Chapter 14

# SECURE CROSS-DOMAIN TRAIN SCHEDULING

Mark Hartong, Rajni Goel and Duminda Wijesekera

**Abstract** Track configurations at cross-domain interchange points, train performance characteristics and cross-domain authentication often produce significant train delays that can impact large segments of a railroad network. This paper presents a model that captures the behavior of trains and the track infrastructure. The model enables railroad signal engineers to quickly estimate the required trust management system performance that will support safe, secure and efficient railroad operations.

**Keywords:** Railroads, trains, cross-domain scheduling, security

## 1. Introduction

Railroads are a major component of the U.S. transportation infrastructure. According to the Association of American Railroads [2], more than 1.7 trillion ton-miles of freight was transported by rail in 2007.

Unlike other transportation modes, trains operate with a single degree of freedom. They are constrained to travel on a single track and are unable to pass other trains operating on the same track except where there are sidings.

Since the early 1820s, various methods for scheduling, dispatching and controlling cross-domain train operations have been devised. These range from simple systems to complex stochastic models that optimize asset locations, times of movement and paths through the rail network. However, the operations research community has largely ignored the issue of cross-domain trust management system performance when trains reach an interchange point. With the implementation of secure positive train control (PTC) [17] in the U.S. railroad system, cross-domain scheduling, train movement and authority management must all work in concert.

This paper proposes a deterministic model that provides railroad signal engineers with the ability to quickly estimate the required trust management

system performance, while precluding train-to-train collisions and optimizing traffic flow at an interchange. The solution facilitates cost containment, a critical consideration for U.S. railroad companies.

## 2. Related Work

Several algorithmic approaches for position, scheduling and routing optimization have been developed since the mid 1970s [5, 9, 37]. These approaches and others have been incorporated in computer dispatch systems from major suppliers such as Alstom, Advanced Railway Concepts, Digital Concepts, GE Transportation, Siemens and Anslado STS. However, details of these systems are proprietary and the exact mechanisms they use for position, scheduling and routing optimization are not known to the research community. Despite the lack of information, it is safe to assume that the proprietary systems engage exact, heuristic and simulation strategies similar to those described by Sutewong [39].

Global visibility of the rail network and rail traffic enables dispatchers to discern bottlenecks in advance, permitting traffic to be rerouted securely, safely and efficiently. This contributes to an increase in overall system velocity (average rate at which trains move through the network) and, consequently, an increase in railroad network throughput. The improved utilization directly translates to cost savings for railroad companies and consumers.

While the positioning problem associated with freight and passenger trains is similar, there are significant differences in the scheduling and routing problems. Passenger service is constrained to fixed schedules and constant routes. Freight service, on the other hand, does not have these restrictions. Since railroad routing is a highly constrained network optimization problem that has confounded traditional optimization methods, we limit the scope of our analysis. No attempts will be made to develop new or improved dispatching methodologies or to examine complex network topologies. Instead, we consider only a single line of track approaching an interchange point with no other topological additions (including merging or branching routes) other than a single siding track off the main line. This enables us to consider the track connecting the railroads through the interchange point as a "single track railroad." Several approaches (e.g., [12, 16, 22–24, 30, 31, 33, 34, 36]) can then be used to minimize the impact of delays.

The security of rail networks and the integration of trust management systems have been the subject of several research efforts (see, e.g., [8, 10, 15, 18–21, 44]). However, these efforts have not made significant progress in integrating secure train control and scheduling or providing railroad signal engineers with the ability to evaluate performance and ensure safe train operations.

## 3. Interchange and Cross-Domain Operations

Determining a global solution to the dispatch problem requires the consideration of cross-domain security mechanisms. This is complicated by the structure

of the United States rail industry. Since railroad companies are distinct commercial entities, they have separate dispatch, scheduling and trust management systems in their respective domains. These differences are most pronounced at interchanges – fixed, geographically-dispersed points where the tracks belonging to one railroad company interconnect with the tracks of another company, and where crews, locomotives and consists are exchanged. Secure exchanges between domains require the ability of the dispatcher in each domain to authenticate the communicating entities and to ensure message integrity.

Before a train can be authorized to pass from one railroad domain to another, the following two activities must occur:

- The train and the crew leaving the first domain for the second domain must be authenticated before a movement authority can be granted by a dispatcher to allow the cross-domain movement.

- Track space must be available to allow the issuance of the movement authority.

For a train moving from one domain to another, delays in the authentication process will delay the granting of the current movement authority as well as subsequent movement authorities. This, in turn, will delay the scheduled movement of subsequent trains. Minimizing or eliminating authentication delays reduces delays in the granting and issuance of movement authorities, which, in turn, reduces traffic delays.

Our choice of unidirectional analysis is deliberate. In high traffic density areas, where large volumes of rail traffic are exchanged between domains, multiple main tracks are often used at the interchange point, with one main track carrying traffic from Domain A to Domain B and a second main track carrying traffic from Domain B to Domain A. Each main track can, therefore, be analyzed as a separate unidirectional track. Single main tracks used for interchange points are generally found on low density lines, where the directional movement of cross-domain traffic is spatially and temporally separated to minimize the numbers of meets and passes; this reduces the number and size of expensive sidings. High degrees of spatial and temporal separation also permit the cross-domain analysis to be treated as unidirectional.

## 3.1 Interchange Movement

Figure 1 shows two railroad companies (Railroad A and Railroad B) that have a common interchange point. The trains can belong to any company. Train 1 ($T_X$), Train 2 ($T_{X+1}$) and Train 3 ($T_{X+2}$) through Train N ($T_{X+N}$) are moving sequentially along tracks operated by Railroad A to the interchange point. The movement of train $T_X$ requires the possession of a valid movement authority ($M_X$) from the dispatcher ($DS$). In the situation involving a single main track with a single siding, four possible situations may be encountered by $T_{X+1}$ that follows $T_X$:

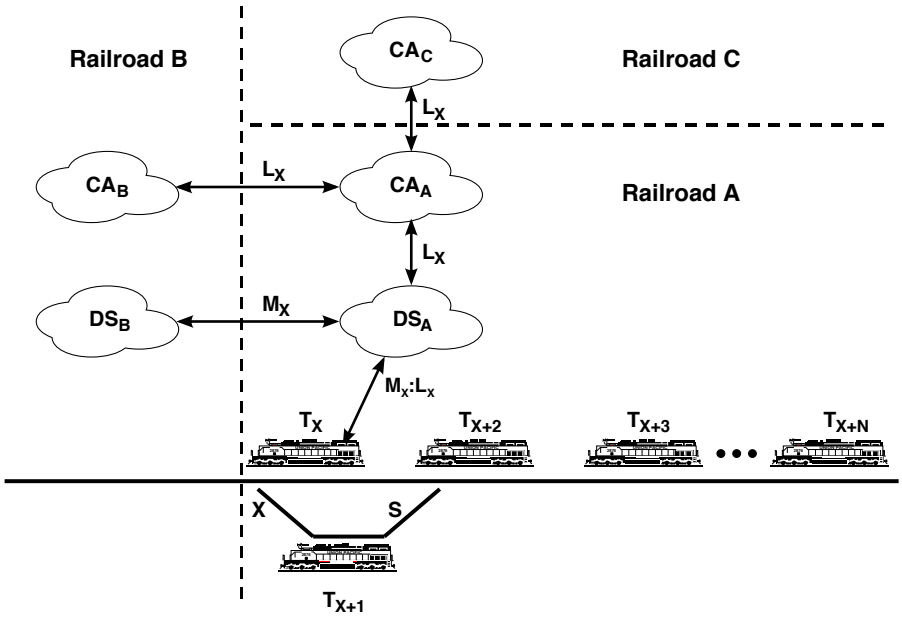


*Figure 1.* Railroad interchange point.

- **The main track and siding are clear:** In this situation, $T_{X+1}$ may take the main track or siding and proceed to the interchange point without any delay.

- **The main track is clear and the siding is blocked:** In this situation, $T_{X+1}$ may take the main track and proceed to the interchange point without any delay.

- **The main track is blocked and the siding is clear:** In this situation, $T_{X+1}$ may take the siding and proceed to the interchange point without any delay.

- **The main track and siding are blocked:** In this situation, $T_{X+1}$ may have to wait until the main track or siding are clear in order to proceed to the interchange point.

If $T_X$ is already at the limits of its movement authority $M_X$ at the interchange point, then $T_X$ stops and remains stopped until a new authority to proceed is received. To preclude a train-to-train collision between the head of $T_{X+1}$ and the tail of $T_X$, $T_{X+1}$ must receive a notification to stop before it proceeds beyond the safe stopping distance $BD_{X+1}$. The movement of subsequent trains such as $T_{X+2}$, $T_{X+3}$ $\ldots T_{X+N}$ must then be rescheduled to preclude collisions and the overrun of their authority limits as necessary.

A delay of $T_X$ at the interchange point is mitigated by the availability of Siding $S$. If the train dispatcher $DS_A$ for Railroad A is aware in advance of an authentication delay associated with $T_X$, the dispatcher could direct $T_X$ to Siding $S$, allowing $T_{X+1}$ to proceed along the main line to the interchange point. However, even if the dispatcher was able to safely divert $T_X$ to Siding $S$, any delay of $T_{X+1}$ at the interchange point would still delay $T_{X+2} \ldots T_{X+N}$.

The cross-domain delay is the sum of the propagation delay between the dispatchers, the processing time required by the communicating entities and the authentication delay that results from the additional overhead associated with the transmission of data required for cross-domain certification and integrity. The propagation and processing delays are fixed and unavoidable, being functions of the media through which the data is transmitted. The authentication delay, however, is a function of the security protocols used to provide cross-domain certification.

The two most commonly-used protocols in the railroad industry are ATCS-200 and TCP/IP that operate in the 40 MHz, 160 MHz or 220 MHz radio-frequency bands. ATCS-200 is a railroad-specific communications protocol designed by the Association of American Railroads as part of the Advanced Train Control System (the precursor to PTC). TCP/IP is the standard TCP/IP v4 (RFC 793) or v6 (RFC 2460).

ATCS and TCP/IP follow the classical three-way handshake to establish and terminate connections over possibly unreliable links. The three-way handshake begins by $A$ initiating a connection by sending a message to $B$. Next, $B$ responds with an acknowledgment. At this point, $A$ sends another message to $B$ confirming that $A$ received B's acknowledgment. The connection between $A$ and $B$ is established when $B$ receives the second message from $A$ that confirms the acknowledgement from $B$. Each protocol has its own set of vulnerabilities and countermeasures [4, 11].

## 3.2 Cross-Domain Certification

Entry into Domain B is controlled by Dispatcher B. Dispatcher B must approve a movement authority $M_X$ for train $T_X$. The request for $M_X$ and the response of Dispatcher B are routed through Dispatcher A (of Domain A). Prior to accepting the request for $M_X$, the authenticity of $T_X$ and the integrity of the request must be verified to the satisfaction of Dispatcher B. This is accomplished by pre-establishing a trust relationship between the certificate authorities of Domain A ($CA_A$) and Domain B ($CA_B$) and Dispatcher A and Dispatcher B. Before it begins operations, train $T_X$ is assigned a certificate $L_X$ via a separate secure channel.

The movement authority authentication process for $T_X$ (shown in Figure 2) begins when $T_X$ submits an $M_X$ request to Dispatcher A. This process is described in Algorithm 1.

The algorithm assumes that Dispatchers A and B have established a secure trust relationship. Based on the response from Dispatcher B, Dispatcher A determines the appropriate moves of $T_X$ as well as moves of subsequent trains

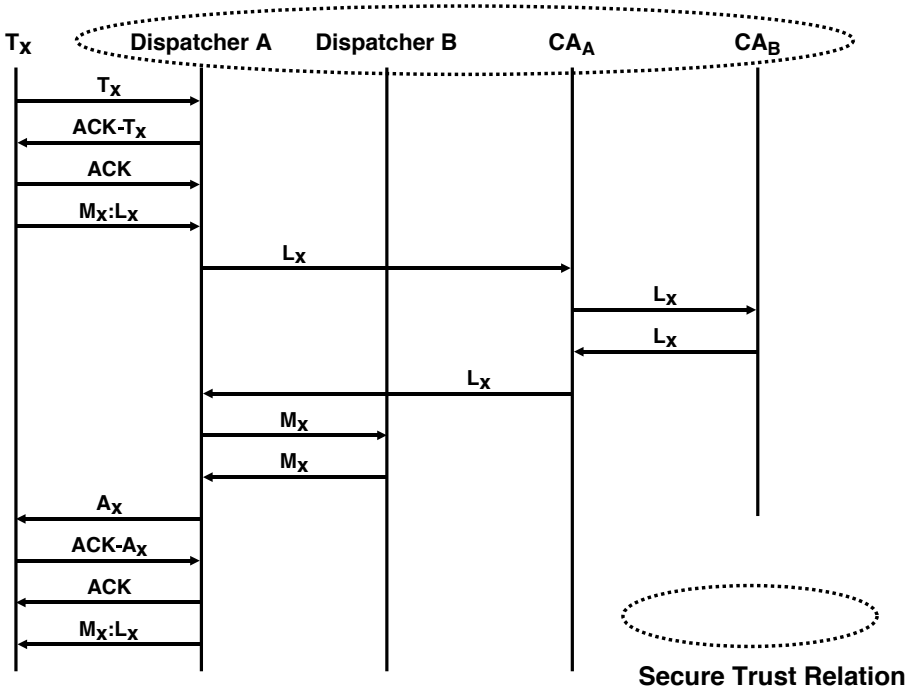


*Figure 2.* Authentication and authorization process.

$T_{X+1} \ldots T_{X+N}$. The total delay time associated with authentication and authority issuance is the time elapsed from when $M_X$ is submitted to Dispatcher A to when the approved or disapproved $M_X$ is received by $T_X$.

The cross-domain authentication and authority process uses open wireless networks to relay data. This exposes the process to a variety of network attacks, which may be classified as passive or active. Passive attacks involve the surreptitious gathering of information, which may facilitate more serious (active) attacks. Active attacks, which specifically target data transmission, can have an immediate impact on cross-domain operations.

Active attacks often involve denial-of-service. Additionally, they may involve an exploitation attempt associated with the sender (identity theft, where an unauthorized user adopts the identity of a valid sender); a weakness associated with the receiver (malicious association, where an unsuspecting sender is tricked into believing that a communications session has been established with a valid receiver); or a weakness associated with the communication path (man-in-the-middle attack, where the attacker emulates the authorized receiver for the sender – the malicious assertion, and emulates the authorized transmitter for the authorized sender – identity theft). These attacks are primarily geared at disrupting integrity in the form of user authentication (assurance that the party is who it says it is); data origin authentication (assurance that the data

**Algorithm 1** : Movement Authority Authentication Algorithm.

```
Grant Authority ()
begin
    Dispatcher A and Train T_X authenticate each other;
    T_X signs M_X using L_X;
    T_X submits M_X:L_X to Dispatcher A;
    Dispatcher A submits L_X to Certificate Authority CA_Y;
    repeat
        Certificate Authority CA_Y validates L_X or
        Certificate Authority CA_Y queries next Certificate Authority;
    until L_X is validated or no more Certificate Authorities remain to query;
        if L_X is valid then
            Dispatcher A submits M_X to Dispatcher B;
            Dispatcher B approves or disapproves M_X;
            Dispatcher B returns M_X to Dispatcher A;
            Dispatcher A and Train T_X authenticate each other;
            Dispatcher A signs M_X with its certificate L_A;
            Dispatcher A submits M_X:L_A to T_X;
            if M_X authorizes the move then
                T_X executes M_X
            else T_X does not move;
        else Dispatcher A disapproves M_X;
end
```

came from where it says it did); and data integrity (assurance that the data has not been modified). Countermeasures implemented for these attacks add additional time delays.

The simple model presented in this paper does not describe the mechanisms used to prevent or mitigate the numerous wireless attacks to which the cross-domain authority and issuance process is susceptible. In general, protection against attacks on message integrity is achieved using cryptographic hash functions. Any input modification would produce a different hash value, which would be detected by the receiver when the computed hash value is not equal to the received hash value.

Protection against identity attacks involves the application of authentication mechanisms that provide accountability for user actions and are considered in terms of user authentication and data origin authentication. User authentication involves the corroboration of the identity of the originator in real time, while data origin authentication involves the corroboration of the source of the data (but provides no timeliness guarantees). User authentication methods range from time-invariant methods such as weak passwords to time-variant cryptographic methods. Data origin authentication provides assurances regarding both integrity and authentication, which rely on the use of symmetric or asymmetric digital signatures.

## 3.3 Authentication Delays

The potential for a collision between trains $T_{X+1}$ and $T_X$ is affected by the velocity of $T_{X+1}$, time of release of $T_X$, communication and processing delays associated with information exchanges between $CA_A$ and $CA_B$, processing delays for dispatchers $DS_A$ and $DS_B$, and PTC system processing times $PTC_A$ and $PTC_B$. The velocity $V_{X+1}$ of train $T_{X+1}$ directly affects its safe stopping distance $BD_{X+1}$. As $V_{X+1}$ increases, $BD_{X+1}$ increases, requiring greater separation of trains $T_X$ and $T_{X+1}$ to preclude a collision. Stopping distances for various types of (freight and passenger) trains have been studied extensively (see, e.g., [3, 25, 35]).

Commercial tools are available for calculating safe braking distances and can be integrated with dispatch system behavior. The tools include the RailSim Train Performance Calculator (TPC) from Systra Consulting and the Train Operation and Energy Simulator (TOES) from the Association of American Railroads. The models used by the tools are quite complex and account for variables such as rail friction, engine latency, in-train forces, track geometry, brake pipe propagation and blended braking. However, these tools are expensive, which limits their availability. Accordingly, we adopt a simplified braking model to illustrate the basic concepts.

The simplified model assumes a straight and level track, but otherwise reflects the same variables that are used in [43] to predict braking distances for the European Train Control System (ETCS) system. The work in [43] is an improvement over the predictive braking curves based on the International Union of Railways (UIC) 546 Standard [6]. A similar U.S. standard [26] is currently under development. Efforts are underway to develop braking algorithms that model track geometry and consist behavior more realistically (see, e.g., [14, 28, 29, 38, 40, 45, 46]).

In order to prevent delays, either the siding or the main track must be clear prior to the arrival of a following train. The authentication delays for a train occupying a siding or mainline block and the clearance time for the train to clear the block must be less than or equal to the time it takes for a following train to cover its braking distance, i.e.,

$$Authentication\ Delay + Time\ to\ Clear\ T_X \leq Time\ to\ Stop\ T_{X+1} \tag{1}$$

The term *Time to Clear* $T_X$ ($t_{Clear}$) is computed as:

$$t_{Clear} = \sqrt{\frac{2(L_f - L_s)}{a_{Clear}}} \tag{2}$$

where $L_f$ is the final location of the tail of train $T_X$ (i.e, the interchange point); $L_s$ is the starting location of the tail of $T_X$; $L_f - L_s$ is the length of $T_X$; and $a_{Clear}$ is the acceleration of $T_X$.

The acceleration $a_{Clear}$ is given by:

$$a_{Clear} = \frac{F - R}{M} \tag{3}$$

where $F$ is the tractive force of the locomotives of $T_X$ in lbs/ton; $R$ is the resistance of $T_X$ in ft lbs; and $M$ is the mass of a train car in $T_X$ in tons.

The value of $R$, which expresses the resistive force, is estimated using the Davis Equation. This equation was originally developed in the mid 1920s for estimating locomotive resistance. The resistance $R$ (lbs/ton) is currently estimated using the new version of the equation, which was created in the 1970s [26]:

$$R = 0.6 + \frac{20}{w} + 0.01V + \frac{KV^2}{wn} \tag{4}$$

where $w$ is the weight of the train per number of axles; $V$ is the velocity in mph; $K$ is a drag coefficient, which has a value of 0.07 when the train is accelerating; and $n$ is the number of axles.

The safe stopping distance is the point ahead of the target that an oncoming train $T_{X+1}$ must begin to brake in order to preclude a collision with the rear of train $T_X$. This point, denoted by $L_b$, where the braking of $T_{X+1}$ begins is computed as:

$$L_b = L_h + Vt + \frac{1}{2}Ka_{Stop}t^2 \tag{5}$$

where $L_h$ is the location at which the head of train $T_{X+1}$ is stopped (i.e., the interchange point); $V$ is the initial velocity of $T_{X+1}$; $t$ is the duration of the deceleration of $T_{X+1}$; $K$ is the deceleration factor, which is equal to 1.4667; and $a_{Stop}$ is the deceleration of $T_{X+1}$.

The deceleration $a_{Stop}$ is given by:

$$a_{Stop} = \frac{F + R}{M} \tag{6}$$

where $F$ is the braking force of the consist cars of $T_{X+1}$ in lbs/ton; $R$ is the resistance of $T_{X+1}$ in ft lbs; and $M$ is the mass of a train car in $T_{X+1}$ in tons.

Train $T_{X+1}$ can continue its movement to the interchange point if the length of time taken for $T_X$ to receive its authority and move beyond the interchange point is less than the time it takes to stop $T_{X+1}$. These computations support the evaluation of a worst-case traffic density scenario and minimize the chance of a signal passed at danger. Rail operations can continue safely as long as the associated trust management systems support the required intra-domain security and traffic-scheduling constraints, and sufficient track space is available.

## 4. Conclusions

The approach presented in this paper addresses the performance issue once authorization has been requested and received by a train waiting at the interchange point to cross domains. However, it does not address the global sequencing of trains between two domains. In general, the movement of trains within a railroad domain is not optimized for behavior at an interchange point, but rather to support the most efficient use of the domain's rail assets (cars, locomotives and track). This operations research problem has been the focus

of considerable study [1, 7, 13, 27, 32, 41, 42] and is outside the scope of this work. It is necessary to construct a more general model for estimating tactical cross-domain authentication and authorization performance. The expansion and integration of tactical and strategic scheduling and routing is a logical extension of the current work. However, since a closed form solution will be unlikely, statistical techniques will have to be applied to solve the problem. Additional work is also required to integrate quality of service constraints, different train types with different operating characteristics, and more complicated track geometries.

Several implementation-related issues have not been fully addressed in this work. In an operational environment, where rail traffic is both heavy and dense, the volume of operational and environmental data that must be transmitted may exceed the communications bandwidth. The required bandwidth capabilities can only be determined in the context of the railroad operating environment and the particular implementation mechanisms. If appropriately chosen and considered in the light of organizational and environmental factors, the combination of managerial, operational and technical controls can synergistically ensure a safe, secure and interoperable rail system. Efforts in this area and in the related security requirements would provide valuable data for detailed system design and cost evaluation.

## References

[1] L. Anderegg, S. Eidenbenz, M. Gantenbein, C. Stamm, D. Taylor, B. Weber and P. Widmeyer, Train routing algorithms: Concepts, design choices and practical considerations, *Proceedings of the Fifth Workshop on Algorithm Engineering and Experiments*, pp. 106–118, 2003.

[2] Association of American Railroads, Class I Railroad Statistics, Washington, DC (www.aar.org/∼/media/AAR/Industry%20Info/Statistics200906 10.ashx), 2009.

[3] D. Barney, D. Haley and G. Nikandros, Calculating train braking distance, *Proceedings of the Sixth Australian Workshop on Safety Critical Systems and Software*, vol. 3, pp. 23–29, 2001.

[4] S. Bellovin, Security problems in the TCP/IP protocol suite, *ACM SIGCOMM Computer Communication Review*, vol. 19(2), pp. 32–48, 1989.

[5] A. Billionnet, Using integer programming to solve the train-platforming problem, *Transportation Science*, vol. 37(2), pp. 213–222, 2003.

[6] British Standards Institution, EN 15179: Railway Applications; Braking; Requirements for the Brake System of Passenger Coaches, Document BS 05/19984709 DC, London, United Kingdom, 2005.

[7] M. Carey and I. Crawford, Scheduling trains on a network of busy complex stations, *Transportation Research, Part B: Methodological*, vol. 41(2), pp. 159–178, 2007.

[8] A. Carlson, D. Frincke and M. Laude, Railway security issues: A survey of developing railway technology, *Proceedings of the International Conference on Computer, Communications and Control Technologies*, vol. 1, pp. 1–6, 2003.

[9] T. Crainic, J. Ferland and J. Rousseau, A tactical planning model for rail freight transportation, *Transportation Science*, vol. 18(2), pp. 165–184, 1984.

[10] C. Craven, A brief look at railroad communication vulnerabilities, *Proceedings of the Seventh IEEE Conference on Intelligent Transportation Systems*, pp. 245–249, 2004.

[11] P. Craven and A. Craven, Security of ATCS wireless railway communications, *Proceedings of the IEEE/ASME Joint Rail Conference*, pp. 227–238, 2005.

[12] A. D'Ariano, M. Pranzo and I. Hansen, Conflict resolution and train speed coordination for solving real-time timetable perturbations, *IEEE Transactions on Intelligent Transportation Systems*, vol. 8(2), pp. 208–222, 2007.

[13] M. Dessouky, Q. Lu, J. Zhao and R. Leachman, An exact solution procedure to determine the optimal dispatching times for complex rail networks, *IEE Transactions*, vol. 38(2), pp. 141–152, 2006.

[14] B. Friman, An algorithm for braking curve calculations in ERTMS train protection systems, *Proceedings of the Tenth International Conference on Computer System Design and Operation in the Railway and Other Transit Systems*, pp. 421–429, 2006.

[15] General Accounting Office, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Report to Congressional Requesters, GAO-04-354, Washington, DC, 2004.

[16] S. Graff and P. Shenkin, A computer simulation of a multiple track rail network, presented at the *Sixth International Conference on Mathematical Modeling*, 1987.

[17] M. Hartong, R. Goel and D. Wijesekera, Communications-based positive train control systems architecture in the USA, *Proceedings of the Sixty-Third IEEE Vehicular Technology Conference*, vol. 6, pp. 2987–2991, 2006.

[18] M. Hartong, R. Goel and D. Wijesekera, Communications security concerns in communications-based train control, *Proceedings of the Tenth International Conference on Computer System Design and Operation in the Railway and Other Transit Systems*, pp. 693–703, 2006.

[19] M. Hartong, R. Goel and D. Wijesekera, Securing positive train control systems, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 57–72, 2007.

[20] M. Hartong, R. Goel and D. Wijeskera, Security and the U.S. rail infrastructure, *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 15–28, 2008.

[21] M. Hartong, R. Goel and D. Wijesekera, Trust-based secure positive train control (PTC), *Journal of Transportation Security*, vol. 1(4), pp. 211–268, 2008.

[22] A. Higgins and E. Kozan, Modeling train delays in urban networks, *Transportation Science*, vol. 32(4), pp. 346–357, 1998.

[23] T. Ho, J. Norton and C. Goodman, Optimal traffic control at railway junctions, *IEE Proceedings on Electric Power Applications*, vol. 144(2), pp. 140–148, 1997.

[24] T. Ho and T. Yeung, Railway junction traffic control by heuristic methods, *IEE Proceedings on Electric Power Applications*, vol. 148(1), pp. 77–84, 2001.

[25] IEEE, IEEE Standard 1474.1-2004: IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements, Piscataway, New Jersey, 2004.

[26] IEEE, Draft Guide for the Calculation of Braking Distances for Rail Transit Vehicles, IEEE Draft Document P1698/D1.3, Piscataway, New Jersey, 2008.

[27] M. Khan, D. Zhang, M. Jun and J. Zhu, An intelligent search technique for the train scheduling problem based on genetic algorithms, *Proceedings of the International Conference on Emerging Technologies*, pp. 593–598, 2006.

[28] E. Khmelnitsky, On an optimal control problem of train operation, *IEEE Transactions on Automatic Control*, vol. 45(7), pp. 1257–1266, 2000.

[29] H. Krueger, E. Vaillancourt, A. Drummie, S. Vucko and J. Bekavac, Simulation within the railroad environment, *Proceedings of the Thirty-Second Winter Simulation Conference*, pp. 1191–1200, 2000.

[30] J. Lee, K. Sheng and J. Guo, A fast and reliable algorithm for railway train routing, *Proceedings of the IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering*, vol. 2, pp. 652–655, 1993.

[31] M. Lewellen and K. Tumay, Network simulation of a major railroad, *Proceedings of the Thirtieth Winter Simulation Conference*, pp. 1135–1138, 1998.

[32] F. Li, Z. Gao, K. Li and L. Yang, Efficient scheduling of railway traffic based on global information of trains, *Transportation Research, Part B: Methodological*, vol. 42(10), pp. 1008–1030, 2008.

[33] Q. Lu, M. Dessouky and R. Leachman, Modeling train movements through complex rail networks, *ACM Transactions on Modeling and Computer Simulation*, vol. 14(1), pp. 48–75, 2004.

[34] M. Lubbecke and U. Zimmermann, Engine routing and scheduling at industrial in-plant railroads, *Transportation Science*, vol. 37(2), pp. 183–197, 2003.

[35] M. Malvezzi, P. Presciani, B. Allotta and P. Toni, Probabilistic analysis of braking performance in railways, *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, vol. 217(3), pp. 149–165, 2003.

[36] D. Parkes and L. Ungar, An auction-based method for decentralized train scheduling, *Proceedings of the Fifth International Conference on Autonomous Agents*, pp. 43–50, 2001.

[37] E. Petersen, Over-the-road transit time for a single track railway, *Transportation Science*, vol. 8(1), pp. 65–74, 1974.

[38] W. Rudderham, Longitudinal control system of the intermediate capacity transit system, *Proceedings of the Thirty-Third IEEE Vehicular Technology Conference*, pp. 183–190, 1983.

[39] W. Sutewong, Algorithms for Solving the Train Dispatching Problem for General Networks, Ph.D. Dissertation, Department of Industrial and Systems Engineering, University of Southern California, Los Angeles, California, 2006.

[40] H. Takeuchi, C. Goodman and S. Sone, Moving block signaling dynamics: Performance measures and re-starting queued electric trains, *IEE Proceedings on Electric Power Applications*, vol. 150(8), pp. 483–492, 2003.

[41] A. Tazoniero, R. Goncalves and F. Gomide, Decision making strategies for real-time train dispatch and control, in *Analysis and Design of Intelligent Systems Using Soft Computing Techniques*, P. Melin, O. Castillo, E. Gomez-Ramirez, J. Kacprzyk and W. Pedrycz (Eds.), Springer, Berlin-Heidelberg, pp. 195–204, 2007.

[42] J. Tornquist, Computer-based decision support for railway traffic scheduling and dispatching: A review of models, *Proceedings of the Fifth Workshop on Algorithmic Methods and Models for Optimization of Railways*, 2005.

[43] B. Vincze and G. Tarmai, Development and analysis of train brake curve calculation methods with complex simulation, *Proceedings of the Fifteenth International Exhibition of Electrical Equipment for Power Engineering, Electrical Engineering, Electronics, Energy and Resource-Saving Technologies and Household Electric Appliances*, 2006.

[44] J. Whittle, D. Wijeskera and M. Hartong, Executable misuse cases for modeling security concerns, *Proceedings of the Thirtieth International Conference on Software Engineering*, pp. 121–130, 2008.

[45] F. Yan and T. Tang, Formal modeling and verification of real-time concurrent systems, *Proceedings of the IEEE International Conference on Vehicular Electronics and Safety*, pp. 1–6, 2007.

[46] L. Zhang, P. Li, L. Jia and F. Yang, Study on the simulation for train operation adjustment under moving block, *Proceedings of the Eighth IEEE Conference on Intelligent Transportation Systems*, pp. 351–356, 2005.