Security Games for Vehicular Networks

Tansu Alpcan, *Member*, *IEEE*, and Sonja Buchegger, *Member*, *IEEE*

Abstract—Vehicular networks (VANETs) can be used to improve transportation security, reliability, and management. This paper investigates security aspects of VANETs within a game-theoretic framework where defensive measures are optimized with respect to threats posed by malicious attackers. The formulations are chosen to be abstract on purpose in order to maximize applicability of the models and solutions to future systems. The security games proposed for vehicular networks take as an input centrality measures computed by mapping the centrality values of the car networks to the underlying road topology. The resulting strategies help locating most valuable or vulnerable points (e.g., against jamming) in vehicular networks. Thus, optimal deployment of traffic control and security infrastructure is investigated both in the static (e.g., fixed roadside units) and dynamic cases (e.g., mobile law enforcement units). Multiple types of security games are studied under varying information availability assumptions for the players, leading to fuzzy game and fictitious play formulations in addition to classical zero-sum games. The effectiveness of the security game solutions is evaluated numerically using realistic simulation data obtained from traffic engineering systems.

Index Terms—Vehicular networks, security, game theory, optimization.

1 Introduction

Vehicular networks (VANETs) enable cars to communicate with each other and/or with a special infrastructure on the road. Communications can be purely ad hoc between cars or facilitated by making use of an infrastructure. The infrastructure typically consists of a set of so-called roadside units (RSUs) that are connected to each other or even to the Internet. Alternatively, existing infrastructure such as cellular networks can be used for this purpose. VANETs pave the way for applications ranging from real-time traffic information for dynamic route optimization and accident prevention to location-dependent services, such as information on local points of interest, and entertainment. The last category includes download of media files or web content at stationary servers such as gas stations exchange of content with other cars, or disseminating content in a delay-tolerant network of cars. VANET applications differ in their requirements of timely message delivery. They can be real time in follow-up accident prevention in the immediate neighborhood of an accident or obstacles on the road, tolerant of small delays for the application of route optimization, or they can be noncritical in the delay-tolerant entertainment scenarios.

As a result of their promising features and potentially wide range of applications, VANETs and their security properties have recently received increased attention in research community [1], [2]. This paper investigates VANET security within a game-theoretic framework where defensive measures are optimized with respect to location-based threats posed by malicious attackers. Since VANET architectures currently continue their evolution, the security games are formulated here in an abstract manner in order to ensure widest possible applicability of the results and models in the future.

A formal and quantitative decision framework to address the issues of attack modeling, optimization of response actions, and allocation of defense resources may benefit VANET security in general. A rich set of tools has been developed within game theory to address problems where multiple players with different objectives compete and interact with each other on the same system, and they are successfully used in many disciplines including economics, decision theory, and control. Therefore, game theory is a strong candidate to provide the much needed mathematical framework for analysis, modeling, and decision processes for VANET security. When compared to a pure optimization approach, game theory allows additional modeling of attacker behavior and interaction between defense and attackers. Such a mathematical abstraction (framework) is useful for generalization of problems, combining the existing ad hoc schemes under a single umbrella, and future research. Unsurprisingly, there has been a growing interest within the research community in game-theoretic approaches to the problem of security in general [3], [4] and wireless network security specifically [5].

VANET security games model the interaction between possible malicious attackers and various defense mechanisms protecting them. The games considered take as an input centrality measures (e.g., betweenness centrality) which are computed by mapping the centrality of the car network to the underlying road topology represented by road segments. The objective of the game is to locate central (vulnerable) points on the road topology as potential attack targets (e.g., for jamming) and deploy countermeasures in the most effective manner. The defense system can be static in the form of RSUs or dynamic in the form of mobile law enforcement units. In the static case, all roadside unit positions are precomputed. In the dynamic case, roadside unit placement is adaptive to conditions in the vehicular

- *T. Alpcan is with the Deutsche Telekom Laboratories, Technical University of Berlin, Ernst-Reuter-Platz 7, D-10587 Berlin, Germany. E-mail: alpcan@sec.t-labs.tu-berlin.de.*
- *S. Buchegger is with KTH, CSC, Osquars Backe 2, 4tr, S-100 44 Stockholm, Sweden. E-mail: buc@kth.se.*

Manuscript received 15 Dec. 2008; revised 21 Sept. 2009; accepted 6 Jan. 2010; published online 2 Aug. 2010.
For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-2008-12-0496. Digital Object Identifier no. 10.1109/TMC.2010.146.

network, such as traffic patterns or attacks detected. In both cases, the defense mechanisms are assumed to be capable of detecting attackers and rendering them ineffective.

The attackers and defenders of security games often have limited information on each others' objectives. In order to model such information constraints, fuzzy games and stochastic fictitious play are investigated in this paper as relevant game-theoretic formulations for VANETs. When the payoffs are only known approximately but not exactly, a fuzzy game formulation allows for definition of a range of outcomes and player tolerance for imprecision. On the other hand, if the players do not know their opponents' preferences at all, they can learn to improve their strategies by observing each others' actions as part of fictitious play. The effectiveness of various security game solutions is evaluated using realistic simulation data obtained from traffic engineering systems. In addition, various types of security games are compared and contrasted with each other numerically through simulations.

1.1 Contributions and Outline

The main contributions of this paper include the following:

- Presenting (one of) the earliest game theoretical models in the context of vehicular networks which take into account attacker behavior for defensive resource allocation.
- Development of a metric based on betweenness centrality that measures importance of segments on a road network.
- Study of static and dynamic security games under various information availability assumptions (to the players), captured by fuzzy games and fictitious play.
- A comprehensive numerical analysis comparing various security games using realistic simulation data obtained from traffic engineering systems.

The rest of the paper is organized as follows: the next section presents the vehicular network model along with network structure and centrality measures. Section 3 discusses zero-sum and fuzzy security games as well as fictitious play as a dynamic alternative. A comprehensive numerical analysis is presented in Section 4 for an example rural and urban region. A discussion on related work is in Section 5. The paper concludes with remarks in Section 6.

2 Vehicular Network Model

2.1 Network Structure

Vehicles are assumed to be able to communicate with neighboring vehicles and roadside units. Neighbors of a vehicle are defined by its limited-radius (e.g., 300 m) radio coverage. The range and data rates can be modeled, for example, as circular and fixed, respectively.[1] Roadside units can communicate with servers and other roadside units via the Internet or other side channels.

The vehicular network model consists of three layers: data traffic, vehicular traffic, and road network. While the former two are dynamic, the last one is naturally fixed. Each network can be formally modeled as a separate graph, yet they are closely related to each other.

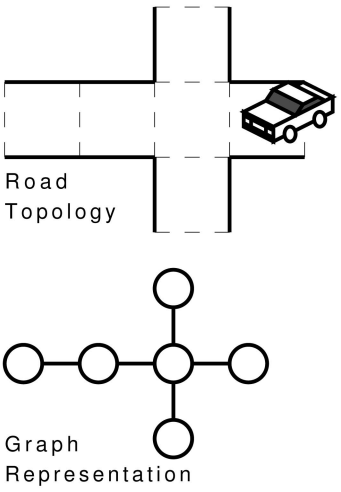

Fig. 1. Graphical representation of a simple road topology obtained by uniform quantization.

2.1.1 Road Network

Consider a map segment, e.g., a city district or rural region, with a road network. A simple model for such a road network is obtained by quantizing the roads to fixed-sized segments along their length, where lanes are ignored for simplicity. Then, road segments constitute the set nodes $\mathcal{N}_r$ of the road graph $\mathcal{R} := \{\mathcal{N}_r, \mathcal{E}_r\}$, where the set of edges $\mathcal{E}_r$ represents neighborhood relationships between the nodes (road segments). A simple example is illustrated in Fig. 1. Taking into account road topology along with vehicle and data traffic, one can calculate centrality (i.e., importance) of a road segment. Thus, a centrality value is associated with each node of the road graph $\mathcal{R}$.

2.1.2 Vehicular Traffic

In a VANET, vehicles are equipped with wireless networking capability allowing them to communicate with their neighboring cars and RSUs within their radio range. Communications can be multihop and RSUs are assumed to be connected with each other. The RSUs can also help vehicle-to-vehicle communication by tunneling data. Then, a vehicular traffic network $\mathcal{V} := \{\mathcal{N}_v, \mathcal{N}_u, \mathcal{E}_v\}$ is defined on the road topology of the selected map segment, where $\mathcal{N}_v$ denotes the set of cars, $\mathcal{N}_u$ the set of RSUs, and $\mathcal{E}_v$ the communication relations (edges) between them. A simple example is shown in Fig. 2.

2.1.3 Data Traffic

The data traffic generated and disseminated on a VANET depends on the specific scenario and applications deployed. For example, in evaluating metrics for roadside unit placement for a time-critical accident warning scenario, the warning messages are disseminated to all cars within the 3-hops broadcast range. Hence, data traffic plays an indirect role in determining the nature of the vehicular traffic network (graph) $\mathcal{V}$ defined above. In security game formulations, the data traffic model is implicitly taken into

1. The abstract nature of the treatment in this paper also allows for more complex radio models, which along with other metrics determine the input parameters of the security game.

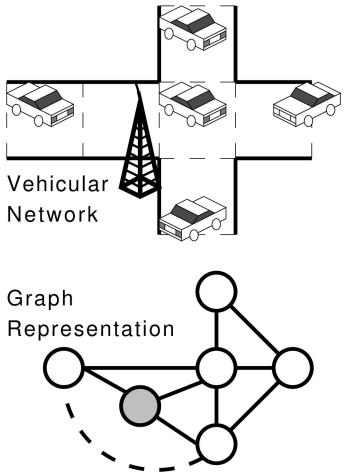

Fig. 2. Graphical representation of the vehicular network (including RSUs) given a radio range.

account when defining the vehicular network $\mathcal{V}$, and hence, in determining the payoff matrices.

2.2 Centrality Measures

Centrality metrics have been developed in social network analysis [6] to quantify how important particular individuals are in social networks. The objective is to find people who are central to communication and important for information dissemination. Centrality metrics are designed such that the highest value indicates the most central node. The interpretation of these centrality indexes is based on two assumptions. First, most routing protocols try to establish communications on the shortest paths. Second, the hop distance is a (scaled) approximation for the real length of the path between two communicating nodes. Under these assumptions, the **closeness centrality** gives an indication how long it would take the node to communicate in a serial manner to all other nodes in the network. The **graph centrality** indicates how long the parallel communication to all other nodes would take at most. The **stress centrality** is measuring on how many shortest paths a node lies. The **betweenness centrality** measures the expected routing service demands of node if every node was communicating with every other simultaneously. This can be interpreted as an approximate congestion sensitivity of the node. While betweenness focuses on the geodesic, **information centrality** focuses on how information might flow through many different paths, weighted by strength of tie and distance.

For communication networks such as VANETs, betweenness centrality provides a good measure as it relates to the expected role a node plays within the VANET communication. Betweenness centrality $C(i)$ quantifies the probability of a node i to be on the chosen shortest path g (geodesic) between all the nodes of a given graph. It can be defined as follows:

$$C(i) := \sum_{j=1}^{n} \sum_{k=1}^{n} \frac{g_{j,k}(i)}{g_{j,k}}, \tag{1}$$

where $g_{j,k}$ is the number of shortest paths from j to k and $g_{j,k}(i)$ is the number of shortest paths from j to k passing through the node i.

Fig. 3. Roads on the (a) rural and (b) urban region maps [8].

2.3 A Centrality Measure for Road Networks

A centrality measure for the road network (graph) is defined by mapping centrality values $C(i)$ of the nodes $i \in \mathcal{N}_v$ of the vehicular network $\mathcal{V}$ snapshot to the corresponding nodes $j \in \mathcal{N}_r$ of the underlying road graph $\mathcal{R}$. The vehicular network and associated data traffic are heavily time varying in contrast to the static road topology. As mobility of the cars changes the topology continuously, the vehicular network is only stable during a snapshot (or a short time window). Therefore, nodes of the road graph $\mathcal{R}$ are best candidates for being associated with certain metrics in order to facilitate security-related decision making. This can be achieved by assigning each vehicle to the corresponding road segment it is located on, at a given time instance. Then, as an example, the centrality values of the respective vehicles on a road segment are averaged over a time window to obtain the value for that node of the road graph. For a node $j \in N_r$ and finite-time window $t = 1, \ldots, T$, the centrality measure $\bar{C}(j)$ can be defined as

$$\bar{C}(j) := \frac{1}{T} \sum_{t=1}^{T} \sum_{i} C(i)\delta(i,j,t), \quad i \in \mathcal{N}_v,\ j \in \mathcal{N}_r, \tag{2}$$

where $C(i)$ denotes the betweenness centrality of a vehicle $i \in \mathcal{N}_v$ and the indicator function δ is defined as

$$\delta(i,j,t) := \begin{cases} 1, & \text{if vehicle } i \text{ is on a road segment } j \text{ at time } t, \\ 0, & \text{else.} \end{cases}$$

Thus, a centrality measure is obtained to assess the importance of a road segment [7]. This measure can be compared and contrasted to vehicle density $D(j)$ on a road segment j, which can be computed in a similar way through averaging

$$D(j) := \frac{1}{T} \sum_{t=1}^{T} \sum_{i} \delta(i,j,t), \quad i \in \mathcal{N}_v,\ j \in \mathcal{N}_r.$$

The vehicle density and betweenness centrality values (over a certain time period) on example rural and urban region maps (Fig. 3) are depicted in Figs. 4, 5, 6, and 7, respectively. The urban scenario has, as expected, higher vehicle density and centrality on the map.

Remark 2.1. In this paper, the region maps considered (rural and urban) are uniformly quantized (divided into equal-sized discrete parts) to a 11×11 grid to facilitate

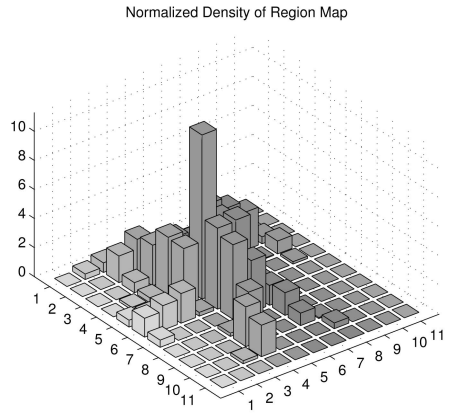

Fig. 4. Vehicle density on the rural region map, which is uniformly quantized to a 11×11 grid.

visualization of results, instead of creating a graph only for the road segments. Therefore, off-road nodes (squares) of the graph (grid) have simply zero vehicle density, and hence, zero betweenness centrality.

3 Security Game Formulations

3.1 Attack and Defense Model

Security games for vehicular networks model the interaction between malicious attackers to VANETs and various defense mechanisms protecting them in an abstract manner. This paper makes the following broad assumptions regarding the nature of possible attacks (defensive measures) and attackers (defenders):

- An attack causes (temporary) damage or disruption to one or more VANET applications at a certain location.
- The attackers have some incentive for (benefit from) causing damage to VANET applications. At the same time, they incur costs such as risk of being captured.
- The defenders have mechanisms that are capable of detecting attacks (attackers) and rendering them ineffective (capturing attackers) with some probability, if they allocate resources to the attack location.

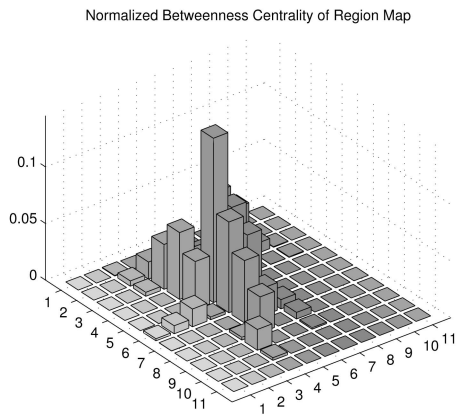

Fig. 6. Betweenness centrality values on the quantized rural region map.

- The defense systems can be static (e.g., deployed in roadside units) or dynamic (e.g., deployed in police cars).
- The attackers and defenders have limited information on each others' objectives.
- Both attackers and defenders deploy randomized (mixed) strategies.

Based on the assumptions above, the general class of attacks (and defensive measures) we envision are location-based. One such attack example is *jamming* which disrupts all communications in a region (road segment). These attacks can be detected early by ordinary users or defensive forces if they are present at that location. Furthermore, the attackers can be identified to some extent by their location using triangulation techniques as long as the attack continues. Another class of attacks involves *bogus messages* disseminated by the attackers for disruption (of traffic) or for selfish aims, e.g., sending a false accident message to clear the road. These messages are restricted to their initial neighborhood first even if they reach a broader area with time. However, the attackers will probably move away by the time the message reaches the infrastructure. Again, deployment of defensive systems at the same location provides better capabilities for checking the correctness of the messages. In addition, mobile defenses such as police

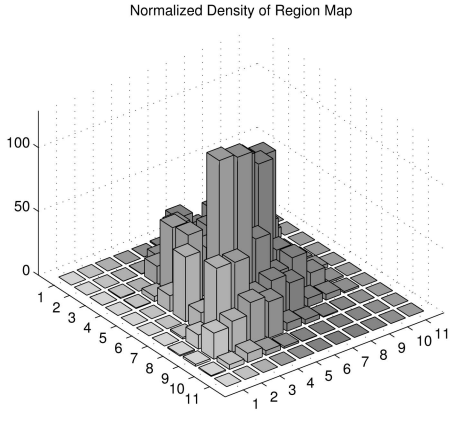

Fig. 5. Vehicle density on the urban region map, which is uniformly quantized to a 11×11 grid.

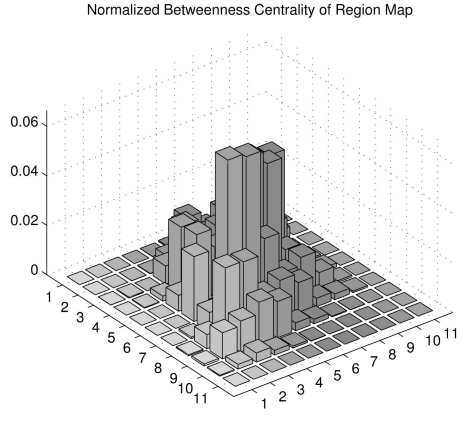

Fig. 7. Betweenness centrality values on the quantized urban region map.

cars may quickly assess the situation and physically capture the perpetrators if necessary, something beyond the capabilities of ordinary users. A third class of relevant attacks involves *Sybil attack* where the attackers create and operate under multiple forged identities for self-protection as well as to increase the intensity of their attacks. Checking the authenticity of these identities may be resourcewise infeasible for the ordinary users nearby due to communication overhead and limited access rights. Deploying appropriate local defensive systems can help in detecting the attacks early and physically identify the attackers.

3.2 VANET Security Game Model

Based on the assumptions in the previous section and as a first iteration, the VANET security games in this paper are finite, two-player (attacker versus defender) and zero sum (in terms of cost structure). The action space of the players is the collection of alternative moves available to the player on the finite road graph $\mathcal{R}$, to either attack or defend a specific road segment. Here, this graph specifically corresponds to the square (11×11) grid obtained by uniformly quantizing rural (or urban) region map.

As an example for the defined security game, an attacker jams (attacks) one road segment (a square in Fig. 6) with some probability according to its mixed attack strategy. In response, the defender, i.e., the network stakeholder (designer, city planner, and law enforcement), allocates defense resources to the same or another road segment according to its own strategy. The outcome of a specific game is determined by the game matrix, which contains the cost (payoff) values for each possible action-reaction combination.

The game matrix maps player actions (attack or defend) on the road segment graph (or here the grid obtained by quantizing the region map) to outcomes, payoff, and cost, for the attacker and defender, respectively. For convenience, the action space (grid) is represented as a vector, in this case, a vector of size $121 = 11 \times 11$. The game matrix entries can be a function of the importance of each road segment (as characterized by, for example, the betweenness centrality), the risk of detection (gain from capture) for the attacker (defender), as well as other factors. For the rest of the paper, the convention is adopted where the attacker is the row player (maximizer) and the defender is the column player (minimizer). Accordingly, the game matrix P is defined as an example:

$$P = [P(i,j)] := \begin{cases} \bar{C}(i), & \text{if} i \neq j, \\ r, \text{if} i = j, & \forall i,j \in \mathcal{N}_r, \end{cases} \tag{3}$$

where $\bar{C}$ is defined in (2) and r is a fixed scalar that represents the risk or penalty of capture for the attacker (benefit for defender), if the defender allocates resources to the location of the attack, i.e., the same square on the map.

3.3 Zero-Sum Game

As a motivating example and the simplest possible formulation, we study first a zero-sum security game [9] for vehicular networks. The game matrix (cost and payoffs) is assumed to be known to both the defender and the attacker. Since the game is defined as zero sum, the attacker's gain is equal to the defender's loss, and vice versa. The zero-sum game has the matrix defined in (3) and follows the conventions described in Section 3.2, e.g., the attacker is the maximizer (row player) and the defender is the minimizer (column player) of the game.

Every such two-player zero-sum matrix game admits a solution in mixed strategies and the solution (saddle point) can be obtained by solving the following pair of primal-dual linear programming problems [9], [10]:

$$\begin{aligned} \max_x \quad & v \\ \text{s.t.} \quad & \sum_i P(i,j)x_i \geq v, \quad \forall j \in \mathcal{N}_r, \\ & \sum_i x_i = 1,\ x_i \geq 0, \quad \forall i \in \mathcal{N}_r, \end{aligned} \tag{4}$$

and

$$\begin{aligned} \min_y \quad & w \\ \text{s.t.} \quad & \sum_j P(i,j)y_j \geq w, \quad \forall i \in \mathcal{N}_r, \\ & \sum_i y_i = 1,\ y_i \geq 0, \quad \forall j \in \mathcal{N}_r. \end{aligned} \tag{5}$$

Since both problems are feasible and mutually dual, by duality theory, the maximum of v will be equal to the minimum of w. Hence, the value $v = w$ is the *value* of the game, which corresponds to the equilibrium (saddle point) gain and loss for the attacker and defender, respectively. Here, the vector x is the equilibrium strategy of the attacker which can also be interpreted as expected attack probabilities. The vector y is the defense strategy which can be used as a guideline to decide where to allocate limited defense resources.

3.4 Fuzzy Game

The players in a game often have limited information about the preferences of their opponents. If payoffs in a game are known or expressed only approximately, then *fuzzy numbers* can be used in the game matrix instead of precise (or crisp) ones. This results in a *fuzzy game* where players attempt to maximize their own utility despite having only access to an imprecise game (payoff) matrix.

Fuzzy numbers can express an approximation and a tolerance for deviation from the true value. The assumption of full and exact information does not hold in complex problems partly due to difficulty of defining an adequate payoff value for each player [11]. With fuzzy set theory, the players can express their preferences heuristically and approximately. This can be useful for interaction with people, as it provides a way for them to communicate their estimations in vague terms. Another benefit of fuzzy games is that fuzzy linear programming often used in solving them may save time in comparison to conduct a full Monte Carlo analysis on the parameter space of the game [12].

The fuzzy numbers in the game matrix of a fuzzy game are defined through membership functions instead of single precise values. At a given point, the value of the membership function represents the membership degree of

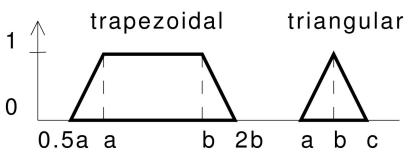

Fig. 8. Trapezoidal and triangular membership functions.

that point to the respective fuzzy set. In this paper, a trapezoidal and a triangular membership function, depicted in Fig. 8, are chosen to describe fuzzy payoffs [12]. Then, without loss of generality, an example fuzzy game matrix P_f is defined as

$$P_f := \begin{cases} \text{trapezoidal fuzzy set, if } i \neq j, \text{ s.t.} \\ \quad a(i) = \min\{\bar{C}(i), D(i)\}, \\ \quad b(i) = \max\{\bar{C}(i), D(i)\}, \\ \text{triangular fuzzy set, if } i = j, \text{ s.t.} \\ \quad a = -0.3,\ b = -0.2,\ c = 0,\ \forall i, j \in \mathcal{N}_r. \end{cases} \tag{6}$$

Here, the off-diagonal entries model a trade-off between density and betweenness centrality. The chosen fuzzy numbers, although quite reasonable for the application domain, are nevertheless arbitrary. Fuzzy sets and membership functions are active areas of research and many other variants are also possible candidates for such security game formulations.

The fuzzy game defined is solved using the fuzzy linear programming approach outlined by Campos [10]. The primal and dual fuzzy linear programs, which are roughly the fuzzy counterparts of the ones in (4) and (5), are

$$\begin{aligned} \min_{u,\alpha} \quad & \sum_i u_i \\ \text{s.t.} \quad & \sum_i P(i,j) u_i \succeq 1 - \tilde{p}(1-\alpha), \quad \forall j \in \mathcal{N}_r, \\ & u_i \geq 0,\ \forall i \in \mathcal{N}_r, \quad \alpha \in (0,1], \end{aligned} \tag{7}$$

and

$$\begin{aligned} \max_{s,\alpha} \quad & \sum_j s_j \\ \text{s.t.} \quad & \sum_j P(i,j) s_j \preceq 1 + \tilde{q}(1-\alpha), \quad \forall i \in \mathcal{N}_r, \\ & s_j \geq 0, \quad \forall j \in \mathcal{N}_r,\ \ \alpha \in (0,1], \end{aligned} \tag{8}$$

where the fuzzy numbers $\tilde{p}$ and $\tilde{q}$ express the tolerance levels of players regarding violations of the constraints, and $\succeq$ and $\preceq$ denote relations for ranking fuzzy numbers. In addition, the following relationships hold:

$$v = \frac{1}{\sum_i u_i}, \quad w = \frac{1}{\sum_j s_j},$$

and

$$x_i = u_i\, v,\ \ y_i = s_i\, w,$$

where u, w, x, and y are defined in a similar way to the classical cases (4) and (5). However, unlike the classical zero-sum game formulation in Section 3.3, the (Nash equilibrium) value of the game may not necessarily match, i.e., $v \neq w$.

There are many alternative methods of *defuzzification* to rank fuzzy numbers, turn $\succeq$ and $\preceq$ into regular inequalities, and hence, converting the fuzzy linear program to a classical one. In this paper, we choose without loss of any generality, the α cut or k-preference index approach defined as

$$F_k(\tilde{a}) := \max\{x : \mu_{\tilde{a}} \geq k\},$$

for a given level α or $k \in [0,1]$, where $\mu_{\tilde{a}}$ is the membership value of the fuzzy number $\tilde{a}$. After the defuzzification, the resulting regular linear and dual linear programs are solved with standard methods.

3.5 Fictitious Play

The security games studied in the previous sections assume that the players have either complete knowledge of the payoff matrix (in the zero-sum game formulation) or at least an approximation thereof (in the fuzzy game formulation). Next, a fictitious play mechanism is investigated, where players know only their own payoff, but not their opponents. In fictitious play, game players repeatedly use strategies that are best responses to the historical averages, or empirical frequencies, of opponents which they observe. If the empirical frequencies of players converge (under some conditions), then it implies a convergence of strategies to a Nash equilibrium [13].

Fictitious play is one of many possible learning schemes, where players observe actions of and learn more about their opponent at each iteration of the game. In this paper, a discrete and stochastic variant of fictitious play is considered. Thus, an evolutionary version of the game is investigated in which the strategies at a given time instance are selected in response to the entire prior history of the opponent's actions. Furthermore, due to its stochastic nature, the game rewards randomization, thereby imposing so-called mixed strategies. This feature is especially relevant to security games where players have an incentive to confuse others and look unpredictable by randomly varying their actions.

Stochastic fictitious play solves the following static security game iteratively without requiring the players to know their opponents' payoff. Each player (attacker, player 1 or defender, player 2) selects a probabilistic strategy $x_i = [x_i(1), \ldots, x_i(N)]$, $i = 1, 2$, such that $\sum_j x_i(j) = 1$ and $0 \leq x_i(j) \leq 1$, and receives a reward according to the utility function $U_i(x_1, x_2)$ defined as

$$\begin{aligned} U_1(x_1, x_2) &= x_1^T P_1 x_2 - \tau x_1^T \log(x_1), \\ U_2(x_1, x_2) &= x_2^T P_2 x_1 - \tau x_2^T \log(x_2), \end{aligned} \tag{9}$$

where $\tau > 0$ is the randomization factor and the matrices P_i are of fixed size (here, 121×121). Here, we adopt a different notation for convenience and denote the strategies of the players as $x_1 = x$ and $x_2 = y$, instead of x and y of zero-sum and fuzzy games.

At each step of the game, player i selects an action a_i according to respective probability distribution (strategy) x_i. The best response mapping β_i, which determines the current strategy x_i, is chosen to maximize the player utility (9) and is defined as

$$\beta_i(x_1, x_2) := \arg\max_{x_i} U_i(x_1, x_2) = \sigma\left(\frac{P_i x_{-i}}{\tau}\right), \quad i = 1, 2, \tag{10}$$

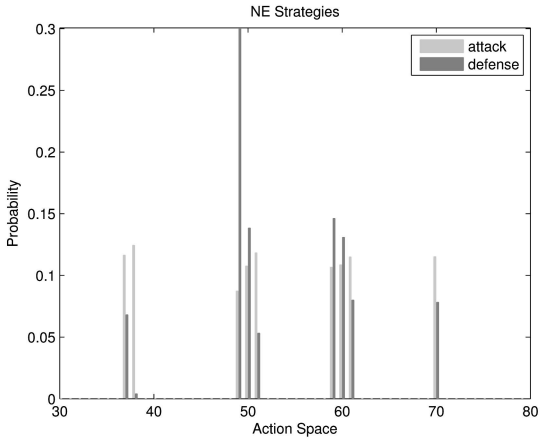

Fig. 9. Nash equilibrium attack and defense probabilities of the **zero-sum game** in the rural scenario. The action space is the collection of alternative moves available to the player on the $121 = 11 \times 11$ squares of the map (road segments) to either attack or defend. Only a subset of the 121-dimensional action space is shown as the other entries are zero.

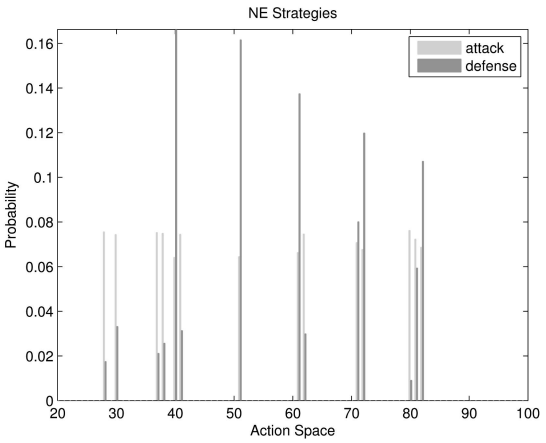

Fig. 10. Nash equilibrium attack and defense probabilities of the **zero-sum game** in the urban scenario.

where x_{-i} is the strategy of the other player and $\sigma(\cdot)$ is the logit or *soft-max* function. The ith element of the soft-max function is

$$(\sigma(x))_i := \frac{e^{x(i)}}{\sum_j e^{x(j)}}.$$

In discrete-time fictitious play, each player then computes the empirical frequency of the opponent at each time step k of the game:

$$q_i(k+1) = q_i(k) + \frac{1}{k+1}(v_{a_i} - q_i(k)),$$

where v_{a_i} is a vector whose ith term equals 1 in accordance with the observed action a_i and the remaining equal to 0. Subsequently, the players update their strategy according to the optimal response to the running average of the opponent's actions, i.e.,

$$x_i(k) = \beta_i(q_{-i}(k)),$$

where β_i is defined in (10). The reader is referred to [13] for details of the algorithm.

4 Numerical Analysis

4.1 Traffic Data and Setup

The traffic data used in the simulations consist of traces of car movements generated by a simulator [8]. This simulator was created at ETH Zurich with maps from Swiss geographic information system (GIS). In the simulations, two specific scenarios are analyzed: one rural and the other urban (Fig. 3), which differ from each other in road and traffic density. The traces offer snapshots in 1-second intervals about the identity of a car, its x- and y-coordinates on the map, and a time stamp. Mobility models range from random way point, where cars pick a random destination and drive there with randomly varying speed, to more complicated models including traffic lights and car following, where the speed not only depends on external constraints (e.g., the maximum allowed on a road segment) but also on the distance to the car in front.

As discussed in Section 2.2, a centrality measure is assigned to the road network by mapping centrality values of the nodes on the vehicular network to the corresponding road segments. Hence, vehicular network centrality is used to derive centrality values for the road network. This is easily accomplished computationally as the traffic traces contain the necessary data (ID, time stamp, x-coordinate, and y-coordinate) for each car. Then, given the time stamp of the vehicular topology snapshot, the properties of each node (such as its betweenness centrality) are transferred to the respective road node (map square) according to the coordinates.

4.2 Zero-Sum Game

The zero-sum security game defined in Section 3.3 is investigated numerically using the realistic traffic simulation data described in the previous section. The game matrix (cost and payoffs) is defined in (3), where the off-diagonal elements are centrality measures as in (2). The diagonal values, which quantify the penalty (or capture risk) for the attacker when both players choose the same square of the map (road segment), are first set to $r = 0.2$ roughly interpreted as 20 percent loss. With this penalty, the equilibrium value of the game amounts to $v = w = 0.4145$. If the penalty is reduced to 0.01, the value increases to 0.6560, i.e., a gain for the attacker as expected. Furthermore, a big penalty for the attacker (higher values in the diagonal of the payoff matrix) leads to diversification in attack probabilities instead of narrowly focusing on most valuable places to achieve the most damage. The results of the game are compared with a naive nongame strategy for the defense, which is to position resources at the squares with the highest potential damage. The results indicate that the naive strategy performs approximately 20 percent worse than the zero-sum game one, at 0.5150 (when $r = 0.2$).

Figs. 9 and 10 compare the mixed strategies of both the attacker and the defender in the rural and urban scenarios, respectively. The action space is the collection of alternative moves available to the player, in our specific case, the squares of the map (road segments) to either attack or defend. The probabilities represent attack and defense attempts by the respective players. The individual NE mixed strategies of the zero-sum game are again shown in a different format on the rural (urban) region map in Fig. 11

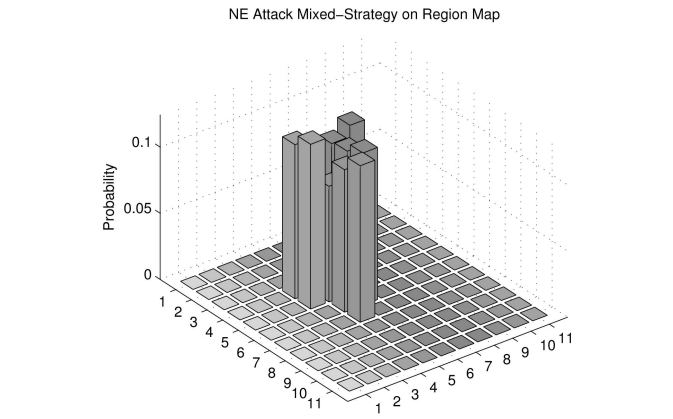

Fig. 11. Nash equilibrium attack probabilities of the **zero-sum game** in the rural scenario shown by arranging the 121-dimensional action space directly on the region map of 11×11.

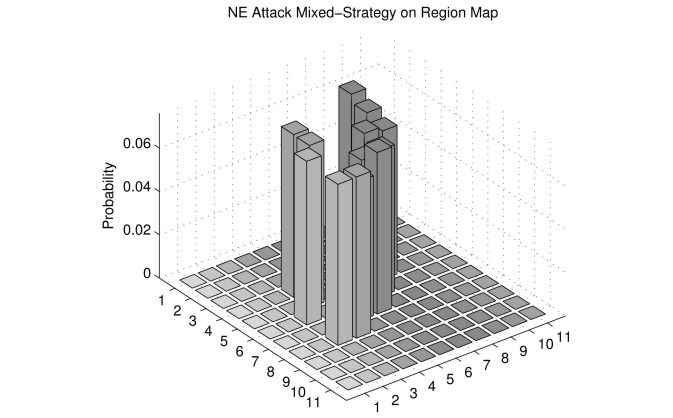

Fig. 12. Nash equilibrium attack probabilities of the **zero-sum game** in the urban scenario shown directly on the region map.

(Fig. 12) for the attacker and in Fig. 13 (Fig. 14) for the defender. While the attacker chooses the important squares with almost equal probability, the defender probabilities on those same squares show more variety. The defense strategy focuses on the most important square in the rural scenario, while the mixed strategies are spread over a larger part of the action space in the urban one due to the existence of multiple squares with high vehicle density and centrality. This is a result of the penalty (or risk) of capture for the attacker being uniform, whereas the defender losses are proportional to the centrality metrics.

4.3 Fuzzy Game

In reality, the players often have limited information about the preferences of their opponents, unlike the ideal formulation of the classical zero-sum game. The fuzzy game defined in Section 3.4 is compared here to the zero-sum game numerically. Fig. 15 (Fig. 16) depicts the Nash equilibrium attack and defense probabilities of both the fuzzy and classical zero-sum game in the rural (urban) scenario. Although the results differ from each other for both scenarios, they are nevertheless close. This should be expected as both games are defined around the same parameter values with the fuzzy one allowing for more uncertainty. The equilibrium value of the fuzzy game for the attacker is around $v = 0.7588$ (gain) and the defender value is $w = 0.5383$ (loss) in the rural case. As opposed to

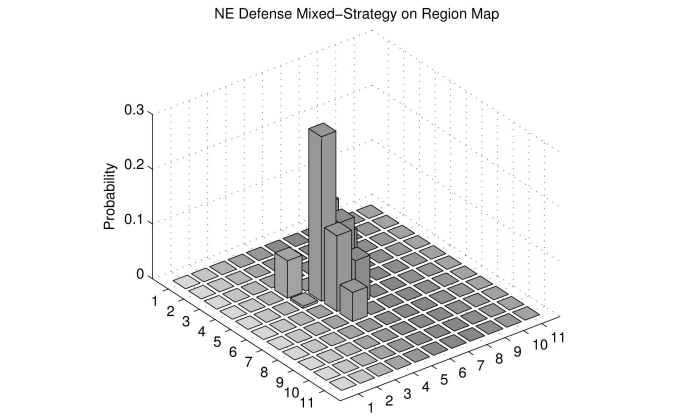

Fig. 13. Nash equilibrium defense probabilities of the **zero-sum game** in the rural scenario shown directly on the region map.

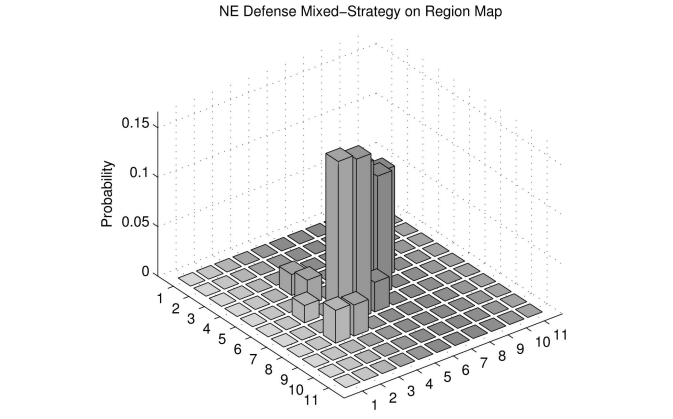

Fig. 14. Nash equilibrium defense probabilities of the **zero-sum game** in the urban scenario shown directly on the region map.

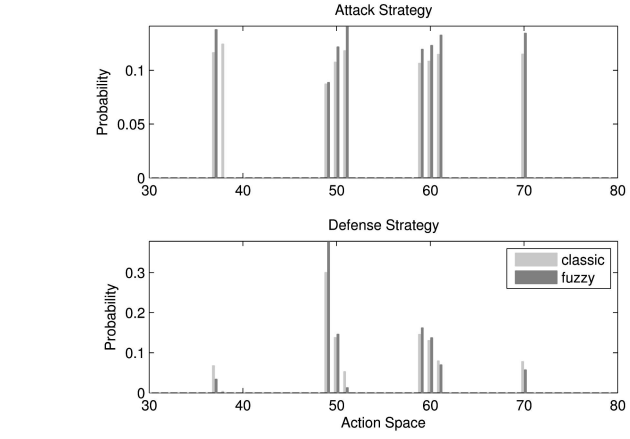

Fig. 15. Comparison of the NE attack and defense probabilities of the **zero-sum and fuzzy games** in the rural scenario. Only a subset of the $121 = 11 \times 11$-dimensional action space is shown as the other entries are zero.

the zero-sum game, equilibrium values v and w do not coincide due to the imprecision of the fuzzy metrics and 20 percent tolerance allowance of the players. Figs. 17 and 18 show the NE mixed strategies of the fuzzy game on the rural region map as an alternative representation, for the attacker and defender, respectively. The results for the urban map are omitted as they are similar to the zero-sum case as in the rural scenario.

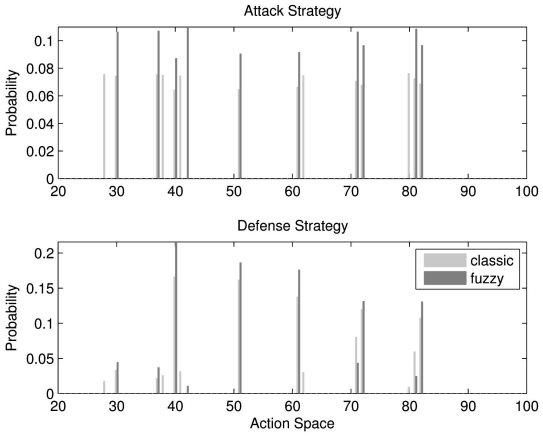

Fig. 16. Comparison of the NE attack and defense probabilities of the **zero-sum and fuzzy games** in the urban scenario.

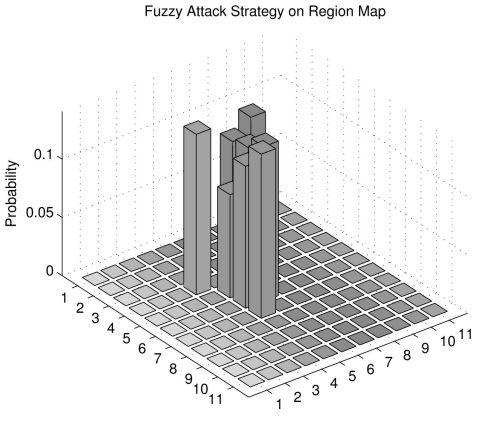

Fig. 17. Nash equilibrium attack probabilities of the **fuzzy game** in the rural scenario shown directly on the region map.

4.4 Fictitious Play

Fictitious play, which provides a dynamic learning mechanism for the players, is studied numerically. Specific properties of the discrete-time stochastic fictitious play mechanism are described in Section 3.5. In effect, the players solve here the original zero-sum game under information limitations and through fictitious play. The randomization parameter τ is chosen to be 0.1. The parameter τ rewards randomization (here with a weight factor of 10 percent), and hence, promotes mixed strategies to partly mislead the opponent. When τ goes to zero, the best response mappings of the players select the best possible action at each instance rather than randomizing.

The Nash equilibrium value of the game at the end of the $3{,}000\text{th}$ iteration of the fictitious play is approximately $v = w = 0.48$. Figs. 19 and 20 show the evolution of the attacker's and the defender's strategies as they observe each others' actions over time and learn (estimate) the respective strategy of the opponent using fictitious play. Each line represents the change in probability of attacking or defending a single square of the region map during this learning process. The graphs showing the evolution of strategies on the urban map are omitted as they are similar to the ones in the rural map. Finally, Figs. 21 and 22 depict the "final" attack and defense strategies on the action space for the rural and urban cases, respectively, after learning stops. The results are similar to the ones in zero-sum game which indicates that fictitious play learning mechanism successfully approximates the full information results.

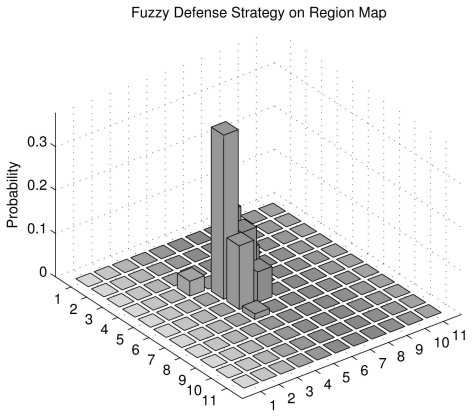

Fig. 18. Nash equilibrium defense probabilities of the **fuzzy game** in the rural scenario shown directly on the region map.

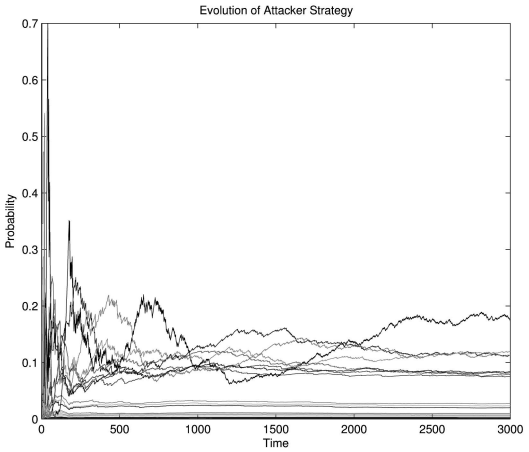

Fig. 19. Evolution of attack strategy (the 121-dimensional probability vector) using fictitious play in the rural scenario. Notice that most of the values are close to zero similar to the results of zero-sum and fuzzy games.

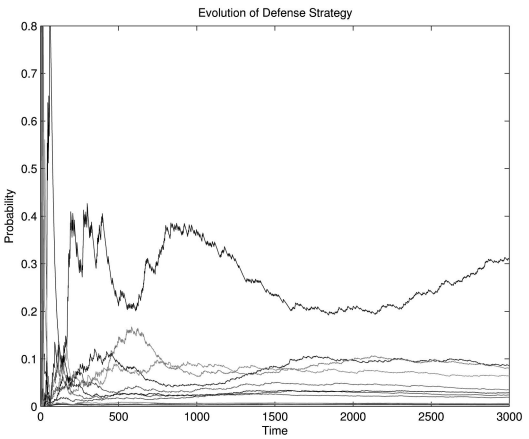

Fig. 20. Evolution of defense strategy using fictitious play in the rural scenario.

5 Related Work

Security vulnerabilities of vehicular networks and various countermeasures have been outlined in [1] and [2].

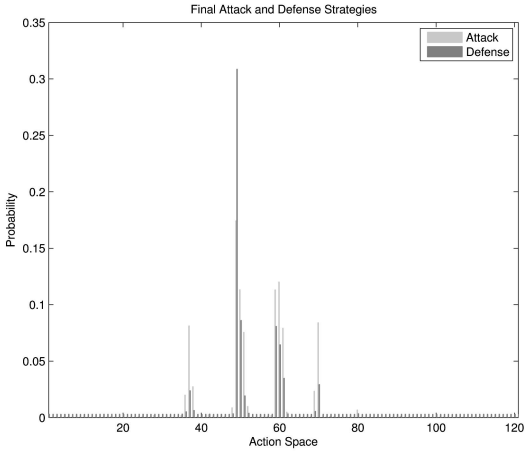

Fig. 21. Attack and defense final strategies in the rural scenario obtained via fictitious play.

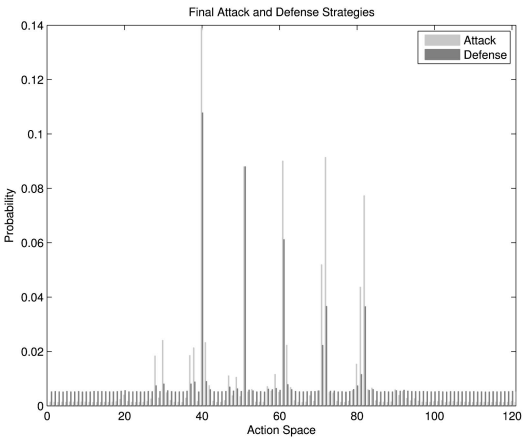

Fig. 22. Attack and defense final strategies in the urban scenario obtained via fictitious play.

Papadimitratos et al. [1] have discussed security requirements for VANETs and proposed a set of design principles. Raya and Hubaux [2] have provided a VANET threat analysis and a set of security protocols, which are analyzed and assessed quantitatively. The IEEE 1609 family of standards for Wireless Access in Vehicular Environments (WAVEs) defines secure message formats and processing of them in addition to other aspects of vehicular communications. In an effort for modeling of vehicular networks, Marfia et al. [14] have assessed the impact of different mobility models on network performance. The data sets used in the simulations of this paper are obtained from a simulator by Sommer [8]. It is chosen for its ease of use while providing realistic vehicular traces. In addition, the Multiagent Microscopic Traffic Simulator (MMTS) [15] by Nagel has been utilized, which provides large-scale traces of Zurich for a 24-hour period.

As a precursor to this work, placement strategies for roadside units in vehicular networks have been investigated by evaluating different metrics such as density, centrality [7], and connectivity [16]. In a related work, Crucitti et al. [17] have computed several centrality indexes for urban streets and studied their distribution. In contrast, in this work, we look at the traffic dynamics rather than the static road network and use centrality metrics of the traffic in all parts of the map. In a vehicular but not security context, Lochert et al. have addressed the placement problem of roadside units to increase travel time savings by using genetic algorithms [18] and evaluated the improvement in connectivity provided by deployment of roadside units to facilitate data dissemination at least at the initial rollout of Vanets when not many cars would have the necessary equipment [19].

Security games, which capture the interaction of attackers and defenders under imperfect observations, have been investigated by Alpcan and Basar in [20] and later in [21]. In [20], a security game between the attacker and the intrusion detection system has been investigated both in finite and continuous kernel versions, where in the latter case, players are associated with specific cost functions. This security game has been extended in [21] to a stochastic and dynamic one by modeling the operation of a sensor network as a finite Markov chain. Optimization of response to intrusion and security attacks has been posed as a resource allocation problem in a different setting in [22]. Grossklags et al. [3], [4] analyze and develop security games for populations of users with individual decisions regarding investments in protection, such as firewalls or antivirus software, and insurance in the form of backups and redundancy. In contrast to this paper, where there is one defender strategically distributing a fixed amount of resources, their scenario involves several defenders whose varying willingness to invest impacts the vulnerability of the whole system. Revocation games in ephemeral networks (which encompass vehicular networks) have been studied by Raya et al. [23], where players jointly decide whether to revoke credentials of potentially malicious players. It differs from the security games in this work by focusing on credentials of players rather than allocation of defensive resources.

6 Conclusion

This paper investigates security aspects of VANETs by providing the first steps for design and application of three different game formulations under various information assumptions. The objective is to develop defensive strategies that are optimized with respect to threats posed by malicious attackers. The game formulations are chosen to be abstract on purpose in order to maximize applicability of the models and solutions to future systems. These security games take as an input the centrality measures computed by mapping centrality metrics of the car networks to the underlying road topology represented by road segments. The resulting strategies help locating most valuable or vulnerable points (e.g., against jamming) in vehicular networks. Thus, optimal deployment of traffic control and security infrastructure is investigated both in the static (e.g., fixed roadside units) and dynamic cases (e.g., mobile law enforcement units).

Three specific types of security games are studied under varying information availability assumptions for the players. When both players know the payoff matrices of each other, a classical zero-sum game is solved to obtain Nash equilibrium attack and defense strategies. When the payoffs are only known approximately but not exactly, a fuzzy game formulation allows for definition of a range of outcomes and player tolerance of imprecision. Finally, when the players do not know each others preferences, they can learn to improve their strategies by fictitious play.

Each game formulation, although different from others, is compared numerically with others by a careful choice of parameters. The numerical analysis is based on realistic simulation data obtained from traffic engineering systems. The zero-sum game is observed to outperform the naive strategy of defending locations according to their metrics ignoring attacker behavior. In addition, fuzzy game results are in the neighborhood of the zero-sum game and fictitious play leads to more randomized mixed strategies.

Future research directions include investigation of other suitable fuzzy membership functions as well as learning algorithms other than fictitious play. A more detailed network model and analysis of its effects on different scenarios constitute other interesting future extensions.

ACKNOWLEDGMENTS

The authors thank Jean-Pierre Hubaux (EPFL) for his insightful comments and Yannick Do (EPFL) for generating centrality and traffic density values during his internship at Deutsche Telekom Laboratories. This work has been supported by Deutsche Telekom Laboratories. An earlier version of this paper was presented in the 46th Annual Allerton Conference on Communication, Control, and Computing, September 2008, Monticello, Illinois. S. Buchegger was with Deutsche Telekom Laboratories during this research.

REFERENCES

[1] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing Vehicular Communications—Assumptions, Requirements, and Principles," *Proc. Workshop Embedded Security Cars (ESCAR)*, 2006.

[2] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad Hoc Networks," *Proc. Workshop Security Ad Hoc Sensor Networks (SASN)*, pp. 11-21, 2005.

[3] J. Grossklags, N. Christin, and J. Chuang, "Secure or Insure? A Game-Theoretic Analysis of Information Security Games," *Proc. 17th Int'l Conf. World Wide Web (WWW '08)*, pp. 209-218, 2008.

[4] J. Grossklags, N. Christin, and J. Chuang, "Predicted and Observed User Behavior in the Weakest-Link Security Game," *Proc. First Conf. Usability, Psychology, and Security (UPSEC '08)*, pp. 1-6, 2008.

[5] L. Buttyan and J.-P. Hubaux, *Security and Cooperation in Wireless Networks*, http://secowinet.epfl.ch. Cambridge Univ. Press, 2007.

[6] S. Wasserman and K. Faust, *Social Network Analysis: Methods and Applications*. Cambridge Univ. Press, 1994.

[7] Y. Do, S. Buchegger, T. Alpcan, and J.-P. Hubaux, "Centrality Analysis in Vehicular Ad-Hoc Networks," technical report, EPFL/T-Labs, 2008.

[8] P. Sommer, "Design and Analysis of Realistic Mobility Model for Wireless Mesh Networks," master's thesis, ETH Zürich, 2007.

[9] T. Başar and G.J. Olsder, *Dynamic Noncooperative Game Theory*, second ed. SIAM, 1999.

[10] L. Campos, "Fuzzy Linear Programming Models to Solve Fuzzy Matrix Games," *Fuzzy Sets and Systems*, vol. 32, no. 3, pp. 275-289, 1989.

[11] J.C.D. Garagic, "An Approach to Fuzzy Noncooperative Nash Games," *J. Optimization Theory Applications*, vol. 118, no. 3, pp. 475-491, 2003.

[12] A. Abebe, V. Guinot, and D. Solomatine, "Fuzzy Alpha-Cut vs. Monte Carlo Techniques in Assessing Uncertainty in Model Parameters," *Proc. Fourth Int'l Conf. Hydroinformatics*, July 2000.

[13] J. Shamma and G. Arslan, "Unified Convergence Proofs of Continuous-Time Fictitious Play," *IEEE Trans. Automatic Control*, vol. 49, no. 7, pp. 1137-1141, July 2004.

[14] G. Marfia, G. Pau, E. Giordano, E. De Sena, and M. Gerla, "Vanet: On Mobility Scenarios and Urban Infrastructure. A Case Study," *Proc. 2007 Mobile Networking Vehicular Environments*, 2007.

[15] K. Nagel, "Realistic Vehicular Traces," http://lst.inf.ethz.ch/ad-hoc/car-traces, 2010.

[16] M. Kafsi, O. Dousse, P. Papadimitratos, T. Alpcan, and J.-P. Hubaux, "VANET Connectivity Analysis," technical report, EPFL/T-Labs, 2008.

[17] P. Crucitti, V. Latora, and S. Porta, "Centrality Measures in Spatial Networks of Urban Streets," *Physical Rev. E (Statistical, Nonlinear, and Soft Matter Physics)*, vol. 73, no. 3, 2006.

[18] C. Lochert, B. Scheuermann, and C. Wewetzer, "Data Aggregation and Roadside Unit Placement for a Vanet Traffic Information System," *Proc. Fifth ACM Int'l Workshop Vehicular Ad Hoc Networks (VANET)*, Sept. 2008.

[19] C. Lochert, B. Scheuermann, M. Caliskan, and M. Mauve, "The Feasibility of Information Dissemination in Vehicular Ad-Hoc Networks," *Proc. Fourth Ann. Conf. Wireless Demand Network Systems and Services (WONS)*, Jan. 2007.

[20] T. Alpcan and T. Başar, "A Game Theoretic Analysis of Intrusion Detection in Access Control Systems," *Proc. 43rd IEEE Conf. Decision and Control*, pp. 1568-1573, Dec. 2004.

[21] T. Alpcan and T. Başar, "An Intrusion Detection Game with Limited Observations," *Proc. 12th Int'l Symp. Dynamic Games and Applications*, July 2006.

[22] M. Bloem, T. Alpcan, and T. Başar, "Intrusion Response as a Resource Allocation Problem," *Proc. 45th IEEE Conf. Decision and Control*, pp. 6283-6288, Dec. 2006.

[23] M. Raya, M.H. Manshaei, M. Felegyhazi, and J.-P. Hubaux, "Revocation Games in Ephemeral Networks," *Proc. ACM Conf. Computer Security (CCS)*, Oct. 2008.

Tansu Alpcan received the BS degree in electrical engineering from Bogazici University, Istanbul, Turkey, in 1998, and the MS and PhD degrees in electrical and computer engineering from the University of Illinois at Urbana-Champaign (UIUC) in 2001 and 2006, respectively. He was a senior research scientist in Deutsche Telekom Laboratories, Berlin, Germany, from 2006 to 2009. He is currently an assistant professor (Juniorprofessur) at Technische Universität Berlin while continuing his affiliation with Deutsche Telekom Laboratories. His research focuses on applications of distributed decision making, game theory, and control to various security and resource allocation problems in complex and networked systems. He received Fulbright Scholarship in 1999 and the Best Student Paper Award at the IEEE Conference on Control Applications in 2003. He received the Robert T. Chien Research Award from the UIUC Department of Electrical and Computer Engineering and the Ross J. Martin Research Award from the UIUC College of Engineering in 2006. He was an associate editor for the the IEEE Conference on Control Applications (CCA) in 2005 and has been a TPC member of several conferences including IEEE INFOCOM 2007-2009. He was the cochair of the Workshop on Game Theory in Communication Networks (GameComm) 2008 and publicity chair of GameNets 2009. He is the (co)author of more than 75 journal and conference articles. He is a member of the IEEE. More information about his research can be found at www.tansu.alpcan.org.

Sonja Buchegger received undergraduate degrees in business administration and in computer science and the graduate degree in computer science from the University of Klagenfurt, Austria, in 1995, 1996, and 1999, respectively, and the PhD degree in communication systems from EPFL, Switzerland, in 2004. She is an associate professor of computer science at the Royal Institute of Technology (KTH), Stockholm, Sweden. From 1999 to 2003, she worked at the IBM Zurich Research Laboratory in the Network Technologies Group. From 2003 to 2004, she was a research and teaching assistant at EPFL. From 2005 to 2006, she was a postdoctoral scholar in the School of Information at the University of California at Berkeley. From 2007 to 2009, she was a senior research scientist at Deutsche Telekom Laboratories, Berlin. Her current research interests are in privacy, security, and economic aspects of peer-to-peer, social, vehicular, sensor, and mobile ad hoc networks. She is a member of the IEEE. More information about her research can be found at www.csc.kth.se/~buc.