Technical Report Documentation Page

1. Report No.	2. Government Accession No. N/A	3. Recipient's Catalog No. N/A
4. Title and Subtitle Timing-based Attacks for HATS		5. Report Date January 30, 2026
		6. Performing Organization Code N/A
7. Author(s) Truman Welling; Aylin Yener, Ph.D. https://orcid.org/0000-0003-0820-3390.		8. Performing Organization Report No. N/A
9. Performing Organization Name and Address The Ohio State University Address: 281 W Lane Ave, Columbus, OH 43210		10. Work Unit No. (TRAIS) N/A
		11. Contract or Grant No. 69A3552348327
12. Sponsoring Agency Name and Address The Ohio State University Address: 281 W Lane Ave, Columbus, OH 43210		13. Type of Report and Period Covered Final (Aug '24 to Dec '25)
		14. Sponsoring Agency Code N/A

15. Supplementary Notes
N/A

16. Abstract

We have addressed attacks on information freshness using a model with application to cooperative autonomous routing networks. In this model, each user monitors the status of each other user in the network, where the statuses are communicated using beacon transmissions over a shared channel. We consider an adversarial attack where a portion of the beacon transmissions are delayed, causing each user to act on outdated information. As a method of mitigation of the adversarial delays, we allow the users to reset beacon transmissions. The users select the rate at which beacon transmissions are started from when the channel becomes idle and how long the users wait before resetting a transmission with the objective of having the most up to date information at the monitors. The adversary selects the average increase by which transmission durations are extended with the objective of having the status information at the users be as outdated as possible.

17. Key Words	18. Distribution Statement
Timing attack, Age of Information, Stackelberg game	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	12 pages	N/A

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

CARMEN+

Center for Automated Vehicles Research with Multimodal Assured Navigation

USDOT University Transportation Centers Program

Final Report: Timing-based Attacks for HATS

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: August 1, 2024 Project End: December 31, 2025 Submission: January 30, 2026

Consortium Members:

The Ohio State University College of Engineering · The University of Texas at Austin · UCI University of California, Irvine · North Carolina Agricultural and Technical State University

Abstract

We have addressed attacks on information freshness using a model with application to cooperative autonomous routing networks. In this model, each user monitors the status of each other user in the network, where the statuses are communicated using beacon transmissions over a shared channel. We consider an adversarial attack where a portion of the beacon transmissions are delayed, causing each user to act on outdated information. As a method of mitigation of the adversarial delays, we allow the users to reset beacon transmissions. The users select the rate at which beacon transmissions are started from when the channel becomes idle and how long the users wait before resetting a transmission with the objective of having the most up to date information at the monitors. The adversary selects the average increase by which transmission durations are extended with the objective of having the status information at the users be as outdated as possible.

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

The future of transportation systems includes Highly Automated Transportation Systems (HATS). These systems perform decision making based on information collected from a variety of on board sensors such as cameras, LIDAR, and RADAR. Cooperative Autonomous Routing is a paradigm that uses network communication to coordinate the movements of autonomous vehicles, providing access to a fundamentally different kind of information for decisions to be based on, which will enable safer and more efficient systems. The goal of this project is to consider new attacks on information freshness as well as potential strategies for mitigation

Within a cooperative autonomous routing network, the value of the information communicated is inherently tied to how recently it was generated, or the freshness of the information. Threats to information freshness in HATS can be both intentional and unintentional. We consider an adversarial attack on a network of vehicles engaged in cooperative autonomous routing. In this setting, each vehicle communicates a status update, consisting of information such as position, velocity, acceleration, preferred path, etc., over a shared channel. To maximize the effectiveness of the cooperative autonomous routing strategy, the updates of each status need to be frequent enough and the information communicated needs to be fresh.

Contents

Introduction

The future of transportation systems includes Highly Automated Transportation Systems (HATS). These systems perform decision making based on information collected from a variety of on board sensors such as cameras, LIDAR, and RADAR. Cooperative Autonomous Routing is a paradigm that uses network communication to coordinate the movements of autonomous vehicles, providing access to a fundamentally different kind of information for decisions to be based on, which will enable safer and more efficient systems.

Within a cooperative autonomous routing network, the value of the information communicated is inherently tied to how recently it was generated, or the freshness of the information. Good decision making should be based on high quality information from a variety of sources. One aspect of high quality information is how fresh the information is. Age of Information (AoI) is a metric that quantifies information freshness of a status update and is defined as the difference between the current time and the generation time of the update [1] [2].

Threats to information freshness in HATS can be both intentional and unintentional. We consider an adversarial attack on a network of vehicles engaged in cooperative autonomous routing. In this setting, each vehicle communicates a status update, consisting of information such as position, velocity, acceleration, preferred path, etc., over a shared channel. To maximize the effectiveness of the cooperative autonomous routing strategy, the updates of each status need to be frequent enough and the information communicated needs to be fresh.

In particular, we consider a cooperative autonomous vehicle network consisting of n vehicles, where each vehicle monitors the status of each other vehicle in the network and the statuses are communicated using beacon transmissions over a shared channel. An adversary attacks the network by delaying a portion of the beacon transmissions [3]. The goal of the vehicles is to minimize the AoI, while the adversary tries to maximize the AoI.

Related Work

We considered a networking model similar to that in [4], though we consider an adversarial attack while the other does not. We also use techniques developed for AoI analysis developed in [5]. Our work is also related to the following works that consider attacks on information freshness. A setting where an adversary wants to jam the legitimate transmissions and both parties choose power levels subject to a power constraint is considered in [6]. A different style of attack on information fresheness, dubbed timestomping, is where the adversary changes the timestamps status updates as it exchanges information with other users in a gossip network [7]. Jamming has also been considered for gossip networks in [8]. A game theoretic analysis of the AoI in a network where the source is updating multiple users and the adversary can block a fixed portion of the transmissions is considered in [9]. Bounds illustrating the scaling of the AoI in a network where a base station updates monitors where an adversary can jam a single user at each transmission block are derived in [10]. [11] considers a sensor network where incorrect information is injected by adversaries.

Problem Setting

Consider a cooperative autonomous vehicle network consisting of n vehicles, where each is a source and a monitor. Specifically, each vehicle monitors the status of all the other vehicles in the network and broadcasts status updates to the other vehicles. We assume that all of the updates are communicated as a beacon, thus the age of the status of vehicle i is the same at all vehicles. We assume that the channel is shared by all vehicles and that a CSMA medium access scheme governs the channel use, meaning each time the channel becomes idle (a transmission terminates) each vehicle generates a backoff time and if no other vehicles has begun transmitting when the backoff time is reached that vehicle begins broadcasting an update. We approximate the CSMA scheme by having vehicle k for $k \in \{1, \dots, n\}$ select an exponentially distributed back-off time with rate R_k. We also operate under the assumption that sensing if the channel is busy can happen instantaneously.

We assume that each vehicle is able to generate the desired update, consisting of position, velocity, acceleration, preferred path, etc., at will. Consequently, the age of the packet being transmitted when the transmission begins is zero. The duration of a transmission by vehicle k is exponentially distributed with rate H_k and let $\boldsymbol{H}$ denote $[H_1 \cdots H_n]$.

The adversary present in the network increases the average transmission duration by a random amount that is exponentially distributed with rate H_A for a fraction $\alpha \in [0,1]$ of the transmissions. We will refer to the transmission delays as an adversarial attack, but these delays could also be due to environmental interference.

To combat adversarial delays, the vehicles can prematurely end a transmission, returning the channel to the idle state. The start of a new transmission is the same whether an update is successfully transmitted or if a transmission is reset. We note that if a transmission is prematurely ended, no status update is by the monitoring vehicles. Since the reset time is exponentially distributed, the resets can be done in the following distributed fashion. Each vehicle generates a maximum transmission duration at the beginning of each new transmission and ends the transmission if the maximum duration is reached. The maximum transmission duration is exponentially distributed at each user with rate $(n-1)H_r$ resulting in a total reset rate of H_r, as exponential reset rates are additive. Note that this formulation is agnostic as to whether a transmission is delayed by the adversary or not.

The vehicles participating in the cooperative autonomous routing network want to minimize the sum of status ages while the adversary wants to maximize status ages minus a cost constraint tied to the delays induced by the adversary. The parameters $\boldsymbol{H}$ are fixed, as they are properties of the channel. The legitimate users set the parameters H_r and R_k for $k \in \{1, \dots, n\}$ and the adversary sets the parameter H_A. For environmental effects delaying the transmission, treating the selection of H_A as an adversary is equivalent assuming the worst-case environmental delays.

Solution Structure

The first result in [3] is an expression for the AoI of the status of vehicle i at the other vehicles, which we denote by $\overline{\Delta}_i(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha)$. Then the sum of status ages at user i is given by

$$\Gamma_i(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha) = \sum_{j \neq i} \overline{\Delta}_j(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha).$$

The objective of the users when selecting a policy is to have each monitor operating with the freshest information with no user having priority over any other user, given the adversary's policy H_A. A mathematical realization of this objective is the average sum of status ages across all users, i.e.,

$$\overline{\Delta}(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha) = \frac{1}{n}\sum_{i=1}^{n} \Gamma_i\,(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha) = \frac{n-1}{n}\sum_{i=1}^{n} \overline{\Delta}_i\,(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha).$$

The goal of the legitimate users is to minimize $\overline{\Delta}(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha)$.

The adversary wants to harm the network as much as possible, but has a cost associated with each attacked transmission. The goal to adversely affect the AoI of the network is captured by maximizing $\overline{\Delta}(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha)$. The cost associated with attacking transmissions is $\gamma D_A(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha)$, with $\gamma \geq 0$. The function $D_A(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha)$ can be interpreted as a rate of delay.

We formulate the solution in terms of a Stackelberg game, with the vehicles as the leader and the adversary as the follower. The vehicles seek to minimize $\overline{\Delta}(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A^*, \alpha)$, where H_A^* is the value of H_A that maximizes $\overline{\Delta}(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha) - \gamma D_A(\boldsymbol{R}, \boldsymbol{H}, H_r, H_A, \alpha)$, i.e., the optimal adversarial strategy given the strategy $\{\boldsymbol{R}, H_r\}$ of the legitimate users.

We have the following insights about the optimal legitimate user policy from [3]. The optimal reset rate H_r does not go to zero as the rate of delay H_A goes to zero when all messages are delayed, i.e., $\alpha = 1$, but becomes a function of $\{\boldsymbol{R}, \boldsymbol{H}\}$. This implies that the vehicles do not just wait for the delayed transmissions to be successful, but as the transmission durations are random, the vehicles reset the transmissions waiting for a shorter transmission to come through.

Another insight is that if the adversary had control over α, it would be optimal to select the largest α possible. This is why we do not consider optimization over α, and instead put in the maximal value for α.

Numerical results

For a communication network with $n = 5$ users based on DSRC [12], we get $R_{UB} = 121.31$ allows us to justify our assumption that there are no collisions. We assume an average transmission time of 5ms for each user, i.e., $H_1 = \cdots = H_5 = 200$, and $\alpha = 0.4$.

To solve the optimization problem, we performed an alternating optimization legitimate users use differential evolution in the minimization and solve for H^* using minimize scalar, where both functions come from scipy [13].

In Figure 1, we see that the adversarial rate of delay increases as the cost parameter increases (the expected increase in duration decreases as the cost parameter increases) and that the reset rate H_r decreases as the adversarial rate increases.

Figure 2 shows that as the cost parameter increases, the optimal policy results in decreased $\bar{\Delta}$. This primarily due to the increase in H_A but is also affected by the decrease in the optimal H_r.

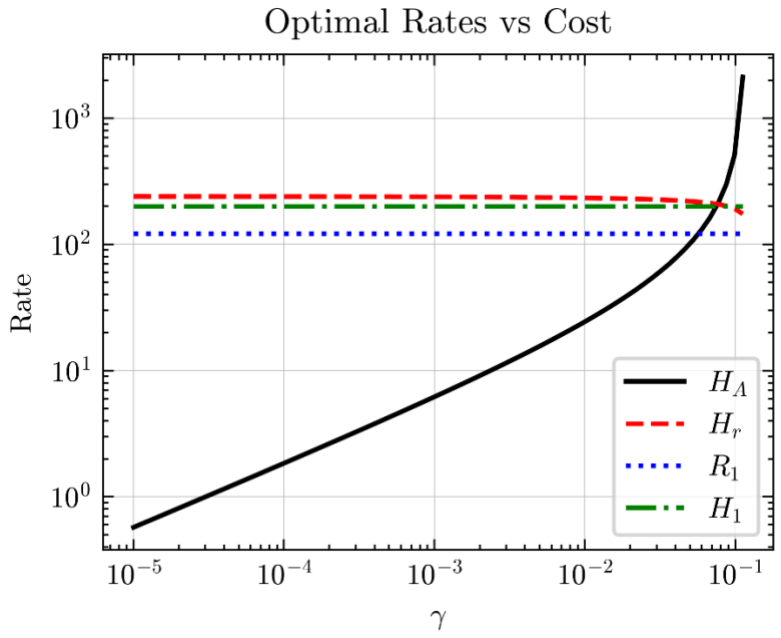

Figure 1: The optimal rate of delay chosen by the adversary and the optimal reset rate selected by the legitimate users for different values of the cost $\boldsymbol{\gamma}$. The result of the optimization gave $\boldsymbol{R_1 = \cdots = R_5}$ and selected $\boldsymbol{H_1 = \cdots = H_5}$ so we only plotted $\boldsymbol{R_1}$ and $\boldsymbol{H_1}$.

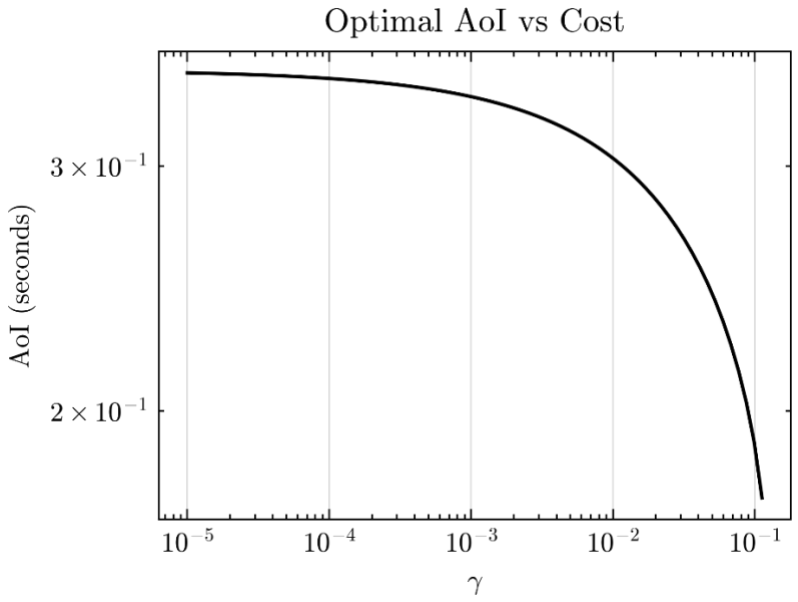

Figure 2: The equilibrium AoI for different values of the cost $\boldsymbol{\gamma}$.

Conclusion

We evaluated the age of information of a cooperative autonomous routing network with transmission delays caused by an adversary and user resets to combat those delays. We formulated the problem as a Stackelberg game where the legitimate user objective is the average AoI and the adversary objective is the average AoI minus a cost constraint. We provided limiting analysis of the resulting optimization problem and numerically showed how the cost on the adversary affects the other rates.

References

[1] S. Kaul, R. Yates and M. Gruteser, "Real-time status: How often should one update?," in *2012 Proceedings IEEE INFOCOM*, 2012.

[2] R. D. Yates, Y. Sun, D. R. Brown, S. K. Kaul, E. Modiano and S. Ulukus, "Age of information: An introduction and survey," *IEEE Journal on Selected Areas in Communications,* vol. 39, no. 5, pp. 1183-1210, 2021.

[3] T. Welling and A. Yener, "How to Mitigate a Timing Attack on Vehicular Networks: Cooperative Resetting Strategies," in *GLOBECOM 2025-2025 IEEE Global Communications Conference*, 2025.

[4] A. Maatouk, M. Assaad and A. Ephremides, "On the age of information in a CSMA environment," *IEEE/ACM Transactions on Networking,* vol. 28, no. 2, pp. 818-831, 2020.

[5] R. D. Yates and S. K. Kaul, "The age of information: Real-time status updating by multiple sources," *IEEE Transactions on Information Theory,* vol. 65, no. 3, pp. 1807-1827, 2018.

[6] G. D. Nguyen, S. Kompella, C. Kam, J. E. Wieselthier and A. Ephremides, "Impact of hostile interference on information freshness: A game approach," *2017 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt),* pp. 1-7, 2017.

[7] P. Kaswan and S. Ulukus, "Timestomping vulnerability of age-sensitive gossip networks," *IEEE Transactions on Communications,* vol. 72, no. 7, pp. 4193-4205, 2024.

[8] P. Kaswan and S. Ulukus, "How robust are timely gossip networks to jamming attacks?," *IEEE Journal on Selected Areas in Information Theory,* vol. 4, pp. 820-832, 2024.

[9] S. Banerjee and S. Ulukus, "Game theoretic analysis of an adversarial status updating system," in *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022.

[10] S. Banerjee and S. Ulukus, "Age of information in the presence of an adversary," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2022.

[11] L. Badia and T. Marchioro, "On the Anarchy of Multiple False Data Injectors for Age of Incorrect Information in Sensor Networks," in *2025 IEEE Wireless Communications and Networking Conference (WCNC)*, 2025.

[12] "IEEE Standard for Information Technology - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999),* pp. 1-1076, 2007.

[13] P. Virtanen and e. al., "SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python," *Nature Methods,* vol. 17, no. 3, pp. 261-272, 2020.