Clock-based Intrusion Detection System の評価

塚本　博之[†1]　櫻澤　聡[†1]　濱田　芳博[†1]　吉田 圭吾[†1]　足立　直樹[†2]
石川 史也[†2]　上口 翔悟[†2]　上田　浩史[†2]　宮下 之宏[†2]　畑　洋一[†1]

概要：コネクティッドカーや自動運転車両の実現に向け，サイバー攻撃対策は重要な課題である．侵入検知は車両がサイバー攻撃を受けたことを検知する技術であり，この検知結果に基づきサイバー攻撃への具体的な対策を開始する．この様な技術の１つとしてFingerprint技術がある．これは，車載ネットワークにおいてメッセージを送信したElectric Control Unit(ECU) を特定し，期待する送信元ECUでない場合に攻撃メッセージとして識別する技術である．本論文では，ソフトウェアベースのFingerprint技術として知られるClock based Intrusion Detection Systems (CIDS) について評価を行い，この技術の脆弱性として知られるClock Phishingやその他の問題点の改善方法について検討を行う．

キーワード：Fingerprint，侵入検知，車載ネットワーク，周期メッセージ，CAN

Evaluation of the Clock-based Intrusion Detection System

Hiroyuki Tsukamoto[†1]　Satoru Sakurazawa[†1]　Yoshihiro Hamada[†1]　Keigo Yoshida[†1]
Naoki Adachi[†2]　Fumiya Ishikawa[†2] Shogo Kamiguchi[†2]
Hiroshi Ueda[†2] Yukihiro Miyashita[†2]　Yoichi Hata[†1]

Abstract: Security measures have become one of the most crucial issues in the realization of autonomous driving and connected cars. Intrusion Detection System (IDS) are known as one such security measure; these systems detect cyber-attacks in order to begin a specific measure to counter the attack. Some IDSs use fingerprint technics. These technics allow for recognition of which Electric Control Units (ECUs) sent a CAN message, and detect a malicious CAN message if the transmission source ECU is different from the legitimate one. In this paper, we will evaluate the Clock-based Intrusion Detection System (CIDS) known as software-based fingerprint technic, and study improvements about the vulnerability of this method known as clock phishing and other problems found by the authors.

Keywords: Fingerprint, Intrusion Detection System, In-vehicle network, Cyclic messages, CAN

1. はじめに

コネクティッドカーや自動運転車両の開発を背景として，自動車でのサイバーセキュリティ技術の開発が急がれている[1].サイバー攻撃に対するセキュリティ対策の１つとして侵入検知がある．これは，サイバー攻撃により車載ネットワークに送信された攻撃メッセージの検知を行い，検知結果に基づいた具体的な対策を開始するために用いられる．この様な侵入検知の研究の一つに，CAN プロトコルにおいて，メッセージを送信したECUを区別するFingerprint技術が知られている[12]．一般的にCANネットワークでは各メッセージは特定のECUに紐づけられており，他のECUが送信することは無いため，この技術により識別した送信元がメッセージを送信すべきECUと異なる場合に攻撃メッセージとして検知する．車両へのサイバー攻撃としては，なりすましメッセージを車載ネットワークに送信して不正に制御を行うものが知られている．この様な攻撃はメッセージの送信周期を乱すため，この逸脱からの検知が可能である[2][3][4]．これに対し，正規のECUが送信するメッセージを停止した後になりすましメッセージを送信する攻撃も知られている．この場合送信周期が乱されないため，攻撃の検知が困難になる．Fingerprint 技術はこの様な場合の検知に適している．本論文ではソフトウェアベースのFingerprint技術であるCIDSについて評価を行い，この方式の脆弱性として知られるClock Phishingや筆者達が発見した問題点に対する改善方法について検討を行う．

1.1 構成

本節以降の構成を示す．第２節ではCANプロトコルとセキュリティ脅威について説明する．第３節では車載ネットワークのセキュリティ技術を示し,第４節ではFingerprintを用いた侵入検知の利点と課題を示し，第５節でCIDSを評価し，第６節にて課題のまとめと改善策について検討を行い，第７節にまとめと今後の展開を示す．

†1 住友電気工業株式会社
SUMITOMO ELECTRIC INDUSTRIES, LTD.

†2 株式会社オートネットワーク技術研究所
AutoNetworks Technologies, Ltd.

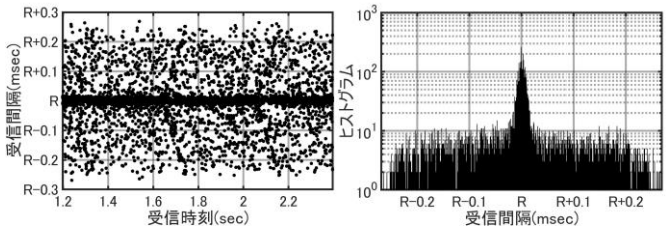
2. CAN プロトコルとセキュリティ脅威

2.1 CAN の特徴

CAN プロトコルと CAN-FD プロトコルの 2 つがある．CAN プロトコルは ISO11898-1(2003)で標準化され，CAN-FD プロトコルは同標準を改訂する形で ISO11898-1(2015)にて標準化された[5][6]．本プロトコルでは，バス型のトポロジ上の複数のノード（ECU）の内，通信調停により送信権を得たノードが最大 8 バイト(CAN)または 64 バイト(CAN-FD)のペイロードをブロードキャスト送信することで，制御システム用途での低遅延なメッセージの通信を実現している．またこれらのプロトコルのメッセージは CAN-ID と呼ばれる一意な識別子で区別される．このため車載ネットワークでは， 運用において排他的に用いられる CAN-ID については，メッセージの送信元 ECU を一意に決定することが可能である．

2.2 メッセージの通信パターン

CAN プロトコルを適用した車載ネットワークでのメッセージの通信パターンは，大きく 2 種類に分類できる．一つは均一な時間間隔で繰り返しメッセージが送信される通信パターンである．本論ではこの様な通信パターンを持つメッセージを「周期メッセージ」と呼ぶ．図 1 に周期メッセージの受信間隔を a)時間軸と b)ヒストグラムにより示す．周期メッセージでは受信間隔は時刻 R を中心に分布しており，その分布は b)の様にガウス状となる．もう一つの通信パターンは不均一な時間間隔でメッセージが送信される「イベントメッセージ」である．本論では，前者の周期メッセージに対する攻撃検知について検討を行う．



a)時間軸　　b)ヒストグラム

図 1. 周期メッセージの受信間隔

2.3 セキュリティに対する脅威

Koscher らは CAN プロトコルについて次に示す 3 つの脆弱性を指摘している[7]．(1)ネットワーク上の制御情報を容易に解析可能，(2)なりすましメッセージを容易に挿入可能，(3)Denial of Service(DoS)攻撃に弱い．なりすましメッセージの挿入や DoS 攻撃は，図 2 に示す様に CAN バスに接続される攻撃 ECU を介して行われる．これは，正常な ECU のファームウェアを改ざんしたものか，不正な ECU を接続したものである．この様な脆弱性を利用した攻撃としては，次に説明する 4 種類の攻撃モデルが考えられる．図 3(A)は共有バスモデル I 型であり，正規 ECU が送信するメッセージに対し攻撃 ECU からなりすましメッセージを挿入する．図 3(B)は共有バスモデルⅡ型であり，正規 ECU の制御を乗っ取った後この ECU からなりすましメッセージを挿入する．これら 2 種類の共有バスモデルでは，受信側の ECU は正常メッセージとなりすましメッセージ両方を受信する．図 4(A)は占有バスモデル I 型であり，正規 ECU が送信するメッセージを停止した後，攻撃 ECU からなりすましメッセージを挿入する．図 4(B)は占有バスモデルⅡ型であり，正規 ECU の制御を乗っ取った後正規 ECU から正常メッセージを上書きしたなりすましメッセージを送信する．これら 2 種類の占有バスモデルでは，受信側の ECU はなりすましメッセージのみを受信する．共有バスモデル I 型と占有バスモデル I，Ⅱ型は，車両への攻撃事例で用いられた攻撃モデルである．これに対し共有バスモデルⅡ型は I 型の派生として考えられた論理的な攻撃モデルである．

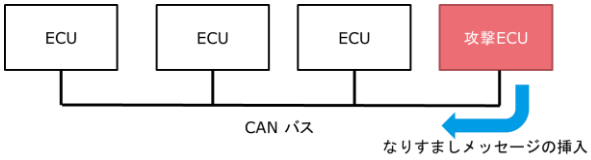


図 2. 攻撃 ECU によるなりすましメッセージの挿入

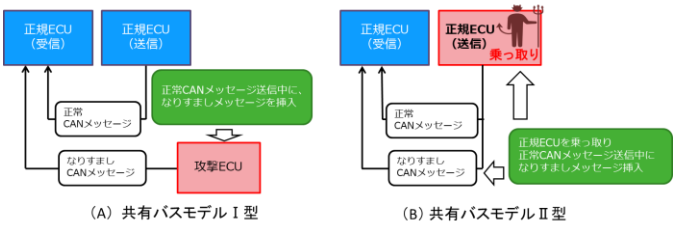


図 3. 共有バスモデル

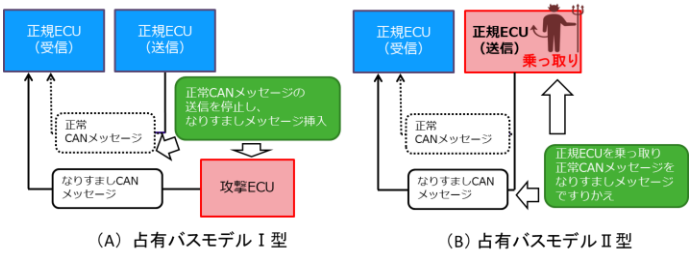


図 4. 占有バスモデル

3. 車載ネットワークのセキュリティ対策

3.1 従来技術

車載ネットワークでのセキュリティに関する研究は以下の 2 つに分類できる．

(1) セキュア通信
　ネットワークプロトコルでのセキュリティ対策を行う．

(2) 侵入検知システム
　ネットワークプロトコル上で動作し，アプリケーションやネットワークでの疑わしい動きを検出する．

3.2 侵入検知システム

3.2.1 技術分類

侵入検知システムは，ネットワーク型とホスト型の 2 つの技術に分類される．ホスト型は一つのノードに設置されるため，システムや接続されたネットワークセグメントの監視を行うことができる．これに対し，ネットワーク型は全てのネットワークセグメントが監視できる場所に設置される．一般的に，車両では複数のネットワークセグメントによって 70 を越える ECU が接続される．本論では，ネットワーク型侵入検知システムを採用することで，多数の ECU を少ない侵入検知システムにより監視する．

3.2.2 従来の車載侵入検知方式

CAN プロトコル用の侵入検知方式の研究として，メッセージの通信周期や頻度を監視する方式や，メッセージのペイロードを監視するメッセージベースが良く知られている[2][3][4][8][9][10][11]．これらに対し，近年 Fingerprint ベースが提案されている.Fingerprint はメッセージの情報から送信元 ECU を特定する技術である．この技術を利用し，受信したメッセージの CAN-ID により識別される送信元 ECU と Fingerprint により識別される送信元 ECU が異なる場合に，受信したメッセージを攻撃メッセージとして検知する．CAN プロトコルにおける Fingerprint の方式としては 2 種類が知られている．1 つは ECU 毎のクロック源が持つスキューを受信メッセージの位相回転から特定する方式であり，Clock-based Intrusion Detection System(CIDS)と呼ばれる[12]．もう一つは ECU が接続される CAN バスでの位置の差異から生じるメッセージ信号の伝搬差異を，CAN バスの電位を測定することで特定する方式である．本論では後者の方式を Voltage-based Intrusion Detection System(VIDS)と呼ぶ[14][15].

4. Fingerprint を用いた侵入検知の利点と課題

4.1 Fingerprint を用いた侵入検知システムの利点

表 1 に Fingerprint ベースとメッセージベースの侵入検知方式からサイバー攻撃に対する定性的なカバー範囲を示す．表では監視メッセージに通信パターンを示し，攻撃モデルにそれぞれの監視メッセージに対するサイバー攻撃モデルを示す．侵入検知方式は大きく Fingerprint ベースとメッセージベースの 2 種類に分けた.さらに Fingerprint ベース方式では CIDS と VIDS の 2 種類，メッセージベースでは通信特性とペイロードの 2 種類の方式に細分した．それぞれの方式によるサイバー攻撃の検知性能について 2 種類の記号で示す．「✔」は検知可能を示し，「×」は検知不可能を示す．またこれらの記号の隣に示した括弧内の左側の値はそれぞれの検知方式で必要となるメッセージ当たりの監視モデルの数を示し，右側の値は監視モデル当たりの計算負荷を，降順で「大」,「中」,「小」で示す．ここで監視モデルは攻撃を検知するためのルールを記載したデータセットである．

表に示すように，メッセージベースのペイロード方式では全てのサイバー攻撃の検知が可能である．しかしこの方式では一つのメッセージを監視するために，メッセージに含まれる複数（n 個）のコンテキストデータ各々についての監視モデルを検証する必要があり計算負荷が高くなる．これに対し Fingerprint ベースやメッセージベースでの通信特性方式では，メッセージ当たり一つの監視モデルを検証すれば良く，監視モデル一つ当たりの計算負荷がメッセージベースのペイロード方式と大きな差異が無いと仮定すれば計算負荷の抑制が可能である．

図 5 に以上のような特性を持つ検知アルゴリズムを組み合わせた侵入検知システムの構成を示す．共有バスモデルⅡ型とⅠ型の攻撃はメッセージベースの通信特性方式で検知を行い．占有バスモデルⅠ型の攻撃については Fingerprint ベースで行い，占有バスモデルⅡ型の攻撃についてはメッセージに含まれる重要なコンテキストデータに限定してメッセージベースのペイロード方式で検知を行う．この様なシステムにおいて，Fingerprint ベースは占有バスモデルⅠ型の攻撃検知の計算負荷の抑制を行う上で重要な役割を担う．

表 1. 侵入検知方式のサイバー攻撃に対するカバー範囲

監視メッセージ	攻撃モデル		侵入検知方式			
			Fingerprintベース		メッセージベース	
			CIDS	VIDS	通信特性	ペイロード
周期メッセージ	占有バスモデル	Ⅰ型	✔(1,中)	✔(1,中)	×	✔(n,中～大)
		Ⅱ型	×	×	×	✔(n,中～大)
	共有バスモデル	Ⅰ型	✔(1,中)	✔(1,中)	✔(1,小)	✔(n,中～大)
		Ⅱ型	×	×	✔(1,小)	✔(n,中～大)

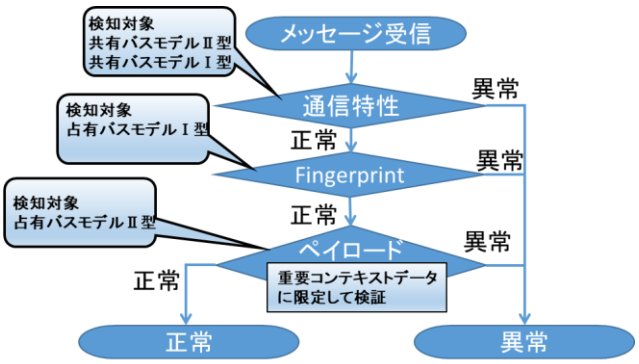


図 5. 侵入検知システム

4.2 Fingerprint 方式の実現

VIDS を実現するには CAN バスの電位を測定する必要があり，A/D コンバータなどハードウェアの追加が必要になる．また検知処理においては CAN の伝送レート以上で電位を測定した後にデータ処理する必要があり，計算負荷が増大する．一方で CIDS の実現はメッセージ受信時の時刻を取得すれば可能である．この様な機能は既存のハードウェアでも備えるものは多いため，VIDS と比較して実現が容易である．また検知処理においても CAN の伝送レート以上でのサンプリングは必要ないため，計算負荷の増大を引き起こす

ことは無い．このため CIDS は，既存のハードウェアにおいてソフトウェアを拡張して侵入検知システムを実現する場合に有利である．

4.3 CIDS

4.3.1 検知方式

Cho らは，Recursive Least Squares（RLS）適応フィルタを用いて，周期メッセージの受信時刻から送信側 ECU の推定を行い，占有バスモデル I 型の攻撃を検知する手法について提案した[15]．この検知処理は，図 6 に示す様に受信した N 個の監視対象メッセージであるチャンク毎に行われる．この処理は大きく 2 つに分かれる．一つは RLS 適応フィルタによる式(1)のパラメータ$S[k]$の更新と，もう一つは直前に更新された$S[k-1]$から式(4)により算出される誤差$e[k]$を評価することにより行う異常検知である．

$S[k]$の更新は累積クロックオフセットO_{acc}を式(2)により求め，式(4)により求められる誤差$e[k]$と，経過時刻$t[k]$から RLS 適応フィルタにより誤差$e[k]$を 0 にする様に行われる．O_{acc}は図 6 に示す様にチャンク内の最初のメッセージの受信時刻を基準時刻とし，実線の矢印で示す実際のメッセージの受信時刻についての基準からの時間間隔と，点線の矢印で示す直前のチャンクで式(3)により算出されたメッセージの平均受信間隔$\mu_t[k-1]$から算出される推定到着時間間隔から算出されるハッチ掛けの領域で示される両者の差異の総和の絶対値を累積した値である．式(3)においてa_nは監視対象メッセージの受信時刻である．

攻撃検知は，式(5)と式(6)により求められる管理限界L^+またはL^-が，スレッショルドを超えた場合に行われる．これらの式でμ_eとσ_eは誤差$e[k]$の平均と標準偏差であり，これらの値は式(7)を満たす場合に更新される．また，Rは検出感度を調整するためのハイパーパラメータであり，値が大きい程感度が鈍化する．L^+は累積オフセットがプラス方向に変化した場合に増加し，L^-はマイナス方向に減少した場合に増加する．

図 7 に，占有バスモデル I 型による攻撃前後での累積クロックオフセットの変化を示す．図において，変化点の左側は正規 ECU から送信されたメッセージから算出した値であり，右側が攻撃 ECU から送信されたメッセージから算出した値である．点線で示すのは正常時の累積クロックオフセットの理想値であり，攻撃後はこの線に対し，プラス側へ変化していることが判る．この場合は，管理限界L^+が増加しスレッショルドを超えた時点で攻撃が検知される．以上より，CIDS は式(2)により直前のチャンク間で算出された受信周期の平均値との差異を累積させた際に現れる傾斜の変化を攻撃として検知するアルゴリズムであることが判る．

$$O_{acc}[k] = S[k] \cdot t[k] + e[k] \quad \text{式(1)}$$

$$O_{acc}[k] = O_{acc}[k-1] + \left| \frac{1}{n+1} \sum_{i=2}^{N} a_i - (a_1 + (i-1)\mu_t[k-1]) \right| \quad \text{式(2)}$$

$$\mu_t[k] = \frac{1}{n} \sum_{i=1}^{N} a_n - a_{n-1} \quad \text{式(3)}$$

$$e[k] = O_{acc}[k] - s[k-1]t[k] \quad \text{式(4)}$$

$$L^+ \leftarrow \max[0, L^+ + \frac{(e-\mu_e)}{\sigma_e} - R] \quad \text{式(5)}$$

$$L^- \leftarrow \max[0, L^- - \frac{(e-\mu_e)}{\sigma_e} - R] \quad \text{式(6)}$$

$$\left| \frac{e-\mu_e}{\sigma_e} \right| < 3 \quad \text{式(7)}$$

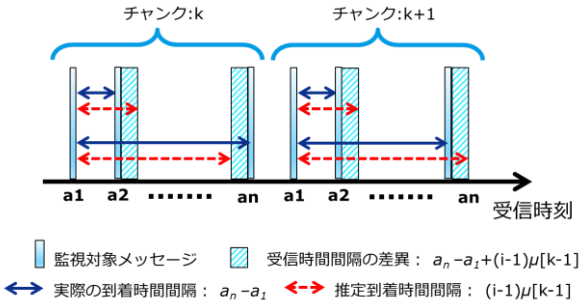


図 6. 累積クロックオフセットの算出

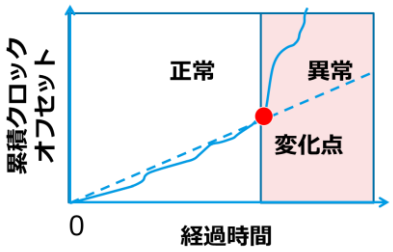


図 7. 累積クロックオフセットとスキューの変化

4.3.2 周期メッセージでの Fingerprint 情報

周期メッセージは，送信側の ECU で動作するプログラムにより一定間隔で送信される．一般的なコンピュータでは，この時間間隔は電子デバイスである振動子から逓倍して生成されるクロック信号を一単位として構成されるため，周期メッセージの送信時間間隔はクロック信号の信号源である振動子のわずかな揺らぎが累積された 3 種類の誤差を持つ．一つは位相ジッタと呼ばれる理想的なクロック信号と実際のクロック信号との時間差であり，これは図 8 に示す様に周期ヒストグラムでの理想的なクロック周期との差異に相当する．本論ではこのジッタを位相回転と呼ぶ．もう一つはピリオドジッタと呼ばれるクロック周期の変動であり，これは図中のヒストグラムのゆらぎの幅に相当する．最後の一つは隣接周期の差異であるサイクル間ジッタである．周期メッセージを送信する ECU を特定するための Fingerprint 情報として，これらの誤差を使用することが

考えられる．ところで CIDS では検知方式から明らかな様に，サイクル間ジッタを Fingerprint 情報として用いる．サイクル間ジッタもピリオドジッタと同様にゆらぎを持つ値である．

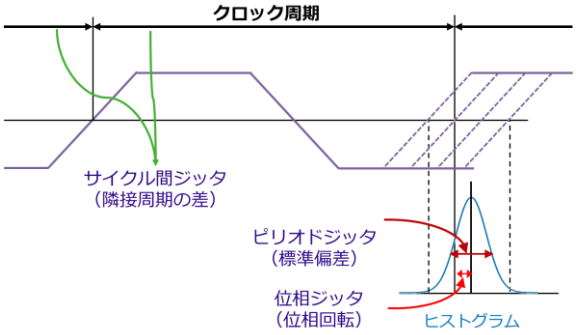


図 8. クロック特性

4.4 CIDS の課題

CIDS における既存の脆弱性として Clock Phishing が知られている[13]．これを占有バスモデル I 型の攻撃と共に用いられると，攻撃の検知が行えなくなる．Clock Phishing は，図 9(A)に示す様に攻撃対象とする ECU が送信するメッセージの受信時刻の標準偏差を学習した後，図 9 (B) に示す様に正規 ECU から送信される攻撃対象となるメッセージを停止させた後に，受信時刻の標準偏差が同一となる様になりすましメッセージを送信することで CIDS による検知を回避している．

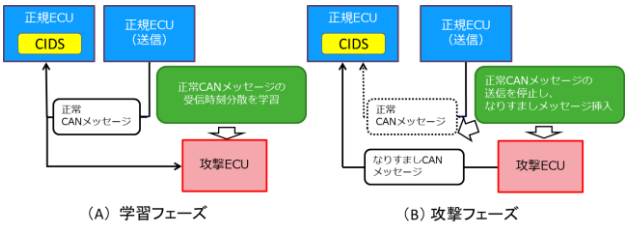


図 9. Clock Phishing を用いた占有バスモデル I 型

5. CIDS の評価

5.1 概要

CIDS を車載 IDS に適用するため，既知の脆弱性である Clock Phishing や，その他の潜在的な脆弱性を，性能評価を通して明らかにする．評価項目は，検知性能，Clock Phishing の 2 つとした．またこれらの評価に先立ち，CIDS のアルゴリズムにおいて送信元 ECU を区別するための Fingerprint 情報として用いられる周期メッセージ受信間隔の標準偏差による判別性能と，CAN 通信において Fingerprint 情報として用いることができるクロック特性について予備評価を行った．

5.2 周期メッセージ受信間隔による Fingerprint

5.2.1 受信間隔の標準偏差による Fingerprint

CIDS は周期メッセージの受信間隔のゆらぎから送信元 ECU を区別するアルゴリズムである．この方式により送信元 ECU の明確な区別が可能か，試験車両を走行して取得したトラフィックデータを用いて確認した． 図 10 では，設計送信周期に対する位相回転毎に設計送信間隔と受信間隔のゆらぎを標準偏差でプロットした．5.2.2 節に後述する様に位相回転の相違は送信元 ECU の相違を意味する．しかし図中 A や B では，位相回転が異なるものの，受信間隔の標準偏差では差異が無いことが判る．これより，CIDS により提案されたアルゴリズムでは送信元 ECU の区別が困難であることが明らかである．

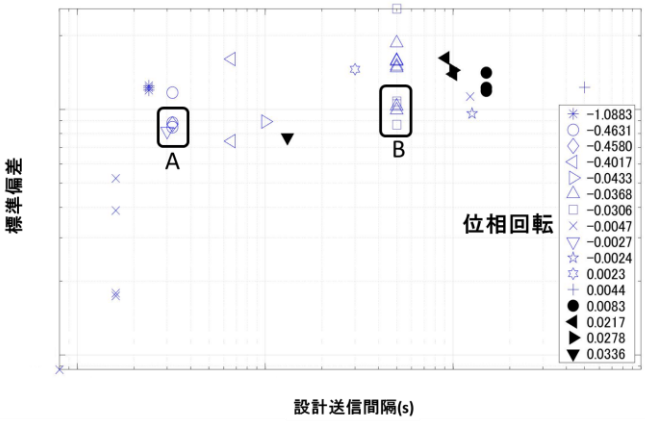


図 10. 周期メッセージの設計送信間隔と標準偏差の分布

5.2.2 Fingerprint 情報としてのクロック特性

概要

周期メッセージの受信情報から取得できる Fingerprint 情報を調査するため， 図 11 に示す実験環境を用いて ECU 模擬基板から送信する周期メッセージについて，送信側と受信側の位相回転と分布の標準偏差について測定を行った．送信側ではオシロスコープを用いて，メッセージ送信のトリガを測定し，受信側ではロガーでの受信時刻を測定した．ECU 模擬基板には表 2 に示す 3 種類の振動子を搭載し，これらを源信とした 100ms の間隔で周期メッセージを送信した．さらに以上の測定では，ログ再生装置からネットワーク利用率が 40%，80%になる様に車載トラフィックを流した．

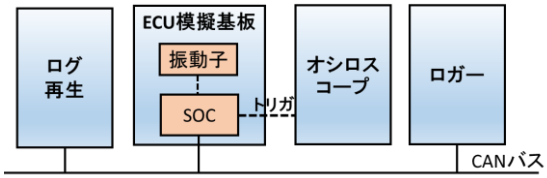


図 11. 実験環境

表 2. 振動子の仕様

	水晶振動子		
	A	B	C
周波数(MHz)	8	8	8
周波数偏差(ppm)	±30	±20	±30

通信間隔の位相回転と標準偏差

図 12 に 3 種類の振動子毎の位相回転の測定結果を示す．図より，送信側では使用する振動子毎に異なる位相回転が現れ，この大小関係はバス利用率の差異の影響を受けずに受信側に現れる．これより位相回転は Fingerprint 情報と

して利用可能であるといえる．ただし本論での実験環境では，受信側の位相回転は送信側よりも 0.001° 程度大きく現れた．これは送信側と受信側での測定系の差異によるものと考える．

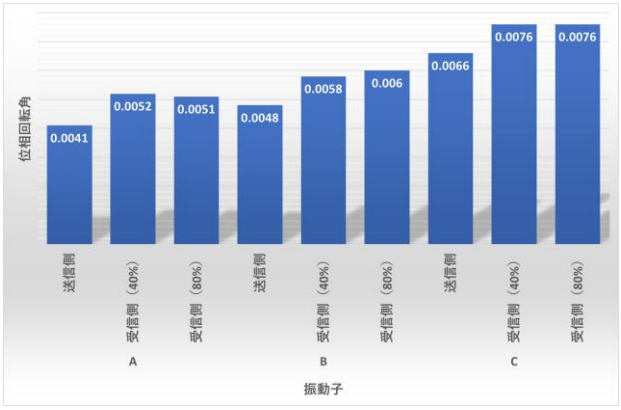


図 12．位相ジッタ（位相回転）

図 13 には 3 種類の振動子毎の標準偏差の測定結果を示す．送信側では振動子の差異により標準偏差の違いを確認することができるが，受信側においてネットワーク利用率 40%，80%のトラフィックが流れる場合に振動子の差異を確認することができない．このため，受信間隔の標準偏差は Fingerprint 情報には適当ではない．

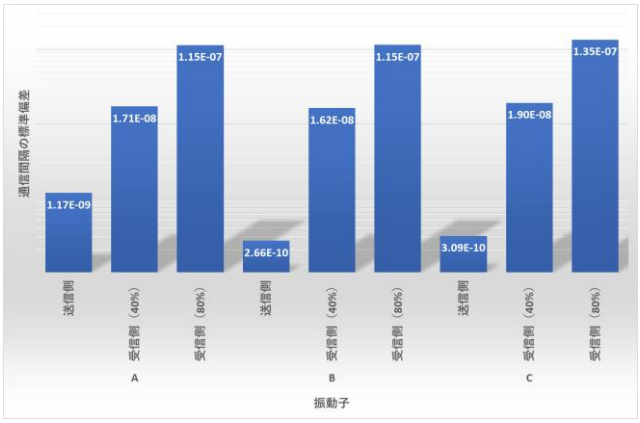


図 13．ピリオドジッタ（標準偏差）

Fingerprint 情報としての部分的な受信間隔の標準偏差

図 14 に振動子 A を用いた場合の受信側での受信間隔分布を示す．A)はネットワーク利用率 0%での結果であり，B)，C)はそれぞれネットワーク利用率 40%，80%の場合の結果である．各グラフで横軸はメッセージの受信間隔，縦軸は頻度または確率密度を示す． 図において，100ms に位置する最も頻度の大きな受信間隔は通信プロトコルによる送信遅延の影響を受けない場合の受信間隔であり， 100ms よりも時間間隔が長くなる場合や短くなる場合は送信遅延の影響を受ける場合である．図 A)のネットワーク利用率 0%での受信間隔の分布は，送信遅延の影響を受けておらず送信側 ECU の特性を示している．これに対し図 B)，C)では，順にネットワーク利用率が上昇し通信調停の影響が大きくなるため， 100ms 周辺への分布が増えることが判る．図 15 に通信調停の受信間隔への影響の度合を，ネットワーク利用率が 40%と 80%について，ネットワーク利用率が 0%の場合の受信間隔の範囲に分布する割合で示した．ネットワーク利用率 40%の場合，この範囲に位置する受信間隔の割合は 15～35%であり，80%の場合は 3～5%となった．受信間隔分布の中央部付近から送信側 ECU の特性が残る分布を抽出可能であれば，この範囲の標準偏差を Fingerprint 情報として利用可能である．

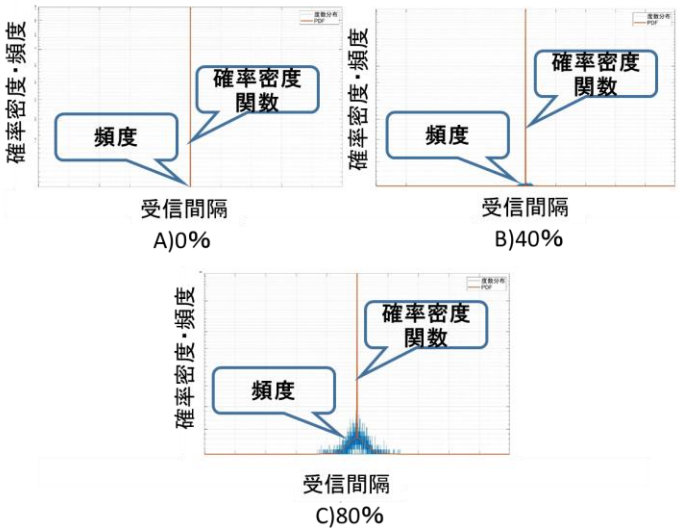


図 14．ネットワーク利用率の差異と受信間隔分布の差異

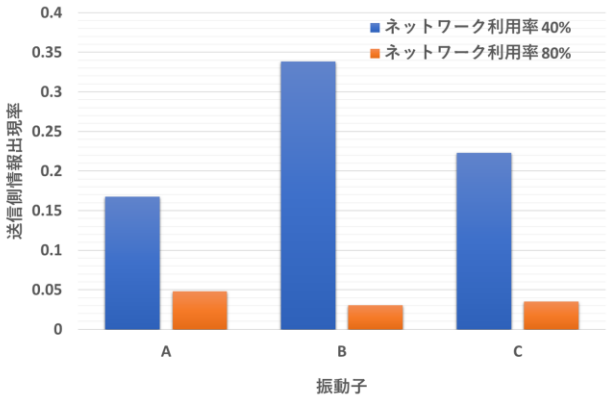


図 15．通信調停の受信間隔への影響

5.3 性能評価

5.3.1 検知性能

評価方法

図 16 に示す構成で，ECU 模擬基板から共有バス I 型の攻撃を行った場合の CIDS による検知時間について，PC 上に検知アルゴリズムを再現しオフラインで評価を行った．この評価では検知アルゴリズムで用いられる受信間隔の平均値μ_tに対して初期値を設定した場合としない場合についての検知時間への影響を確認した．また，この評価で使用したアルゴリズムのハイパーパラメータを表 3 に示す．

評価に用いたメッセージは疑似的に作成した．ログ再生装置から実際の車両で記録した監視対象のメッセージを含

む車載トラフィックを流してロガーで記録し直した正常なメッセージと，ログ再生装置から監視対象メッセージを除いた車載トラフィックを流す中 ECU 模擬基板からメッセージを送信しロガーで記録した攻撃メッセージを結合して，約 180 秒のメッセージセットを作成した．受信間隔の平均値μ_tでの初期値有りに代入される値は，評価に用いた監視対象メッセージの設計送信周期である．これ以外のパラメータは CIDS の論文で推奨される値を用いた．

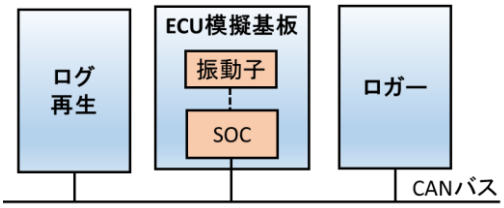


図 16．実験環境

表 3．アルゴリズムハイパーパラメータ一覧

	チャンク当たりのメッセージ数	スレッショルド	R	μ_tの初期値	
				有り	無し
ハイパーパラメータ	20	5	5	0.02	0

検知性能

表 4 に評価結果を示す．初期値有りは，μ_tに初期値を設定した場合の結果であり，初期値無しはこれを行わない場合の結果である．攻撃開始時刻には共有バス I 型の攻撃を開始した時刻を示し，検知時刻には CIDS により攻撃を検知した時刻を示す．検知時間は攻撃が開始されてから検出されるまでの時間を示す．初期値有りの場合には 14.5 秒で攻撃を検出したが，無しの場合には攻撃を検知できなかった．

図 17 と図 18 に，初期値有りの場合と無しの場合の検知結果の詳細として，(A) にクロックオフセット$O_{acc}[k]$，(B) に identification error $e[k]$，(C)と(D)に管理限界L^+およびL^-を各々示す．各グラフにおいて，89 秒付近の点線は，攻撃開始時刻を示している．これらより，$O_{acc}[k]$および$e[k]$は，初期値の有無に関わらず攻撃開始時刻以降に変化しているが，攻撃の有無を示す管理限界L^+，L^-は初期値ありではL^-が攻撃開始後に増加しているものの，初期値無しではL^+，L^-いずれも変化しなかった．この差異は，両図での (B) identification error $e[k]$に現れている．初期値ありの場合，$e[k]$は攻撃開始前に 0 付近に収束しているが，初期値なしの場合は図 18(B)中の(A)部の様に動作直後に$e[k]$が大きく変動した．異常度を示す管理限界L^+，L^-は式(5)，(6)に示す様に$e[k]$と平均μ_eの差分を標準偏差σ_eで除算する項が含まれる．初期値が無い場合での動作直後の$e[k]$の大きな変動は，σ_eに大きな外れ値を記憶させる．一度大きな外れ値が入力されると，この外れ値の影響が継続するため，攻撃が行われても管理限界L^+，L^-の変動が大きなσ_eで除算されて打ち消され，攻撃を検知することができない．

表 4．攻撃検知時間

	初期値あり	初期値なし
A:攻撃開始時刻[Sec]	89.9980	
B:検知時刻[Sec]	104.5087	検知せず
検知時間(A-B)	14.5107	

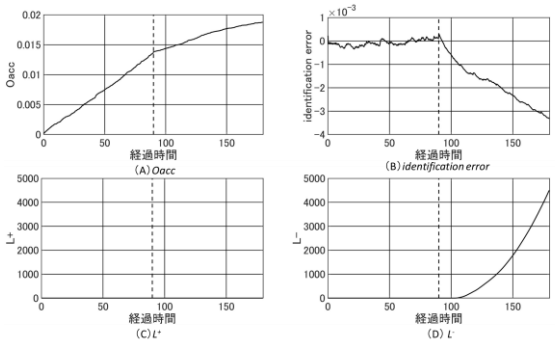


図 17．検知性能の結果（μ_tの初期値設定あり）

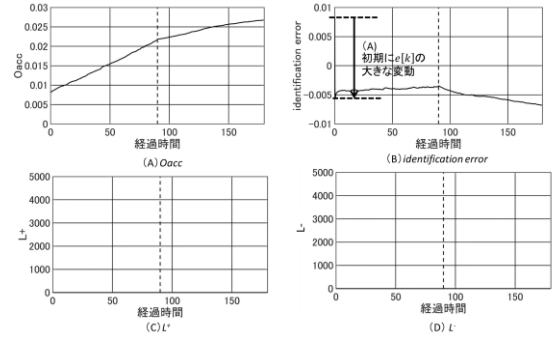


図 18．検知性能の結果（μ_tの初期値設定なし）

5.3.2 Clock Phishing

評価環境

図 16 に示す構成で，ECU 模擬基板から Clock Phishing と共に共有バス I 型の攻撃を行った場合の CIDS による検知可否について，5.3.1 と同様にオフラインで評価を行った．アルゴリズムのハイパーパラメータは表 3 に示すものを使用し，μ_tについては初期値有りとした．この評価では，Clock Phishing により偽装されるメッセージの受信時刻の標準偏差を変更し，CIDS での検知可否を確認した．

評価に用いたメッセージは 5.3.1 と同様に疑似的に作成した．また ECU 模擬基板での監視対象メッセージに対する Clock Phishing は，直前のメッセージとの送信間隔を式(8)に示す様に監視対象メッセージの送信周期を中心に一定の誤差を交互に発生させることで行い，この式の誤差を変更することで，表 5 に示す標準偏差が異なる 4 種類のメッセージセットを作成した．

$$送信間隔 = 送信周期 + \left(-1^{t}\right) \times 誤差 \quad \text{式(8)}$$

$$t = t + 1$$

評価結果

表 5 に CIDS による攻撃検知結果を示す．評価用メッセージセット番号毎に，ロガーで記録された正常メッセージ

の受信時刻の標準偏差と攻撃メッセージの標準偏差をしめし，また CIDS で攻撃メッセージを検知したか否かをそれぞれ「✔」と「×」で示す．評価用メッセージセット 2 と 3 は CIDS により攻撃の検知ができず Clock Phishing による共有バス I 型の攻撃が成功している．この時の攻撃メッセージと正常メッセージの標準偏差の差異が最も大きくなったのはメッセージセット番号 2 の場合であり，攻撃メッセージの標準偏差の差異は正常メッセージに対して約＋32%となった．また攻撃メッセージの標準偏差が正常メッセージの標準偏差よりも小さくなる場合のメッセージセットは番号 4 であるがこの場合 CIDS による攻撃検知は成功しており，攻撃メッセージの標準偏差の差異は正常メッセージに対して約-28%となった．以上より Clock Phishing により監視対象メッセージの標準偏差に対して±20～30%以内の精度で疑似メッセージを送信されると，CIDS では検知が困難になる．

表 5. CIDS による攻撃検知結果

評価用メッセージセット番号	正常メッセージの標準偏差	攻撃メッセージの標準偏差	CIDSによる攻撃検知
1	3.9e-4	6.4e-4	✔
2	3.9e-4	5.2e-4	×
3	3.9e-4	4.0e-4	×
4	3.9e-4	2.8e-4	✔

6. CIDS の課題と改善検討

6.1 課題

CIDS の課題は送信元 ECU を区別することが困難な受信時刻の標準偏差を Fingerprint 情報として使用することである．このため標準偏差を±20～30%程度の誤差で偽装する粗い Clock Phishing による偽装メッセージについても正常メッセージと区別することができないことが課題である．

6.2 改善検討

送信元 ECU を区別するための Fingerprint 情報としてはバス利用率の影響を受けないメッセージ受信間隔の位相回転が適している．しかし，この値は監視対象メッセージの設計送信周期が推定できる場合は偽装が容易である．

受信間隔分布の中央部分は，バス利用率によって送信元 ECU の特性が反映される範囲が変わるが，Fingerprint 情報として利用可能である．本論ではこの範囲の標準偏差を Fingerprint 情報として用いる方法について議論を行ったが，この範囲の確率密度関数を推定しピークの数や尖度などの分布の形状を細かく評価する様な値を Fingerprint 情報として用いることで，精度良く送信元 ECU を識別することが可能になると考える．この実現手段として，筆者達が以前に提案を行った混合ガウス分布を用いた受信間隔の確率密度関数の動的な推定方式が利用できる[4]．この方式では推定の際にガウス分布を 2 つ以上用いることで推定対象となる分布に柔軟にフィッティングさせた確率密度関数を得ることができるため，分布中央に位置する Fingerprint 情報を抽出することが可能である．

7. おわりに

車載ネットワークでの Fingerprint 技術の一つである CIDS について，検知性能，既知の脆弱性である Clock Phishing について評価を行い，方式の課題を明らかにし．改善策について検討を行った．CIDS は占有バスモデル I 型の攻撃を検知する上で有用であるため，今後は本論文で検討した改善策に基づき，提案手法の開発を進める．

参考文献

[1] Miller, C., and Valasek, C., “Remote Exploitation of an Unaltered Passenger Vehicle,” presented at DEF CON 23, August 2015.

[2] Müter, M., and Asaj, N., “Entropy-Based Anomaly Detection for In-Vehicle Networks,” *2011 IEEE Intelligent Vehicle Symposium (IV)*, 2011.

[3] Otsuka, S., Ishigooka, T., Oishi, Y., and Sasazawa, K., “CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems,” SAE Technical Paper 2014-01-0340, 2014.

[4] Hamada, Y., Inoue,M, Ueda, H., Miyashita, Y, et. al., “Anomaly-Based Intrusion Detection Using the Density Estimation of Reception Cycle Periods for In-Vehicle Networks,” SAE International Journal of Transportation Cybersecurity and Privacy, Vol1, 2018.

[5] International Organization for Standardization, “Road vehicles-Controller area network (CAN) - Part 1: Data link layer and physical signaling,” ISO11898-1, Rev. 2003.

[6] International Organization for Standardization, “Road vehicles-Controller area network (CAN) - Part 1: Data link layer and physical signaling,” ISO11898-1, Rev. 2015.

[7] Koscher, K., Czeskis, A., Roesner, F., Patel, S. et al., “Experimental Security Analysis of a Modern Automobile,” *2010 IEEE Symposium on* Security and Privacy , 2010.

[8] Larson, U.E., Nilsson, D.K., and Jonsson, E., “An Approach to Specification-Based Attack Detection for In-vehicle Networks,” *2008 IEEE Intelligent Vehicle Symposium,* 2008

[9] Markovitz, M. and Wool, A., “Field Classification, Modeling and Anomaly Detection in Unknown CAN Bus Networks,” presented at the 13th escar Europe Conference, November 11–12, 2015.

[10] Wasicek, A., Pesé, M., Weimerskirch, A., and Burakova, Y. et al., “Context-aware Intrusion Detection in Automotive Control System,” presented at the 5th escar USA Conference, USA, June 21–22, 2017.

[11] Hamada, Y., Inoue, M., Tateishi, H., Adachi, N., et. al., “Virtual Secsing Anomaly Detection for In-Vehicle Network,” 2018 Symposium on Cryptography and Information Security, January, 2018.

[12] Cho, Kyong-Tak, and Kang G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," 25th {USENIX} Security Symposium ({USENIX} Security 16), 2016.

[13] Tayyab, Muhammad., Hafeez, A. and Malik, H., “Clock Phishing Attack on Clock Based Intrusion Detection Systems for CAN Protocol,” presented at the 6th escar USA Conference, June 20–21, 2018

[14] Hafeez, A., Ponnapalli, S. and Malik, H., “Transmitter Identification for CAN protocol using channel distortion,” presented at the 7th escar USA Conference, June 12–13, 2019

[15] Ahmed, S., Juliato, M., Gutierrez, C., Zhao, L. and Sastry, M., “Two-Point Voltage Fingerprinting: Increasing Detectability of ECU Masquerading Attacks,” presented at the 7th escar USA Conference, June 12–13, 2019