in [3] and [4], where we directly design the signals and the transmission scheme to be unconditionally secure. Encryption (the state of the art used in todays application layer based security approach) assumes that the transmitter and receiver share a key and that decryption (breaking the key) is hard enough that it is not feasible for the attacker to decode the message. Our set up is fundamentally different. We assume that the eavesdropper has all information that a legitimate receiver would need in order to correctly decode the transmitted message; The transmitter and legitimate receiver do not start the transmission sharing any information that the eavesdropper is not privy to. Specifically, our formulation uses signal design to take advantage the noise present in the communication channel to unconditionally secure the message from the eavesdropper. Our information theoretic approach provides security guarantees against a computationally unbounded adversary. Although in our work we mention a scret key, this key is distilled from the information at the legitimate receiver and the sensing data in such a way that the eavesdropper is not privy to it. When the secret key is used, it is not used in an encryption sense, it is used in a one-time-pad sense, causing the eavesdropper's observation to not contain any information about the message secured with the key. A significant contribution of our work is that the sensing used to improve the secure communication.

As a concrete use case addressed by our work, consider autonomous cooperative routing over a vehicular communication network. Each vehicle needs to communicate with nearby vehicles to coordinate routing while simultaneously sensing the environment to localize pedestrians, other vehicles, and other obstacles [5]. This communication needs to be secure to prevent malicious adversaries from learning private information or interfering with cooperative routing based on information obtained from observing the sensing/communication waveform [6] [7]. Similarly, the information needs to be protected from any object (eg. out of network vehicles) even if they are not malicious entities. These are the cases we addressed in this year's effort. Because these systems open up new foundational problems that were unseen before, we targeted solving them in first asymptotic (traditional) information theoretic fundamental limits and then considered the finite block length regime in which we are able to assess the precise penalty for ultra-low latency.

Related Work

The foundational information theoretic ISAC model [8] considers two scenarios, a transmitter communicating with a single receiver while simultaneously localizing the receiver based on the transmitted signal and sensing data, and a transmitter communicating with and localizing two receivers simultaneously This information theoretic model was extended to include security in [9] by considering a transmitter communicating with one receiver over a noisy channel in the presence of an eavesdropper. The transmitter wants to reliably communicate a message with the legitimate receiver while obfuscating the message from the eavesdropper. The transmitter uses the sensing information to improve the secure communication. This secure ISAC model was extended in [10] to consider the low-latency constraints, giving achievable secure communication rates for specific transmission length. The work in [11] derives the secure communication rates for an ISAC model where the noisy channel is a binary input additive white Gaussian noise channel.

Our work this year extends ISAC model in [9] and the secure ISAC model [10] by the addition of transmitter actions. The concept of transmitter actions that we consider was inspired by the transmitter actions in [12], where the transmitter can take an action at each channel use where the action affect the noise in the channel. There is also significant prior work on the wiretap channel, which is using the noise of the channel to provide security, when the transmitter has feedback, see [13] [14] [15] [16] [17] [18].

Other information theoretic security formulations for ISAC include [19] which considers a model where the transmitter chooses the signals in a way that the signal the eavesdropper observes does not contain information about the legitimate receiver's location. The formulation in [20] considers the case where the transmitter chooses the signal in a way that the eavesdropper cannot infer information about the legitimate receiver's intended message or location.

Asymptotic Formulation

The following work is published in full detail in [3]. Specifically, we consider integrated sensing and communication model with a transmitter, a legitimate receiver, and an eavesdropper. The model is monostatic, meaning that the transmit and receive antennas are colocated. The transmitter has three objectives, communicate reliably with the legitimate receiver, hide sensitive information from the eavesdropper, and sense (localize) the legitimate receiver and eavesdropper. This formulation is asymptotic in that the communication and sensing rates are possible in the limit as the number of uses of the channel goes to infinity.

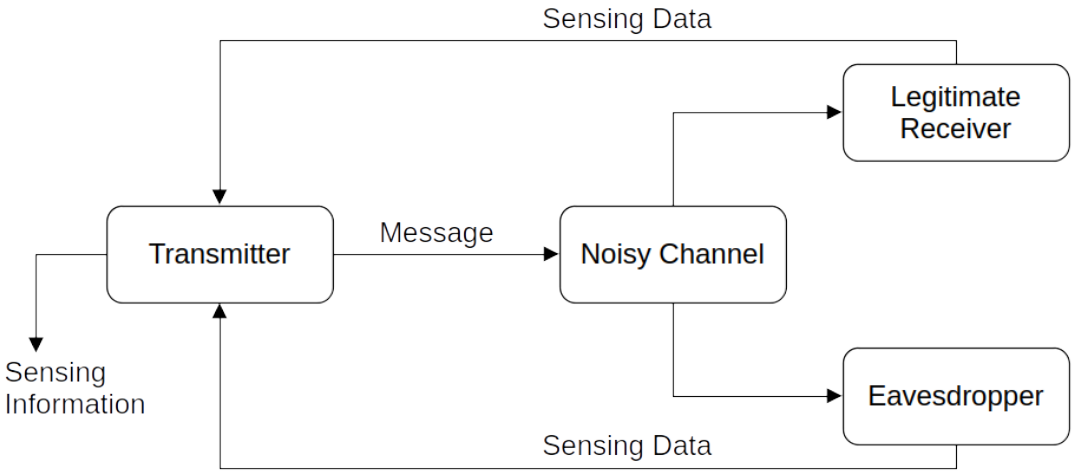

Figure 2: The transmitter sends a message over a noisy channel, of which both the legitimate receiver and eavesdropper observe resulting outputs. The transmitter wants to communicate with the legitimate receiver while minimizing the information the eavesdropper has about the message. The sensing data lines to the transmitter are the reflections of the transmitted waveform of both receivers. Based on the reflections the transmitter estimates the sensing information. The sensing data is also used to securely communicate with the legitimate receiver.

In practice, the sensing information, e.g. location of the legitimate receiver and eavesdropper, is correlated with the quality of the communication link between the transmitter and (potential) receiver.

In our work, we assume that the sensing information is the location of the receiver, and thus is known to the receiver. We assume that the transmitter has access to sensing data, which corresponds to the transmitter observing the reflections of the transmitted waveform off of the sensing targets.

The specific contribution of our work is the introduction of transmitter actions, which change the noisy channel. Consider the case where the sensing information is the location of the targets/receivers and the transmitter actions are physically moving the transmit antenna. The physical relocation of the antenna changes the propogation path of the signal, thus changing the noisy channel. Moving the antenna also changes the physical location of the targets with respect to the antenna, thus changing the sensing information that is estimated by the transmitter.

In our formulation, a communication rate-distortion constraint combination is achievable if the transmitter can communicate reliably with the legitimate receiver at that rate, the security constraint on the message is satisfied, and the expected estimation distortion at the transmitter is below the distortion constraint. Reliability is defined as the probability that the legitimate receiver reconstructs the incorrect message goes to zero as the length of the transmission goes to infinity. The security constraint is strong secrecy, guaranteeing that the eavesdropper cannot infer any information about the message communicated between the legitimate parities from its observation.

We derived the set of achievable communication rate-distortion constraints (capacity) for a few special cases. First, where the eavesdropper's observation Y_2 is a noisy version of what the legitimate receiver's observation Y_1. In this case, we showed that the capacity region is

$$R_1 \leq I(V; Y_1, S_1)$$

$$R_2 \leq \min\{R_2',\ I(V; Y_1, S_1) - R_1\}$$

$$D_j \geq E\left[d_j\left(S_j, \widehat{S_j}\right)\right] \qquad \text{for } j = 1,2$$

where

$$R_2' = I(V; Y_1, S_1)\ -\ I(V; Y_2, S_2) + H(Y_1|V, Y_2, S_2).$$

R_1 is the rate of the part of the message with no secrecy constraint; the first inequality denotes that the public portion of the message cannot exceed the capacity of the noisy channel between the transmitter and the legitimate receiver. In the second inequality, R_2' is the maximum possible secure rate. The minimum in the second inequality implies that the rate of the secure portion of the message R_2 must not exceed the maximum possible secure rate and that $R_1 + R_2$, or the total rate of the message, must not exceed the reliable communication rate. The maximum possible secure rate R_2' is made up of two terms. $I(V; Y_1, S_1) - I(V; Y_2, S_2)$ is the wiretap coding rate for this noisy channel, which is the rate at which the noise from the channel can conceal information about the message from the eavesdropper, and $H(Y_1|V, Y_2, S_2)$ is the rate at which a secret key can be extracted by the legitimate parties and subsequently used to secure part of the message via the one-time-pad operation. The final inequality above denotes that the estimation of the sensing information from the sensing data for both the legitimate receiver and the eavesdropper falls within the predetermined estimation error tolerance.

The case where the legitimate receiver's observation Y_1 is a noisy version of the eavesdropper's observation Y_2 yields the same inequalities as above for R_1, R_2, and D_j, but differs giving the maximum possible secure

$$R_2' = H(Y_1|V, Y_2, S_2).$$

Note that in this case, R_2' consists only of the secret key rate. This is because if the legitimate receiver's observation is a noisy version of the eavesdropper's observation, then any information that the noise inherent to channel obfuscates about the message from the eavesdropper, will also be irrecoverable at the legitimate receiver.

We also derived the capacity of the ISAC channel when the whole message is sensitive and should be kept secret from the eavesdropper in two specific cases. First, where the eavesdropper's observation is a noisy version of what the legitimate receiver's observation the capacity region is

$$R \leq \min\{I(A, X; Y_1, S_1) - I(A, X; Y_2, S_2) + H(Y_1|A, X, Y_2, S_2),\ I(A, X; Y_1, S_1)\}$$

and D_j satisfies the constraints on the estimation of the sensing information considered in the previous cases. In this setting, R denotes the secure message rate, which as in the case where only part of the message should remain secure, consists of a minimum. The first term is once again made up of a wiretap coding rate and a secret key rate, the form is different, with (A, X) in place of V , because the whole message is being kept secret. The second term in the minimum implies that R must remain within the reliable communication rate.

Finally, in the case where the whole message must remain secure and the legitimate receiver's observation is a noisy version of the eavesdropper's observation, we showed that

$$R \leq \min\{H(Y_1|A, X, Y_2, S_2),\ I(A, X; Y_1, S_1)\}$$

Where the simplification comes because the wiretap coding rate is zero, so the maximum possible secure rate is the secret key rate.

A significant implication of our result is that even when the legitimate receiver observes a noisy version of what the eavesdropper observes secure communication is still possible; This is because of the improvement to the secure communication is due to the sensing. We also note that because the transmitter actions affect the sensing information, the sensing information contains information about the message the transmitter is sending.

Low-latency Setting

In [4], we consider the low-latency setting. In the asymptotic formulation in [3], the transmitter is allowed to use the sensing data (the reflected signals) to improve the communication. In the low-latency setting we remove this assumption in order to allow low-latency constraints to be satisfied [10].

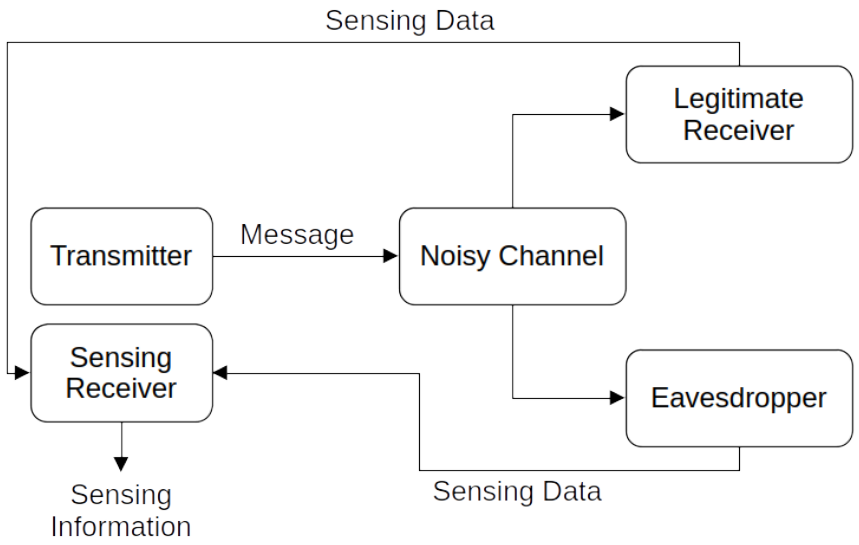

Figure 3: The transmitter sends a message across a noisy channel, of which both the transmitter and eavesdropper observe outputs. Unlike the asymptotic case, the transmitter does not use the sensing data to improve communication; the sensing data is only used to estimate the sensing information.

We first found the asymptotic set of communication rate-distortion constraints, which differs fromthe asymptotic limit in [3] because that work allowed the transmitter to improve the communication using the sensing data. Specifically, we showed that the capacity for the ISAC channel that does not use sensing data to improve communication when the eavesdropper observes a noisy version of the legitimate receiver's observation is

$$R_1 + R_2 \leq I(V; Y_1, S_1)$$

$$R_2 \leq I(V; Y_1, S_1) - I(V; Y_2, S_2)$$

$$D_j \geq E\left[d_j\left(S, \widehat{S}_j\right)\right] \qquad \text{for } j = 1,2.$$

In this case, similar to the results above, the total rate of the message $R_1 + R_2$ is limited to the channel capacity and the estimation of the sensing information is similarly constrained. The difference here with the formulation in [3] is that the sensing data is not used to improve communication so the maximum possible secure rate R_2 consists only of a wiretap coding rate; There is no secret key rate.

We then derive a set of achievable secure communication rates for a specific transmission length n, given specific security, reliability, and sensing tolerances, δ_{sec}, δ_{r}, and δ_{D}, respectively. The achievable region is defined as

$$R_1 + R_2 \leq \left[I(V; Y_1, S_1) - O\left(\frac{\log n}{n}\right) - Q^{-1}\left(\theta\left(\delta_{\text{r}} + O\left(\frac{1}{\sqrt{n}}\right)\right)\right)\sqrt{\frac{V_{Y_1 S_1}}{n}} \right]^+$$

$$R_2 \leq \left[I(V;Y_1,S_1) - I(V;Y_2,S_2) - O\left(\frac{\log n}{n}\right) - Q^{-1}\left((1-\theta)\left(\delta_{\text{sec}} + O\left(\frac{1}{\sqrt{n}}\right)\right)\right)\sqrt{\frac{V_{Y_2S_2}}{n}} - Q^{-1}\left(\theta\left(\delta_{\text{r}} + O\left(\frac{1}{\sqrt{n}}\right)\right)\right)\sqrt{\frac{V_{Y_1S_1}}{n}} \right]^{+}$$

where $\theta \in [0,1]$ and $[a]^{+} = \max(a, 0)$. These rate conditions are the rate conditions for the asymptotic case with extra terms representing a penalty term which decreases as the length of the transmission n increases. The term $V_{Y_1S_1}$ is a variance term, called the dispersion of the channel, that represents the variance of the capacity of the channel for a single use. In the proof, these penalty terms are driven to zero as n increases by the central limit theorem. Note that this achievable region is more general than the asymptotic capacity presented up to this point, there is no defined relationship between which receiver's observation is noisier.

We now consider a simple example that illustrates the finite transmission length penalty to the secure communication rate. We let the input X and the outputs Y_i of the channel be binary with Bernoulli multiplicative states, i.e.

$$Y_i = S_i \cdot X \qquad \text{for } i = 1,2.$$

The transmitter actions affect probability of the states. This model example serves as a course approximation of fading channels with high signal-to-noise ratio. Specific formulation of the evolution probabilities is the same as the example in [3] with $p = .25$, $q = .35$, $\alpha = .4$, and $\lambda = .2$. Figure 4 shows the achievable rate when the whole message should be secured as the length of the transmission increases.

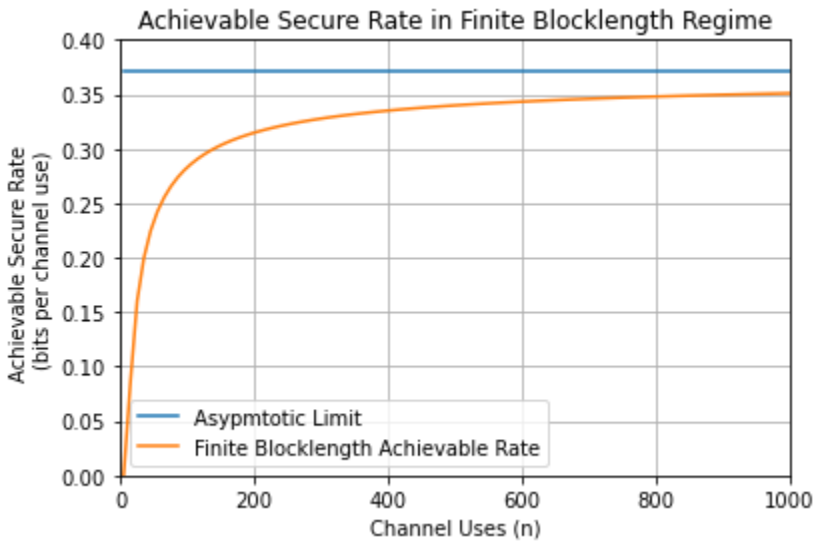

Figure 4: The achievable rate given in **[4]** for the example as described above with $\boldsymbol{\delta_{\text{sec}} = \delta_r = 0.001}$ for the example in **[3]**. Note that is the number of channel uses increases the finite blocklength limit approaches the asymptotic limit. This shows the characterization of the exact penalty of operating in low-latency settings.

Conclusion

In this project we studied secure integrated sensing and communication with autonomous cooperative routing over a vehicular network as a specific use case. The security metric that we considered gives unconditional security against an eavesdropper. Our works shows that the sensing improves the secure communication rate between the transmitter and legitimate receiver in the presence of an eavesdropper.

In considering autonomous cooperative routing over a vehicular network, low-latency is an important characteristic. As such, we also derived the achievable rates of secure communication for a specific transmission length. This allowed us to characterize the precise penalty that low-latency requirements exact on the secure communication rate.

References

[1] J. Huang, D. Fang, Y. Qian and R. Q. Hu, "Recent Advances and Challenges in Security and Privacy for V2X Communications," *IEEE Open Journal of Vehicular Technology,* vol. 1, pp. 244 - 266, 2020.

[2] A. Ghosal and a. M. Conti, "Security issues and challenges in V2X: A survey," *Computer Networks,* vol. 169, p. 107093, 2020.

[3] T. Welling, O. Günlü and a. A. Yener, "Transmitter actions for secure integrated sensing and communication," in *2024 IEEE International Symposium on Information Theory (ISIT)*, Athens, Greece, 2024.

[4] T. Welling, O. Günlü and a. A. Yener, "Low-latency Secure Integrated Sensing and Communication with Transmitter Actions," in *2024 IEEE 25th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Lucca, Italy, 2024.

[5] T. Wild, V. Braun and H. Viswanathan, "Joint Design of Communication and Sensing for Beyond 5G and 6G Systems," *IEEE Access,* vol. 9, pp. 30845 - 30857, 2021.

[6] Z. Wei, F. Liu, C. Masouros, N. Su and A. P. Petropulu, "Toward Multi-Functional 6G Wireless Networks: Integrating Sensing, Communication, and Security," *IEEE Communications Magazine,* vol. 60, no. 4, pp. 65 - 71, 2022.

[7] N. Su, F. Liu and C. Masouros, "Secure Radar-Communication Systems With Malicious Targets: Integrating Radar, Communications and Jamming Functionalities," *IEEE Transactions on Wireless Communications,* vol. 20, no. 1, pp. 83 - 95, 2021.

[8] M. Ahmadipour, M. Kobayashi, M. Wigger and G. Caire, "An Information-Theoretic Approach to Joint Sensing and Communication," *IEEE Transactions on Information Theory,* vol. 70, no. 2, pp. 1124 - 1146, 2024.

[9] O. Günlü, M. R. Bloch, R. F. Schaefer and A. Yener, "Secure Integrated Sensing and Communication," *IEEE Journal on Selected Areas in Information Theory,* vol. 4, pp. 40-53, 2023.

[10] O. Günlü, M. Bloch, R. F. Schaefer and A. Yener, "Nonasymptotic Performance Limits of Low-Latency Secure Integrated Sensing and Communication Systems," in *2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Seoul, Korea, 2024.

[11] O. Günlü, M. Bloch, R. F. Schaefer and A. Yener, "Secure IIntegrated Sensing and Communication for Binary Input Additive White Gaussian Noise Channels," in *2023 IEEE 3rd International Symposium on Joint Communications & Sensing (JC&S)*, Seefeld, Austria, 2023.

[12] T. Weissman, "Capacity of Channels With Action-Dependent States," *IEEE Transactions on Information Theory,* vol. 56, no. 11, pp. 5396 - 5411, 2010.

[13] R. Ahlswede and a. N. Cai, "Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder," in *General Theory of Information Transfer and Combinatorics*, Berlin, Springer, 2006, pp. 258-275.

[14] A. Cohen and A. Cohen, "Wiretap Channel With Causal State Information and Secure Rate-Limited Feedback," *IEEE Transactions on Communications,* vol. 64, no. 3, pp. 1192 - 1203, 2016.

[15] X. He and A. Yener, "The Role of Feedback in Two-Way Secure Communications," *IEEE Transactions on Information Theory,* vol. 59, no. 12, pp. 8115 - 8130, 2013.

[16] G. Bassi, P. Piantanida and S. S. Shitz, "The Wiretap Channel With Generalized Feedback: Secure Communication and Key Generation," *IEEE Transactions on Information Theory,* vol. 65, no. 4, pp. 2213 - 2233, 2019.

[17] E. Ardestanizadeh, M. Franceschetti, T. Javidi and Y.-H. Kim, "Wiretap Channel With Secure Rate-Limited Feedback," *IEEE Transactions on Information Theory,* vol. 55, no. 12, pp. 5353 - 5361, 2009.

[18] M. Tahmasbi, M. R. Bloch and A. Yener, "Learning an Adversary's Actions for Secret Communication," *IEEE Transactions on Information Theory,* vol. 60, no. 3, pp. 1607 - 1624, 2020.

[19] Y. Chen, T. Oechtering, H. Boche, M. Skoglund and Y. Luo, "Distribution-Preserving Integrated Sensing and Communication with Secure Reconstruction," in *2024 IEEE International Symposium on Information Theory (ISIT)*, Athens, Greece, 2024.

[20] M. Ahmadipour, M. Wigger and S. Shamai, "Integrated Communication and Receiver Sensing with Security Constraints on Message and State," in *2023 IEEE International Symposium on Information Theory (ISIT)*, Taipei, Taiwan, 2023.