自動車向けIDS技術に関する研究
Research on intrusion detection system for Vehicle Security Techniques

松下綾香・ネットワーク分科会・情報セキュリティ大学院大学

Abstract The purpose of this paper is to identify the factors that cause the characteristics of voltage waveforms of ECUs in automotive networks, and to discuss the challenge of using voltage waveforms. In order to identify these factors, we categorize the data that can be detected by IDS. Based on these data, we focus on IDS using voltage waveforms of CAN messages sent from ECUs. Then, we clarify the characteristics of several modules used in the evaluation environment system and analyze the factors that cause differences in the voltage waveforms used by the detection techniques. Based on the results of this analysis, we will discuss the technologies that can be used in the detection method to identify the source ECU.

研究の目的

車載ネットワークに存在するECUの電圧波形を用いて，電圧波形の特徴が生じる因子を特定するし自動車向けIDS技術を提案することを目的とし，不正ECUや不正機器が車載ネットワークに接続された際や，攻撃CANメッセージを検知するIDSの既存セキュリティ対策技術をまとめる．自動車向けIDS技術の一つである電圧波形を用いた検知方法に着目し，汎用モジュールを用いて一部実験を行った．実験の分析結果から送信元ECUを特定する検知手法に活用可能な技術を考察する．

自動車向けIDS技術の分類

不正CANメッセージを検出する際には，CANメッセージの周期やデータに基づいた検知方法が提案され，自動車内に不正ECUや不正機器が接続されたことを検知する際には，電圧波形の特徴に基づいた車載IDSが提案されていた．

検知対象	目的
論理層	不正なCANメッセージを検知
物理層	送信元ECUを識別

自動車向けIDS技術の課題

課題①：CANメッセージの送信元を特定できない
課題②：なりすましCANメッセージの検知が困難
課題③：DoS攻撃やバスオフ攻撃を受けた際に，通信が阻害されて検知できない

汎用モジュールを用いた実験

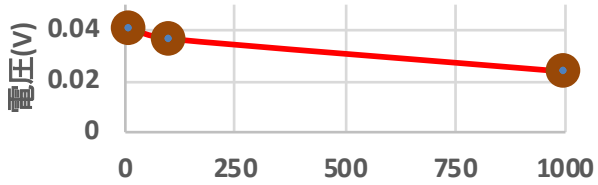
実験：CAN通信を行うためのモジュールが波形に与える影響

汎用モジュールを用い，CANメッセージの電圧波形を観測し比較した．

	測定位置	立ち上がり時間と立ち下がり時間の差(ns)
WB ECU	送信側	23.2
	受信側	46.4
Raspberry Pi+PiCAN2	送信側	144.93
	受信側	138.332
Arduino +CAN Bus Shield	送信側	52.17
	受信側	64.97
Arduino + PiCAN2	送信側	162.33
	受信側	168.13

実験：CAN線の線長が波形に与える影響

Raspberry Piのモジュールを２台用意し，間のCAN線の線長を，10cm，100cm，1000cmと変化させた際に電圧波形に与える影響の観測した．CAN線の線長が長くなればなるほど，送信元の電圧と比べ，受信側では電圧平均の差がが減少していた．



実験の考察

- CANコントローラ・CANトランシーバ以外が，電圧波形に影響を与えている
- 基盤の回路が異なるものを用いれば，電圧波形での識別が容易となる可能性がある
- 攻撃用モジュールとして用いられる汎用モジュールの識別ができる可能性がある
- CANメッセージの電圧波形において，立ち上がり後の電圧値を用いることにより、送信元ECUとの距離が認識できる可能性がある

まとめ

車載IDSの研究は盛んに行われており，不正CANメッセージを検出する際には，CANメッセージの周期やデータに基づいた検知方法が提案され，自動車内に不正ECUや不正機器が接続されたことを検知する際には，電圧波形の特徴に基づいた車載IDSが提案されていた．実験の結果から，CAN線の線長により電圧波形に違いが生じることと，CANコントローラ・CANトランシーバ以外が、電圧波形に影響を与えていることが明らかになった．

今後の課題

- 自動車ECUにおいても特定した電圧波形の特徴が現れるかの確認
- 周期性のないCANメッセージの送信元ECUの検知方法の検討
- 電圧波形を用いた車載IDSの実装