論 文 内 容 の 要 旨

博士論文題目　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

（論文内容の要旨）

コネクテッドカーの普及に伴い、Controller Area Network (CAN)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、Denial-of-Service (DoS)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、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。

氏　名	大平 修慈

（論文審査結果の要旨）

インターネットに繋がる自動車が普及し、車載ネットワークに対するサイバー攻撃の脅威が懸念されている。車載ネットワークの事実上の標準規格である Controller Area Network (CAN)は、電子制御ユニット(Electronic Control Unit: ECU)間の通信に用いられている。また、CAN はメッセージの送信 ECU の特定ができないことや Denial-of-Service (DoS)攻撃に脆弱であることが指摘されている。こうした脆弱性に対し、これまで CAN において侵入検知システム(Intrusion Detection System: IDS)や認証機構が提案されてきた。しかしながら、IDS は高い検知性能を持つが、攻撃に対する防御は提供しない。加えて、認証機構が実装された CAN においても DoS 攻撃によって帯域を占有可能であるため、既存の対策では DoS 攻撃を無効化できない。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 つの側面からの提案を行なっている。

具体的には、既存の最先端の DoS 攻撃検知手法に対する回避攻撃と 3 つの手法からなる防御戦略を提案している。提案した回避攻撃は、既存の Entropy ベースの IDS で用いられる Entropy の値を操作し IDS の検知を回避しながら DoS 攻撃を行う。このような新たな DoS 攻撃を検出するために、スライディングウィンドウに基づく類似度ベースの IDS とそのパラメータを最適化するアルゴリズムを提案している。

類似度ベースの IDS は、DoS 攻撃を検知することは可能であるが、どの ECU が DoS 攻撃を実行しているか識別することはできない。この問題に対し、CAN の物理層特性に基づく識別手法(Physical-Layer Identification: PLI)を提案している。また、IDS や PLI は DoS 攻撃を検知し、DoS 攻撃を行う ECU を識別可能だが、DoS 攻撃を防御することはできない。そこで、IVNPROTECT と呼ばれる CAN ドライバ上で DoS 攻撃に対する防御機能を提供する手法を提案している。

これらの防御に関する提案手法は、既存研究と比較して、検知・識別・防御性能を向上できている。また、既存の車両にも導入することが可能であり、車載ネットワークにおける DoS 攻撃に対する防御戦略をある程度確立できたと言える。

本論文は、車載ネットワークにおける新たな DoS 攻撃とその防御戦略の提案、ならびに、その有効性を客観的に評価していることから、一定の学術的意義があるものと評価できる。よって、論文は、博士(工学)の価値があるものと認める。