ITS Department Article to appear in IEEE Intelligent Systems July/August 2007 issue

Protecting Transportation Infrastructure

Daniel Zeng, ***University of Arizona***

Sudarshan S. Chawathe, ***University of Maine***

Fei-Yue Wang, ***Chinese Academy of Sciences***

Protecting transportation infrastructure is an important component of today's homeland security effort. This article highlights related technical challenges and provides a brief survey of several IT research streams in this important application area, along with two case studies.

Keywords: Critical Infrastructure; Transportation Security

In the context of homeland security, critical infrastructures are "those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security, or economic well-being of citizens or the effective functioning of governments."[1] Transportation infrastructures are a key component of a nation's critical infrastructures, covering physical assets such as airports, ports, and railway and mass transit networks as well as software systems such as traffic control systems. In effect, among various critical infrastructures spanning a range of economic sectors and government operations,[2] transportation is widely viewed as one of the most significant and impactful. A 2002 study concerning the significance of infrastructure components andand the consequences of a destructive event rated transportation as "extremely significant." Other components at this highest level of significance were communications, power, emergency response personnel and assets, and national security resources.[3]

Transportation infrastructures are frequent targets of terrorist attacks because of their significance in several dimensions. Because physical transportation networks attract large numbers of people, they're high-value targets for terrorists intending to inflict heavy casualties. Transportation infrastructures themselves are important to the modern economy, and related damages and destruction can have quick ripple effects. Operationally, transportation systems interact with and provide support for other systems, such as emergency response and public health, in complex ways. Terrorists can perceive an attack on such a link (that is, one that connects many systems) as an efficient means to create confusion, counter the counter-measures, and damage the targeted society as a whole. Furthermore, transportation infrastructures can be both the means and the end of an attack, making them a critical part of almost all terrorist attacks in the physical world.

Tables 1 and 2 further illustrate the importance of protecting transportation infrastructures. Table 1 lists a number of attacks involving transportation infrastructures.[4] Table 2 shows the yearly counts of transportation-related terrorist incidents from 1998 to 2004, broken down by transportation mode. The information in table 2 is based on the Global Terrorism Database (GTD), "an open-source database including information on terrorist events around the world" from 1970 to 2004 (www.start.umd.edu/data/gtd).

Table 1. A partial list of terrorist attacks involving transportation infrastructures.[4]

Year	Incidents
2006	Bombs planted on two German trains (but failed to explode) 209 people killed by bombs on commuter trains in Mumbai, India**//OK? yes//** A plot to flood Manhattan commuter rail tunnels uncovered
2005	London mass transit bombings; 52 killed and more than 700 injured
2004	A plot to bomb New York subway stations foiled Madrid commuter train bombing; 191 killed and nearly 2,000 injured Moscow subway explosions; 40 killed
2003	Al-Qaeda reportedly called off a planned cyanide attack on the New York subway system
2002	Truck loaded with propane detonated at a Tunisian synagogue, killing and wounding dozens
1997	A plot to bomb a New York subway station foiled
1996	Multiple suicide attacks on buses in Israel
1995	Cult members released sarin gas on the Tokyo subway; 12 killed, 50 severely injured, and nearly 1,000 experienced temporary vision problems

Table 2. Transportation-related terrorism incidents from 1998 to 2004 by transportation mode (based on GTD data).

Year	Transportation mode		
	Maritime	Air	Ground
2004	2	5	25
2003	1	5	41
2002	0	10	41
2001	2	12	28
2000	2	11	56
1999	2	9	54
1998	1	7	36

Major areas of transportation security

Here, we aim to alert AI and IT researchers to the challenges facing transportation infrastructure protection. We start by discussing the main areas of transportation security technology from an application

perspective. We follow the program structure of the Department of Homeland Security's Transportation Security Laboratory,[5] whose mission is to "develop and evaluate next-generation security technology that can lead to successful deployment of products across all modes of transportation and the related transportation infrastructure."

The first major area is concerned with enhancing the security of infrastructure critical to transportation. As we defined it earlier, this infrastructure includes physical facilities, equipment, assets, service networks, and communication and computing hardware and software that enable information access and transactions. Airports, rail stations, bridges and tunnels, maritime ports, and bus terminals are examples of relevant application contexts. Critical practical challenges include

* physical access management and control of employees and passengers,
* perimeter intrusion detection,
* vulnerability assessment,
* intrusion detection and access control in the cyberspace in which pertinent information systems operate and exchange data, and
* related simulation and decision-support tools.

The remaining three major areas are commerce inspection, passenger inspection, and conveyance protection.[5] These all directly relate to transportation infrastructure protection and, when combined with infrastructure protection, provide a comprehensive approach to addressing practical security needs. Commerce inspection mainly concerns threat detection in checked passenger baggage, mail, commercial cargo and logistical/supply chain shipments, and any other form of commercial transportation activity. Sensor technologies for detecting explosives and weapons are critical in this area. Effective, efficient management of various resource types (for example, equipment, its human operators, and their training) also plays an important role in commerce inspection practices. Passenger inspection refers to the capability to inspect passengers at transportation system screening and entry points for concealed weapons, explosives, or other prohibited items. Conveyance protection focuses on enhancing the conveyance security of the entire transportation system. Key conveyance-protection technologies include characterization of explosives, analysis of the effects of blasts and related structural response modeling and simulation, material sciences, and sensor technologies.

With a particular emphasis on IT, we now discuss several active technical research areas that can facilitate transportation infrastructure protection efforts. Many of these technologies can apply to more than one application area.

Video surveillance

This technology is invaluable for transportation security. For years, numerous major cities around the world have used video feeds to monitor airports, sea ports, and railway and subway stations. Recent developments in computer networks and video-capturing hardware, such as thermal and infrared technologies, and algorithmic advances in image processing and computer vision, have made video surveillance increasingly versatile and cost effective.[4] Researchers and practitioners are paying more attention to IT research on extracting useful information (for example, face recognition and intention detection) from video streams in real time, either in a fully automated operational mode or as to help human operators make decisions.[6,7]

Tracking and location technologies

Technologies such as GPS and RFID enable operators to monitor key assets or moving objects of interest in space and time. Their use in the transportation domain is widespread, as evidenced by increasing

commercial activities and government initiatives in this space. Meanwhile, such technologies introduce their own information security vulnerabilities, which researchers are studying. From a research standpoint, finding interesting and relevant patterns from spatial data streams and using them in transportation security applications present both opportunities and challenges.

Authentication and access control

In the transportation security context, access control ensures that only authorized individuals have access to secured areas. Biometrics is quickly gaining ground as an enabling technology to make authentication and access-control systems more effective and efficient. Two predominant biometric applications are fingerprinting and iris scanning. In addition to traditional biometric research topics such as pattern recognition and data management, researchers are starting to explore the role of biometrics in the broad context of authentication and study issues such as privacy and secure system interoperability.

Information sharing, fusion, and management

Effective information sharing across datasets and system boundaries, the ability to fuse information and data from sources that provide (partially) overlapping and complementary coverage, and efficient, secure data management have long been identified as key drivers of effective intelligence and homeland security-related information systems.[8] Information systems for protecting transportation infrastructure share the same design objectives. To support counterterrorism efforts such as preparing, detecting, and responding to terrorism events, large amounts of information in different modalities from many sources must be acquired, integrated, and interpreted in the right context, often in real time.[2] In addition, a critical need exists for a data-management infrastructure that can support information flows across jurisdictional and organizational boundaries (for example, intelligence, law-enforcement, and emergency-response communities). Despite existing efforts, researchers and practitioners must still make significant progress in this area from both technical and policy perspectives, with careful attention to laws and regulations, privacy considerations, and civil rights.

Target hardening

This aims to make transportation facilities less vulnerable. Many transit systems have implemented such efforts through their crime-prevention programs (for example, removing trash cans or using ballistic-resistant ones, installing blast-resistant glass, and eliminating dead spots where bombs might be hidden). On a much larger scale, strategic facilities such as bridges, tunnels, and terminals are being fortified to improve their chance of surviving attacks. Research on threat assessment and resource allocation that helps determine where and how to pursue target-hardening efforts can provide important actionable knowledge guiding such efforts in practice.

Human factors

Researchers in this area aim to optimize the human element in transportation infrastructure protection to make the overall human-machine system perform better. Researchers have actively pursued two lines of work, one of which focuses on recruiting and training. For instance, a systematic approach to selecting airport screeners, developing and evaluating screener-training programs, and developing procedures for measuring and improving screener performance has been put into practice.[5] The second line of work has traditional HCI goals: to improve operator performance by designing equipment and user interfaces that maximize user perceptual, cognitive, and physical abilities while minimizing errors.

Systems science and engineering

Systems science frameworks are helping practitioners understand complex transportation systems'

performance and vulnerabilities and the interactions among their subsystems. In addition, the systems that protect transportation infrastructure are themselves complex engineering systems with data from networked sensors, complex workflow and command and control structures, and real-time intrusion detection and access control functions. Systems engineering principles provide important guidelines for designing, developing, and implementing such systems.

In recent years, an academic discipline called intelligence and security informatics has emerged. ISI aims to develop advanced information technologies, systems, algorithms, and databases for national- and homeland-security-related applications, through an integrated technological, organizational, and policy-based approach.[9] Many of the technical research areas we've discussed are part of ISI study. Transportation infrastructure protection is an important application domain for ISI frameworks and techniques. It also presents interesting technical challenges motivating ISI research.

Example research projects

Two transportation infrastructure protection research projects illustrate these application context and research issues. The first, a critical infrastructure protection study in Virginia,[10] assessed the risks of terrorist attacks to the surface transportation system. Researchers jointly with government officials analyzed eight critical assets, including one intelligent transportation system traffic-control center, two major interstate interchanges, three bridges, one bridge-tunnel, and one tunnel. At each site, researchers performed a risk assessment study by soliciting from domain experts and practitioners answers to three questions:

* What can go wrong?
* What's the likelihood that something will go wrong?
* What are the consequences if something does go wrong?

In the follow-up risk-management step, the researchers first evaluated risk-management options. On the basis of input from the Virginia Department of Transportation domain experts, they put these options (including cost estimates) into two categories: prevention and response. Next, they selected optimal options using Pareto-optimal graphs, plotted separately for preventative and responsive options. (In multicriteria decision making, a Pareto-optimal option is one where an objective can be improved only at the expense of another.) This study, although preliminary, illustrates a direct application of a general risk-assessment and management framework in transportation infrastructure protection with real-world findings.

BorderSafe is a much larger, ongoing project. Although only indirectly related to transportation infrastructure protection, this project illustrates important data mining applications that generally apply to transportation security. It also demonstrates the value of cross-jurisdictional information sharing.[9] BorderSafe is a collaborative research effort involving the University of Arizona's Artificial Intelligence Lab, the San Diego Super Computer Center, and law enforcement agencies including the Tucson Police Department, the Phoenix Police Department, the Pima County Sheriff's Department, the Tucson Customs and Border Protection, and the San Diego Automated Regional Justice Information Systems. BorderSafe includes several cross-jurisdictional data sharing initiatives, such as one integrating TPD, PCSD, and CBP data sets. Using this integrated data set, the research team evaluated the impact of cross-jurisdictional information on crime analysis. They constructed a criminal activity network based on associations that occur when individuals or vehicles are listed together in a crime incident report. The research findings indicate that border-crossing activities generate useful leads for investigating certain types of crimes. In addition, automated data mining targeted at correlating stolen vehicle reports with border crossings and

targeted individuals could help in many investigations, enabling real-time analysis that's prohibitively time-consuming using the traditional manual process.

Transportation infrastructure protection provides a potentially fruitful application domain for many subdisciplines of AI and closely related fields—from data mining, sensor networks, and video processing to risk analysis, real-time decision support, and human-machine interaction. We believe that cross-cutting research in AI, ISI, and critical infrastructure protection including transportation systems will produce tangible, practically relevant research results benefiting these research communities.

The authors wish to acknowledge support from research grants (IIS-0428241 and IIS-0646178) from the U.S. National Science Foundation, research grants (60573078 and 60621001) from the National Natural Science Foundation of China, an international collaboration grant (2F05N01) from the Chinese Academy of Sciences, and a National Basic Research Program of China (973) grant (2006CB705500) from the Ministry of Science and Technology.

References

1. Commission of the European Communities, *Critical Infrastructure Protection in the Fight against Terrorism*, Communication from the Commission to the Council and the European Parliament, October 2004; http://eur-lex.europa.eu/LexUriServ/site/en/com/2004/com2004_0702en01.pdf.
2. Committee on Science and Technology for Countering Terrorism, Nat'l Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Nat'l Academies Press, 2002.
3. W.M. Biersack et al., "An Infrastructure Vulnerability Assessment Methodology for Metropolitan Areas," *Proc. 36th Ann. Int'l Carnahan Conf. Security Technology*, IEEE Press, 2002, pp. 29–34.
4. S. Greiper and M. Sauter, "Beyond Aviation: The Emerging Ground Transportation Security Market," market report, Legend Merchant Group, September 2006; http://legendmerchant.com/docs/2006/2006-09-BeyondAviation.pdf.
5. S.F. Hallowell and P.Z. Jankowski, "Transportation Security Technologies Research and Development," *Proc. IEEE Military Communications Conf.* (MILCOM 05), IEEE Press, 2005, pp. 1753–1756.
6. M.L. Jensen et al., "Identification of Deceptive Behavioral Cues Extracted from Video," *Proc. 8th Int'l IEEE Conf. Intelligent Transportation Systems*, IEEE Press, 2005, pp. 1135–1140.
7. H. Niels and S. Khurram, "Automatic Visual Analysis for Transportation," *Proc. IEEE Conf. Technologies for Homeland Security*, IEEE Press, 2007, pp. 13–18.
8. US General Accounting Office, "National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy," Congressional Testimony, GAO-02-811T, 7 June 2002.
9. H. Chen, F.-Y. Wang, and D. Zeng, "Intelligence and Security Informatics for Homeland Security: Information, Communication, and Transportation," *IEEE Trans. Intelligent Transportation Systems*, vol. 5, no. 4, 2004, pp. 329–341.
10. E.V. Jones et al., "Virginia's Critical Infrastructure Protection Study," *Proc. 2003 IEEE Systems and Information Eng. Design Symp.*, IEEE Press, 2003, pp. 177–182.

Daniel Zeng is an associate professor and the director of the Intelligent Systems and Decisions Laboratory in the Department of Management Information Systems at the University of Arizona's Eller College of Management. He's also an affiliated professor at the Institute of Automation, Chinese Academy of Sciences. Contact him at zeng@eller.arizona.edu.

Sudarshan S. Chawathe is an assistant professor of computer science at the University of Maine. Contact him at chaw@cs.umaine.edu.

Fei-Yue Wang is the director of the Key Laboratory of Complex Systems and Intelligence Science at the Chinese Academy of Sciences. He's also a professor in the University of Arizona's Systems & Industrial Engineering Department and the director of the university's Program in Advanced Research of Complex Systems. Contact him at feiyue@sie.arizona.edu.