Towards a Game Theoretic Approach For Defending Against Crime Diffusion

(Extended Abstract)

C. Zhang, A. X. Jiang, M.B. Short[1], P. J. Brantingham[2] and M. Tambe
University of Southern California
{zhan661,jiangx,tambe}@usc.edu
[1]Georgia Institute of Technology
mbshort@math.ucla.edu
[2]University of California, Los Angeles
pjb@anthro.ucla.edu

ABSTRACT

In urban transportation networks, crime diffuses as criminals travel through the networks and look for illicit opportunities. It is important to first model this diffusion in order to recommend actions or patrol policies to control the diffusion of such crime. Previously, game theory has been used for such patrol policy recommendations, but these applications of game theory for security have not modeled the diffusion of crime that comes about due to criminals seeking opportunities; instead the focus has been on highly strategic adversaries that plan attacks in advance. To overcome this limitation of previous work, this paper provides the following key contributions. First, we provide a model of crime diffusion based on a quantal biased random movement (QBRM) of criminals opportunistically and repeatedly seeking targets. Within this model, criminals react to real-time information, rather than strategically planning their attack in advance. Second, we provide a game-theoretic approach to generate randomized patrol policies for controlling such diffusion.

Categories and Subject Descriptors

I.2.11 [**Artificial Intelligence**]: Distributed Artificial Intelligence

General Terms

Algorithms, Human Factors, Security

Keywords

Game theory, Security games, Optimization

1. INTRODUCTION

Crime in transportation networks is a threat to passengers. Given the structure of these networks, crime diffuses as criminals traveling by public transportation seize opportunities to commit crimes. Unlike strategic adversaries who may carefully plan to exploit security weaknesses and attack targets, criminals may opportunistically react to real-time information, which means that crime diffuses dynamically. Indeed, recent research in criminology shows that crimes are often crimes of opportunity and how offenders move and mix with their potential targets or victims is a key determinant of the structure of any crime opportunity [1, 3].

Indeed, transportation networks play an important role in driving local crime patterns and in the diffusion of crime [8]. Individual transit hubs that are strong crime generators export that propensity to other locations on the transit network. Such diffusive potential may be particularly strong since a substantial portion of criminals use public transportation as their primary means of transportation [7]. Transportation networks may themselves be at unique risk of crime because of the way in which they concentrate large numbers of people in time and space [8, 12, 2]. Within a transportation network, not all locations are at equal risk. Certain transit stations, and certain transit vehicles, may have design features that promote crime, be it poor lighting and lack of natural surveillance [6] or environmental cues such as poor maintenance and graffiti that suggest that the facility is not well protected [5]. Some transit locations are therefore more likely to attract offenders than others.

We take a metro rail network as a concrete example. In such a network, crimes such as thefts and snatches usually occur at nodes, such as stations or junctions where it is easy for criminals to escape. These potential crime spots are connected by trains with a fixed timetable. Crime at one node can diffuse to a far-away node without affecting its neighbors. This diffusion may be stochastic, with higher probabilities of crime at more attractive stations.

Deploying police to patrol in such transportation networks is a way to suppress crime and control its diffusion. In our example metro rail network, the police patrols throughout all stations by trains. Previous work applying game theory in a metro network has successfully generated randomized patrol schedules for police [4]. These works deal with highly strategic attackers who conduct full surveillance and plan their illegal acts in advance; they assume attackers cannot adjust these plans given real-time information. Another difference of that work from ours is that attackers have fixed routes. As a result, the crime does not diffuse.

There are two key contributions in this paper. The first contribution is a new model of crime diffusion. In this model, criminals visit targets based on a quantal biased random movement (QBRM), which has been used to model criminal motion previously [11], instead of executing fixed routes. In addition, rather than planning their attack in advance, criminals opportunistically react to real-time information in the network.

The second contribution is a game-theoretic approach to generate

Appears in: *Alessio Lomuscio, Paul Scerri, Ana Bazzan, and Michael Huhns (eds.), Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2014), May 5-9, 2014, Paris, France.*

randomized patrol schedules. We model the interactions between criminals and the police as a Stackelberg game, with the police acting as the leader and criminals as followers. However there are two differences with previous work in Stackelberg Security games. First, criminals react to real-time information in our model as mentioned earlier, which is different from previous work. Second, after one attack, criminals can still stay in the network and find another target to attack using our QBRM model, which is modeled as crime diffusion. Our objective is to find a randomized patrol strategy for the police that optimizes her expected utility against crime diffusion. We formulate the problem as a nonlinear optimization problem on a Markov chain model.

2. RELATED WORK

There has been research on a wide range of topics related to controlling diffusion in networks. One line of work considers game-theoretic models of controlling contagion in networks. These are games between defenders and attackers where the attacker attempts to maximize its diffusion influence over the network while the defender tries to minimize this influence. Algorithms have been proposed to approximately solve such games under different models of diffusion, including [14] for the Independent Cascade Model (ICM) and [9] for the Linear Threshold Model (LTM). In these contagion games, the two players can only select a number of initial seed nodes and their influence diffuses automatically. Such models are thus not applicable to model the opportunistic criminals.

Another line of research uses recent advances in criminology on opportunistic criminal behavior to describe crime diffusion in networks. [11] applied a biased random walk model for house burglary, and [15] analyzed the effect of the police on controlling the crime diffusion in the house burglary domain. In their works, criminals have no knowledge of the overall strategy of the police, and their behavior is only affected by their observation of the current police allocation in their immediate neighborhood. Also in [15], police behave in a similarly reactionary way, allocating their resources in an instantaneously optimal way in response to the current crime risk distribution rather than optimizing over the time horizon and within a transportation network.

The motions of both criminals and police in [15] also vary significantly from those in the current work. Each instance of a criminal's motion in [15] may only be between adjacent locations, after which the nearby police allocation is observed anew and another movement can be made, leading to highly localized diffusion of criminals. In contrast, criminals in the current work may make “large" directed movements over the transportation network between distant locations, as they see fit, before updating their beliefs and moving again, leading to much less localized crime. Furthermore, in [15] there is no notion of the “movement" of police - rather, the distribution of police is chosen to be instantaneously optimal, with no regard for the mechanics of exactly how the allocation may transform from one timestep to the next.

Game theoretic approaches have been successfully applied to security domains for generating randomized patrol strategies against strategic adversaries, e.g., [13] generated schedules for the Federal Air Marshals to protect flights; [10] generated schedules for the US Coast Guard to protect ports; and [4] generated schedules for Los Angeles Sheriff Department to conduct fare checking on the LA Metro network. We have discussed our differences with that literature in the Introduction Section.

Our approach combines and generalizes the randomized patrolling model of previous security applications and the criminology-based random-walk diffusion model of [11]: now police can move inside the network in a randomized fashion, and the criminals are opportunistic and can diffuse throughout the network.

3. ACKNOWLEDGEMENT

This research is supported by MURI grant W911NF-11-1- 0332.

4. REFERENCES

[1] P Jeffrey Brantingham and George Tita. Offender mobility and crime pattern formation from first principles. *Artificial crime analysis systems*, 2008.

[2] Patricia Brantingham and Paul Brantingham. Criminality of place. *European Journal on Criminal Policy and Research*, 3(3):5–26, 1995.

[3] Marcus Felson and Ronald Victor Gemuseus Clarke. *Opportunity makes the thief: Practical theory for crime prevention*, volume 98. Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, 1998.

[4] Albert Xin Jiang, Zhengyu Yin, Chao Zhang, Milind Tambe, and Sarit Kraus. Game-theoretic randomization for security patrolling with dynamic execution uncertainty. In *AAMAS*, 2013.

[5] Kees Keizer, Siegwart Lindenberg, and Linda Steg. The spreading of disorder. *Science*, 322(5908):1681–1685, 2008.

[6] Anastasia Loukaitou-Sideris. Hot spots of bus stop crime: The importance of environmental attributes. *JAPA*, 65(4):395–411, 1999.

[7] Anastasia Loukaitou-Sideris, Robin Liggett, and Hiroyuki Iseki. The geography of transit crime documentation and evaluation of crime incidence on and around the green line stations in los angeles. *JPER*, 2002.

[8] Stephen A Matthews, Tse-Chuan Yang, Karen L Hayslett, and R Barry Ruback. Built environment and property crime in seattle, 1998–2000: A bayesian analysis. *Environment and planning. A*, 42(6):1403, 2010.

[9] Thanh H Nguyen, Jason Tsai, Albert Jiang, Emma Bowring, Rajiv Maheswaran, and Milind Tambe. Security games on social networks. In *AAAI Fall Symposium Series*, 2012.

[10] Eric Shieh, Bo An, Rong Yang, Milind Tambe, Craig Baldwin, Joseph DiRenzo, Ben Maule, and Garrett Meyer. Protect: A deployed game theoretic system to protect the ports of the united states. In *AAMAS*, 2012.

[11] Martin B Short, Maria R D'Orsogna, Virginia B Pasour, George E Tita, Paul J Brantingham, Andrea L Bertozzi, and Lincoln B Chayes. A statistical model of criminal behavior. *Mathematical Models and Methods in Applied Sciences*, 18(supp01):1249–1267, 2008.

[12] Ralph B Taylor and Adele Harrell. *Physical environment and crime*. US Department of Justice, Office of Justice Programs, National Institute of Justice, 1996.

[13] Jason Tsai, Christopher Kiekintveld, Fernando Ordonez, Milind Tambe, and Shyamsunder Rathi. Iris-a tool for strategic security allocation in transportation networks. In *AAMAS Industry Track*, 2009.

[14] Jason Tsai, Thanh H Nguyen, and Milind Tambe. Security games for controlling contagion. In *AAAI*, 2012.

[15] Joseph R Zipkin, Martin B Short, and Andrea L Bertozzi. Cops on the dots in a mathematical model of urban crime and police response. 2013.