② 列車運転支援情報伝送の妨害対策に関する検討

交通システム研究部　※林田 守正　工藤 希　竹内 俊裕　大野 寛之
東京大学　水間 毅

1．はじめに

無線通信を列車制御や運転支援に利用するシステムでは、情報伝送における妨害の対策に関する評価が必要である。そこで、ケーススタディとして、人為的又は偶発的な妨害への対策の評価方法について、国際規格との整合やセキュリティの観点を含めて検討するため、伝送システムのモデルを用いた走行実験を実施した。本報告では、その結果を述べる。

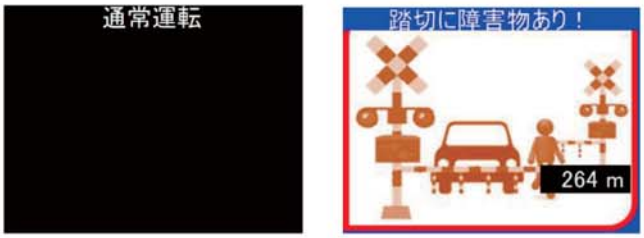
2．実験装置と実験方法

実験は、鉄道路線上での実列車による走行実験（以下、「実列車走行実験」という。」）及び当研究所構内での自動車による模擬的な走行実験（以下、「模擬走行実験」という。）を行った。

2．1．モデルとした伝送システム

図1にモデルとした伝送システム（先年度に当研究所が構築した「踏切事故防止支援システム[1)]」）の概念を示す。列車が接近中の踏切上又は近傍に自動車が位置する場合、自動車から列車に対し、各々に設置された無線通信装置（以下、「自動車側装置」及び「列車側装置」という。）を通じて「停滞無し」又は「停滞有り」の踏切情報が伝送される。列車側装置は受信した踏切情報を処理して、図2(a)(b) に示すような運転士支援画面上への表示（以下、「画面表示」という。）を行う。踏切情報が「停滞有り」で、列車と踏切の相対距離が一定値以下となった場合は、図2(b)の画面表示によって列車運転士に警告し、非常ブレーキ等の運転操作を支援するという機能を有する。

図1　モデルとした伝送システムの概念[1)]



(a)通常運転　　(b)踏切に障害物あり(警告)

図2　運転士支援画面表示

2．2．模擬的な伝送の妨害と対策の設定

本実験では、模擬的な伝送の妨害の要因として、「なりすまし」と「ノイズ」の2種類を想定した。

2．2．1．模擬的な「なりすまし」による妨害

模擬的な「なりすまし」による伝送妨害（以下、「なりすまし妨害」という。）の概要を図3に示す。　踏切に停滞があり、停滞自動車から列車に向けて正規の踏切情報（停滞有り）を送信中に、この情報を第三者が傍受し、偽の踏切情報（停滞無し）に改ざんしたうえで、列車側装置に送信するという想定である。その対策を図4に示す。踏切情報に32ビット CRC（Cyclic Redundancy Check、巡回冗長検査）コ

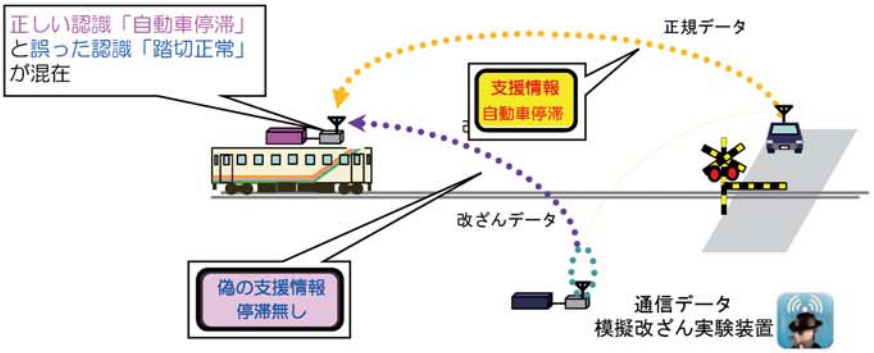


図3　模擬的な「なりすまし妨害」の概要

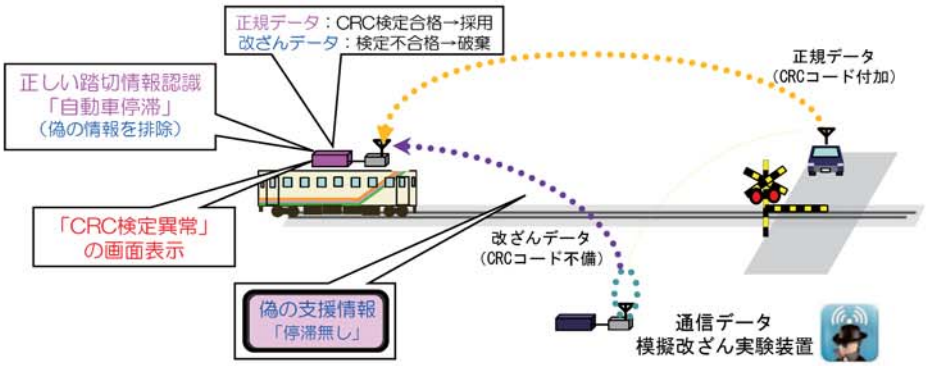


図 4　模擬的な「なりすまし妨害」の対策

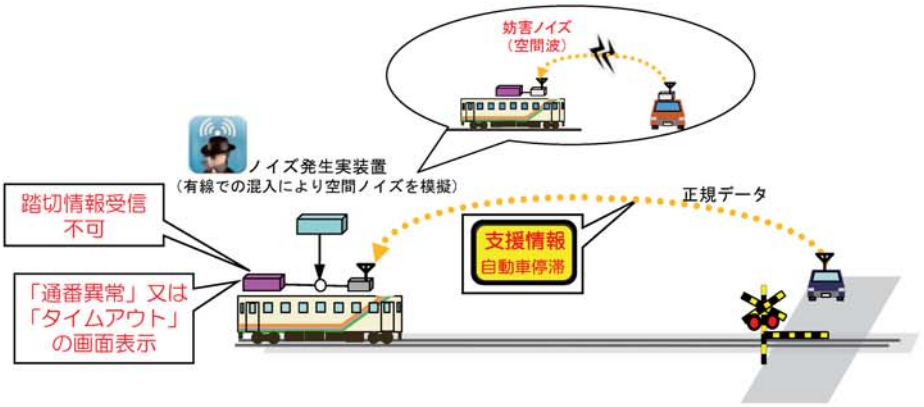


図 5　模擬的な「ノイズ妨害」の概要と対策

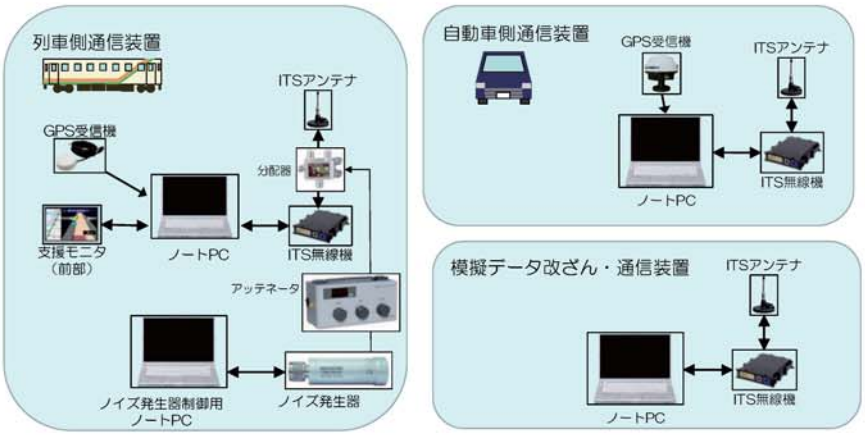


図 6　実験装置の構成

ードを追加し、列車側装置で受信時に検定を行うことにより、合格した正規データのみが採用され、CRC コードが不備な改ざんデータは破棄される。

2．2．2．模擬的なノイズによる妨害

模擬的なノイズによる伝送妨害（以下、「ノイズ妨害」という。）の概要を図 5 に示す。自動車側装置からの踏切情報の伝送が偶発的又は意図的なノイズにより妨害され、列車側装置での受信が途絶するという想定である。受信が途絶した場合、踏切情報に関わらず、画面表示は図 2 (a)となる。

2．3．実験装置

2.2.に前述した模擬的な伝送妨害による事象と対策効果を確認するための実験装置の構成を図 6 に示す。2.1.で前述した伝送システムを本実験向けに一部仕様変更したものである。妨害対策として、異常検知や画面表示に関する以下(1)～(4)の機能を追加した。それらの追加機能について図 4、図 5 及び表 1 に示す。

(1) データ受信中は「受信中」を図 2 (a)に併記する。
(2) 改ざんデータが CRC 検定で破棄された場合、これを検知し、図 2 (a) (b)に「CRC 検定異常」を併記する。

(3) データ内容に通番を追加し、受信データの通番が一定値以上飛躍した場合、これを検知し、「通番異常」を図 2 (a) (b)に併記する。
(4) 受信が一定時間以上途絶した場合、これを検知し、「タイムアウト」を図 2 (a) (b)に併記する。

表 1　追加した異常検知と画面表示併記の機能

	検知の指標	標準値	異常検知のしきい値	検知・画面表示（併記）のタイミング
CRC異常	CRC関数値（余り）	送信側と受信側の一致	送信側と受信側の不一致	送信側と受信側の不一致時点
通番異常	データ通番から次データ通番の増分	1	15番（3s相当）以上の飛躍	次データ受信（再開）時点
タイムアウト	前データ受信後、次データ受信までの経過時間	200ms	6s以上	前データ受信後、次データ未受信のまま6s経過時点

列車側装置、自動車側装置の他に、模擬データ改ざん装置を追加した。また列車側装置のアンテナと無線機本体の間に、想定する空間ノイズと等価なノイズ（無線通信と同じ周波数帯の正弦波）を模擬的に有線で印加する装置を挿入した。自動車側装置から停滞情報を受信中の列車が当該踏切手前の所定地点（以下、「警告地点」という。）を越えると、画面表示が図 2 (a)から(b)に遷移する仕様とした。

2．4．実験方法

2．4．1．実列車走行実験

実列車走行実験は、地方鉄道の営業路線において実施した。実験の状況を図 7 に示す。2.3.に前述した装置を実験用の列車及び自動車に設置し、実験走行区間内の踏切の近傍に自動車を駐車させて踏切内停滞を模擬し、また模擬データ改ざん装置を自動車の近くに配置したうえで、列車を踏切に向けて走行させた。なお、この実験における図 2 の支援画面の視認状況に基づいて、2.3.に前述した対策機能を追加することとし、2.4.2 に後述する模擬走行実験において確認した。

図 7　実列車走行実験の状況

2．4．2．模擬走行実験

模擬走行実験は、当研究所の構内において実施した。実験の状況を図 8 に示す。列車側装置及び自動車側装置の配置は実列車走行実験と同様としたが、列車は自動車で、停滞自動車は定置架台で、踏切は舗装路面上のマーキングでそれぞれ模擬した。模擬列車の走行は、実列車走行における距離と速度を縮尺し、2 種類のコース（「起点①→起点②→模擬踏切」及び「起点②→模擬踏切」）を設定した。

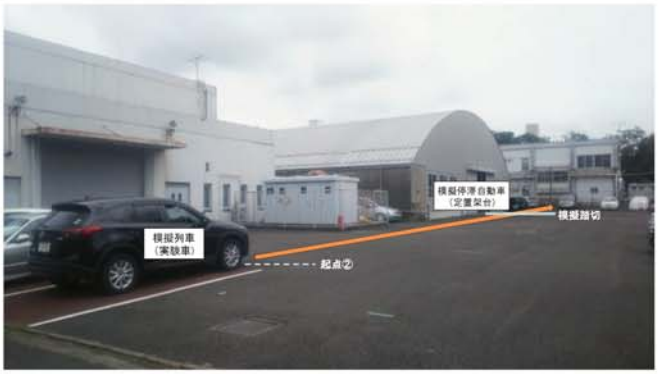


図 8　模擬走行実験の状況（起点②→模擬踏切）

3．実験結果

3．1．実列車走行実験について

3．1．1．なりすまし妨害

列車側装置が「停滞有り」の踏切情報を受信し、なりすまし妨害が無い場合の画面表示は、列車が警告地点以遠においては図 2 (a)であり、同地点を超えて接近すると図 2 (b)に遷移することを確認した。なりすまし妨害がある場合の画面表示は、警告地点を超えると図 2 (a)と(b)が交互に切り替わることを確認した。その対策として踏切情報に対し CRC 検定が行われた場合は、同時受信した正規データ（停滞有り）と改ざんデータ（停滞無し）のうち前者のみが採用されることにより、図 2 (b)の画面表示が継続することを確認した。

3．1．2．ノイズ妨害

列車側装置が「停滞有り」の踏切情報を受信し、列車が警告地点を越えて画面表示が図 2 (a)から(b)に遷移した時に、十分な強度のノイズを印加すると、受信が途絶し、画面表示が図 2(a)に戻ることを確認した。またノイズ印加を中止すると、直後に受信が再開され、画面表示が図 2 (b)に復帰することを確認した。

3．2．模擬走行実験について

3．2．1．妨害無し

踏切情報が「停滞無し」の場合、模擬列車の進行に伴い、画面表示は図 2 (a)から「図 2 (a)＋『通信中』」に遷移して、そのまま模擬踏切に達することを確認した。踏切情報が「停滞有り」の場合、画面表示は図 2 (a)→「図 2 (a)＋『通信中』」→図 2 (b)と遷移することを確認した。

３．２．２．なりすまし妨害

3.1.1.に前述した実列車走行実験結果と同様の結果を得た。また追加対策の検証として、改ざんデータがCRC 検定により破棄された時に、図 2 (a) (b)の画面表示に「CRC 異常」が併記されることを確認した。

３．２．３．ノイズ妨害

3.1.2.に前述した実列車走行実験結果と同様の結果を得た。また追加対策の検証として、表 1 に示す受信途絶に関する異常検知機能により、「通番異常」又は「タイムアウト」が、図 2 (a) (b)の画面表示に併記されることを確認した。

４．考察と今後の方向性

４．１．妨害への対策の効果について

４．１．１．「通信中」の併記

「通信中」の図 2 (a)（通常運転）への併記については、自動車停滞の有無に関わらず、踏切情報が不達であるか、又は「停滞無し」の情報を受信中かを容易に判別できることが検証された。したがって、踏切情報が不達の場合に「通信中」が併記されない仕様は、画面表示が図 2 (a)でも「停滞有り」の可能性を意識させる効果があると考える。

４．１．２．なりすまし妨害対策

CRC については、CRC コードも同時に改ざんされない限り有効であることが検証された。「CRC 検定異常」の併記については、妨害の存在を視認できることが検証され、画面表示の真偽に注意を喚起する効果があると考える。なお本実験装置の試行的な仕様では、CRC 検定無しで改ざんデータを受信した場合、3.1.1.に前述した画面表示（図 2 (a) (b)の交互表示）となるが、図 2 (a)が継続するケースについても検討したい。

４．１．３．ノイズ妨害対策

「通番異常」及び「タイムアウト」の図 2 (a) (b)への併記については、一時的な受信の途絶を容易に視認できることが検証された。したがって、前述の「通信中」の併記と併せて、「停滞有り」情報の見逃しや受信遅れに関する注意を喚起する効果が期待できる。特に図 2 (b)の画面が(a)に遷移した時に「通信中」が併記されない場合、伝送妨害の存在を推定できると考えられる。これらの併記は、実際の運転士支援に向けては、シンボルマーク化等を検討する必要があると考える。また、検知機能の表示以外への応用も検討したい。

４．２．国際規格及びセキュリティとの関連について

鉄道の安全関連の通信に関する国際規格である IEC 62280 に記述される「伝送システムに対する 7 つの脅威と防護」[2] と、本実験での「妨害と対策」との関連を表 2 に示す。本実験の「なりすまし妨害」及び「ノイズ妨害」は、IEC 62280 の「なりすまし」及び「削除」に該当すると考える。「なりすまし」はセキュリティに関わる人為的な脅威であり、IEC 62280 では「暗号化技術」等の対策が有効とされている。本実験では、「なりすまし」に有効とはされていないものの、2.2.1.に前述したように、「安全符号」（CRC はその 1 種）を試用した。今後は、暗号化技術等が採用された場合の評価についても検討する予定である。「削除」に関しては、IEC 62280 では「通番」が有効な対策とされ、本実験でも採用した。「タイムアウト」は、IEC 62280 では「削除」の有効な対策とされていないが、本実験では採用した。これは、IEC 62280 では「遅延」（過負荷起因に限定）の有効な対策とされ、一方、本実験では「ノイズ妨害」による通信途絶は「遅延」の一種であると解釈したためである。

表 2　伝送システムに対する脅威と防護対策[2]

IEC 62280で定義される7つの脅威	IEC 62280に記述される防護対策（○：有効　△：条件付で有効）							
	通番	タイムスタンプ	タイムアウト	送信元/受信先ID	フィードバックメッセージ	同一証明手順	安全符号	暗号化技術
繰り返し	○	○						
削除（本実験：ノイズ妨害）	○（採用）		（採用）					
挿入	○			△	△	△		
再順序	○	○						
劣化							○	○
遅延（過負荷起因）		○	○					
なりすまし（本実験：なりすまし妨害）					△	△	（採用）	○

５．まとめ

列車制御や運転支援に利用される無線通信に対する妨害と対策に関し、既存の伝送システムをモデルとした実験的なケーススタディにより検討し、国際規格やセキュリティとの関連を含めて考察した。さらに、IEC 62280 に挙げられている他の 5 つの脅威への対策について検討する等、情報伝送システムの妨害対策に関する評価法の確立に向けて取り組んでいきたい。

参考文献

1) 竹内俊裕ほか，“通信技術等を活用した鉄軌道・道路交通間における安全性向上に関する取組”，交通安全環境研究所フォーラム 2016 講演概要集，pp.61-64（2016）

2) IEC 62280 Edition 1.0 2014-02