DoS 攻撃の無効化に向けた車載ネットワークにおける回避攻撃と防御戦略に関する研究

氏　　名　大平　修慈

研 究 室 名　情報基盤システム学研究室

主指導教員名　藤川　和利

内 容 梗 概（1ページ目に収めること）

コネクテッドカーの普及に伴い，CAN(Controller Area Network)に対するサイバー攻撃が深刻な問題となっている．CAN には，DoS(Denial-of-Service)攻撃や送信者の特定ができない等の脆弱性が指摘されており，これらの脆弱性への対策が研究されている．既存研究として，CAN 上の侵入検知システム(IDS)と認証機構が提案されている．しかし，IDS は Spoofing 攻撃，Replay 攻撃，DoS 攻撃に対し高い検知性能を持つが，これらの攻撃に対する防御は提供しない．また，DoS 攻撃を検知する IDS は，最高優先度のメッセージでの DoS 攻撃等の単純な条件下でのみ有効である可能性がある．つまり，攻撃者は IDS が使用する特徴量を偽装することで，IDS を回避する恐れがある．一方，認証機構は，Spoofing 攻撃や Replay 攻撃に対する防御に重点を置いている．つまり，既存の IDS や認証機構では，CAN に対する DoS 攻撃を無効化することはできない．そこで，本論文では，CAN 上の DoS 攻撃を無効化するために，DoS 攻撃を攻撃と防御の 2 つの側面から分析を行う．

本論文の主な貢献は，新たな回避攻撃を明らかにすること，および，回避攻撃を含む DoS 攻撃を無効化するための 3 つの防御戦略（検知，識別，防御）を提案することである．まず，CAN における Entropy ベースの IDS では検知できない Entropy 操作攻撃という新たな回避攻撃を発見した．この IDS に対する回避攻撃に対処するため，我々の類似度ベースの IDS は，Sliding Window に最適化された類似度を用いて，回避攻撃を含む DoS 攻撃の検知を行う．次に，攻撃者の制御下にある ECU を特定するために，CAN の物理層特性に基づく送信者識別手法(Physical-Layer Identification: PLI)を提案する．IDS や PLI は，DoS 攻撃を検知し，DoS 攻撃を行う ECU を特定することができるが，IDS や PLI では DoS 攻撃を防御することができない．そこで最後に，CAN ドライバ上で防御機能を提供する IVNProtect を提案する．CAN のプロトタイプと実車において，3 つの防御戦略を評価したところ，各防御戦略が各環境において攻撃にうまく対処できることを示した．