A Colonel Blotto Game for Security of Interdependent Intelligent Transportation and Communications Systems

Aidin Ferdowsi and Walid Saad
Wireless@VT, Bradley Department of Electrical and Computer Engineering, Virginia Tech
Blacksburg, VA, USA, {aidin.walids}@vt.edu

I. Introduction

The operation of future intelligent transportation systems (ITSs) and communications infrastructure (CI) will be highly interdependent [1]. Tomorrow's ITS will encompass autonomous connected vehicles (ACVs) which require significant wireless data transmissions through a CI such as a wireless cellular system. Thus, any failure in the CI will result in a non-optimal ITS traffic flow leading to traffic jams and inefficient fuel consumption. Meanwhile, road traffic congestions in the ITS will, in turn, require additional resources (e.g., bandwidth, power) from the CI due to interference and increased wireless traffic load. Such interdependencies render both ITS and CI vulnerable to traffic jam attacks on ITS. In such attacks, an adversary hijacks some of the ACVs and reduces their speed thus causing road traffic jams which in turn will strain the capacity of the CI. Remarkably, despite significant prior works on ITS or CI security [2], to our best knowledge, no work has analyzed this security interdependency among the two. The main contribution of this paper is to propose a novel Colonel Blotto game (CBG) framework [3] to analyze attacks on interdependent ITS and CI systems and devise optimal countermeasures to minimize the non-optimality in both ITS and CI caused by the physical attack. Simulation results show that the proposed CBG increases the security level of the ITS and CI compared to scenarios in which the administrator of the ITS and CI do not apply the solutions of such game.

II. Interdependent ITS and CI Model

Consider an ITS composed of a set $\mathcal{S}$ of N streets. This ITS has three main macroscopic characteristics in each street ij (direction of movement is from intersection i to intersection j) [2]: *Flow*, $q_{ij}(t)$ (in veh/h/lane), *density*, $k_{ij}(t)$ (in veh/km/lane), and *space-mean-speed*, $v_{ij}(t)$ (in km/h) [2].

These three parameters are related to each other as follows: $q_{ij}(t) = k_{ij}(t)v_{ij}(t), , k_{ij}(t) = \dfrac{1}{c_{1_{ij}} + \frac{c_{2_{ij}}}{v_{f_{ij}} - v_{ij}(t)} + c_{3_{ij}} v_{ij}(t)}$, where $v_{f_{ij}}$ is the free flow speed, $v_{c_{ij}}$ is the peed at capacity, and $k_{x_{ij}}$ is the traffic jam density. Also we have $c_{1_{ij}} = \frac{v_{f_{ij}}\left(2v_{c_{ij}} - v_{f_{ij}}\right)}{k_{x_{ij}} v_{c_{ij}}^2}$, $c_{2_{ij}} = \frac{v_{f_{ij}}\left(v_{f_{ij}} - v_{c_{ij}}\right)^2}{k_{x_{ij}} v_{c_{ij}}^2}$, and $c_{3_{ij}} = \frac{1}{q_{c_{ij}}} - \frac{v_{f_{ij}}}{k_{x_{ij}} v_{c_{ij}}^2}$. The maximum flow at each street is called flow at the capacity, $q_{c_{ij}}$ and its associated density is the density at capacity, $k_{c_{ij}}$. At each intersection, we consider that the sum of in-flow is equal to sum of out-flow. Let $\mathcal{I}_i$ be the set of intersections with in-flow towards intersection i, and $\mathcal{O}_i$ be the set of intersections towards which i has out-flow. Then, we will have $\sum_{j\in\mathcal{O}_i} q_{ij}(t) = \sum_{j\in\mathcal{I}_i} q_{ji}(t)$.

This research was supported by the U.S. National Science Foundation under Grants ACI-1541105, ACI-1638283, and IIS-1633363.

Furthermore, we consider a vehicular CI modeled as a Cox process as in [3], where the spatial layout of the streets is a Poisson line process and the locations of nodes on each line are modeled as a 1D Poisson point process. In this model, each vehicle or road side unit (RSU) can transmit data to other vehicles or RSUs. The success probability of any link when considering each street independently is given by [3]:

$$P_{c_{ij}} = \exp\left[-\frac{\beta\sigma^2 z^\alpha}{P_t} - 2p\gamma k_{ij}\beta^{1/\alpha} z \frac{\pi}{\alpha}\csc(\frac{\pi}{\alpha})\right], \quad (1)$$

where p_t is the transmission power, β is the target SINR threshold, σ^2 is the noise power. z is the distance of a receiver from the closest transmitter, α is the path loss exponent, p is the probability of each vehicle or roadside unit transmitting independently, and γ is a conversion parameter. From (1), we can see that an increase in the density of street ij results in lower success probability of communication links in ij.

A. Attack Model

Consider an attacker that can take control of R^a vehicles in an urban area. The attacker's goal is to reduce the flow in the streets by reducing the speed of ACVs that it can control. This action will cause higher density on the streets and will cause higher interference in the communication links. The flow between intersections i and j has the following relationship with the microscopic characteristic of the vehicles in the street [2]: $q_{ij}^{-1}(t) = \frac{1}{r_{ij}}\sum_{l=1}^{r_{ij}} h_{ij_l}(t)$, where r_{ij} is the number of vehicles between i and j and h_{ij_l} is the headway of the l-th vehicle between i and j. Let d_{ij} be the proportion of safe vehicles and a_{ij} be the proportion of the under attack vehicles in street ij and the defender's desired flow is $q_{ij}^d(t)$. Then the flow of street ij can be written as:

$$q_{ij}^{-1}(t) = \frac{a_{ij} q_{ij}^{a^{-1}}(t) + d_{ij} q_{ij}^{d^{-1}}(t)}{a_{ij}+d_{ij}} = \delta_{ij} q_{ij}^{a^{-1}}(t) + (1-\delta_{ij}) q_{ij}^{d^{-1}}(t), \quad (2)$$

where $\delta_{ij} = \frac{a_{ij}}{a_{ij}+d_{ij}}$. From (2), we can see that for $\delta_{ij} \to 1 \equiv a_{ij} \gg d_{ij}$, we have $q_{ij}(t) \to q_{ij}^a(t)$, while for $\delta_{ij} \to 0 \equiv a_{ij} \ll d_{ij}$, we have $q_{ij}(t) \to q_{ij}^d(t)$. This means that if either the attacker or the defender take control of more vehicles than their opponent, then it can take the control of street ij's flow. Considering that the attacker and the defender can control limited number of ACVs simultaneously, thus, they have to choose the number of ACVs to control at each street. Thus, we first define a valuation for each street. To this end, we find two consequences of a traffic jam at each street: 1) the flow drop in all streets of the ITS (ITS value) and 2) the total decrease in the success probability of communications link caused by the increase in traffic density (CI value).

We derive the normalized ITS value of each street, $\phi_{t_{ij}}$, by finding the total flow drop in all streets of the ITS. Moreover, we find the normalized CI value of each street, $\phi_{c_{ij}}$, by calculating the total decrease in the success probability of communications link caused by the increase in traffic density. Next, we can define combine the ITS and CI value of each street ij using a weighted sum as $\phi_{ij}(\zeta) = \zeta\phi_{t_{ij}} + (1-\zeta)\phi_{c_{ij}}$, where $\phi_{ij}(\zeta)$ is street ij's interdependent ITS and CI value and $0 \leq \zeta \leq 1$ is an indicator of importance of ITS and CI for the attacker and the defender. Next, we will analyze the decision making process of the attacker and the defender in a game-theoretic framework.

III. Colonel Blotto Game for Security of the Interdependent ITS and CI

We address the defender-attacker interactions in interdependent ITS and CI systems as a CBG [4] $\{\mathcal{P}, \{\mathcal{Q}^j\}_{j\in\mathcal{P}}, \{R^j\}_{j\in\mathcal{P}}, N, \{\phi_i^a, \phi_i^d\}_{i=1}^N, \{u^j\}_{j\in\mathcal{P}}\}$ defined by six components: a) the *players*, attacker a and defender d, set $\mathcal{P} \triangleq \{a, d\}$, b) the *strategy* spaces $\mathcal{Q}^j, \forall j \in \mathcal{P}$, c) maximum number of under control ACVs $R^j, \forall j \in \mathcal{P}$, d) *number* of the streets N, e) normalized *value* of each street $i, \forall j \in \mathcal{P}$, ϕ_i^j, and f) the *utility function*, u^j, for each player. Consequently, two players must simultaneously choose which ACVs on N streets to control [5]. For both players, the set of *pure* strategies $\mathcal{Q}^j$ corresponds to the different possible resource allocations across the streets: $\mathcal{Q}^j = \left\{ \boldsymbol{r}^j \middle| \sum_{i=1}^N r_i^j \leq R^j, r_i^j \geq 0 \right\}$, where $\boldsymbol{r}^j = [r_1^j, \ldots, r_N^j]^T$ denotes player j's under control ACV vector across N streets. As discussed before, if d controls more ACVs than a on street i, then d wins street i, and vice versa. Also, in case of equal allocation of resources, which has the probability of zero due to the continuous action space of the players, we share the normalized value of each street equally between players. Thus, at each street i, the *normalized* payoff for the players is:

$$v_i^j(r_i^j, r_i^{-j}) = \begin{cases} \phi_i^j, & \text{if } r_i^j > r_i^{-j}, \\ \frac{\phi_i^j}{2}, & \text{if } r_i^j = r_i^{-j}, \\ 0, & \text{if } r_i^j < r_i^{-j}, \end{cases} \quad (3)$$

where $-j$ is the opponent of j. The total payoff of the players resulting from choosing ACVs across all N streets is the sum of the individual payoffs in (3) received from each street: $u^j(\boldsymbol{r}^j, \boldsymbol{r}^{-j}) = \sum_{i=1}^N v_i^j(r_i^j, r_i^{-j})$. Both players aim to increase this utility function by maximizing the number of compromised streets. The mixed-strategy Nash equilibrium of this game when the number of streets N is high and $R^d > R^a$ is given by:

$$F_i^d(r) = \left(\frac{\frac{\phi_i^a}{\lambda^a} - \frac{\phi_i^d}{\lambda^d}}{\frac{\phi_i^a}{\lambda^a}} \right) + \frac{r}{\frac{\phi_i^a}{\lambda^a}}, \; F_i^a(r) = \frac{r}{\frac{\phi_i^d}{\lambda^d}}, r \in \left[0, \frac{\phi_i^d}{\lambda^d}\right], \quad (4)$$

where $\{F_i^j\}_{i=1}^N : \mathbb{R}_+ \to [0, 1]$ for each street i is *distribution of ACVs on each streets* i and (λ^a, λ^d) can be derived from the solution of a system of equations linking (λ^a, λ^d) to $(R^a, R^d, \phi_i^d, \phi_i^d), \forall i \in \mathcal{S}$ [4] (omitted due to space limitations).

IV. Simulation Results and Analysis

Consider the ITS as shown in Fig. 1 that has 9 intersections and 24 streets. This ITS has 8 central streets flowing in to and out of intersection 5 and 16 marginal streets. The central streets have higher flow capacity than the marginal

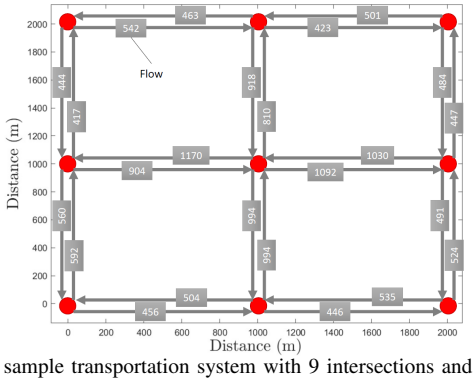

Fig. 1. A sample transportation system with 9 intersections and 24 streets.

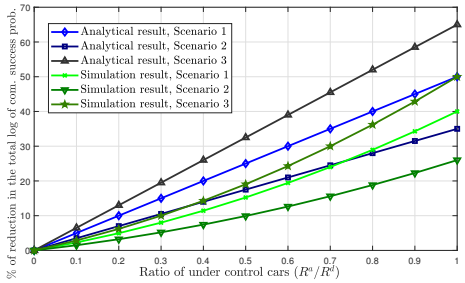

Fig. 2. Effect of the attack on the communication system.

streets. We consider three scenarios: *Scenario 1*: the attacker and the defender assign equal valuations on the ITS and CI, *Scenario 2*: $\zeta^a = \zeta^d = 0$, which means the defender does not protect the transportation system while the attacker values both systems equally, and *Scenario 3*: the defender does not assign a value for the CI while the attacker aims at compromising both systems. We consider that the defender can control $R^d = 1000$ cars on all network while the attacker can control $R^a = [0 - 1000]$ cars.

Fig. 2 shows the effect of the attack on the ITS and CI. From Fig. 2 we observe two key points: 1) When the defender reduces its valuation on the CI (ITS), it can better protect the CI (ITS), however, the attacker can further reduce the total communication success probability (total traffic flow) more. This emphasizes the interdependencies between the CI and ITS, which the defender must protect jointly and 2) As R^a/R^d gets closer to 1 the simulation and analytical results have a higher gap due to the nature of the CBG valuation function which has a sharp discontinuity. These preliminary results clearly demonstrate that the use of CBG and the consideration of interdependencies between ITS and CI systems is necessary for securing them in future smart cities.

References

[1] A. Ferdowsi, U. Challita, and W. Saad, "Deep learning for reliable mobile edge analytics in intelligent transportation systems: An overview," *IEEE Vehicular Technology Magazine*, vol. 14, no. 1, pp. 62–70, March 2019.

[2] H. Rakha and B. Crowther, "Comparison of greenshields, pipes, and van aerde car-following and traffic stream models," *Transportation Research Record: Journal of the Transportation Research Board*, no. 1802, pp. 248–262, 2002.

[3] V. V. Chetlur and H. S. Dhillon, "Success probability and area spectral efficiency of a vanet modeled as a cox process," *IEEE Wireless Communications Letters*, pp. 1–1, 2018.

[4] A. Ferdowsi, W. Saad, B. Maham, and N. B. Mandayam, "A Colonel Blotto game for interdependence-aware cyber-physical systems security in smart cities," in *Proceedings of the 2Nd International Workshop on Science of Smart City Operations and Platforms Engineering*, ser. SCOPE '17. Pittsburgh, Pennsylvania: ACM, 2017, pp. 7–12.

[5] A. Ferdowsi, A. Sanjab, W. Saad, and T. Başar, "Generalized Colonel Blotto game," in *2018 Annual American Control Conference (ACC)*, Milwaukee, WI, USA, June 2018, pp. 5744–5749.