GN Workshop 2014
The 11th Workshop on Groupware and Network services

情報処理学会
グループウェアとネットワークサービス研究会
2014年11月27日, 28日

車車間通信環境における信頼度共有アルゴリズムを用いた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†

車車間通信システム上の脅威のうち１つとして、パケット破棄攻撃が存在する。車車間通信システムにおいて、既存のアドホックネットワーク向けの手法でパケット破棄攻撃に対策することは難しい。そこで、周辺の通信を監視することで攻撃を検知する既存方式を改善した方式を提案する。提案方式は、周辺ノードの信頼度を計算し、信頼度情報を共有することで、信頼度情報の統計から攻撃者を特定する新たな方式を提案する。本提案方式は、誤検出を抑え、パケット破棄を行う攻撃者を検出・特定できる特徴を有している。提案した手法に対し、シミュレーションを行い、誤検出率・検出率・検出時間といった項目を既存方法と比較し、提案方式の有効性を検証する。

A countermeasure against Packet Dropping Attacks with Confidence Share Algorism in VANET

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

One of the threats of inter-vehicle communication systems, packet dropping attack exists. On the inter-vehicle communication systems, it is difficult to take measures against a packet dropping attack by existing technique suggested for ad hoc networks. Improving existing technique by introducing index of Confidence between vehicle nodes, we propose Confidence Share Algorism that aims for reducing misdetection. This algorism calculates Confidence of around vehicle nodes; shares index of Confidence with around vehicle nodes, and detects attackers by shared Confidence. In this paper, we estimate the proposed method by simulation and compare the ratio of misdetection, detection and detection time with the existing method.

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、交通事故の減少は渋滞の解消に役立つことが期待されている。しかし、車車間通信システムには様々な脅威が存在する。車車間通信において発生することが予想される脅威[1]を表１に示す。

車車間通信システムにおいて発生が予想される脅威には、改ざん、なりすまし、盗聴、偽の情報の送信、パケット破棄攻撃、ルーティングに対する攻撃など、様々な脅威が存在する。特に、自動車システムにおいて発生する脅威の中でも、中継すべきパケットを中継せず破棄するパケット破棄攻撃への対策は従来のアドホックネットワーク向けに提案された方法では第２章で述べたように難しい。車車間通信の環境では、各車両が高速で移動し、ネットワークの構成は頻繁に変化する上、不特定多数の車両と通信を行うため事前に通信相手のする情報を入手しておくことは難しく、外部ネットワークからの情報の入手も行えない可能性があるためである。そこで本論文では、車車間通信システム向けのパケット破棄攻撃への対策手法について提案し、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。本論文の構成は以下のとおりである。2 章ではアドホックネットワーク向けに提案されているパケット破棄攻撃の対策の既存手法について述べる。3 章では提案方式について述べる。4 章では本研究で行った評価実験について述べる。5 章では評価実験の結果について考察する。6 章では、本論文で述べたことをまとめる。

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。
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. 関連研究

2.1 中継監視を行う方法

2.1.1 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

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

でパケットの中継を監視する。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。単独で監視と検出を行うタイプの方式と、監視結果をネットワークで共有し協調動作しながら攻撃者を検出するタイプの方式の２つが存在する。

Watchdog & Pathrater[2]や AODV-BDA[3]、AODV に監視機能を追加した手法[4]、Spontaneous Watchdog 方式[5]、Witness 方式[6]、CONFIDANT[7]などがある。

2.1.2 問題点

単独で車両の監視・検出を行う方法には、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。[8]

監視結果をネットワーク内で共有し、協調動作を行って攻撃者を検出する方法は、誤検出を低く抑えられるが、虚偽の情報への耐性が低い、または考慮されていないという問題や、外部ネットワークから信頼できるノードのリストを入手することが前提となっており、車車間通信の環境では利用に適さないという問題がある。

2.2 レポート交換を用いる方法

2.2.1 特徴

ネットワーク上でノードが隣接ノードの動作を記録し、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手法である。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方法である。HADOF[9]。Voting based scheme[10]、SAODV[11]などの方法がある。

2.2.2 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、ネットワークに参加するノード数が増加するとオーバーヘッドが大きくなり、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、レポートチェックが正しく行えない可能性がある。

2.3 インセンティブプライシングを用いる方法

2.3.1 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手法である。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。Nuglets[12]、貢献度の高いノード同士で信頼性の高いルートを構成する手法[13]、DHT を用いたポイント管理を行う手法[14]などがある。

2.3.2 問題点

ネットワークに対して積極的な貢献を促すインセンティブを与え、貢献していないノードにペナルティを与えることで、利己的な理由でパケット中継をしないノードをネットワーク参加させることが可能である[15]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ず、攻撃者の検出をする機能を持たない。また、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。

2.4 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 2 にまとめる。単独で中継の監視を行う方式は、外部の機構を必要とせず、比較的小さなオーバーヘッドで素早く攻撃者の検出が可能である。しかし、無線ネットワークでは隠れ端末問題により通信の衝突が発生するため、通信の衝突による監視の失敗と誤検出が避けられないことが欠点である。単独での監視を行う方法誤検出により、正当なノードがルーティングから除外されることで、ネットワークが分断され目標車両までのパスが消滅するなどネットワーク全体のパフォーマンスの低下が低下する。

それぞれの方式は一長一短であるが、本論文では、中継監視方式の誤検出率の低減を目標とし、監視結果をネットワーク内で信頼度情報として交換し、信頼度情報の統計から攻撃者の検出を行う信頼度共有アルゴリズムを提案する。

表 2　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	特別な機能
中継監視（単独）	**早い**	高い	**小さい**	**不要**
中継監視（協調動作）	中程度	**低い**	中程度	それぞれの方式に依存
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

3. 提案方式

3.1 提案方式の前提条件

3.1.1 暗号化・署名・認証

各ノードは暗号化、署名を行って通信を行い、パケットの改竄攻撃は検知可能である。暗号化通信の鍵共有問題については、ID ベースの公開鍵暗号[16]を用いるなどの方法で解決されているものとし、本提案方式では更なる検討をしない。また、ネットワークには認証された車載器のみが参加可能であり、なりすましなどは行われない。

3.1.2 マルチホップ通信

各車両は、通信を行う際に、宛先の車両が自身の通信範囲内に存在しない場合、周辺車両にパケットの中継を行わせることで宛先の車両へパケットを送信する。パケットの

中継は１台の中継車両が選ばれるものとし、フラッディングによる通信は行わないものとする。

3.1.3 想定する攻撃者と攻撃方法

本研究では、パケットを破棄する攻撃者と虚偽の情報を送信する攻撃者の２つを想定する。

パケットを破棄する攻撃者は、自身が中継車両として指定されたパケットを受信しても、パケットの中継を行わずにパケットを破棄する。

虚偽の情報を送信する攻撃者は、パケットを破棄する攻撃に加え、周辺車両の信頼度の計算を正しく行わず、取りうる範囲の最低の信頼度を送信する。

また、実際の車車間通信環境上ではパケット破棄攻撃だけでなくデータ内容の改ざん等の他の攻撃を同時に行う攻撃者が存在することは十分に考えられるが、パケット破棄攻撃以外の攻撃には本研究の提案方式と併せて他の方法を用いることで対策を行うものとする。

3.2 提案方式のアルゴリズム

提案方式は、大きく分けて３つのステップで動作する。

3.2.1 信頼度の計算

各車両は、周辺車両の通信を監視し、監視結果からそれぞれの車両についての信頼度を計算する。信頼度の計算は以下の手順で行う。

① 周辺車両のパケット中継動作を監視
② パケットの中継が確認できれば信頼度を増加
③ パケットの中継が確認できなければ信頼度を減少

3.2.2 信頼度の共有

計算した周辺車両の信頼度情報を周辺車両と共有する。以下の手順で行う。

① 計算した周辺車両についての信頼度を HELLO メッセージ等に付加して交換する
② 受け取った各車両についての信頼度の平均値をその車両の総合的な信頼度とする

3.2.3 攻撃者の検出

周辺車両の信頼度情報に外れ値の検出処理を行い、外れ値として検出された信頼度をもつ車両を攻撃者と判断する。以下の手順で処理を行う。

① 周辺車両の信頼度情報に対し、外れ値の検定を行う
② 外れ値として検出されたものは攻撃者と判断する

外れ値の検出処理は以下の計算方法で行う。

μ はネットワーク内の車両の信頼度の平均とする。

σ はネットワーク内の車両の信頼度の標準偏差とする。

X_a は車両 A の信頼度とする。

λ は検出する信頼度の境界を決定するための定数であり、以後検出閾値と呼ぶ。

各車両に対して以下の式が成り立つがチェックを行う。

$$X_a < \mu - \lambda \cdot \sigma$$

成り立つ場合、車両 A を攻撃者として検知する。

攻撃者として検知された車両はパケット中継の候補から除外され、パケットの中継を行わせない。

4. シミュレーション

4.1 シミュレーション条件

マルチエージェントシミュレータ Artisoc2.6[17]を用いて提案方式と既存方式それぞれについてシミュレーションを行う。シミュレーション条件を表 3 に示す。

シミュレーションエリアは片側 2 車線の直線 500m とし、車両速度は第 1 車線を平均時速 50km、第 2 車線を平均時速 60km とする。ドライバモデルは最適速度モデル[18]を使用した。パケット発生間隔は平均 1000ms のポアソン分布で決定し、ネットワーク内のうちパケット発生率の割合の車両がパケットを生成する。ネットワーク内の攻撃者の割合は 0.2 とする。通信距離は 100m とする。平均車間距離を変化させずにパケット発生率を 10~50%に変化させる場合と、パケット発生率を変化させずに平均車間距離を 20~60m に変化させる場合に対してシミュレーションを行い、それぞれの結果に対して評価を行う。

提案方式は閾値 λ が 1.25,1.5,1.75,2.0 の場合それぞれに対してシミュレーションを行う。既存方式ではパケットの破棄を検出した回数が閾値以上となった車両を攻撃者として検知する手法を比較対象とし、閾値 T が 1,2,3,4 の場合に対してシミュレーションを行う。シミュレーションは、1 時間分のシミュレーションをそれぞれの条件に対して 10 回実行し、それぞれの値の平均を結果とした。評価項目は、誤検出率・検出率・検出時間について評価する。

表 3 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	第 1 車線・平均 50km/h 第 2 車線・平均 60km/h
ドライバモデル	最適速度モデル
平均車間距離	20m, 30m, 40m, 50m, 60m, 70m, 80m
通信距離	100m
パケット発生間隔	平均 1000ms（ポアソン分布）
パケット発生率	0.1, 0.2, 0.3, 0.4, 0.5
攻撃者の割合	0.2
シミュレーション時間	1 時間（10 回）
閾値 T（既存方式）	1, 2, 3, 4
閾値 λ（提案方式）	1.25, 1.5, 1.75, 2.0

4.2 評価項目

4.2.1 誤検出率

誤検出率は、正当な車両が誤検出される確率を示す。

正当な車両の数を Number of Normal Vehiles、誤検出された車両の数を misDetected とし、以下の計算方法で求める。

$$MR = \frac{misDetected}{Number\ of\ Normal\ Vehicles}$$

誤検出率が大きい場合、ネットワーク内の多くの車両がネットワーク中継の候補から除外され、目標までのルートの消失などネットワーク全体のパフォーマンスに悪影響を与える。誤検出率は低ければ低いほど検出性能が高いと評価できる。

4.2.2 検出率

検出率は、ネットワークに参加した攻撃者が、目標距離を走行するまでに攻撃者として検出できる確率である。今回の実験では、500m を目標距離としている。

攻撃者全体の合計数を Number of Attackers、検出された攻撃者の合計を DetectedAttackers として、検出率は以下の計算方法で求める。

$$DR = \frac{DetectedAttackers}{Number\ of\ Attackers}$$

検出率は高ければ高いほど検出性能が高いと評価できる。

4.2.3 検出時間

検出時間は、攻撃者が最初に攻撃を行ってから攻撃者を検出するまでにかかる平均時間である。

各攻撃者の検出にかかった時間の合計を TotalDetectTime、検出された攻撃者の合計を DetectedAttackers として、以下の計算方法で求める。

$$DT = \frac{TotalDetectTime}{DetectedAttackers}$$

検出時間は低ければ低いほど検出性能が高いと評価できる。

4.3 シミュレーション結果

4.3.1 平均車間距離の変化と検出性能の変化

パケット発生率 30%、平均車間距離を 20m から 60m まで変化させながらシミュレーションを行った結果を図 1、図 2、図 3 に示す。図 1 は誤検出率、図 2 は検出率、図 3 は検出時間の結果を示す。

図 1 より、既存方式は平均車間距離の影響を受けやすく、平均車間距離が小さくなるほど誤検出率が高くなる傾向にあることがわかる。既存方式は閾値 T が 1 のとき、非常に誤検出率が高くなり、誤検出率は 20~50%となる。閾値を大きくするほど誤検出率は低くなり、T=4 のとき、0.05%~5%の誤検出率となる。

提案方式は閾値λが 1.25 のとき、誤検出率は 1~9%程度となる。閾値を大きくするほど誤検出率は低くなり、λ=2.0 のとき、誤検出率は平均車間距離が 20~60m 全ての場合で 0.01%以下となる。提案方式も既存方式と同様に平均車間距離によって誤検出率が高くなる傾向があるが、その影響は既存方式に比べて小さい。

図 2 より、既存方式では、平均車間距離の変化の影響は小さいことがわかる。検出率は T=1 のとき、99%以上の検出率があり、ほとんどの攻撃者を検出可能である。T を大きくするごとに検出率は低下していき、T=4 の時の検出率は 87~90%程度まで低下する。

提案方式は閾値λが 1.25 のとき、98~99%の検出率がある。提案方式はλを大きくするごとに検出率は低くなり、λ=2.0 のとき、検出率は 30~85%になる。提案方式の検出率は車間距離の影響が大きく、平均車間距離が 20m の場合は 85%程度の検出率があるが、平均車間距離が 60m の場合は 30%まで検出率が低下する。

図 3 より、既存方式は平均車間距離が変化しても、検出時間はあまり変化せず、車両密度の変化の影響を受けにくいことがわかる。既存方式では、T=1 の場合が最も検出時間が短く、1050~1100ms 程度で検出可能である。T を大きくするごとに攻撃者の検出に必要となる検出時間も大きくなっていき、T=4 のとき約 13000~13700ms 程度の検出時間が必要となる。

提案方式では、λ=1.25 の場合が最も検出時間が短く、約 860~3000ms で攻撃者を検出可能である。λを大きくすると検出に必要となる時間も大きくなり、λ=2.0 の場合には検出時間は 11200ms~18100ms まで大きくなる。また、平均車間距離が大きくなるごとに検出にかかる時間も大きくなる傾向にあり、提案方式の検出時間は平均車間距離の影響を受けやすい。

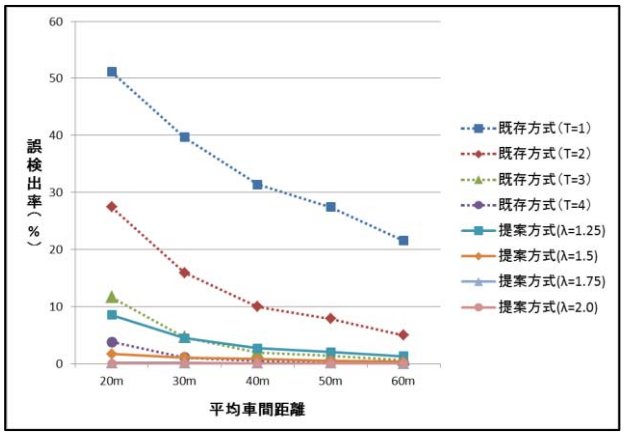

図 1　平均車間距離が変化した場合の誤検出率

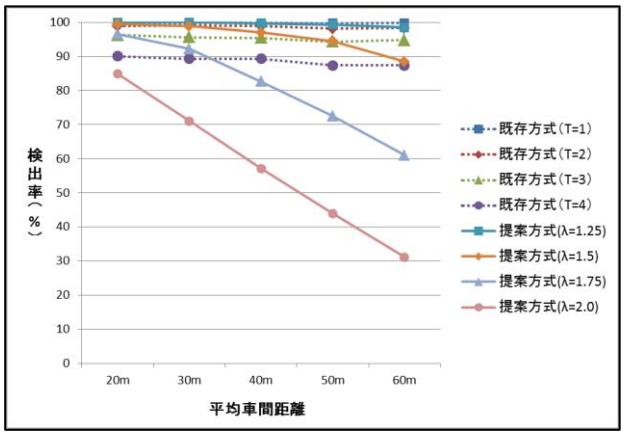

図 2　平均車間距離が変化した場合の検出率

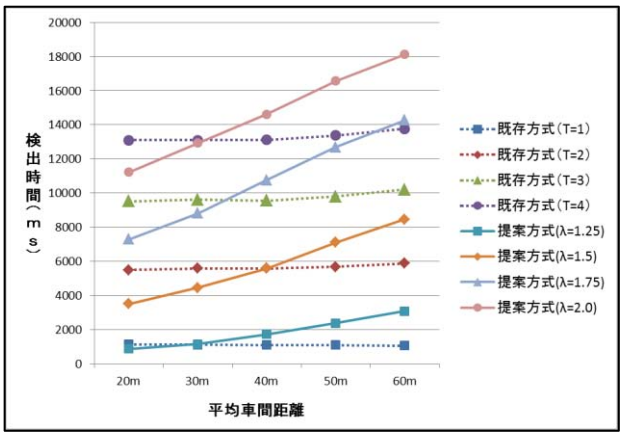

図 3　平均車間距離が変化した場合の検出時間

4.3.2 パケット発生率の変化

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った結果を図 4、図 5、図 6 に示す。図 4 は誤検出率、図 5 は検出率、図 6 は検出時間の結果を示す。

図 4 より、既存方式はパケット発生率が高くなるほど、誤検出率も高くなることがわかる。閾値 T=1 の場合、誤検出率は 7~45%程度まで変化する。T=2 の場合は 0.3%~26%、T=3 の場合は 0.03%~12%、T=4 の場合は 0.01%~4%まで変化する。

提案方式の誤検出率は、λ=1.25 の場合は 0.5%~4%、λ=1.5 の場合は 0.08%~1.7%、λ=1.75 の場合は 0.009%~0.2%、λ=2.0 の場合は 0.001%~0.004%まで変化する。また、提案方式の誤検出率も既存方式と同様にパケット発生率が大きくなると誤検出率が高くなる傾向にあるが、その影響は既存方式よりも小さい。

図 5 より、既存方式はパケット発生率が高くなるほど、検出率も高くなることがわかる。閾値 T=1 の場合、検出率は 98~99%の検出率があり、ほとんどの攻撃者を検出可能である。T=2 の場合は 75%~99%、T=3 の場合は 50%~99%、T=4 の場合は 27%~98%まで変化する。

提案方式の誤検出率も既存方式と同様に、パケット発生率が高くなるほど検出率は増加する。λ=1.25 の場合は 92%~99%、λ=1.5 の場合は 76%~99.4%、λ=1.75 の場合は 57%~93%、λ=2.0 の場合は 36%~67%まで変化する。

図 6 から、既存方式はパケット発生率が高くなるほど検出時間が減少することがわかる。閾値 T=1 の場合、パケット発生率の変化による影響は小さく、780ms~1160ms 程度の検出時間で攻撃者を検出できる。T=2 の場合は 4550ms~8300ms、T=3 の場合は 7600ms~13800ms、T=4 の場合は 10650ms~17100ms まで変化する。

提案方式の検出時間は、閾値 λ=1.25 または 1.5 のとき検出時間はパケット発生率が大きくなるほど検出時間が減少し、λ=1.75 の場合パケット発生率の変化による影響は小さく、λ=2.0 の場合パケット発生率が高くなると検出時間は増加する。閾値 λ=1.25 の場合 1250ms~3000ms、λ=1.5 の場合は 4200ms~6600ms、λ=1.75 の場合は 9550ms~10550、λ=2.0 の場合は 12100ms~14600ms まで変化する。

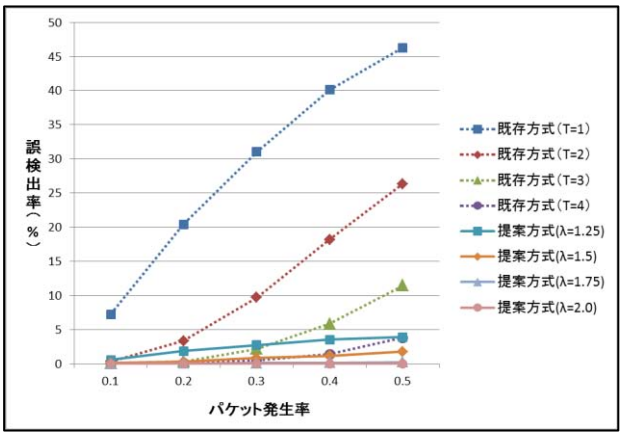

図 4　パケット発生率が変化した場合の誤検出率

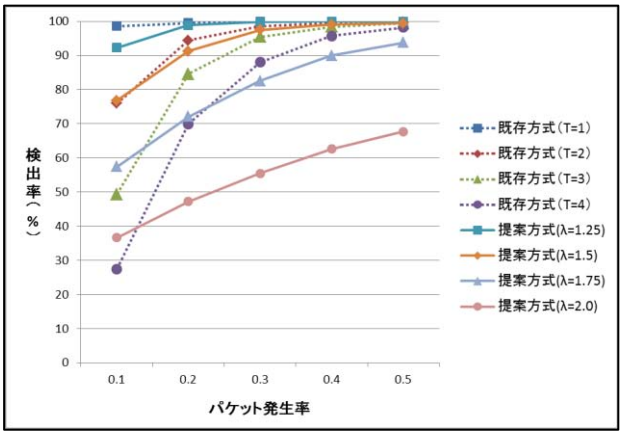

図 5　パケット発生率が変化した場合の検出率

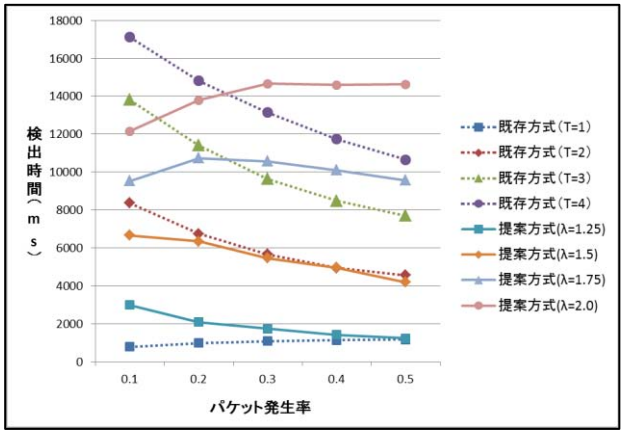

図 6　パケット発生率が変化した場合の検出時間

4.3.3 虚偽の信頼度情報を送信する攻撃者が存在する環境での検出性能（平均車間距離を変化）

虚偽の信頼度情報を送信する攻撃者が存在する場合に関してパケット発生率 30%、平均車間距離を 20m から 60m まで変化させながらシミュレーションを行った結果を図 7、図 8、図 9 に示す。図 7 は誤検出率、図 8 は検出率、図 9 は検出時間の結果を示す。

図 7 より、虚偽の信頼度情報を送信する攻撃者が存在する場合、提案方式の誤検出率はやや増加する。λ=1.25 の場合は通常の攻撃者の場合であれば誤検出率は

1.25%~8.4%、虚偽の情報を送信する攻撃者の場合であれば誤検出率は 1.7%~8.8%となり、約 0.4%程度誤検出率が増加する。λ=1.5 の場合は虚偽の情報を送信する攻撃者が存在する場合に誤検出率は最大で 0.1%増加する。λ=1.75 の場合は最大で 0.3%、λ=2.0 の場合は 0.006%増加する。特に閾値の小さい場合に虚偽の信頼度情報を送信する攻撃者の影響を受けやすい。

図 8 より、虚偽の信頼度情報を送信する攻撃者が存在する場合、提案方式の検出率は増加する。λ=1.25 の場合は最大で 0.5%、λ=1.5 の場合は最大で 5%、λ=1.75 の場合は最大で 20 %、λ=2.0 の場合は最大で 30%の検出率が増加する。特に閾値が大きい場合に信頼度を送信する攻撃者が存在する環境で検出率が上昇する。

図 9 より、虚偽の信頼度情報を送信する攻撃者が存在する環境では、閾値が低い場合は検出時間が増加し、閾値が大きい場合では検出時間は減少する。虚偽の信頼度情報を送信する攻撃者が存在する環境では λ=1.25 の場合検出時間が 200ms~1000ms 増加、λ=1.5 の場合は 500ms~1400ms 増加、λ=1.75 の場合は平均車間距離 20m のとき 400ms 増加、平均車間距離 60m のとき 150ms 減少数する。λ=2.0 の場合、検出時間は 1400ms 減少する。

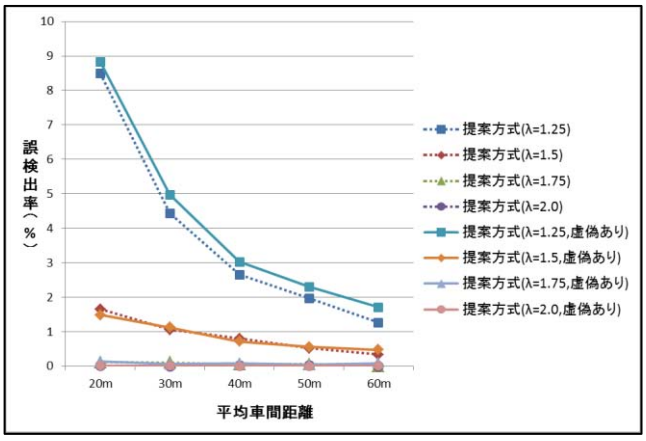

図 7　虚偽の信頼度情報を送信する攻撃者と誤検出率
（平均車間距離を変化）

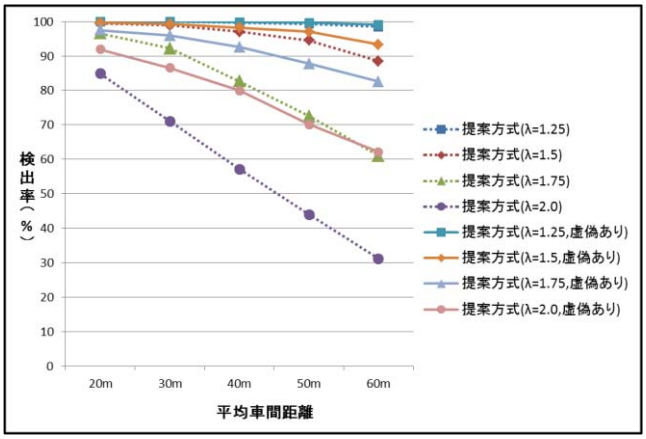

図 8　虚偽の信頼度情報を送信する攻撃者と検出率
（平均車間距離を変化）

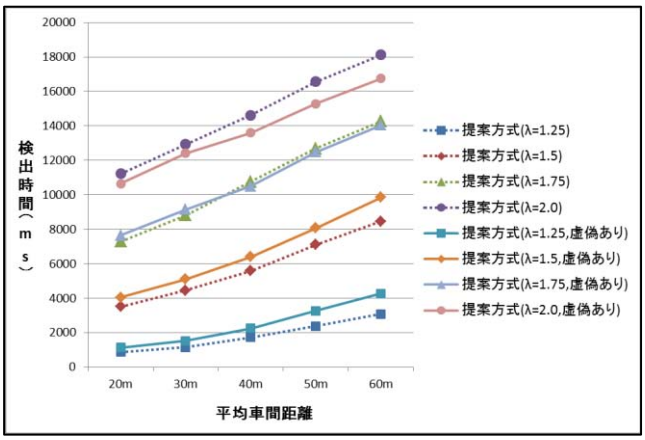

図 9　虚偽の信頼度情報を送信する攻撃者と検出時間
（平均車間距離を変化）

4.3.4 虚偽の信頼度情報を送信する攻撃者が存在する環境での検出性能（パケット発生率を変化）

虚偽の信頼度情報を送信する攻撃者が存在する場合に関して平均車間距離 40m として、パケット発生率 10%から 50%まで変化させシミュレーションを行った結果を図 10、図 11、図 12 に示す。図 10 は誤検出率、図 11 は検出率、図 12 は検出時間の結果を示す。

図 10 より、虚偽の信頼度情報を送信する攻撃者が存在する場合、誤検出率はやや増加する傾向にあることがわかる。特に、閾値が小さいほど影響を受けやすい。

虚偽の情報を送信する攻撃者が存在する場合、λ=1.25 の場合は最大で 0.7%、λ=1.5 の場合は最大で 0.1%、λ=1.75 の場合は最大で 0.09%、λ=2.0 の場合は最大で 0.01%増加する。

図 11 より、虚偽の信頼度情報を送信する攻撃者が存在する場合、提案方式の検出率は増加する。特に、閾値が大きい場合、影響を受けやすい。
λ=1.25 の場合は最大で 3%、λ=1.5 の場合は最大で 9%、λ=1.75 の場合は最大で 16%、λ=2.0 の場合は最大で 24%増加する。

図 12 より、虚偽の信頼度情報を送信する攻撃者が存在する環境では、パケット発生率が小さい場合検出時間が低下し、パケット発生率が大きい場合は検出時間が増加する傾向にある。

λ=1.25 の場合パケット発生率 0.1 のとき 300ms 低下し、パケット発生率が 0.5 のとき 500ms 増加する。λ=1.5 の場合パケット発生率 0.1 のとき 1000ms 低下し、パケット発生率が 0.5 のとき 1500ms 増加する。λ=1.75 の場合パケット発生率 0.1 のとき 1300ms 低下し、パケット発生率が 0.5 のとき 500ms 増加する。λ=2.0 の場合パケット発生率 0.1 のとき 1800ms 低下し、パケット発生率が 0.5 のとき 200ms 低下する。

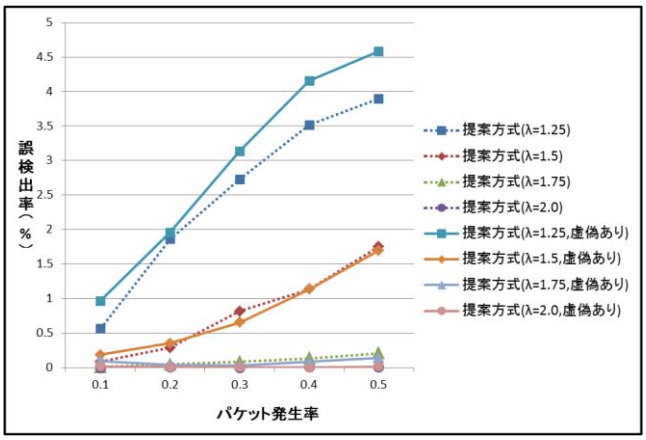

図 10　虚偽の信頼度情報を送信する攻撃者と誤検出率
（パケット発生率を変化）

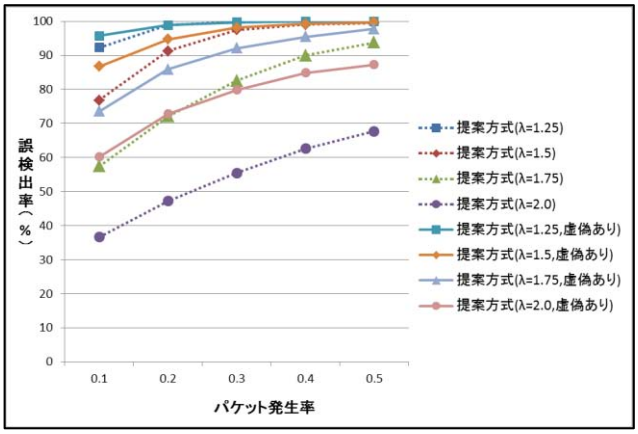

図 11　虚偽の信頼度情報を送信する攻撃者と検出率
（パケット発生率を変化）

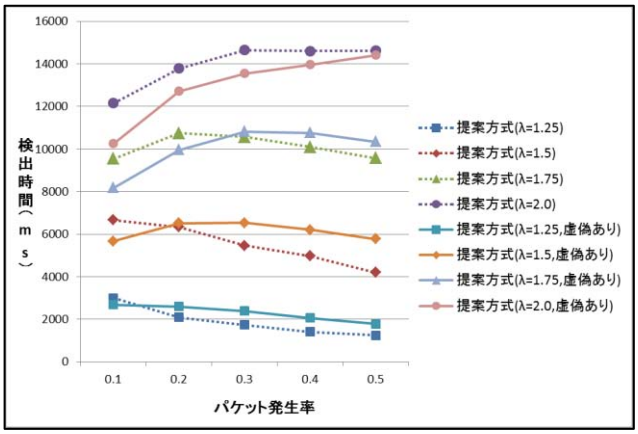

図 12　虚偽の信頼度情報を送信する攻撃者と誤検出率
（パケット発生率を変化）

5. 考察

5.1 平均車間距離の変化と検出性能

結果より、どの平均車間距離であっても既存方式は誤検出率を抑えることができることがわかる。

また、既存方式は平均車間距離が小さくなることにより、誤検出率が増加するが、これは車両密度が増加することで通信の衝突によるパケットロスと監視の失敗が発生しやすくなったためだと考えられる。

提案方式は平均車間距離が小さくなるほど検出時間・検出率の性能が向上するが、これは車両の密度が高くなることで信頼度情報のデータ数が多くなり、より早く正確な統計を取ることが可能になるためであると考えられる。

5.2 パケット発生率の変化と検出性能

結果より、どのパケット発生率であっても提案方式は誤検出率を抑えることに成功していることがわかる。

また、既存方式・提案方式ともにパケット発生率が高くなることで誤検出率が増加する傾向にあるが、これはネットワークが混雑することで通信の衝突が頻発するようになり、パケットの中継の監視に失敗するためであると考えられる。既存方式に比べて提案方式はパケット発生率が増加することによる誤検出率への影響が小さいが、これは信頼度情報の統計から相対的に攻撃者を判断しているため、監視の失敗が発生しやすい環境であっても正確に攻撃者を判断できるためであると考えられる。

パケット発生率が小さくなることで既存方式・提案方式ともに検出率が低下し、検出時間も大きくなっているが、これは通信が行われる回数が減ることにより、攻撃者が中継車両として選ばれる回数そのものが減り、結果として攻撃回数が減っているため、攻撃者が検出されにくくなっていると考えられる。

5.3 提案方式と既存方式の比較

図 1、図 2、図 3 の結果から、提案方式と既存方式を比較する。

既存方式の T=1 と提案方式の λ=1.25 の結果を比較すると、提案方式は車間距離の大きな環境では検出時間が 2000ms ほど増えてしまうが、誤検出率は 20~43 ポイントほど減少させることに成功している。既存方式の T=2 と提案方式の λ=1.25 を比較すると、提案方式は誤検出率を 3~19 ポイント減少させ、検出時間も 2800ms~4500ms 減少させることができる。既存方式の T=と提案方式の λ=1.5 を比較すると、提案方式は誤検出率を 0.3~10 ポイント減少させ、検出時間は 1500ms~6000ms 減少させることが可能である。既存方式の T=4 と提案方式の λ=1.75 を比較すると、誤検出率は 0.05~3 ポイント減少させることができ、検出時間は平均車間距離が 60m の場合は 500ms 程度増加してしまうが、平均車間距離が 20m の場合は 5800ms 減少させることができる。提案方式の λ=2.0 は、検出時間が多くかかるが、本論文で行ったシミュレーションの全ての場合で誤検出率は 0.01%以下となり、非常に検出率を低く抑えることが可能である。

提案方式には、既存方式の T=1、T=2、T=3、T=4 それぞれに対してより効果的に誤検出率を低下させることのできる閾値が存在する。そのため、ネットワーク環境に合わせて閾値を選択することで、提案方式はより効果的に誤検出を抑えることが可能であるといえる。

5.4 検出閾値の変化と検出性能

結果より、提案方式では検出速度と誤検出率はトレードオフの関係にある。そのため、ネットワークの状況や要求される検出時間等に合わせて検出閾値を変更する必要がある。また、一度ブラックリストに追加され、ネットワークから追放された車両が時間経過により再度ネットワークに復帰可能であり、ブラックリストに登録される度に指数関数的に復帰に必要となる時間を増加させることで、攻撃ノードのみをネットワークから排除することを目標とする適応型ブラックリスト[19]などの手法と併用することで、検出閾値を小さくし検出速度を早くした上で、発生する誤検出の影響を最小限に抑えることが可能であると考えられる。

5.5 虚偽の信頼度情報を送信する攻撃者と検出性能

結果より、虚偽の信頼度情報を送信する攻撃者が存在する環境であっても提案方式が動作可能であることがわかる。虚偽の信頼度情報が送信されることで誤検出率はやや増加するが、最大でも 0.7%誤検出率が増加する程度であり、ネットワークのパフォーマンスへの影響は大きくない。

また、閾値が高い場合などでは、攻撃者が虚偽の情報を送信すると、検出率や検出時間の性能が向上する。これは虚偽の信頼度情報が送信され通常の車両の信頼度が低下させられることで、通常の信頼度の分布に比べ、初期値の信頼度である 0 付近に多くの信頼度が集まり標準偏差が小さくなることが影響している。標準偏差が小さくなることで同じ閾値であっても攻撃者として検出される信頼度の有意点が高くなり、攻撃者が検出されやすくなるためであると考えられる。

6. おわりに

車車間通信環境向けのパケット破棄攻撃への対策手法として、信頼度情報を共有し、集めた信頼度の情報から統計的に攻撃者を検出する、信頼度共有アルゴリズムを提案した。本アルゴリズムにより、ネットワークの状況から統計的に攻撃者を判断することで、効果的に誤検出を低減可能である。

提案手法と既存手法に対してシミュレーションを行い、誤検出率、検出率、検出時間の３つの項目から提案手法と既存手法を比較した。比較の結果から、提案手法は検出率や検出時間の性能の低下を最小限に抑えながら、効果的に誤検出を低減させることが可能であることを示した。

また、提案手法について虚偽の信頼度情報を送信する攻撃者が存在する環境についてもシミュレーションを行い、提案方式が虚偽の信頼度情報を送信する攻撃者が存在する環境においても動作可能であることを示した。

今後の課題としては、選択的にパケットを破棄する攻撃者に関する検討や、変化する道路状況に対する最適な閾値の決定方法に関する検討が挙げられる。

謝辞

本研究の一部は、平成 26 年度文部科学省科学研究費補助金基盤研究(C)(24500087, 24500088)の支援を受けて行った。

参考文献

[1] 運転支援通信システムに関するセキュリティガイドライン「ITS FORUM RC-009 1.0 版」, ITS 情報通信システム推進会議,2011.
[2] MARTI S. ,Mitigating Routing Misbehavior in Mobile Ad Hoc Networks ,Proceedings of the Sixth annual ACM/IEEE International Conference onMobile Computing and Networking, 2000
[3] ビザンチン攻撃の検出と回避を考慮した Hop by Hop ベースルーティングプロトコルの提案と実装・評価,森 郁海,IEICE Technical Report MoMuC2008-24
[4] 周辺ノードの相互監視情報に基づく AODV における不正ノードの検出と対策,朴 在赫,電子情報学会論文誌 A vol.J92-A No.3 pp.150-162
[5] R.Roman,J.Zhou,and J.Lopez.Applying Intrusion Detection Systems to Wireless Sensor Networks.In Proceetings of Consumer Communications and Networking Confence (CCNE'06) , pp.640-644
[6] アドホックネットワークにおける高精度な不正動作ノードの検出と防御方式の提案および実装評価,横山 信,情報処理学会論文誌 Nol.49.No.2,2008
[7] BUCHEGGER S. ,Performance analysis of the CONFIDANT protocol , Pro-ceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Net-working and Computing, June 2002, 2002
A.shamir,"Identity-basedcryptosystemand signature schemes".In Proc.
[8] 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
[9] WeiYu, HADOF: defense against routing disruptions in mobile ad hoc networks, INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, 13-17March 2, 1252-1261,2005
[10] C.Crepeaw,C.R.Davis,A Certifiate Revocation Scheme for Wireless Ad Hoc Networks,Proc. Of ACm Workshop Security of Ad Hoc and Sensor Network,
[11] M.G.Zapata and N.Asokan Securing Ad hoc Routing Protocols , In Proceedings of the ACM workshop on Wireless Security,2002
[12] 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
[13] 松嶋 一樹,アドホックネットワークにおける信頼度情報に基づく利己的な端末の検出及びルーティング方式の提案,情報処理学会創立 50 周年記念（第 72 回）全国大会 3Z-6
[14] 荻野剛,DHT を用いた新しい Selfish Node 対策手法の提案,IPSJ SIG Technical Report 2006-DPS-126
[15] 佐藤 文明,MANET におけるノードの信頼度を用いた利己的ノードの検出方法, IPSJ SIG Technical Report 2008-DPS-137
[16] A.shamir,"Identity-based cryptosystem and signature schemes".In Proc. CryPTO1984,volume 196 of Lecture Notes in Computer Science,pp47-53.Springer-verlag,1985.
[17] Artisoc2.6Mas コミュニティ http://mas.kke.co.jp/modules/tinyd0/index/php?id=8
[18] Bando,M.,Hasebe,K.,Nakagawa,A.,Shibata,A.,Sugiyama,Y.,et al:Dynamical model of traffic congestion and numeriacal simulation,Physical review.E,Statisical physics,plasmas,fluids,and related interdisciplinary topics, Vol.51,No.2,pp.1035(1095)
[19] 佐藤 研, 適応型ブラックリストを用いたブラックホール攻撃の防御法, IEICE Technical Report NS2007-197,2008