SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

車載 Ethernet 環境におけるフロープローブの性能評価
Performance Evaluation of Flow Probe in Automotive Ethernet

加賀 有貴 * 岸川 剛 * 安達 貴洋 * 平野 亮 *
Tomoki Kaga Takeshi Kishikawa Takahiro Adachi Ryo Hirano

氏家 良浩 * 芳賀 智之 * 松島 秀樹 *
Yoshihiro Ujiie Tomoyuki Haga Hideki Matsushima

キーワード 車載 Ethernet, IDS, フローベース IDS

あらまし

次世代車載ネットワーク技術として Ethernet の導入が進みつつある．従来の車載ネットワークの CAN（Controller Area Network）ではセキュリティの問題が指摘されていたが，車載 Ethernet も同様のリスクが存在する可能性がある．実際の車両の Ethernet に対する攻撃事例はまだ少ないが，車両制御につながる例も報告されている[1]．また ECU（Electronic Controller Unit）の仮想化･統合化によりシステムが複雑になるとともに，コネクテッド化のため外部インターフェイスが増加することから，車載ネットワークへの侵入リスクが高まることが考えられる．そのため車載 Ethernet のセキュリティ確保は重要な課題である．

車載ネットワークセキュリティには，暗号化や認証による通信路の保護と侵入検知技術がある．車載 Ethernet では，従来の IT 分野のセキュリティ技術である IPsec や MACsec を適用できるため，通信路の保護が可能である．対して侵入検知技術は，CAN 向けのものは検討が盛んに行われてきたが，車載 Ethernet 向けのものは CAN と比べるとまだ少ない．車載 Ethernet では，サービス指向通信プロトコルや暗号通信が適用されるなど，CAN とは通信内容が大きく変わることから，CAN 向けの侵入検知技術をそのまま車載 Ethernet に適用することが困難である．また車載 Ethernet を監視するためには，大容量かつ高速な通信に対応可能な軽量な攻撃検知技術が求められる．

そこで我々は，軽量な侵入検知技術として，フローベースの侵入検知技術を車載 Ethernet に適用することに着目している[2]．フローとはあらかじめ定義された属性の組により通信パケットを分類し，分類したパケットごとに所定期間の統計情報を収集したものである．フローベースの侵入検知では，収集したフロー情報を基に異常検知を行う．パケットの受信タイミングにおいては，フロー情報の分類と統計情報の更新の処理のみを行うため，軽量に動作することが期待される．

本稿では車載 Ethernet Switch 上でフロー情報を収集する想定で，フロー情報収集モジュール（フロープローブ）の実現性を評価する．具体的には，パケット分類から統計情報の更新にかかる処理時間やスループット，フロー情報を車載ネットワーク上で転送する際のデータ量の評価などを行う．これにより車載 Ethernet のフロー情報を，少ないオーバーヘッドで収集・監視できることを示す．

参考文献

[1] S. Nie, et al.: “Free-fall: Hacking Tesla from Wireless to CAN bus”, Black Hat USA 25 (2017).

[2] 岸川他 : “車載 Ethernet 向けフローベース IDS の提案 : SOME/IP への攻撃例に対するフロー分析”, 暗号と情報セキュリティシンポジウム（2021）.

* パナソニック株式会社, 〒571-8501, 大阪府門真市大字門真 1006 番地, Panasonic Corporation, 1006, Oaza Kadoma, Kadoma City, Osaka, 571-8501, Japan