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に関する研究

加藤　平成　　指導教員：井手口 哲夫

1　はじめに

近年,車車間通信を用いた安全運転支援システム等が実用化に向けて盛んに研究されている.車車間通信を用いた運転支援システムが実現すれば,事故の回避や渋滞の解消などへの活用が期待できる.しかし,車車間通信にはセキュリティ上の課題がいくつか存在する.特に,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難しい.本論文は,車車間通信環境向けのパケット破棄攻撃への対策手法を提案・評価する.

2　提案方式

提案方式は,互いの通信を監視しながら監視結果を信頼度情報として共有し協調して動作することで,車車間通信環境であっても誤検出を抑え,より素早く攻撃者を検出することを目標とする方式である.

提案手法の大きな特徴として以下の３点が挙げられる.

- 常に互いの通信を監視し素早く攻撃者を検出する
- 信頼度情報を共有することで誤検出を抑える
- 共有された信頼度情報から統計的に攻撃者を判断することでネットワーク環境の変化に強い

提案方式は信頼度の計算,信頼度の共有,攻撃者の検出の３つのステップで構成される.

① 各車両は,周辺車両の通信を監視し,正しく中継している車両の信頼度を増加,中継が確認できない車両の信頼度を減少しそれぞれの車両についての信頼度を決定する.
② 各車両の信頼度情報を周辺車両と共有する.
③ 受け取った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.

信頼度の計算方法は,タイプ A,タイプ B の２つの計算方法を使用する.

タイプ A

① パケットの中継が確認できた場合,信頼度を+1
② パケットの中継が確認できない場合,信頼度を-1

タイプ B

① パケットの中継が確認できた場合,信頼度を+1
② パケットの中継が確認できない場合,今までにパケットの中継を確認できなかった回数の 2 乗を信頼度から引く

タイプ A は,単純に信頼度を１ずつ増減し,タイプ B は中継が確認できない場合に-1,-4,-9 という形で信頼度が減少する方式である.

攻撃者の特定に関する外れ値の検出処理は, τ_a を車両 A の信頼度, μ を信頼度の平均値, C を検出のために用いる定数, σ を標準偏差とし,

$$\tau_a < \mu - C \times \sigma$$

が成り立つとき,車両 A を攻撃者として判断し,今後パケットの中継を行わせない.

3　評価実験

本研究で使用したシミュレーション条件を表 1 に示す.シミュレーションエリアは片側２車線 500m,平均速度は第 1 車線が 40km/h,第 2 車線が 50km/h とし,ドライバモデルは最適速度モデル[1]を使用する.攻撃者の割合は 0.2 とする.各車両は毎秒 0.3 の確率でパケットを生成する.提案方式の閾値 C は 1.25 から 2.0 まで 0.25 間隔,既存方式の閾値 T は 1 から 4,平均車間距離は 20m から 60m まで 10m 間隔で変化させながら各条件のシミュレーションを行う.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 を使用する.

提案方式は信頼度の計算方法タイプ A,タイプ B の２つに対してシミュレーションを行い,信頼度の計算方法タイプ A を使用したものを提案方式 A,タイプ B を使用したものを提案方式 B と呼ぶ.

表 1　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
通信距離	100m
パケット発生間隔	平均 1000ms
パケット発生率	0.3
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 C（提案方式）	1.25,1.5,1.75,2.0

また,本シミュレーションで比較対象として使用する既存方式のアルゴリズムは以下のように動作する.

① 自身が中継を依頼したパケットを中継する車両が正しく送信しているか監視する
② パケットの中継が監視できなければ,周辺にパケットの中継が確認できなかったことを報告する
③ 報告された回数が閾値以上となった場合,その車両を攻撃者として判断する

4　結果・考察

シミュレーションの結果を図１,図２,図３,図４,図５,図６に示す.図１は提案方式の誤検出率,図２は既存方式の誤検出率,図３は提案方式の検出率,図４は既存方式の検出率,図５は提案方式の検出時間,図６は既存方式の検出時間に関するグラフである.

図１，図２より，提案方式・既存方式ともに平均車間距離が減少すると誤検出率が増加し，平均車間距離が増加すると誤検出率が増加することがわかる．これは，平均車間距離が小さい場合は車両の密度が高く，通信が衝突しやすくなることが原因であると考えられる．

図３，図５より，提案方式は平均車間距離が大きくなると検出率が低下し検出時間が増加，平均車間距離が小さくなると検出率が増加し検出時間が減少することがわかる．これは，車両の密度が増加すると信頼度情報のデータ数が増加することでより早く多くの攻撃者を検出可能となり，車両の密度が低下すると信頼度情報のデータ数が減少するために検出に時間がかかり攻撃者を検出しづらくなるためであると考えられる．

図４，図６より，既存方式は平均車間距離が変化しても検出率や検出時間の変化が小さいことがわかる．これは，車両の密度が３倍に増え，送信されるパケットの数が３倍に増えた場合であっても，パケットの中継を行わせる候補の車両の数も３倍に増えているため，それぞれの攻撃者が攻撃を行う確率や間隔には変化がないためである．

シミュレーション結果から，既存方式の各閾値と平均車間距離に対して３つの検出性能全てを向上させることができた閾値を表２に示す．

表２より，T=1 の 40～60m，T=4 の 60 の場合を除き，提案方式には３つの評価項目全ての向上させることができる値が存在することが分かる．また，T=1 に対しては誤検出率を大幅に減少可能であり，T=4 に対しては３つの評価項目全てを向上させることができる閾値は存在しないが，誤検出率と検出時間，または検出率と検出時間の２つを同時に向上させることが可能な閾値は存在するため，求められる要件に合わせて閾値を選択することが有効である．

表 2 既存方式より３項目全てにおいて高い性能を持つ閾値

閾値	20m	30m	40m	50m	60m
T=1	A(C=1.25)	A(C=1.25)	×	×	×
T=2	B(C=1.25)	B(C=1.25)	B(C=1.25)	B(C=1.25)	B(C=1.25)
T=3	A(C=1.5)	A(C=1.5)	A(C=1.5)	A(C=1.5)	A(C=1.5)
T=4	A(C=1.75)	A(C=1.75)	A(C=1.75)	A(C=1.75)	×

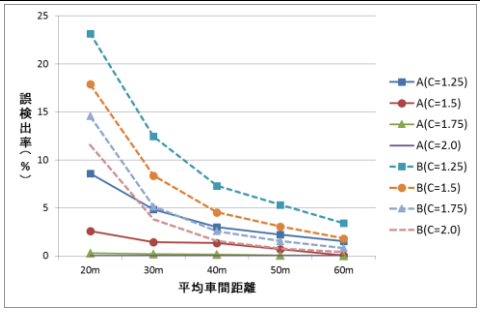

図 1 平均車間距離の変化と誤検出率（提案方式 A,B）

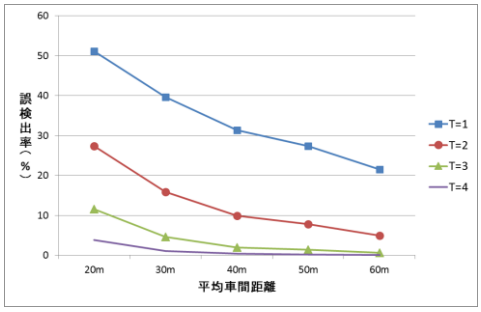

図 2 平均車間距離の変化と誤検出率（既存方式）

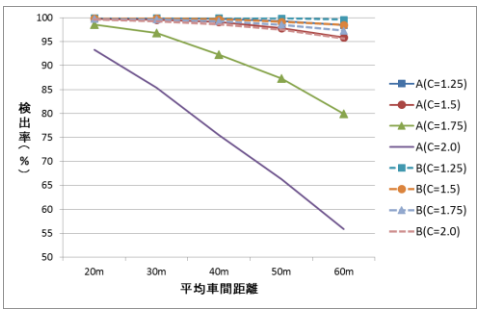

図 3 平均車間距離の変化と検出率（提案方式 A,B）

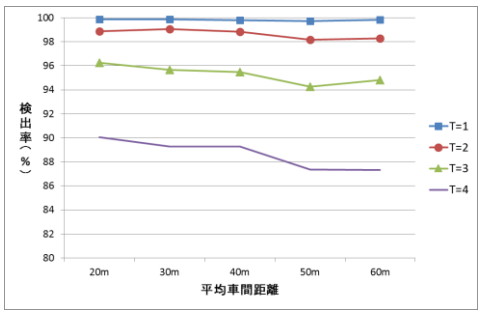

図 4 平均車間距離の変化と検出率（既存方式）

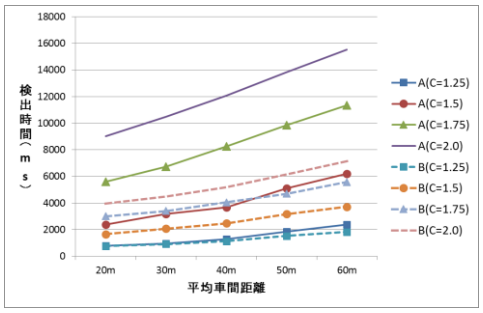

図 5 平均車間距離の変化と検出時間（提案方式 A,B）

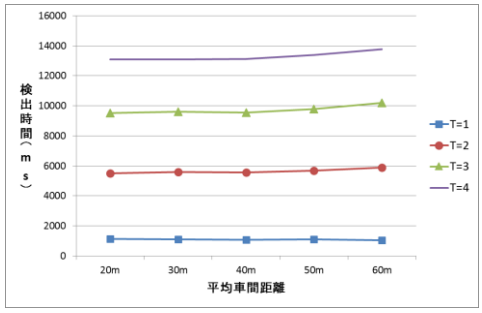

図 6 平均車間距離の変化と検出時間（既存方式）

5 まとめ

パケット破棄攻撃への対策手法として，周辺ノードの監視結果を信頼度として周辺ノードと共有し，信頼度情報から攻撃者を特定する手法を提案した．

提案した方式と既存方式に対してシミュレーションを行い，ネットワーク環境の変化による検出性能の変化について考察を行った．

また，提案方式は平均車間距離が変化する環境において適切な閾値を選択することで，既存方式よりも高い性能を発揮できることを示した．

参考文献

［1］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)