「マルチメディア，分散，協調とモバイル
(DICOMO2013)シンポジウム」 平成25年7月

自動車システムのセキュリティ・セイフティポリシに基づくパケット破棄攻撃への対策

加藤平成† 井手口哲夫† 奥田隆史† 田学軍†

本稿では、自動車システムの内部と外部の情報の連携の安全性と信頼性を実現するために、これらの情報の連携を行う自動車システムに対して、セキュリティ・セイフティポリシを策定する。

また、ポリシの策定に関して、特に車車間通信を利用した自動車システムにおいて予測される脅威と、それらの対策方法を示し、車車間通信環境においては既存の方法では対策困難な脅威の一つであるパケット破棄攻撃に対する方策として、既存の watchdog を用いて周辺ノードの中継監視する方式に、攻撃が疑われる車両に関して周辺の車両の監視記録に対して問い合わせを行う機能を追加することで、誤検出を抑え、パケット破棄を行う攻撃者を検出・特定できる方策を提案し、提案した手法に対し、シミュレーションを行い、検出率・誤検出率・オーバーヘッドといった項目を既存方法と比較する。

A countermeasure against Packet Dropping Attacks based on Security & Safety Policy of Vehicle System

HIRANARI KATO† TETSUO IDEGUCHI†
TAKASHI OKUDA† TIAN XUEJUN†

1. はじめに

現在、車車間通信を利用する様々なシステムが提案されている。安全運転支援アプリケーションに車車間通信機能を用いることで、これまでの車載センサを用いたシステムの限界を補い、交通事故件数を減らすことが可能であるが、安全運転支援に車車間通信機能を用い、外部からの情報を車両の制御に利用するためには、そのセキュリティについても十分に検討される必要がある。

そこで本稿では、自動車システムの内部と外部の情報の連携の安全性と信頼性を実現するために、これらの情報の連携を行う自動車システムのセキュリティ・セイフティポリシを策定する。また、ポリシ実現のための課題の一つであるパケット破棄攻撃に対する方策として、車両が周辺の通信の監視記録を保存し、攻撃が疑われる車両に関して周辺車両に問い合わせを行うことで、誤検出を抑える方策を提案し、提案した手法に対し、シミュレーションを行い、各評価項目を既存方法と比較する。

本稿の構成は以下のとおりである。2 章では車車間通信において予想される脅威とその対策法について述べる。第 3 章では脅威とその対策法から策定したポリシとその実現のための課題について述べる。4 章では既存のパケット破棄攻撃の対策法について述べる。5 章では提案方式について述べる。6 章では、既存方式と提案方式の比較を行う。

†愛知県立大学情報科学研究科
Graduate School of Information Science and Technology
Aichi Prefectural University

2. 予想される脅威とその対策

2.1 車車間通信において予想される脅威

車車間通信において発生することが予想される脅威を表 1 に示す。

表 1 予想される脅威

なりすまし	ほかの車両になりすまして通信を行う攻撃
改ざん	中継時にデータを改ざんする攻撃
盗聴	他の車両の通信を盗聴する
パケット破棄	中継時にパケットを中継せず破棄する攻撃。
リプレイ攻撃	他の車両の送信したパケットを複製し、再送信する攻撃
偽情報の送信	事実と異なる偽の情報を送信することでシステムの混乱を狙う攻撃
サービス不能攻撃	大量のサービス要求をかけることでサービスを妨害する
ジャミング	妨害電波を用いることで通信を妨害
個人情報の漏えい	ドライバーの個人情報を外部に送信
ルーティング攪乱攻撃	マルチホップ通信のルーティングを攪乱することで、通信を妨害する攻撃

2.2 予想される脅威に対する対策法

予想される脅威に対する対策方法を表 2 に示す。

表 2 脅威とその対策

なりすまし	認証を行う
改ざん	署名によって改ざんを検知する
盗聴	通信を暗号化する
パケット破棄	ネットワーク上でパケット破棄を検知する機能を動作させる

リプレイ攻撃	パケットにタイムスタンプを付加
偽情報の送信	署名による否認防止・真正性確認を行う
サービス不能攻撃	同じ車両からのサービス要求に制限をかける
ジャミング	物理的・法的に対策する
個人情報の漏えい	ドライバーの個人情報を外部に送信しない。送信時は暗号化を行う。
ルーティング攪乱攻撃	対策方法はルーティングプロトコルに依存する

3. セキュリティ・セイフティポリシ

3.1 基本方針

セキュリティ・セイフティポリシの基本方針を示す。

① 悪意ある攻撃やシステムの誤動作により、ドライバーが危険に晒されない。
② ドライバーの個人情報等の漏洩を防ぐ。
③ 攻撃を受けることにより、ネットワークが利用不能になることを防ぐ。
④ 車車間通信による遅延時間・パケット到達率等は、要求条件[1]を満たすこと。
⑤ 攻撃者の検出・特定を行うことができる。

3.2 対策基準

策定した対策基準の一部を以下に示す。

① 機密性の維持のため、必要な通信については、暗号化により情報の漏えいを防止する。
② システムの可用性の維持のために実時間性が要求される通信においては、要求時間内に通信が行えること。
③ システムの可用性の維持のために、パケット破棄攻撃を検出する機能を車両ネットワーク上で動作させる。

3.3 車車間通信の課題(ポリシ実現のための課題)

課題１

先のセキュリティ・セイフティポリシにおいて、パケット破棄攻撃への対策のために、ネットワーク上でパケット破棄攻撃に対する対策が必要であると述べたが、既存の方法を車両ネットワーク上で適用するのは困難であり、既存の方法を、車両ネットワーク向けに改良する必要がある。

課題２

暗号化や署名を用い、なおかつ実時間性が要求される通信に対して、想定される環境内で、要求時間内の遅延内に送信が行えるか検討する必要がある。

4. パケット破棄攻撃に対する方法

無線ネットワークにおける、パケット破棄攻撃の対策のための手法は、大きく分けて、中継監視を行う方法[2]、レピュテーションを用いる方法[3]、レポート交換を用いる手法[4]、インセンティブプライシングを用いる手法[5]の４つの手法が存在する。それぞれの特徴と、車車間通信において適用するための問題点について述べる。

4.1 中継監視を行う方法

4.1.1 特徴

中継監視を行う方法では、無線の同報性を利用することでパケットの中継を監視し、パケットの中継が確認できない場合は、攻撃者として検出し、ルーティングから除外する。

4.1.2 問題点

この方法には、watchdog の誤検出率が大きく、正当なノードも誤検出されてしまうという問題がある。特に、ノードが移動する環境では誤検出率が大きくなる。[6]

4.2 レピュテーションを用いる方法

4.2.1 特徴

各ノードに対してパケットの中継に対する信頼度を計算し、ノードの情報をネットワークで共有し、信頼度の低いノードにはパケットを中継させないことで、正当なノードにパケットを中継させ、確実にパケットを到達させることを目標とする。前述した方法とは異なり、各ノードが計算した信頼度を共有し、レピュテーション（評判）とすることが特徴となる。

4.2.2 問題点

周辺ノードと情報を共有することで、誤検出を抑えたうえで、パケット破棄を行う攻撃者を検出することが可能であるが、通常は正当なノードとして振る舞い、選択的にパケットを破棄する攻撃者の検出が困難であり、すべてのパケットを破棄する攻撃者に対しても、一定回数の攻撃は許容してしまう。また、各ノードが個々に信頼度を計算する方法は、ネットワーク構成の変化が激しい車両ネットワークでは困難であり、ネットワーク全体で信頼度を共有・集計するのであれば、全体のノードの信頼度の集計・共有を行える機構が必要となる。

4.3 レポート交換を用いる方法

4.3.1 特徴

ネットワーク上で隣接ノードの動作を監視し、各ノードが周辺ノードの動作に関するレポートを作成・配布することで攻撃者の検出を行う。周辺ノードから受け取ったレポートをチェックすることで各ノードに対する信頼度を計算し、信頼度の低いノードをネットワークから除外する。

4.3.2 問題点

この手法は、各ノードが一定時間ごとに周辺ノードに対するレポートを送信するため、オーバーヘッドが大きく、ネットワークに大きな負荷がかかる。また、周辺ノードが激しく変化する環境では正確なレポートの作成が困難となることも考えられ、パケット破棄が行われた時点での検出ができず、検出に時間がかかることも問題である。

4.4 インセンティブプライシングを用いる方法

4.4.1 特徴

ネットワークに貢献したノードに報酬を与え、利用しただけのノードからは徴収する。ネットワークを利用するた

めには必ず他のノードのためにも働く必要があるので、各ノードに対してネットワークへの貢献を促すことができる。

4.4.2 問題点

ネットワークに対して積極的な貢献を促すことで、利己的な理由でパケット中継をしない、Selfish Node[7]のようなノードをネットワーク参加させることが可能であるが、悪意をもってネットワークを攻撃するノードの攻撃を防ぐことはできない。ネットワーク貢献度を安全に統計・管理する機構が必要である。報酬がノードに対して実利的価値のあるものでなければ、この手法は成り立たない。

4.5 既存方式の比較

既存方式の車両ネットワークで使用する場合の、各方式の性能についての特徴を表 3 にまとめる。

表 3　車車間通信環境においての既存方式の比較

方式	検出時間	誤検出率	オーバーヘッド	外部の機構
中継監視	**早い**	高い	**小さい**	**不要**
レピュテーション	遅い	**低い**	中程度	必要
レポート交換	遅い	**低い**	大きい	**不要**
インセンティブプライシング	検出しない	なし	**小さい**	必要

上記の方式は一長一短であるが、本稿では、中継監視方式の誤検出率の低減を検討する。

5. 提案方式

5.1 特徴

提案方式は、既存の、中継監視を行う方法を車両ネットワーク向けに改良し、誤検出率を抑えることを目標とする。誤検出を抑えるために各車両は、周辺の中継パケットを傍受し、中継が確認できた場合、それを監視ログに保存する。

5.2 アルゴリズム

5.2.1 監視ログの作成

① 各車両は、周辺の通信を傍受する。
② 中継パケットの送信が確認できた場合、その送信元、中継者、パケット番号を監視ログに記録する。
③ 監視ログに記録されてから一定時間経過したデータは破棄する。

5.2.2 問い合わせと応答

① 車両 A が車両 B に、あて先が車両 C のパケットを送信した場合、A は車両 B があて先 C に対して、中継を行っているか監視する。
② 一定の時間内に中継が行われていることが確認できない場合、A は、B がパケットを中継したか周辺に問い合わせる。
③ 周辺車両は、車両 B が中継したパケット番号のリストを A に送信する。なければ送信しない。
④ A は、周辺車両から受信したパケット番号のリストから、B が中継を行っていたか確認する。一定時間内に確認できなかった場合、A は周辺に、B によるパケットの中継が確認できなかったことを報告する。
⑤ 閾値以上の回数の報告が行われた車両は、攻撃者であるとし、ネットワークから排除する

5.2.3 再送処理

パケットの到達率を上げることで、中継車までのパケット到達率を上げるために、再送処理の導入についても検討する。再送処理は、中継を一定時間以内に確認できなかった場合、送信元車両が中継車両へ再度パケットを送信するものとする。

6. 評価実験

6.1 シミュレーション条件

表 4 の条件で 10 回シミュレーションを行い、その平均値を結果とする。シミュレーションには、マルチエージェントシミュレータの Artisoc2.6 を用いた。

表 4　シミュレーション条件

項目	数値
シミュレーションエリア	片側２車線 500m
車両速度	75～105km/h 第 1 車線・平均 80km/h 第 2 車線・平均 100km/h
ドライバモデル	最適速度モデル
平均車間距離	20m～80m
通信距離	100m
パケット発生率	毎秒 0.2～0.5（1 台）
攻撃者の割合	0.3
シミュレーション時間	１時間 （１ステップ 1ms として 3,600,000 ステップ実行）

6.2 評価項目

6.2.1 誤検出率

提案方式、既存方式それぞれに対して評価する。
ノード監視によって検出されたノードが、攻撃ノードではない正当なノードである確率である。

$$\text{誤検出率} = \frac{\text{誤検出されたノード数}}{\text{誤検出されたノード数} + \text{検出された攻撃ノード数}}$$

6.2.2 オーバーヘッド

既存方式では評価せず、提案方式のみ評価する。
通常パケットに対する、提案方式によって発生したパケットの割合である。

$$\text{オーバーヘッド} = \frac{\text{問い合わせパケット数} + \text{応答パケット数}}{\text{通常のパケット数}}$$

6.2.3 問い合わせ成功率

既存方式では評価せず、提案方式のみ評価する。
提案方式の問い合わせにより、正当なノードの誤検出を防止できる確率である。

問い合わせ成功率

$$= \frac{\text{問い合わせにより誤検出を防止できた回数}}{\text{正当なノードに対する問い合わせ数}}$$

6.2.4 パケット到達率

既存方式では評価せず、提案方式のみ評価する。
送信元から中継車までのパケットの送信成功率である。

$$\text{パケット到達率} = \frac{\text{パケット受信成功数}}{\text{パケット送信数}}$$

6.2.5 攻撃者検出時間

検出閾値による検出性能の変化を評価するために用いる。攻撃者がネットワークに参加してから、攻撃者を検出するまでにかかる時間である。

$$\text{攻撃者検出時間} = \frac{\text{各攻撃者の検出にかかった時間の合計}}{\text{攻撃者検出数}}$$

6.2.6 検出率

検出閾値の検出閾値による検出性能の変化を評価するために用いる。

$$\text{検出率} = \frac{\text{攻撃者検出数}}{\text{攻撃者検出数} + \text{検出失敗数}}$$

6.3 ネットワークの混雑状況による両方式の比較

平均車間距離を 40m とし、パケット発生率を 10%から 50%まで変化させながらシミュレーションを行う。
誤検出率を図 6-1、問い合わせ成功率を図 6-2、提案方式のオーバーヘッドを図 6-3、パケット到達率を図 6-4 に示す。

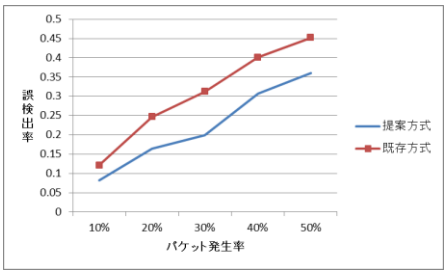

図 6-1　パケット発生率と誤検出率

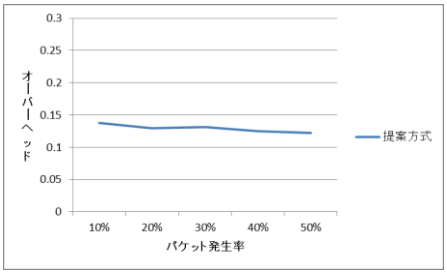

図 6-2　パケット発生率とオーバーヘッド

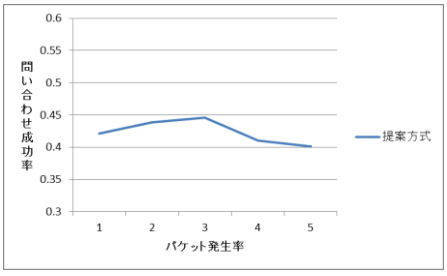

図 6-3　パケット発生率と問い合わせ成功率

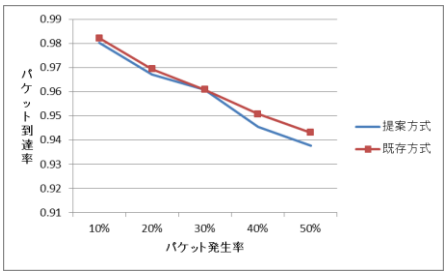

図 6-4　パケット発生率とパケット到達率

図 6-1 より、提案方式の効果は、ネットワークの混雑状況（各車両のパケット発生率）により変化しており、パケット発生率が 30%から 50%のときは効果が大きく、0.11 ポイント程度の誤検出率を低減させることがわかる。しかし、パケット発生率が 10%のときは効果が 0.04 ポイント程度まで下がっている。これは、ネットワークの混雑度が下がることで、パケットの衝突による監視失敗そのものが少なくなっているためだと考えられる。図 6-2 より、問い合わせ成功率は、0.41 から 0.45 程度の間を変化しており、変化が小さく、ネットワーク混雑の影響を受けにくいことが分かる。

図 6-3 より、オーバーヘッドも、0.14 から 0.13 程度と、変化が小さく、ネットワークの混雑度の影響を大きく受けないことがわかる。

図 6-4 より、パケット到達率は、両方式とも、大きな差は見られないが、ネットワークが混雑すると、既存方式に対して、パケットの到達率が 0.005 ポイント程度落ちることがわかる。これは、ネットワークが混雑することにより、提案方式のオーバーヘッドの影響を受けやすくなってしまうためであると考えられる。

6.4 車両密度の変化による両方式の比較

パケット発生率を 20%とし、平均車間距離を 20m から 80m まで変化させながらシミュレーションを行う。その結果を図 6-5～図 6-8 に示す。

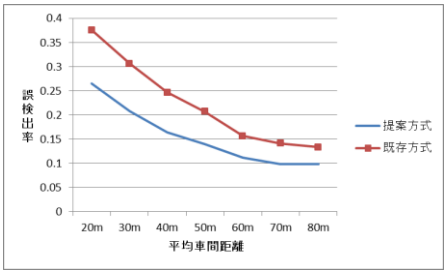

図 6-5　平均車間距離と誤検出率

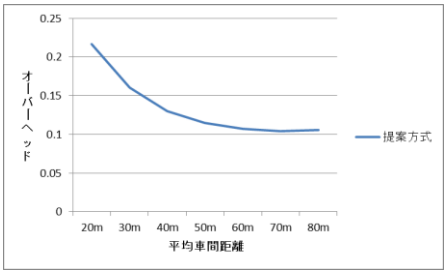

図 6-6　平均車間距離とオーバーヘッド

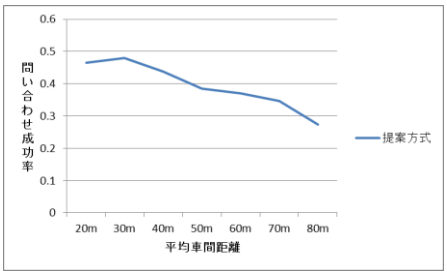

図 6-7　平均車間距離と問い合わせ成功率

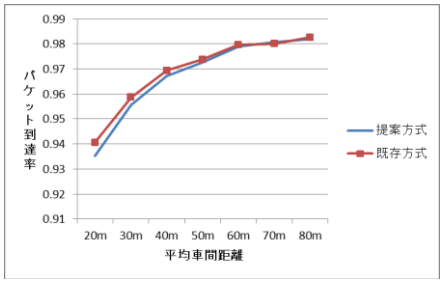

図 6-8　平均車間距離とパケット到達率

図 6-5 より、提案方式が誤検出率が低減させる効果は、車間距離によって変化しており、特に車間距離が短いときにその効果が大きいことがわかる。車間距離 20m のときが最も効果が大きく、0.11 ポイント程度低減できている。車間距離が 60m 以上になると効果が小さくなり、0.05～0.04 ポイント程度に低下する。

図 6-6 より、提案方式による問い合わせは、車両の密度が高いとき成功しやすく、0.48 程度であり、車両の密度が低下することにより低下していくことがわかる。

図 6-7 より、オーバーヘッドは、車両密度が高いときに大きくなる。これは、車両密度が上がることにより、衝突が起こりやすくなり、監視の失敗が頻発していることや、一つの問い合わせに対して多数の応答が返されていることなどが原因として考えられる。

図 6-8 より、パケット到達率は、平均車間距離が大きくなると良くなることがわかる。

6.5　再送処理の導入による両方式の比較

既存方式、提案方式の両方式に再送処理を導入し、シミュレーションを行う。平均車間距離を 40m とし、パケット発生率を 10%から 50%まで変化させた結果を図 6-9 から図 6-11 に示す。また、パケット発生率を 30%とし、平均車間距離を 20m から 80m に変化させた結果を図 5.13 から図 5.15 に示す。

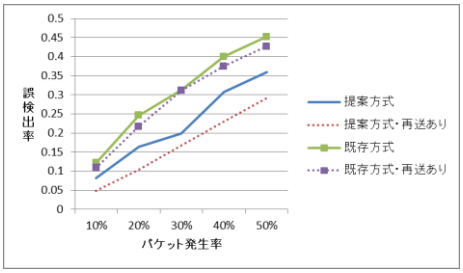

図 6-9　パケット発生率と誤検出率（再送あり）

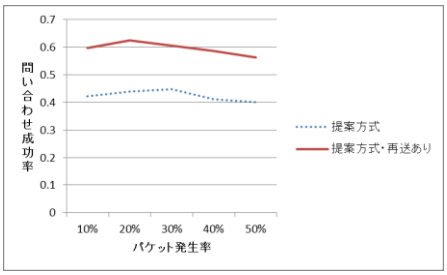

図 6-10　パケット発生率と問い合わせ成功率（再送あり）

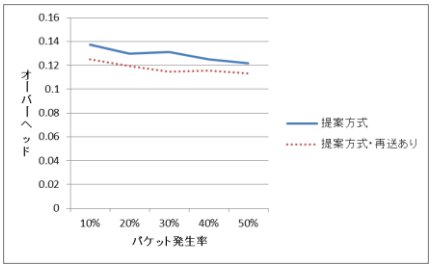

図 6-11　パケット発生率とオーバーヘッド（再送あり）

図 6-9 より、車間距離が 40m のとき、再送処理の導入は、提案方式に導入した場合は既存方式よりも誤検出率を抑える効果が大きいことがわかる。また、図 6-10 より、再送処理の導入により、0.2 ポイント程度、問い合わせ成功率を上昇させることがわかる。これは、中継車両の中継パケットの受信失敗により中継が行われないことによる誤検出が少なくなっているためである。

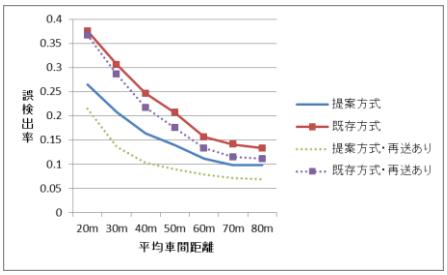

図 6-12　平均車間距離と誤検出率（再送あり）

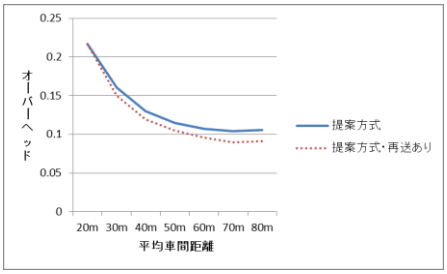

図 6-13　平均車間距離とオーバーヘッド（再送あり）

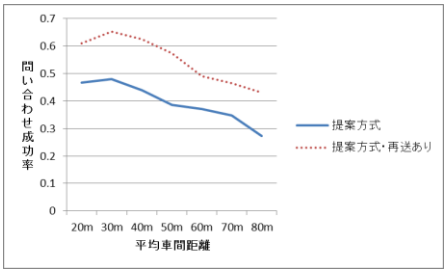

図 6-14　平均車間距離と問い合わせ成功率（再送あり）

図 5.13 より、既存方式に再送処理を導入したとき、車間

距離が広がるほど誤検出を抑える効果が大きく、提案方式に再送処理を導入したとき、車間距離 30m から 50m のときに最も効果が大きいことがわかる。

6.6 検出閾値の変化による両方式の比較

平均車間距離を 30m とし、パケット発生率を 10%から 50%、検出閾値（D）を 1 から 3 まで変化させながらシミュレーションを行い、その結果を図 6-15 から図 6-18 に示す。

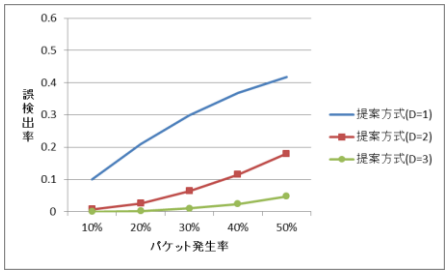

図 6-15　検出閾値を変化させた場合の誤検出率(提案方式)

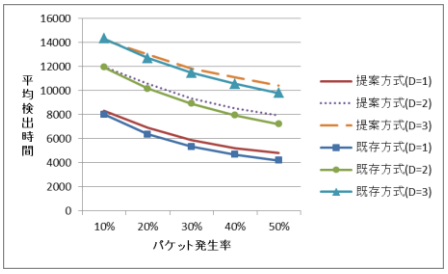

図 6-16　検出閾値を変化させた場合の平均検出時間

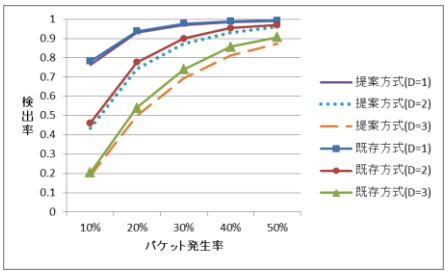

図 6-17　検出閾値を変化させた場合の検出率

図 6-15 より、検出閾値を大きくすることで、誤検出率を大きく低下させることが可能である。特に、検出閾値を 1 から 2 に変化させた場合の変化が大きい。また、検出閾値 3 のとき、提案方式では、ネットワーク混雑度が低いとき、誤検出率を 0.0001 以下に抑えることができており、ネットワーク混雑度が上がっても、0.05 程度までの誤検出率に抑えることができる。

図 6-16 より、検出閾値を大きくすると、攻撃者の検出にかかる時間が大きくなることがわかる。ネットワーク混雑度が低いとき、平均検出時間が大きくなり、検出閾値 1 のとき、8000ms 程度であるのに対し、検出閾値 2 のときは 12000ms、検出閾値 3 のときは 14000ms となる。また、提案方式では、問い合わせの応答の待ち時間があり、提案方式より 300ms 程度余分な検出時間がかかるため、検出時間が既存方式より大きくなる。

図 6-17 より、検出率は検出閾値を大きくすると低下することがわかる。特にネットワーク混雑度が低いときにその影響が大きく、検出閾値が 1 のときに 0.8 程度であるのに対し、検出閾値 3 では 0.2 程度まで低下する。

7. おわりに

7.1 まとめ

本稿では、車車間通信に関する脅威とその対策方法について検討し、車車間通信に関するセキュリティ・セイフティポリシを策定した。また、セキュリティ・セイフティポリシ実現のための問題点の 1 つである、パケット破棄攻撃に対する対策方式を提案し、提案方式の有効性を評価するためにシミュレーションを行い、既存の方式と比較を行った。シミュレーションの結果、提案方式は、車両密度による影響を大きく受け、車両密度が低くなると応答の成功率が低下し、提案方式の効果が低下するが、車間距離をすべての距離において提案方式が誤検出率を抑えることができていることがわかった。また、検出閾値の変化を 1 から 3 まで変化し、検出性能を比較した。

7.2 今後の課題

今後の提案方式の課題として、片側 2 車線の道路だけでなく、両側車線の道路や、平均速度の異なる道路など様々な道路状況を想定しシミュレーションを行い、変化する道路状況による最適な検出閾値の決定方法についての検討を行う必要がある。

また、セキュリティ・セイフティポリシ実現のための課題として、暗号化や署名を用いた車車間通信の実時間性に関しての別途考察・シミュレーションが必要である。

謝辞

本研究の一部は、平成 25 年度文部科学省科学研究費補助金基盤機構(C)(24500087,24500088)の支援を受けて行った。

参考文献

[1]　総務省,ITS 無線システムの高度化に関する研究会報告書, 平成 21 年 6 月

[2]　MARTI S. ,Mitigating Routing Misbehavior in Mobile Ad Hoc Networks ,Proceedings of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking, 2000

[3]　BUCHEGGER S. ,Performance analysis of the CONFIDANT protocol ,Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 2002, 2002

[4]　HADOF: defense against routing disruptions in mobile ad hoc networks, Wei Yu, INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, 13-17 March 2, 1252-1261, 2005

[5]　L.Buttyn and I.-P.Hubaux,Stimulation cooperation in self-organizing mobile ad hoc networks, Technical Report no.DEC/2001/046,Swiss Federal Institute of Technology,Lausanne,Aug.2001

[6]　内山 彰:MANET における複数共謀ノードによるパケットドロップ攻撃の検出手法の提案,IPSJ SIG Technical Report 2006-MBL-36

[7]　荻野 剛,DHT を用いた新しい Selfish Node の対策手法の提案,IPSJ SIG Technical Report 2006-DPS-126

[8]　Artisoc2.6Mas コミュニティ ,http://mas.kke.co.jp/modules/tinyd0/index/php?id=8