Vol.2014-CSEC-66 No.8
Vol.2014-SPT-10 No.8
2014/7/3

車車間通信における自律分散型認証手法の提案

日浦 博昭[1,a)]　北山 翔馬[1,b)]　双紙 正和[1,c)]　大場 充[1,†1]

概要：近年，走行する車輌間の情報交換にアドホックネットワークを応用した car2car (car to car) 通信が構想されている．その技術を用いた VANET (Vehicle Ad hoc Network) においては，RSU (Road Side Unit) を利用し，個々の車輌に認証情報を登録させる認証方法が提案されている．しかし RSU が機能しないと実現できないという問題点がある．本論文では， RSU を用いず個々の車輌で認証を行い，car2car 通信で想定される大規模な自律分散環境を考慮した方式を提案する．

キーワード：car2car,VANET, 認証, ゲーム理論, 多数決の原理

Proposal of Autonomous and Distributed Authentication for VANET

Hiroaki Hiura[1,a)]　Shoma Kitayama[1,b)]　Masakazu Soshi[1,c)]　Mitsuru Ohba[1,†1]

Abstract: Car2car (car to car) communication has attracted much attention these years. In car2car systems, vehicles exchange information with one another while running on roads and in turn constitute an ad hoc network, which is so called VANET (Vehicular Ad hoc Network). In VANET, each vehicle is authenticated via RSUs (Road Side Units). However, the obvious disadvantage of such an authentication scheme is that authentication could not be performed if RSUs fail. In order to alleviate this problem, in this paper we propose a method by which each vehicle can authenticate one another without help of RSUs in an autonomous and distributed manner.

Keywords: car2car, VANET, Authentication, Game theory, Majority rule

1. はじめに

近年，アドホックネットワークを応用した機器がさまざまな分野で開発・応用されている．特に，走行している車輌間にアドホックネットワークを用いたの通信により，car2car 通信の実現を目指している．そのネットワークにおける VANET と呼ばれる技術では，RSU を認証機構 (CA:Certification Authority) として利用し，個々の車輌には pseudonym と呼ばれる認証情報を登録させる認証方法が存在する [1]．しかし，この認証方法には，いくつか問題点がある．1 つ目の問題点として，認証された車輌が送信する情報が正しい情報である保証があるとは限らないというものがある．2 つ目の問題点は pseudonym を登録させる認証方法では RSU が存在し，正常に機能しないと実現できないことである．3 つ目の問題点は，car2car においては周囲の車輌の数が膨大な場合も想定される．このような場合，ネットワークは大規模でヘテロジニアスな環境であると想定される．そのような環境では多数の車輌がそれぞれ個々に一対一の認証をしていると，処理に時間がかかることで，不完全のまま認証を終了する事態が発生してしまう可能性がある．従って，以上のような問題点を解決するために，CA を利用せず，かつ，大規模自律分散環境でも認証を行えるプロトコルが必要となる．本論文では，全車輌が認証を行うための CPU を搭載していることを想定し，一対多の状況でも認証が可能なプロトコルを提案する．

本論文では，2 節で本研究に関連する研究や技術につい

[1] 広島市立大学 情報科学部
Hiroshima City Uniersity,l Faculty of Information Sciences
[†1] 現在，有限会社 工房 知の匠
Presently with Koubou-Chinotakumi CO., LTD
[a)] hiura@sos.info.hiroshima-cu.ac.jp
[b)] shouma@sos.info.hiroshima-cu.ac.jp
[c)] soshi@hirosima-cu.ac.jp

表 1　囚人のジレンマにおける利得表
Table 1　Gain table for Prisonar's dilemma

(囚人 A) ＼ (囚人 B)	自白しない	自白する
自白しない	-1 -1	0 10
自白する	-10 0	-3 -3

て紹介し，3 節で認証プロトコルを提案する．4 節で本論文のまとめや今後の課題について述べる．

2. 関連研究

本節では，本研究に関連した研究および技術について議論する．

2.1 ゲーム理論

ゲーム理論 [2] [3] は，複数のプレイヤーが存在し，それぞれの行動が影響し合う状況において，各プレイヤーの利益の期待値に基づいて相手の行動を予測し，意思決定を行うための理論である．この理論は，主に経済学に用いられる．

2.1.1 囚人のジレンマ

ゲーム理論の代表的な例として，囚人のジレンマというものが存在する．囚人のジレンマとは以下の 3 つの条件を満たすものである．

（条件 1）相手が何をしても非協力的に行動した場合，自分の利益は上がる
（条件 2）自分が非協力的に行動をとった場合，相手の利益は下がる
（条件 3）両者が私的利益を追求することで，協力した時と比べてそれぞれの利益が下がる

このとき，罪を犯し警察に取り調べられている犯人が二人いるとする．警察は証拠がつかめずにいるため，以下の条件を付け加え，取り調べを行った．

（条件 4）両者が自白した場合，両者とも懲役 3 年
（条件 5）1 人が自白し，1 人が黙秘した場合，自白した者は無罪 (懲役 0 年)，黙秘した者は懲役 10 年
（条件 6）両者が黙秘した場合，両者とも懲役 1 年

以上の条件に基づいた利得表を表 1 に示す．この表におけるセルの左下の数値は囚人 A の利得を，右上の数値は囚人 B の利得を表している．

支配戦略とは，ほかのプレイヤーがとる戦略の組み合わせすべてに対して，最適な行動をとる戦略のことを言う．表 1 の場合，より高いリスクを避けるために，両者は自白する戦略をとる可能性が高い．このような戦略が均衡し，安定してしまう状態をナッシュ均衡という．ナッシュ均衡とは，プレイヤー全員が互いに最適の戦略を選択し，これ以上戦略を変更する動機がない安定的な均衡状態になるような戦略の組み合わせのことを言う．

しかし，今回の囚人のジレンマでは，両者にとって自白しない方が高い利益を得られることが分かるため，そこにジレンマが生まれる．

ゲーム理論を車車間通信に適用した場合，表 2 のようになる．車車間通信では，自身の車輌と通信相手となる車輌がプレイヤーとして存在すると仮定する．このとき，自身の車輌は通信相手から伝えられた情報を信頼するか否か，そして通信相手は，正しい情報を伝える，もしくは誤った情報を伝えるというような戦略が考えられる．

車車間通信を実現するためには (自分)/ (通信相手) に関して，(信頼する)/ (正しい情報を伝える) ことが必要である．しかし，通信相手はコンピュータ誤動作や故意に誤った情報を送信するなどの原因により，常に正しい情報を伝えるとは限らない．仮に，(信頼する)/(誤った情報を伝える) 状態が生起した場合には，事故を起こす可能性がある．さらに，(信頼しない)/(誤った情報を伝える) の状態では，相手は故意に誤った情報を送ってきたにも関わらず，自分はその情報を誤った情報だと見抜き，事故が起こる可能性を回避したと考えることができる．これはゲームとして考えると自分にとって大きな利益であり，相手は大きな損失 (騙そうとした意図が失敗した) と考えられる．

また，利得に関しては自分の戦略に関わらず，相手の戦略が (正しい情報を伝える) の利得と (誤った情報を伝える) の利得に大きな差をつける必要がある．なぜならば，通信相手が (正しい情報を伝える) 確率に比べて，誤った情報を伝える確率は圧倒的に小さい確率で起こると考えられるためである．このことを考慮してまとめた利得表を表 3 にまとめる．この表におけるセルの左下の数値は自分の利得を，右上の数値は通信相手の利得を表している．

表 3 より支配戦略は，自分は信頼しない，通信相手は正しい情報を伝える，となる．したがって，ナッシュ均衡は (信頼しない)/(正しい情報を伝える) となる．これは第

表 2　車車間通信を考慮したゲームの勝敗
Table 2　The outcome (victory or defeat) for ca2car communications

(自分) ＼ (通信相手)	正しい情報を伝える	誤った情報を伝える
信頼する	正の利得	負の利得
信頼しない	負の利得	正の利得

表 3　ゲーム理論を車車間通信に適用した場合の利得表
Table 3　Gain table for game theory in car2car communication

(自分) ＼ (通信相手)	正しい情報を伝える	誤った情報を伝える
信頼する	-1 1	99 -99
信頼しない	1 -1	-99 99

2 種の過誤 (誤った情報を信頼してしまう) を防ぐためである．そうすると，通信相手の戦略に関わらず，自分は「信頼しない」の戦略を採択してしまい，車車間通信は意味が無くなる．

また，本研究では，ゲーム理論のなかでも，繰り返しゲームにおけるトリガ戦略を採用している．繰り返しゲームとは，表 1 や表 2，表 3 で説明したようなゲームを繰り返し行うものをいう．その中にトリガ戦略と呼ばれるものがあり，繰り返しゲームの代表的な戦略の一つである．

トリガ戦略は，以下に示す 3 つの条件を満たす．

（条件 A）最初は必ず協力する
（条件 B）相手が協力する限り，自分も協力行動をとる
（条件 C）相手が非協力的な行動を 1 度でも取れば，自分はそれ以降非協力的な行動を取り続ける．

このように，繰り返しゲームの戦略は，自分と相手の行動の履歴に応じて，自身の行動を決定する行動プログラムである．トリガ戦略を用いれば，故意に誤った情報を提供する攻撃者に対して，その攻撃を防ぐことは可能である．また，通信範囲にいる間，認証を 1 回のみ行うのではなく，一定期間ごとに複数回行うことでリアルタイムな判断を下す必要がある．しかし，ハードウェアやソフトウェアの誤動作によって誤った情報が提供された場合，その車輌の情報も今後信用しないこととなる．実社会において，1 度も誤動作を起こさないコンピュータは，どんなに高精度なであっても存在しない．よって，長期間でのこの認証を考慮すると，無意味なことになってしまうので，実社会の車車間通信では，トリガ戦略を用いることはできないことが分かる．そこで，トリガ戦略を改良し，コンピュータに誤りがあることを仮定し繰り返しゲームを応用したアルゴリズムを提案をする必要がある．3.2 節でそのアルゴルリズムを説明する．

2.2 多数決の原理

大規模でヘテロジニアスな環境における分散処理では，一部の要素で発生した誤りが通信により他要素へと伝藩した場合，システム全体として誤作動する可能性がある．このような場合に備え，システム自体の誤り発生確率を低減する，または発生してもリスクを最小限に抑えるような対策を行うなど，許容可能な安全を確保することが必要となってきた．

このような分散処理に存在する本質的な問題としてビザンチン問題がある [4] [5] ．

[6] では，ビザンチン問題に対する経験的解法である多数決原理，多様性原理について数学的考察を試み，これらの有効性について検証した．その結果，「CPU が誤動作で判断を誤る，もしくは，ソフトウェアが判断を誤るとしても，全体の 2/3 が正しいと判断している場合，その判断 (多数決の結果) は正しいものである」と結論付けることができた．しかし，[6] では，多数決を行う集団について，分散性を考慮していないため，対象とする集団が大規模な場合でなければ，多数決の原理における「CPU が誤動作で判断を誤る，もしくは，ソフトウェアが判断を誤るとしても，全体の 2/3 が正しいと判断している場合，その判断 (多数決の結果) は正しいものである」の理論は信頼性が低くなってしまう．また，車車間通信においては，集団が大規模の場合，その集団の個体それぞれと認証を行うと，その処理に費やす時間がかかる問題点がある．そのため，不十分な認証となってしまうことや，個々の車輌の CPU に負荷がかかりすぎてしまうことが想定されるため，車車間通信における認証では多数決の原理を応用することで一対多における認証を実現する．

3. 提案プロトコル

本研究は，VANET を利用する環境において，周囲に車輌が多数存在する場合でも認証可能な方法の提案を目的とし，ゲーム理論および多数決の原理を用いた認証手法を提案する．以下で説明するプロトコルを用いることにより，周囲の車輌が信頼できるか否かを判断することを目的とする．その結果をもとに自身の車輌の安全性をより高める様な動作をさせることを実現する．

3.1 提案プロトコルにおける定義

本節では，提案手法に用いる定義を説明する．

定義 1 (動作環境) 提案するプロトコルの動作環境では，RSU は用いず，各車輌間が無線で相互に通信をしている完全結合のトポロジーである．このトポロジーは，1 つのノードが壊れても他のノードに影響はないため，耐障害性に優れている．よって，無線の通信範囲内であればトンネルの中でも通信は可能である．

定義 2 (車輌の定義) 本研究で提案する認証において，車輌は認証実施車輌，認証対象車輌，情報提供車輌の 3 種類の車輌がいることを前提とする．また，情報提供車輌は，認証の途中で，選出車輌とそうでない車輌に選別される．各車輌に対する詳細を以下に記す．

(認証対象車輌):認証の対象となる車輌であり，認証対象車輌が「認証要求」を認証実施車輌に通知することにより，認証が開始される．以後，ATV (Authentication Target Vehicle) と略記する．

(認証実施車輌):認証を実際に行う車輌である．認証対象車輌から「認証要求」を受信することにより，認証対象車輌に対する認証を開始する．以後，AV (Authentication Vehicle) と略記する．

(情報提供車輌): 認証実施車輌に対し，情報を提供する車輌である．情報提供車輌は，既に認証対象車輌に対し信用状態を決定していると仮定する．

このとき，認証実施車輌から「認証開始」を受信する

と，認証実施車輌に対し，情報を提供する．また，認証対象車輌から「認証要求」を受信し，すでに認証し終えている車輌であれば情報提供車輌として，まだ認証をしていない車輌であれば，認証実施車輌として振る舞う．以後，PV (Provide Vehicle) と略記する．

(選出車輌):認証の際に，認証車輌が選出した情報提供車輌である．選出車輌となった情報提供車輌は，認証実施車輌から情報を要求された際に，要求された情報に対する返答を認証実施車輌に送信する．以後，SPV (Selected Provide Vehicle) と略記する．

以上のことを考慮した車輌の関係図を図 1 に示す．

定義 3 (通信能力) 認証では無線を用いて通信を行い，通信範囲は約 500m 半径であると仮定する [7]．このとき，状況に応じて，ブロードキャスト・チャネルとユニキャスト・チャネルの 2 種類の周波数帯を用いて通信をすることにより，認証を実現する．2 種類の周波数帯を用いることにより，混信を防ぎ認証が不完全で終了することや認証が途中で停止する頻度を軽減させる目的がある．

(ブロードキャスト・チャネル):通信において，周囲の車輌全体に情報を通知する周波数帯のことである．通信環境内では，1 つ存在することと仮定する．以後，BC (Broadcast Channel) と略記する．

(ユニキャスト・チャネル):通信において，送信先の車輌のアドレスを指定して個別に情報を通知する周波数帯のことである．通信環境内では，混信を防ぐため，認証実施車輌の数に応じた数存在することと仮定する．以後，UC (Unicast Channel) と略記する．

定義 4 (攻撃者) 本研究では認証を行う際に，認証実施車輌に対し攻撃者がいることを想定する．攻撃者は誤った情報を伝え，その情報を受信している車輌に対し，大きな損失を与えることで攻撃をする．このとき，誤った情報とは，運転者がブレーキを踏んだ場合，本来であれば「ブレーキを踏んだ」というメッセージを認証実施車輌に伝えるはずだが，「ブレーキを踏んでいない」もしくはまったく関係のないメッセージを伝えることをいう．このとき，攻撃者の車輌の CPU を改造し誤った情報を伝える，または，無線で通信している電波を改ざんして情報を書き換えて攻撃することが考えられる．

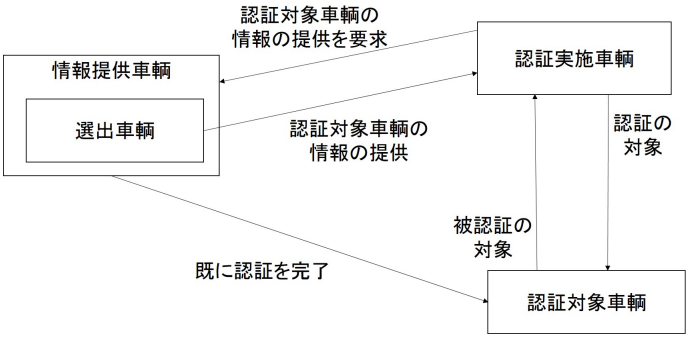

図 1 定義 1 した車輌の関係図
Fig. 1 Relationship diagram of vehicles difined by Definiton 1

そのため，上で述べた 2 つの攻撃の方法に対し，対策を施したプロトコルが必要となる．

定義 5 (認証対象車輌の信用状態) 認証において，認証実施車輌は認証対象車輌のそれぞれに状態遷移図を 1 つずつ持っていると仮定する．認証対象車輌の信用状態は，選出車輌から送信される信用状態によって認証実施車輌が決定し，「未定」,「信用する」,「当面信用する」,「現時点のみ信用する」,「現時点のみ信用しない」,「当面信用しない」,「信用しない」の 7 つの状態に分類される．また，選出車輌が提供する情報は,「信用できる」,「信用できない」のいずれかである．このとき，通信相手の信用状態が「信用する」,「当面信用する」に該当している場合，通信相手の情報を信用し，自身の車輌の行動を決定する．

3.2 繰り返しゲームおよび多数決の原理を用いたアルゴリズム

CA の存在を仮定せず，通信相手 (情報提供車輌および認証対象車輌) が CPU の誤動作や悪意を持って故意に誤った情報を伝える場合も考慮し，実社会で想定される大規模な自律分散型の認証アルゴリズムを提案する．

そのアルゴリズムでは，認証対象車輌は，定義 5 で述べたように「未定」,「信用する」,「当面信用する」,「現時点のみ信用する」,「現時点のみ信用しない」,「当面信用しない」,「信用しない」の 7 つの状態に分類される．通信相手がどの状態に該当するかによって，自身の車輌 (認証実施車輌) がどのように対応するかを決定する方法である．分類は 2 段階で実施される．

第一段階として，情報提供車輌から無作為に抽出した選出車輌から認証対象車輌に対して下した「信用状態 (信用できる，もしくは信用できない)」を提供してもらうと仮定する．認証実施車輌は，選出車輌の総数，選出車輌から提供された信用状態も用いて，分類を行い「当面信用する」,「現時点のみ信用する」,「現時点のみ信用しない」,「当面信用しない」のいずれかに遷移をする．

第二段階として，認証対象車輌との通信回数，認証対象車輌が通信において誤った情報を伝えた回数，認証対象車輌の CPU が誤動作をする場合の誤動作数の期待値を用いて，すでに遷移された信用状態からさらに状態を遷移させる．また，認証対象車輌が認証実施車輌の通信範囲にいる間は，一定時間ごとに常にこの動作を繰り返して，状態の遷移を繰り返していく．

このとき，CPU の誤動作とは，ハードウェアの精度により，起こりうるミスのことで，誤った判断を下してしまうことである．おおよそ，ハードウェアの動作数において，1/1000000 回で起こると仮定する．

上で述べた方法で分類を行い，認証対象車輌が「信用す

Vol.2014-CSEC-66 No.8
Vol.2014-SPT-10 No.8
2014/7/3

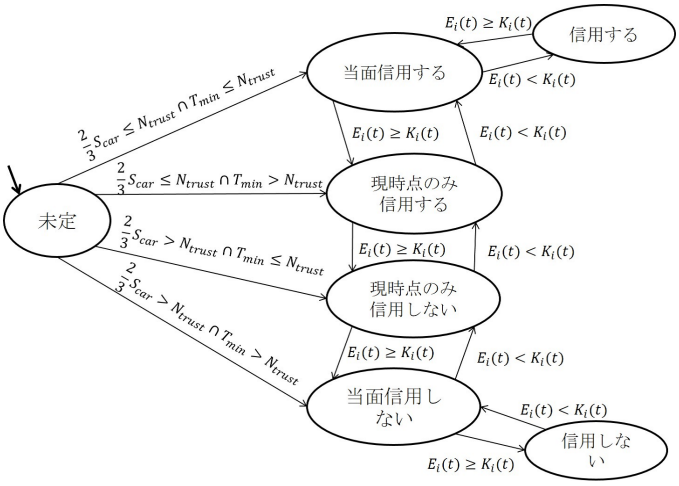

図 2 提案手法のアルゴリズムにおける状態遷移図
Fig. 2 State transition tiagram of this proposed algorithm

る」または「当面信用する」の 2 つのいずれかの場合に該当する場合のみ，送信された情報を信用し，その情報を考慮に入れて動作を決定する．これにより，悪意のある車輌 (故意に誤った情報を伝える車輌) からの悪影響を低減し，より安全な走行を実現させる．

以下にアルゴリズムで使用する記号を定義し，図 2 に状態遷移図を示す．また，状態遷移の説明を行う．

S_{car}... 選出車輌の総数
N_{trust}... 選出車輌が「信用できる」と送信した選出車輌の総数
N_{PV}... 認証時に選出される PV の台数
T_{min}...N_{trust} の最小数
K_i(t)... ある時点 t までの通信回数 i 回目までに実際に誤った情報を送った情報が伝えられた数の総数
E_i(t)... ある時点 t までの通信回数 i 回目までに起こりうるコンピュータ誤動作の期待値

[手順 1] 認証対象車輌は，認証対象車輌の通信範囲に入った時点から認証が開始される．いずれの認証対象車輌に対しても，はじめは「未定」に遷移される．[手順 2] 図 3.4 に示す手順に基づいて，「当面信用する」，「現時点のみ信用する」，「現時点のみ信用しない」，「当面信用しない」のいずれかに遷移される．以下の手順は，処理ごとに時間制約を設けて，タイムアウトをしたら，処理を中止して，[手順 2-1] からやり直す．また, 手順の説明を図 3 以降に示す. 説明内の (BC)，(UC) はそれぞれ (ブロードキャスト・チャネルでの通信)，(ユニキャスト・チャネルでの通信) を表している．

(手順 2-1):ATV は, AV に認証リクエストを送信する (BC).
(手順 2-2):AV は，認証を行うための PV を N_{PV} 台選出する．その後，AV が選出した PV を無作為に SPV を選出する．

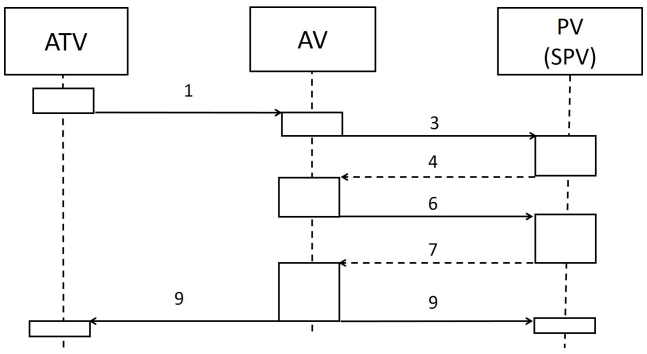

図 3 第一段階の認証手順
Fig. 3 Authentication procedure of first stage

(手順 2-3):AV は，センサ ID，ソフトウェアの型，ATV の M 秒間の速度，ATV との距離の要求を送信する (BC).
(手順 2-4):SPV は，AV にセンサ ID，ソフトウェアの型，ATV の M 秒間の速度，ATV との距離を送信する (UC).
(手順 2-5):AV はセンサ ID，ソフトウェアの型が共に重複しないような SPV を選択する．その際，ATV の M 秒間の速度が AV の車輌の走行速度と同様であり，かつ ATV との距離が近いものから選択をしていく．
(手順 2-6):AV は SPV に ATV に対する判断の要求を送信する (BC).
(手順 2-7):SPV は，AV に ATV に対する判断を送信する (UC).
(手順 2-8):ATV に対する判断の集計において，多数決の原理を考慮して，AV は以下のルールに従って， ATV に対する信用状態を決定する．

〈 $\frac{2}{3}\ S_{car} \leq N_{trust} \cap T_{min} \leq N_{trust}$ の場合 〉
AV は「ATV の信用状態」を「未定」から「当面信用する」に遷移する．

〈 $\frac{2}{3}\ S_{car} \leq N_{trust} \cap T_{min} > N_{trust}$ の場合 〉
AV は「ATV の信用状態」を「未定」から「現時点のみ信用する」に遷移する．

〈 $\frac{2}{3}\ S_{car} > N_{trust} \cap T_{min} \leq N_{trust}$ の場合 〉
AV は「ATV の信用状態」を「未定」から「現時点のみ信用しない」に遷移する．

〈 $\frac{2}{3}\ S_{car} > N_{trust} \cap T_{min} > N_{trust}$ の場合 〉
AV は「ATV の信用状態」を「未定」から「当面信用しない」に遷移する．

(手順 2-9):AV は PV・SPV・ATV に [認証終了] を送信する (BC).

[手順 3] AV は一定時間 (例:5sec) ごとに「ATV の信用状態」を遷移させる．その時，以下のルールに従って遷移させる．また，「ATV の信用状態」は「信用する」，「当面信用する」，「現時点のみ信用する」，「現時点のみ信用しない」，

「当面信用しない」,「信用しない」の順に信頼度が下がる．E_i(t)≥K_i(t) の場合，信頼度が一つ上の信用状態 (例:「当面信用する」→「信用する」) に遷移する．

E_i(t)<K_i(t) の場合，信頼度が一つ下の信用状態 (例:「当面信用する」→「現時点のみ信用する」) に遷移する．

3.3 考察

[手順 2-2] の処理において，PV を N_{PV} 台に選出する．実際には，周囲に存在する車輌の数に応じて，N_{PV} は変化させる．通常の道路であれば，N_{PV}= 20 程度であると考えられる．PV や SPV を選出する理由として，車車間通信が適用される場面では，周囲に，莫大な数の車輌が存在することが想定される．そのとき，周囲の車輌すべてと通信すると仮定すると，通信の際に混信が発生することで，認証ができないことが考えられる．また，AV が情報を受信したのちの処理を行う際に時間がかかり，ATV や AV が通信範囲から抜け出し，認証が不完全のまま終了してしまうことが考えられる．これらの問題点に対処するため，実際に通信をする車輌数を制限することで，混信を防ぎ，また，認証プロトコルの処理を迅速に終了させることで，認証の成功率を上げることを目標としている．

[手順 2-3]，[手順 2-4] でセンサ ID，ソフトウェアの型を用いて精度の高い判断を下すことを目的としている．センサ ID，ソフトウェアの型が異なるものを用いることにより，より同一の判断で下した意見だけにならないためである．ATV の M 秒間の速度，ATV との距離は，車は高速で走行しているので，認証中に通信範囲を抜けられると，認証が不完全のままになる危険性があるので，より認証実施車輌の近辺にいる車輌を選び出して，認証が完遂する可能性を高めるための情報である．

[手順 2-7] では，$\langle\ \frac{2}{3}\ S_{car} \leq N_{trust} \cap T_{min} \leq N_{trust}$ の場合 $\rangle$ のような，不等式を判断基準としている．$\frac{2}{3}$ のパラメータに関しては，2.2 の多数決原理より，[ATV に対する信用状態] を送信している SPV の総数の $\frac{2}{3}$ が「信用する」と送信してきた場合は，「当面信用する」もしくは「現時点のみ信用する」に遷移させる．また，T_{min} に関して，現時点では，SPV の半数程度が妥当だと考える．以上で示した 2 つの条件によってより細かく状態を分類することにより，精度の高い解を導くことを目的とする．

[手順 3] の処理は AV の通信範囲の中にいる場合は，常に行われる．また，情報提供車輌に対しても [手順 3] の処理を行い，「現時点のみ信用する」,「現時点のみ信用しない」,「当面信用しない」,「信用しない」に該当する状態に遷移された場合には，その情報提供車輌からの情報は，信用しないとする．

周囲の車輌 (ATV，PV) の信用状態が「信用する」「当面信用する」に該当する場合は，その車輌の情報を信用して， AV は行動を決定する．

実際に，プログラムを構築し簡単なシミュレーションを行った．シミュレーションでは，認証実施車輌 1 台，認証対象車輌 1 台，情報提供車輌 5 台がいることを仮定して実装した．その結果より，3.2 節で提案したプロトコルが稼働することを確認した．

4. 結論

本論文では，車車間通信における大規模な自律分散環境の通信における認証に，ゲーム理論と多数決の原理を用いることにより，RSU を用いずに認証方法を提案した．実際に提案プロトコルの際の車輌台数のシミュレーションを行うことで, 提案手法が機能することを確認し, 提案プロトコルの妥当性も確認した．今後の課題としては,3.3 節で示した周囲の車輌ではなく，実環境で想定される周囲に存在する車輌数が大規模な場合を考慮したシミュレーションを行わなければならない．また，本論文では認証を迅速に終了することを目的としたので，暗号などのセキュリティ技術を用いていない．したがって，暗号等を用いた場合，認証にかかる時間やセキュリティが向上するか検証する必要がある．そして，提案プロトコルの 3.2 節で示した [手順 2-2] や [手順 2-7] で用いている N_{PV} や T_{min} 等の変数や実際に車車間通信で用いられる CPU の誤動作の起こる確率などについて，妥当な値を調査してプロトコルに改善を加えなければならない．

以上で示した課題を改善することで，実現性や有用性を改めて確認することが必要となる．

参考文献

[1] Giorgio Calandriello : “Efficient and Robust Pseudonymous Authentication in VANET”, VANET ’07 Proc of the 4th ACM International workshop on Vehicular ad hoc networks,p19-p28, 2007.
[2] 神戸伸輔 : “ゲーム理論と情報の経済学”, 日本評論社 (2004).
[3] 鈴木光男 : “新ゲーム理論”, 頸草書房 (2000).
[4] L. Lamport, R. Shostak, and M. Pease : “The Byzantine General Problem”, ACM Transaction on Programing Languages and Systems, 4(3), 1982.
[5] M. Castro and B. Liskov : “Practical Byzantine Fault Tolerance”, In the Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999.
[6] 松尾和昭 : “複雑系におけるビザンチン問題の解決法に関する数学的考察”, 平成 22 年度広島市立大学大学院修士論文, 2011.
[7] Lucas Wang, Ryuji Wakikawa, Romain Kuntz, Rama Vuyyuru, and Lixia Zhang : “Data Naming in Vehicle-to-Vehicle Communications”, Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on. IEEE, 2012.