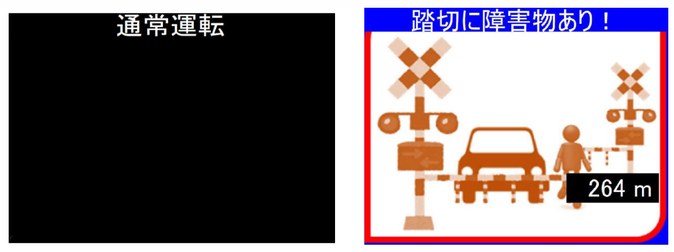
② 列車運転支援情報伝送の妨害対策に関する検討

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

○概　要

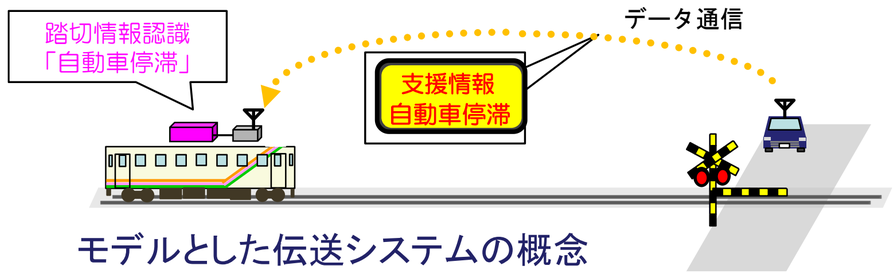
・無線通信を列車制御や運転支援に利用するシステムでは、情報伝送妨害の対策に関する評価が必要。
・人為的、偶発的な妨害への対策の評価方法検討のため、伝送システムモデルによるケーススタディを実施。
・鉄道路線上での実列車走行実験及び当研究所構内での自動車による模擬走行実験により事象再現と検証。
・さらに情報伝送システムの妨害対策に関する評価手法の確立に向けて取り組んでいく予定。



通常運転　踏切に障害物あり
運転士支援画面

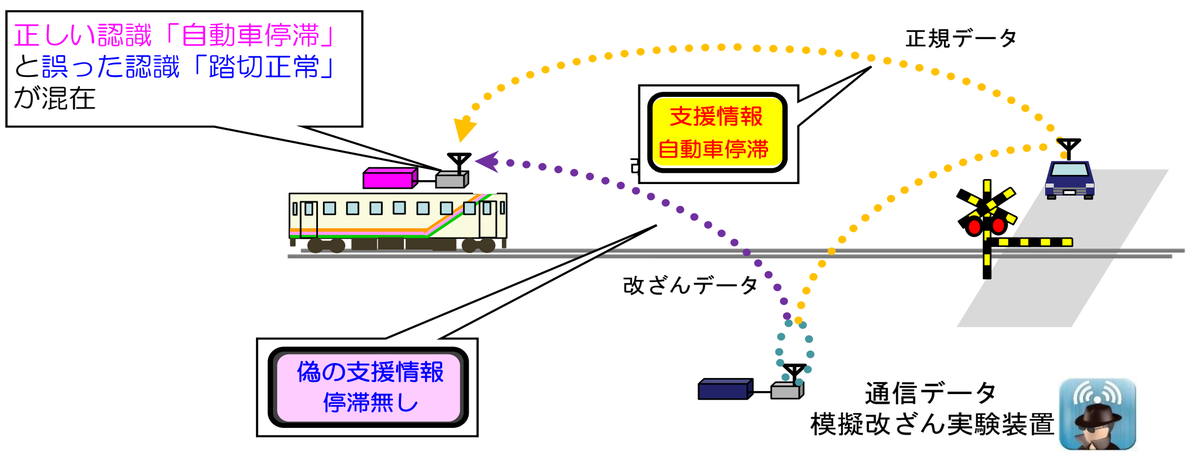
○モデルとした伝送システム

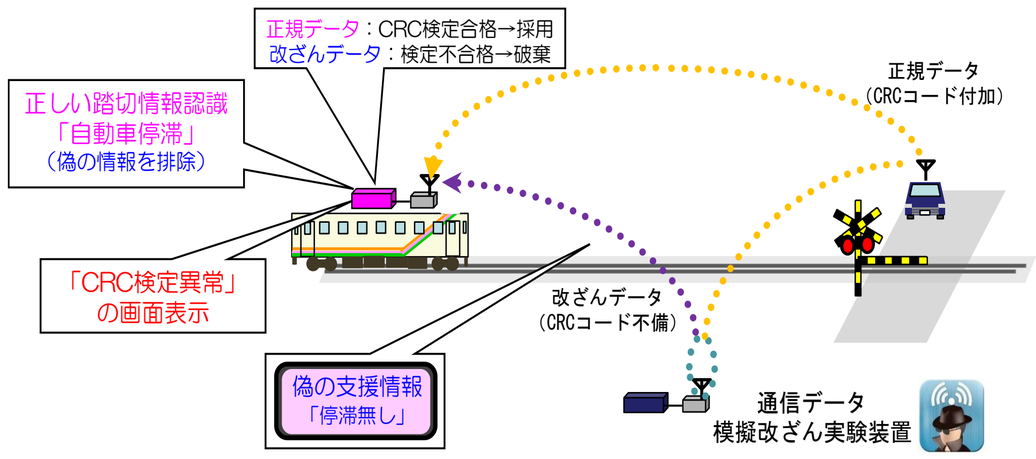
・ケーススタディ対象は当研究所が構築した踏切事故防止支援システム(実機)。
・踏切近傍の自動車から接近中の列車に「踏切情報」を送信し運転台に支援画面表示。
・自動車が踏切に停滞の場合は列車側で警告画面を表示し非常ブレーキ操作等を支援。



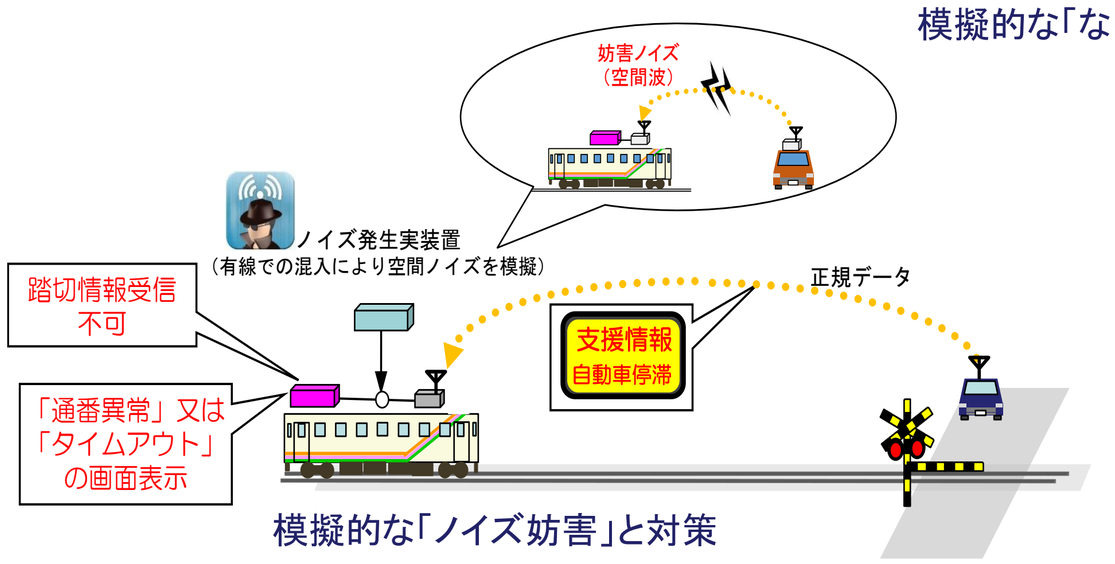
モデルとした伝送システムの概念

○模擬的な伝送の妨害と対策の設定





模擬的な「なりすまし妨害」と対策



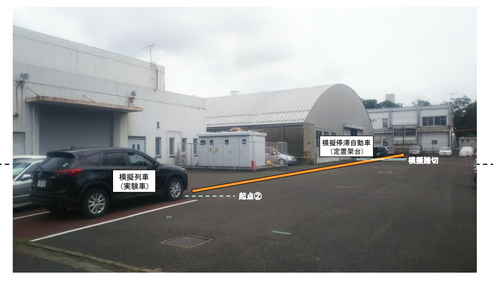
模擬的な「ノイズ妨害」と対策

伝送妨害の検知と支援画面上への文字列併記

	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

○走行実験での確認結果 (「停滞有り」の情報受信時)


実列車走行実験



模擬走行実験

①実列車走行実験
(1)妨害無し
・警告地点以遠では「通常運転」→警告地点を越えると「踏切に障害物あり」に遷移。
(2)なりすまし妨害
・CRC検定無し:警告地点を越えると「踏切に障害物あり」(真)と「通常運転」(偽) が交互表示。
・CRC検定有り:改ざんデータは破棄され、警告地点を越えると「踏切に障害物あり」が継続。
(3)ノイズ妨害
・「踏切に障害物あり」→ノイズ印加→受信が途絶し「通常運転」に遷移→ノイズ印加中止→受信再開→「踏切に障害物あり」に復帰。

②模擬走行実験(文字列併記機能追加)
(1)妨害無し
・踏切情報が「停滞無し」:「通常運転」→「通常運転＋通信中」に遷移→模擬列車が模擬踏切に到達。
・踏切情報が「停滞有り」:「通常運転」→「通常運転＋通信中」→「踏切に障害物あり」に遷移。
(2)なりすまし妨害
・CRC検定有り:改ざんデータの破棄時に「通常運転」又は「踏切に障害物あり」に「CRC異常」併記。
(3)ノイズ妨害
・受信途絶検知により「通常運転」又は「踏切に障害物あり」に「通番異常」又は「タイムアウト」併記。

運転士支援画面への文字列併記例

○国際規格及びセキュリティとの関連

・「なりすまし」はセキュリティに関わる人為的脅威であり、IEC 62280では「暗号化技術」等が有効とされているが、本実験では「安全符号」(CRCはその1種)を試用。
・「削除」に関しては、IEC 62280では「通番」が有効とされ、本実験でも試用。
・「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、本実験では試用。
※「タイムアウト」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。

伝送システムに対する脅威と防護対策

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	ﾀｲﾑｽﾀﾝﾌﾟ	ﾀｲﾑｱｳﾄ	送信元/受信先ID	ﾌｨｰﾄﾞﾊﾞｯｸﾒｯｾｰｼﾞ	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)	○