

A Game-Theoretic Approach for Distributed Attack Mitigation in Intelligent Transportation Systems

Talal Halabi
University of Winnipeg
Manitoba, Canada
t.halabi@uwinnipeg.ca

Omar Abdel Wahab
Université du Québec en Outaouais
Quebec, Canada
omar.abdulwahab@uqo.ca

Mohammad Zulkernine
Queen's University
Ontario, Canada
mzulker@cs.queensu.ca

Abstract—Intelligent Transportation Systems (ITS) play a vital role in the development of smart cities. They enable various road safety and efficiency applications such as optimized traffic management, collision avoidance, and pollution control through the collection and evaluation of traffic data from Road Side Units (RSUs) and connected vehicles in real time. However, these systems are highly vulnerable to data corruption attacks which can seriously influence their decision-making abilities. Traditional attack detection schemes do not account for attackers' sophisticated and evolving strategies and ignore the ITS's constraints on security resources. In this paper, we devise a security game model that allows the defense mechanism deployed in the ITS to optimize the distribution of available resources for attack detection while considering mixed attack strategies, according to which the attacker targets multiple RSUs in a distributed fashion. In our security game, the utility of the ITS is quantified in terms of detection rate, attack damage, and the relevance of the information transmitted by the RSUs. The proposed approach will enable the ITS to mitigate the impact of attacks and increase its resiliency. The results show that our approach reduces the attack impact by at least 20% compared to the one that fairly allocates security resources to RSUs indifferently to attackers' strategies.

Index Terms—Intelligent Transportation Systems, connected vehicles, security resources, security game, distributed attacks, maxmin game, attack mitigation, resiliency.

I. INTRODUCTION

Intelligent Transportation Systems (ITS) are rapidly evolving Cyber-Physical Systems (CPS) that exploit existing and emerging communication technologies, computing infrastructures, and systems engineering concepts to improve transportation in all aspects. In ITS, complex and dynamic data generated by the connected vehicles and the infrastructure are communicated and processed in real time to enable a plethora of services such as road driving conditions and safety improvement, traffic management, pollution control, and vehicle maintenance. Connected vehicles are usually equipped with On-Board-Units (OBUs) that enable them to exchange traffic-related critical information with the Road Side Units (RSUs). Connected vehicles are becoming increasingly essential in the operations of ITS to improve their efficiency by overcoming the limitations of static infrastructures. However, the high level of openness and connectivity in Vehicle-to-Infrastructure (V2I) communications makes the whole transportation system highly vulnerable to various threats that target the data, services, and decisions.

Security has been identified as one of the major challenges to the implementation of a dependable ITS. For instance, the legitimacy and accuracy of the data and measurements collected

and transmitted via the vehicles and RSUs to the Traffic Management Center (TMC), which is the entity responsible for traffic-related decision making in ITS, are critical to the performance and quality of delivered services (e.g., reliable collision avoidance warnings, optimal traffic congestion management). These data may be manipulated by malicious vehicles that seek to produce some damage within the transportation system (e.g., accidents, traffic jam). However, due to the highly volatile nature of the intelligent transportation environment and the ephemeral interactions between connected vehicles and the underlying infrastructure, traditional security solutions for data integrity protection which revolve around cryptography and centralized security schemes fail to support the required levels of mobility and flexibility. Moreover, security attacks are increasingly evolving to become more sophisticated and intelligent with the objectives of rendering their detection less straight-forward and increasing their impact. For instance, in ITS, an attacker controlling a set of malicious or compromised vehicles might target different infrastructural entities at different magnitudes to reduce the system's detection probability and prolong the attack duration as much as possible before being detected. Therefore, attack detection schemes in ITS should take into consideration these kinds of adversarial strategies in the defense process and be able to counter the potential of possible distributed attacks. This aspect has been missing in traditional attack detection approaches for ITS.

Moreover, ITS are large-scale systems, hence applying traditional anomaly detection schemes without accounting for the constraints on resources dedicated for security and the trade-off between security and effectiveness might lead to serious performance limitations. For instance, monitoring and analyzing the legitimacy of collected information at each RSU is not realistic, since it will affect the ability of the ITS to respond to traffic events in real time. Thus, the ITS must optimize the implementation of attack detection load among the RSUs in a way that minimizes the impact of distributed attacks launched by the army of malicious connected vehicles. This paper responds to the limitations described above by proposing an attack mitigation approach that recognizes the potential of sophisticated attack strategies and adheres to the finite amounts of dedicated security resources in the defense process. The approach is based on a non-cooperative game-theoretic model in which the payoffs of the TMC and the attacker are quantified in terms of detection rate, attack damage, and relevance of the information transmitted by the RSUs.

The model mainly involves an optimization problem, whose solution will lead the TMC to the optimal defense strategy. The latter consists in optimally distributing the attack detection load within the transportation infrastructure to mitigate the attack impact and increase the resilience of the ITS against distributed attacks. This high-level resiliency scheme can be integrated into different kinds of anomaly detection techniques (e.g., machine learning, profile-based).

The contributions of the paper are described as follows:

- First, we investigate the power of distributed data corruption attacks in ITS through a realistic threat model, where multiple RSUs are targeted at different timings throughout the attack lifetime and according to distinct proportions to reduce detection chances.
- Second, we devise a maxmin game model that describes the system and attacker's mixed strategies and computes their respective expected payoffs. The game is considered as an optimization problem, which we solve using linear programming. The attacker's optimal strategy is to follow an attack probability distribution over the set of RSUs in a way that maximizes the attack impact, and the TMC's optimal defense strategy is to distribute the available security resources among the RSUs in a way that minimizes the attack impact in the worst case attack scenario.

The proposed approach is evaluated through a set of simulations, and results prove that the integration of distributed attack strategies into the mitigation scheme increases system utility compared to an approach that equally distributes the detection load among the RSUs. The remainder of the paper is structured as follows. Section II discusses related work. Section III describes the threat model. Section IV presents the game model. In Section V, simulations are conducted and results are analyzed. Finally, Section VI concludes the paper.

II. RELATED WORK

This paper focuses on the mitigation of intelligent attacks that target data sensing and transmission in ITS to negatively impact system decisions. Data corruption attacks include data fabrication or alteration, which in turn can be carried out by Sybil and Wormhole attacks [1]. The safety of transportation infrastructure depends on its security against computer-based attacks. Fig. 1 shows the main ITS applications usually managed by the TMC, whose performance can be seriously degraded due to suboptimal decisions caused by corrupted data. Ghena et al. [2] investigated the security of networked traffic signal control systems and discovered a number of systematic security flaws, which they later exploited to create attacks that gain control of or an unfair advantage on the ITS. Chen et al. [3] performed a detailed security analysis of the transportation systems that are based on connected vehicles. They targeted a realistic threat, namely data spoofing from malicious vehicles, with the goal of creating traffic congestion. Yen et al. [4] compared the performance of different traffic scheduling algorithms when they are under attack. They Focused on time spoofing attacks where individual vehicles arriving at an intersection can alter their arrival times. Feng et al. [5] investigated the vulnerability of actuated and adaptive traffic control systems in a connected environment. Their results showed that various attack scenarios

can lead to increased system delay.

To counter such threats, the ITS normally implements defense mechanisms based on certification, trust establishment, and data analytics (e.g., statistical or learning-based). For instance, Khan et al. [6] proposed a cluster-oriented model in which a cluster head evaluates trust in the network by following a watchdog approach. On the other hand, Minhas et al. [7] combined entity-oriented and data-based trust by using reputation and experience to evaluate the plausibility of broadcasted events. Other approaches use machine learning techniques to detect the anomalies in the data collected from the infrastructure [8]. However, existing attack detection schemes do not consider the possibility of distributed attacks and ignore the constraints on available security resources. For example, analyzing the legitimacy of the data transmitted by all RSUs in the transportation infrastructure is an exhaustive task to be performed by the TMC at runtime, which can affect its performance and lead to suboptimal responses to traffic events.

Game theory is generally perceived as a potential mathematical language to model the conflicted interactions between attackers and defenders in modern computer systems with the goal of generating the optimal decision for a defender under adversarial settings [9]. Several attack detection games have been already proposed to secure ITS and address traffic prediction and decision-making issues [10]. In such games, usually of non-cooperative type, players aim at maximizing their own payoffs and minimizing the payoffs of their opponents. The attacker's payoff can be modeled as her gain from launching the attack on the transportation infrastructure or the impact of her attack on system performance. For instance, Laszka et al. [11] provided theoretical foundations for the protection of ITS against the attacks that tamper with traffic-signal schedules by introducing a game-theoretic model for attack detection and mitigation. Alpcan and Buchegger [12] proposed a game-theoretic framework that optimizes defensive measures in Vehicular Ad Hoc Networks (VANETs). Moreover, several game theory methods like the evolutionary game, the stochastic game, and the Bayesian game have been applied to alleviate the Sybil attack within ad hoc networks [13]. Finally, cooperative game theory may also be applied to design secure collaboration schemes in CPS like the connected vehicles [14]. In this paper, a maxmin game is devised to derive the TMC's optimal defense strategy under distributed attack scenarios.

III. THREAT MODEL

ITS are data-driven systems in nature, hence the accuracy of sensed or collected measurements and data is crucial to the quality of delivered applications. These applications are often directly related to public safety and economy. Thus, the use of corrupted data generated by malicious vehicles or compromised RSUs in the decision-making process could lead to disastrous consequences including extreme traffic congestion and accidents, especially if information inaccuracy is being propagated on the long run. Data fabrication or alteration may be carried out through several forms of attacks:

- False Data Injection: Apart from the case of a malfunctioning sensor transmitting inaccurate information, spreading bogus data can be deliberately performed by malicious

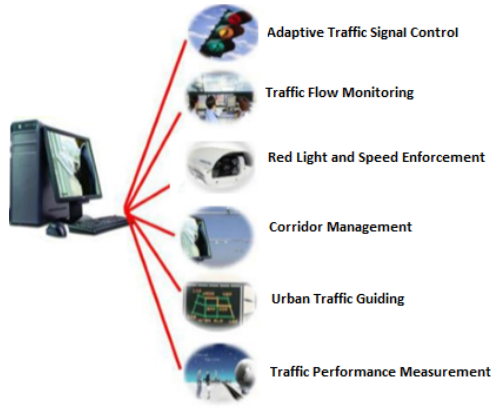


Fig. 1: Major ITS applications managed by the TMC.

vehicles to alter system decisions throughout the data aggregation process. Also, in vehicular crowdsourcing, vehicles may locally modify the collected data before sending it to the system for mining and analysis. Such an attack may be launched in two forms: 1) Wormhole, where an attacking vehicle transfers the messages received in a certain area to a different one to compromise the RSUs, and 2) Replay, where the attacker vehicle replays the same message multiple times to sabotage the accuracy of collected data at the TMC.

- Data or time spoofing: This occurs when the malicious vehicle changes the speed or location broadcasted in its Basic Safety Message (BSM) to set the arrival time and the requested phase of its choice and thus increase the RSU's corresponding arrival table element by one. Communication-based attacks such as data packet injection and channel overhearing/jamming may fall under this category as well [15].
- Sybil: This attack occurs when a single vehicle possesses multiple fake identities in the system [16] and uses them to either directly provide falsified information or to alter the traffic-related measurements collected at the RSUs like the traffic flow rate or vehicle queue length.
- Collusion: Such an attack is usually carried out by multiple malicious vehicles having similar interests, when they co-operate to transmit unified low quality or falsified information that could negatively influence system measurements and lead to unexpected decisions.

Such attacks may be carried out in an evolved and distributed fashion to alter the functioning of ITS more discretely without being rapidly detected. This is a highly realistic threat model that requires reasonable amounts of adversarial resources and sufficient reconnaissance of system operations to be materialized into a lethal and long-lasting cyberattack (e.g., Advanced Persistent Threat or APT). A distributed data corruption attack may cause serious performance degradation in large-scale CPS such as ITS when propagated over a long period of time without effective detection. Attack load distribution over several targeted RSUs, which could be traffic signal controllers as depicted in Fig. 2, is reflected by a probability distribution according to which the attacker exploits her malicious vehicles to send misleading information to the RSUs at different timings and rates. The attack becomes even more powerful if targeting a

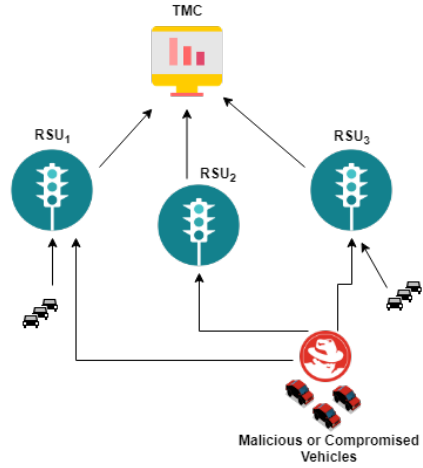


Fig. 2: Distributed Attack on ITS.

specific application. Moreover, the attacker does not have to be a vehicle belonging to the system or physically present within the transportation infrastructure, but could be a malicious entity who had compromised and recruited a set of connected vehicles in her army to launch a persistent attack on the TMC through external command and control operations. The motivation of the attacker behind such a sophisticated attack strategy lies in the possibility of bypassing detection by the defense mechanism deployed at the TMC and increasing the attack impact.

IV. OPTIMAL DEFENSE STRATEGY: A MAXMIN GAME

A maxmin game model is proposed to derive the optimal defense strategy of the ITS, according to which the TMC distributes its security resources among RSUs while considering the distributed attack strategy. Game theory provides a mathematical language to model the conflicted interactions between attackers and defenders in networked systems. It has already been used to handle service management in vehicular networks [17]. Several games proposed to secure ITS applications such as traffic prediction, where the attacker's payoff is quantified in terms of the attack impact on system performance. In our game, we integrate a complex attack strategy into the formulation of the mitigation problem to provide the TMC with more resiliency against sophisticated and evolving attack scenarios, such as distributed data corruption. Moreover, our game enables the TMC to optimize the distribution of available attack detection load in the transportation infrastructure, since monitoring and analyzing the legitimacy of collected data at all RSUs is time and resource-consuming, and may substantially degrade system performance.

In our model, we consider a set of RSUs geographically distributed in the transportation infrastructure, and denoted by $\mathcal{N} = \{i, i \in \mathbb{N}^*, i \leq N\}$, where N is the number of RSUs. The RSUs participate in V2I communications and collect traffic-related data from connected vehicles. The data are then transmitted to the TMC for mining and decision making. The attacker in our system follows a mixed strategy that consists in spreading the attack load between multiple RSUs to increase the attack impact on intelligent road traffic application. To achieve this, the attacker adopts a probability distribution vector denoted by $\alpha = (\alpha_1, \dots, \alpha_N)$, such that

$\alpha_i \geq 0 \forall i \in \mathcal{N}$ and $\sum_{i \in \mathcal{N}} \alpha_i = 1$, to attack the RSUs in the system with the objective of minimizing the detection rate of the TMC. This may be translated by targeting the RSUs at different timings, with different rates, and also by feeding them with distinct proportions of corrupted data. This sophisticated strategy allows the attacker to increase the attack impact and probably succeed in bypassing being detected through the defense mechanisms deployed by the TMC. It is assumed that the attacker possesses sufficient resources and time to continuously monitor system behavior and operations and acquire the necessary reconnaissance of defense strategies to launch coordinated and persistent attacks.

On the other hand, the TMC will adopt a mixed strategy to defend targeted ITS applications against malicious data and to reduce the impact of the attack on their decisions. This strategy will consist in following a probability distribution vector denoted by $\beta = (\beta_1, \dots, \beta_N)$, such that $\beta_i \geq 0 \forall i \in \mathcal{N}$ and $\sum_{i \in \mathcal{N}} \beta_i = 1$, according to which the TMC will distribute the security resources available for attack detection among the RSUs of the infrastructure with the objective of maximizing the minimization sought by the attacker. By taking into account the distributed attack strategy while generating the optimal defense strategy of the TMC, the latter will stay one step ahead in the defense process, constantly preparing for the worst case scenario. This will enable the ITS to manage its intelligent operations in a more resilient fashion.

The utility of the TMC, which reflects its gain from following a certain defense strategy, is determined according to the payoff matrix A defined as follows:

$$A_{ij} = \begin{cases} -(1-\delta)D_i w_i & i = j \\ -D_j w_j & i \neq j \end{cases} \quad (1)$$

where the rows and columns represent the pure strategies of the TMC and the attacker, respectively. A TMC's pure strategy consists in continuously monitoring the accuracy of transmitted data from a specific RSU to detect malicious information, whereas an attacker's pure strategy consists in attacking the system through only one RSU each time. The term A_{ij} quantifies the utility of the TMC when the deployed defense mechanism is protecting RSU_i while the attack is performed on RSU_j . The utility of the TMC is equal to the negation of the attack impact, i.e., a higher utility value reflects a lower attack impact. The attack impact is quantified in terms of the achieved detection rate, denoted by δ , the attack damage that occurs at RSU_i , denoted by D_i (evaluated based on the influenced decisions by the application), and the relevance of the information collected from RSU_i , denoted by w_i . The latter may be determined according to the delivered ITS application, amount of transmitted data, and nature of the traffic event in question. For instance, an RSU collecting voluminous amounts of information from an urban area may be assigned a higher weight in the data aggregation process performed by the TMC than other RSUs. Also, if the decision made by the TMC is related to an event that occurred at a specific location, the data broadcasted by the vehicles through the closest RSU to that location will be the most relevant to the decision.

If the TMC is monitoring the RSU targeted by the attack

TABLE I: An example of players' utilities in a scenario with 3 RSUs.

	RSU_1	RSU_2	RSU_3
RSU_1	$-(1-\delta)D_1 w_1$	$-w_2 D_2$	$-w_3 D_3$
RSU_2	$-w_1 D_1$	$-(1-\delta)D_2 w_2$	$-w_3 D_3$
RSU_3	$-w_1 D_1$	$-w_2 D_2$	$-(1-\delta)D_3 w_3$

(e.g., $i = j$), the attack impact will be computed as the product of D_i , w_i , and the rate of attacks not being detected by the defense mechanism, i.e., $1 - \delta$. On the other hand, if the TMC is watching over RSU_i while the attack is performed on RSU_j (e.g., $i \neq j$), the impact will be equal to the product of D_j and w_j . Note that the values of the parameters involved in the computation are all normalized to be between 0 and 1. It is also important to mention that the monitoring cost was not considered in the computation of the utility since it is assumed to be negligible with respect to the attack damage. Table I shows an example of the TMC's utility (row strategies) when there are three RSUs that may be targeted by an attack.

The utility of the attacker is equal to the opposite of that of the TMC (i.e., the occurred attack impact), which means that the attacker will gain what the system will lose. This leads us to a two-players zero-sum maxmin game, in which the objective of the attacker is to distribute her attack load over the set of RSUs to maximize the attack impact, and the objective of the TMC is to distribute the available security resources among the RSUs in such a way that minimizes this maximization. The optimal defense strategy of the TMC, represented by the probability distribution vector β , is derived by solving the following optimization problem:

$$\text{Maximize } \min_{j \in \mathcal{N}} \sum_{i \in \mathcal{N}} A_{ij} \beta_i \quad (2)$$

Subject to:

$$\sum_{i \in \mathcal{N}} \beta_i = 1 \quad (3)$$

$$\beta_i \geq 0 \forall i \in \mathcal{N} \quad (4)$$

A maxmin strategy is one that maximizes the player's worst-case payoff. In this problem, the TMC strives to maximize its minimum achieved utility, a conservative strategy that adds a level of resiliency against attacks. Since the TMC's utility value is always negative, maximizing the minimum utility value is equivalent to minimizing the largest attack impact that may occur. This is equivalent to the following linear program:

$$\text{Maximize } \rho \quad (5)$$

Subject to:

$$\rho \leq \sum_{i \in \mathcal{N}} A_{ij} \beta_i \quad \forall j \in \mathcal{N} \quad (6)$$

$$\sum_{i \in \mathcal{N}} \beta_i = 1 \quad (7)$$

$$\beta_i \geq 0 \forall i \in \mathcal{N} \quad (8)$$

Similarly, the optimal attack strategy can be derived by solving a minmax game problem, in which the attacker tries to minimize the maximization that the TMC achieves, i.e., maximizing

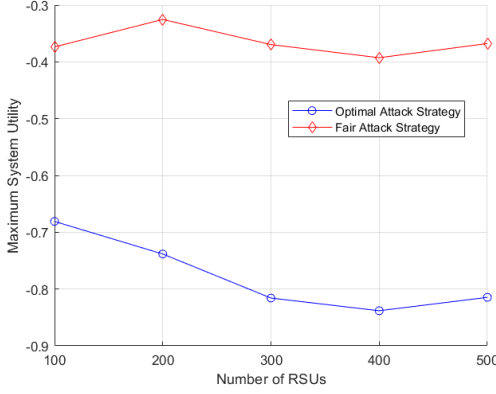


Fig. 3: Through the optimal attack strategy, the attacker increases her attack impact by minimizing the highest utility value achieved by the TMC.

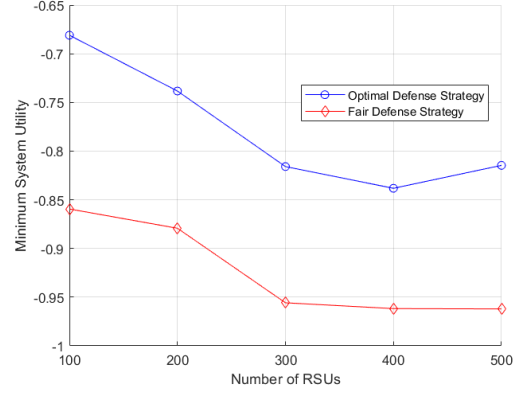


Fig. 4: Through the optimal defense strategy, the TMC reduces the attack impact by maximizing the minimum utility it may achieve.

the minimum impact yielded by the attack. This strategy will be determined by solving the following optimization problem:

$$\text{Minimize } \max_{j \in \mathcal{N}} \sum_{i \in \mathcal{N}} A_{ij} \alpha_i \quad (9)$$

Subject to:

$$\sum_{i \in \mathcal{N}} \alpha_i = 1 \quad (10)$$

$$\alpha_i \geq 0 \quad \forall i \in \mathcal{N} \quad (11)$$

This is equivalent to the following linear program:

$$\text{Minimize } \theta \quad (12)$$

Subject to:

$$\theta \geq \sum_{i \in \mathcal{N}} A_{ij} \alpha_i \quad \forall j \in \mathcal{N} \quad (13)$$

$$\sum_{i \in \mathcal{N}} \alpha_i = 1 \quad (14)$$

$$\alpha_i \geq 0 \quad \forall i \in \mathcal{N} \quad (15)$$

The two optimization problems are dual. Following the duality theorem [18], the maximum value achieved by the TMC is equivalent to the minimum value achieved by the attacker, which is equal to the value of the game. Moreover, according to the minimax theorem [19], any maxmin strategy profile (or, equivalently, minmax strategy profile) is a Nash equilibrium.

V. SIMULATION AND RESULTS

In this section, a set of simulations is conducted to evaluate the security and performance of our attack mitigation approach. The game model was implemented in a MATLAB environment. A MILP solver was used to produce the solutions to the optimization problems. The solver first reduces the problem size, then uses heuristics to solve a relaxed version of the problem and produce an initial feasible solution, and finally performs an exhaustive search for the optimal solution using a Branch and Bound algorithm [20]. The simulation is performed on a 64-bit Windows 10 machine equipped with an Intel Core

i7-3612QM CPU @ 2:10 GHz Processor and 12 GB of RAM. Due to the unavailability of data related to the attack damage in current ITS, the data required to compute the utilities of the TMC and the attacker were generated according to a random probability distribution. The values of parameters δ , D_i , and w_i were set between 0 and 1 for all RSUs. The evaluation is performed for different numbers of RSUs involved in the data acquisition process within the ITS. The results shown in all figures are the average of fifty runs.

Fig. 3 depicts the maximum utility achieved by the TMC when the attacker is following an optimal or a fair attack strategy. The optimal attack strategy consists of the vector of probability distribution generated by the minmax optimization problem defined in Eq. 9, and according to which the attack load will be distributed between the RSUs. On the other hand, the fair attack strategy consists in distributing the attack load equally between the RSUs indifferently to the objective of maximizing the attack impact. The results show that, by following the optimal attack strategy, the attacker was able to minimize the highest utility value achieved by the TMC. For example, in the case of 100 RSUs, this value dropped from -0.374 when the fair strategy was adopted to -0.681 when the optimal attack vector α was used. These values, when multiplied by -1, reflect the maximum attack impact that may occur within the ITS. Adopting the optimal attack strategy proved to be a way for the attacker to transform her attack to be more sophisticated and complex, yielding higher impact.

Fig. 4 illustrates the minimum utility value that may be achieved by the TMC, which reflects the highest attack impact occurred in the worst case scenario. This value was computed in both cases, the adoption of the optimal or fair defense strategies by the TMC. The optimal defense strategy consists of the vector of probability distribution β , produced by solving the maxmin optimization problem defined in Eq. 2. According to this vector, the TMC will split the available security resources among the RSUs of the infrastructure to defend the intelligent transportation application more effectively and counter the optimal attack strategy deployed by the attacker. The fair defense strategy consists in distributing these resources with equal probabilities among the RSUs, without taking into account the optimal attack

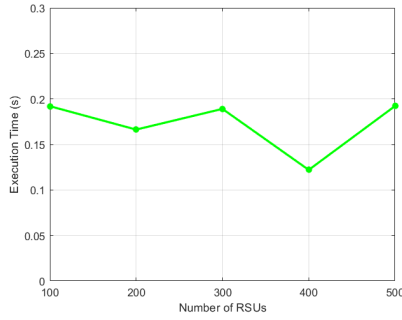


Fig. 5: The execution time of the game.

strategy that the attacker may be playing. The results show that, by following an optimal defense strategy, the TMC was able to maximize its minimum utility in the game, which is equivalent to minimizing the highest level of impact that may be caused by an attack. For instance, in the case of 100 RSUs, this value increased from -0.86 when a fair strategy was applied to -0.681 when an optimal strategy was played. This proves that the security game enabled the TMC to reduce the attack impact, making the ITS more resilient and tolerant to attacks. It is also worth noting that the values on the blue lines in Figs. 3 and 4 represent the values of the game, as described by the duality theorem, i.e., the minimum value achieved by the attacker is equivalent to the maximum value achieved by the TMC.

In Fig. 5, we measure the execution time of the MILP solver while increasing the number of RSUs involved in the decision making of the ITS application. The results show that the model can be scalable and may be applied in a large-scale transportation infrastructure without introducing considerable overhead on the TMC. The solver was fast in producing the solution to the optimization problem defined for the defense game. The optimal probability distribution vector applied on the available security resources can then be used by the TMC in real time to distribute these resources among the RSUs.

VI. CONCLUSION

Traditional attack detection schemes in ITS do not account for attackers' sophisticated and evolving strategies and ignore the constraints on security resources. In this paper, we investigated the power of distributed attacks on ITS, where the attacker splits the attack load among multiple RSUs to increase the attack impact and bypass the detection mechanism. Since the detection of such complex attacks is more difficult for the defense mechanism, we proposed an attack mitigation approach that aims at reducing the attack impact by following a mixed strategy of defense, consisting in distributing the available security resources optimally among the RSUs. The approach is based on a maxmin game model. Solving the game generates the optimal probability distribution vectors of attack and defense. Our approach reduces the attack impact by at least 20% compared to the one that fairly allocates security resources to RSUs indifferently to attackers' strategies. This enables the ITS to increase its resiliency and tolerance to attacks and mitigate their impact. In the future, we will apply the model on specific road traffic applications and evaluate the impact of data corruption attacks. Also, our model will be extended

to involve a secure cooperation scheme between the RSUs to mitigate the attack impact in a more distributed fashion.

ACKNOWLEDGMENT

This work is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Canada Research Chairs (CRC) program.

REFERENCES

- [1] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, no. 99, pp. 1–17, 2018.
- [2] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure," in *8th {USENIX} Workshop on Offensive Technologies ({WOOT} 14)*, 2014.
- [3] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," in *Network and Distributed Systems Security (NDSS) Symposium*, 2018.
- [4] C.-C. Yen, D. Ghosal, M. Zhang, C.-N. Chuah, and H. Chen, "Falsified data attack on backpressure-based traffic signal control algorithms," in *2018 IEEE Vehicular Networking Conference (VNC)*, pp. 1–8, IEEE, 2018.
- [5] Y. Feng, S. Huang, Q. A. Chen, H. X. Liu, and Z. M. Mao, "Vulnerability of traffic control system under cyber-attacks using falsified data," in *97th Annual Meeting of the Transportation Research Board*, 2018.
- [6] U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (dmn) in vehicular ad-hoc networks," *Procedia computer science*, vol. 46, pp. 965–972, 2015.
- [7] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 3, pp. 407–420, 2011.
- [8] S. Wang, J. Wu, S. Zhang, and K. Wang, "Ssds: A smart software-defined security mechanism for vehicle-to-grid using transfer learning," *IEEE Access*, vol. 6, pp. 63967–63975, 2018.
- [9] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Resource-aware detection and defense system against multi-type attacks in the cloud: Repeated bayesian stackelberg game," *IEEE Transactions on Dependable and Secure Computing*, 2019.
- [10] H. Sedjelmaci, M. Hadji, and N. Ansari, "Cyber security game for intelligent transportation systems," *IEEE Network*, 2019.
- [11] A. Laszka, W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Detection and mitigation of attacks on transportation networks as a multi-stage security game," *arXiv preprint arXiv:1808.08349*, 2018.
- [12] T. Alpcan and S. Buchegger, "Security games for vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 280–290, 2011.
- [13] A. Vasudeva and M. Sood, "Survey on sybil attack defense mechanisms in wireless ad hoc networks," *Journal of Network and Computer Applications*, 2018.
- [14] T. Halabi and M. Zulkernine, "Trust-based cooperative game model for secure collaboration in the internet of vehicles," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2019.
- [15] S. Ucar, S. C. Ergen, and O. Ozkasap, "Ieee 802.11 p and visible light hybrid communication based secure autonomous platoon," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8667–8681, 2018.
- [16] E. G. AbdAllah, M. Zulkernine, Y. X. Gu, and C. Liem, "Towards defending connected vehicles against attacks," in *Proceedings of the Fifth European Conference on the Engineering of Computer-Based Systems*, p. 9, ACM, 2017.
- [17] M. Aloqaily, B. Kantarci, and H. T. Mouftah, "Fairness-aware game theoretic approach for service management in vehicular clouds," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, IEEE, 2017.
- [18] D. G. Luenberger, *Introduction to linear and nonlinear programming*, vol. 28. Addison-Wesley Reading, MA, 1973.
- [19] J. v. Neumann, "Zur theorie der gesellschaftsspiele," *Mathematische annalen*, vol. 100, no. 1, pp. 295–320, 1928.
- [20] J. Clausen, "Branch and bound algorithms-principles and examples," *Department of Computer Science, University of Copenhagen*, pp. 1–30, 1999.