5ZA-04

CAN-Ethernet 変換 Switch における不正アクセスの検証

田付 洋大† 布田 裕一† 鈴木 智道‡ 田中 覚・

東京工科大学コンピュータサイエンス学部† 株式会社 PitApp ‡ 東京都立産業技術高等専門学校・

1. はじめに

近年、自動運転車やコネクテッドカーの開発によって、国際標準である CAN では通信速度が不十分なため、CAN に変わる車載ネットワークが必要である。そこで注目されたのが Ethernet である。しかし、安全面と導入コストの影響があるので、段階的な移行となる。すなわち、CAN と Ethernet の異なる車載ネットワーク間のデータ中継を可能する Gateway が必要となる。そこで、開発されたのが CAN-Ethernet 変換 Switch である。

現在、CAN のセキュリティ対策に関しての問題が指摘されており、Liu[1]らは、CAN プロトコルがもつ脆弱性について、分析した結果、ブロードキャスト、無認証、平文通り、ID ベースの優先度の 4 つに分類された。また、自動運転車やコネクテッドカーはクラウドの利用が予想され、外部のインターネットを利用して、車載 Ethernet との接続を持ち、車載 Ethernet は CAN-Ethernet の変換 Switch を経由して、CAN に接続される。すなわち、ECU は物理的なアクセスを除くと、外部ネットワークからの接続を試みる場合、必ず CAN-Ethernet 変換 Switch を経由する。つまり、攻撃者は外部からのネットワークから攻撃する場合、CAN-Ethernet 変換 Switch を経由して、CAN に侵入し ECU を不正制御する脅威が考えられる。そこで、本研究では CAN-Ethernet 変換 Switch における外部ネットワークからの不正アクセス検証システムついて提案する。

Detection of unauthorized access for CAN-Ethernet conversion
†Youta Tatsuke, Yuichi Futa, Tokyo University of Technology
‡Tomomichi Suzuki, PitApp Inc
・Satoru Tanaka, Tokyo Metropolitan College of Industrial

2. 提案システム

現在、CAN-Ethernet の変換 Switch において、CAN 側からのセキュリティ対策が行われている。しかし、Ethernet 側のセキュリティ対策が行われていない。そこで、本研究では Ethernet から CAN-Ethernet 変換 Switch を経由し CAN に向けてパケットを流した時に、フィルタリングを行い外部から不正アクセスを防ぐシステムを提案し、図 1 のようなシステムを構成する。

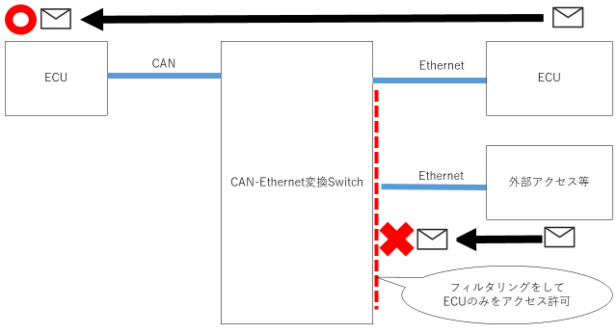

図 1：提案システム

提案システムについて詳細を述べる。Ethernet 側の ECU から CAN-Ethernet 変換 Switch を経由して CAN 側 ECU に向けて、パケットを流す。これを正規パケットとする。また、外部アクセスからのパケットも同じように変換 Switch を経由して、CAN 側にある ECU 向けて、パケットを流す。これを攻撃パケットとする。攻撃パケットを遮断するために、Ethernet 側の ECU と Ethernet-CAN 変換 Switch の間にフィルタを形成する。このフィルタは正規パケットと攻撃パケットを IP アドレスで振り分けて、正規パケットのみのアクセスを許可する。

3.検証システム

本研究では、図 2 のような検証システムを構成する。

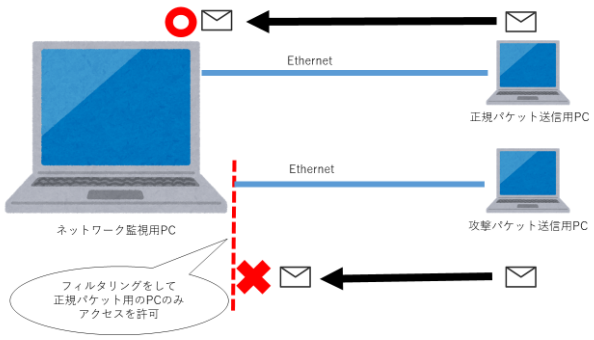

図 2：検証システム

前項の本研究の提案システムにおいて、Ethernet-CAN 変換 Switch を攻撃パケットから保護するために有効であり、また、リアルタイム性があるため、実車のシステムに対しても有効であり、実用性があると考えられる。

しかし、Ethernet-CAN 変換 Switch では、フィルタリングを行った際に、フィルタリングの影響によって生じるパケットの遅延とロストパケットの 2 点について問題が起こると考えられる。本研究では Ethernet と Ethernet-CAN 変換 Switch の間にフィルタリングを実装し、フィルタを使用時と未使用時のバッファから溢れた Ethernet のパケット数とその際に生じた遅延時間についての計測結果について比較し、検証する。

そこで、図 2 のような検証システムを提案する。正規パケット送信用 PC と攻撃パケット送信用 PC からネットワーク監視用 PC に向けて、同時にパケットを流す。その際に、正規パケット送信用 PC、攻撃パケット送信用 PC とネットワーク監視用の PC の間にフィルタリングを形成する。正規パケット送信用 PC から送られてきたパケットのみをアクセス許可し、攻撃パケット送信用 PC から送られてきたパケットはアクセスを拒否して、遮断する。この時、フィルタリング使用時と未使用時のロストパケットの数と遅延時間について計測し、評価を行う。

4.評価結果と考察

実装した検証システムに対して、評価実験を行った。評価方法としてはフィルタリングを未使用時と使用時の遅延時間とロストパケットの数について、それぞれ 10 回計測をおこなった。また、ネットワーク監視用 PC に向けて、パケットを 1 回につき約 3000 個を流した。

計測した結果、10 回の平均値でフィルタリング未使用時と使用時の計測時間は約 0.755 秒の遅延、ロストパケットの数は 0.5 個の差があった。ロストパケットの数については、フィルタリングを行った影響ではなく、使用したプログラム、もしくは仮想マシン、仮想環境の影響が高いと考えられる。一方、計測時間については、フィルタリングを使用した影響であると考えられる。しかし、約 0.775 秒の遅延時間は極めて小さい。なぜなら、CAN の通信速度を超える Ethernet パケットを CAN 側に飛ばすことはあり得ない。よって最大伝送速度 125Kbps の低速 CAN に Ethernet パケットを送り付けても、約 0.775 秒の遅延時間は極めて小さい。したがって、Ethernet-CAN 変換スイッチにおいて外部からの不正アクセス、またはなりすまし ECU に関しても、現実の車載ネットワークにおいて、実用的であることを示した。

5.謝辞

本研究の一部は，JSPS 科研費 JP17K00182 の助成を受けたものです。

参考文献

[1] Jiajia Liu ； Shubin Zhang ； Wen Sun ； Yongpeng Shi, “ In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions,” IEEE Network, 2017.