講演番号：40

VANET における不正侵入検知システムの学習モデル統合手法

A Learning Model Integration Method of Intrusion Detection Systems for VANET

黄　崇裕 † 小野　翔多 †† 三好　匠 †,†† 山崎　託 †
Takahiro KOU Shota ONO Takumi MIYOSHI Taku YAMAZAKI

† 芝浦工業大学システム理工学部
College of Systems Engineering and Science
Shibaura Institute of Technology

†† 東京大学生産技術研究所
Institute of Industrial Science
The University of Tokyo

1. まえがき

急速に発展する自動運転技術において，車車間・路車間通信を実現する車両アドホックネットワーク（VANET: Vehicular ad-hoc network）は不可欠な技術である．脆弱性への対策として不正侵入検知システム（IDS: Intrusion detection systems）による手法が検討されているが，実際の車両上で収集されるデータは限定的で偏りがあり，1 台の車両だけでは多様な攻撃に対応できる IDS の構築は困難である．本稿では，VANET における IDS の学習モデル統合手法を提案する．

2. 関連研究

文献 [1] では，VANET におけるトラヒック予測のためのアンサンブル学習モデルが提案されている．本手法では，同一データを学習させたベースモデルのうち，高性能なモデルをスタッキングで統合して予測モデルを構築する．本手法の予測精度は 94.1% と高いが，統合するベースモデルの選別はデータに依存するため，メタモデルの汎用性の低さが懸念される．

文献 [2] では，VANET における連合学習を用いた侵入検知手法が提案されている．本手法では，異なるデータで学習した 1 次元畳み込みニューラルネットワーク（1D-CNN）モデルを加重平均により統合する．その結果，複数種類の攻撃推定において 98.1% の精度が得られている．しかし，全ての学習データには同じ種類の攻撃データが含まれており，車両ごとの収集データの偏りは考慮されていない．

3. 提案手法

本稿では，VANET における IDS の学習モデル統合手法を提案する．本手法では，各車両上で収集されたデータを用いてモデルの学習を行い，それらのモデルをスタッキングを用いて統合することで，各モデルの識別性能を保ちつつ，より汎用性の高い IDS の構築を実現する．

本手法の手順を図 1 に示す．まず，各車両上で攻撃を含む通信データを収集し，IDS を用いてラベリングする．車両上の IDS をラベリングデータで自己学習させた後，サーバに送信する．次に，サーバ上でスタッキングを用いてモデルを統合する．各車両から受信した IDS をベースモデルとして，全ての攻撃データを含むデータに対する予測を行う．そして，全ての予測値を特徴量としてメタモデルの学習を行う．上記の手順で統合されたモデルを IDS として各車両に分配する．

4. 評価

攻撃データの種類に偏りがあるデータで学習したベースモデルの統合の有効性を検証した．本実験では，DoS 攻撃（D），ファジー攻撃（F），誤作動攻撃（M），リプレイ攻撃（R），及び正常通信（N）により構成される VANET データ [3] を使用し，異なる攻撃データを学習させた 4 つのベースモデルを統合した 2 種類のメタモデル $\mathscr{M}_{\text{D\_F\_M\_R}}$, $\mathscr{M}_{\text{D\_FM\_R\_R}}$ により検証を行う．なお，モデル表記の添字は各ベースモデルに学習させた攻撃の種類を示し，モデルには 1D-CNN を用いた．

2 種類のモデルで上記 5 種類の通信データの分類を行った結果を表 1 に，混同行列を図 2 に示す．表 1 より，提案手法は約 92% の精度で攻撃を分類可能であることから，多様な攻撃を検出できていると言える．また，2 つのモデルの性能に差がないことから，データの偏り方によらずモデル統合が有効に動作していると考えられる．一方，図 2 より誤作動攻撃がファジー攻撃に，リプレイ攻撃が正常通信に誤分類されている．要因として，互いの通信特性が類似しており，学習に使用した特徴量では不十分であることが考えられる．

5. むすび

本稿では，VANET における IDS の学習モデル統合手法を提案した．今後は，更なる精度向上のほか，複数種類の攻撃データを学習させたベースモデルの統合や他の機械学習モデルを使用した際の精度検証をする予定である．

謝辞 本研究成果は，国立研究開発法人情報通信研究機構（NICT）の委託研究（JPJ012368C05201）により得られた．

文献

[1] P.A.D. Amiri and S. Pierre, “An ensemble-based machine learning model for forecasting network traffic in VANET,” *IEEE Access*, vol. 11, pp. 22855–22870, March 2023.

[2] M. Arya et al., “Intruder detection in VANET data streams using federated learning for smart city environments,” *Electronics*, vol. 12, no. 4: 894, 13 pages, Feb. 2023.

[3] S. Rajapaksha et al., “AI-based intrusion detection systems for in-vehicle networks: a survey,” *ACM Comput. Surv.*, vol. 55, no. 11: 237, 40 pages, Feb. 2023.

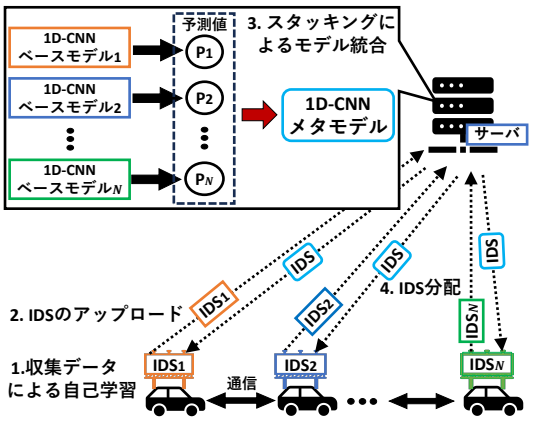
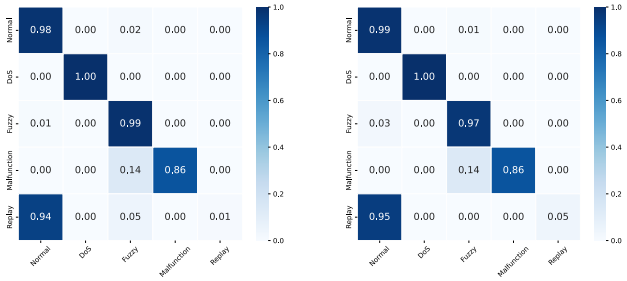


図 1　提案手法の手順

表 1　2 種類のメタモデルによる識別結果

モデル	精度	適合率	再現率	F 値
$\mathscr{M}_{\text{D\_F\_M\_R}}$	0.922	0.833	0.768	0.750
$\mathscr{M}_{\text{D\_FM\_R\_R}}$	0.926	0.847	0.772	0.771



(a) $\mathscr{M}_{\text{D\_F\_M\_R}}$　(b) $\mathscr{M}_{\text{D\_FM\_R\_R}}$

図 2　各攻撃に対する混同行列