IoT 時代に向けた基地局補助による効率的なセキュアルーティングの設計

研究代表者　　佐　藤　光　哉　　東京理科大学 工学部 電気工学科 助教

1 はじめに

モノのインターネット(IoT: Internet of Things)やスマートフォンの普及に伴い、無線端末の数が指数的に増加している。使用目的や使用場所といった要件も多様化しており、数百億台もの端末が社会を構築する基盤として多種多様な通信を行なう時代を迎えようとしている。無線通信においては、移動端末がアドホックネットワーク(MANET: Mobile Ad-hoc NETwork)を構築し、端末間で情報をバケツリレー式に繰り返し伝送するマルチホップ通信を行なうことで容易に情報共有の範囲を拡大できる。その応用先は広く、自動運転における周辺車両との安全情報の共有[1]や、無線センサネットワークにおける無数の端末からの遠隔サーバへの情報集約[2]など様々な利用シーンでの活用が期待されている。しかし、無線通信においては情報が不特定多数の方向へ伝搬することから、原理的に第三者による信号の受信が容易である。一方で、上記のようなアプリケーションには秘匿すべき情報も多数含まれることから、実用上は情報セキュリティ面の対策が重要である。一般的に、情報の傍受を防ぐためには情報の暗号化や送信信号のビームフォーミングといった技術が用いられる。しかし、これらの技術単体で秘匿性の確保が可能なシステムは 1 対 1 の直接通信となる。そのため、マルチホップネットワークにおいてはこれら種々の技術を併用したセキュアなプロトコル設計が重要である。

セキュアなルーティングプロトコルの実現に対しては複数の議論があるが、いずれも「秘匿性は確保できるが極端に通信効率や演算効率が悪い」「通信効率は良いが秘匿性が一定確率で破綻する」など一長一短である。そこで本研究では、秘匿性、通信効率、演算効率を両立したプロトコルの確立を目的とした。

一般的に、MANET においては経路構築から通信までの一切が移動端末間で完結することが前提となる。しかし、この前提とセキュリティを両立するためには端末側で複雑な演算や観測を行なう必要があり、プロトコルを複雑化させる要因となっている。一方、近年は携帯電話基地局や無線 LAN アクセスポイントのような固定無線局が無数に配備されており、移動端末から送信された情報が、何らかの固定無線局に到達する可能性が高い。これらのうち信頼可能なものを補助的に活用したプロトコル設計を行なうことで、効率的かつ安全に経路構築できる可能性がある。そこで本研究では、関連分野における従来の検討での前提条件であった「プロトコルの一連が端末間で完結する」という条件を見直し、外部基地局を補助的に使用できる場合のシステムについて検討した。具体的には、端末の過去の行動履歴から算出された信頼値(トラスト)に基づくルーティング手法に着目した設計を行なった。トラストに基づく手法は、暗号理論に基づくルーティング手法と比較して効率的に悪意のある端末のネットワークへの介入を回避できるものの、トラストの改ざんの余地が存在するなど、課題も多い。トラストの管理および不正検知を外部基地局に一任し、かつ端末-基地局間の通信を不正検知時の基地局からのブロードキャストのみとするルーティング手法の提案を行ない、不正検知性能の計算機シミュレーション評価や通信時のオーバヘッド特性の関連手法との比較を行なった。

1 年間の活動を通して、関連検討の調査とその課題の整理、関連手法における通信特性の評価、手法提案、およびその性能評価を行なった。次章以降に、各検討の結果の要約を記す。

2 関連検討とその課題

MANET における代表的なルーティングプロトコルに、DSR (Dynamic Source Routing) と AODV(Ad-hoc On-demand Distance Vector)がある。いずれも通信効率面で優れる一方、秘匿性を考慮しないことから悪意を持った攻撃者がネットワークに参加し、経路情報の改ざんやパケットの破棄といった攻撃が可能である[3]。そこで、これらの代表的なプロトコルをベースに、セキュリティ技術を搭載したルーティングプロトコルの議論が長年に渡って行われてきた[4]。関連手法は、大きく暗号理論に基づく手法と端末のトラストに基づく手法の 2 種類に大別される。ここでは、これら 2 種類に関する検討について概説する。

公益財団法人電気通信普及財団
研究調査助成報告書 第35号 2020年度

2-1 暗号理論に基づく手法

これらの方式では、ルーティング時の経路要求パケットやその返信に対し中継端末による電子署名を付与することで、パケットの改ざん検知等の機構を実装する。最も代表的な手法に、ARAN(Authenticated Routing for Ad-Hoc Networks)がある[5]。これはAODVに基づく手法であり、あらかじめ外部の認証局によって公開鍵証明書を受け取った端末のみがルーティングに参加可能な方式である。端末はパケットを中継する際、自身の秘密鍵を用いて電子署名を生成し、自身の公開鍵や電子署名、証明書といった情報を追加する。これにより第三者によるパケットの生成元の正当性および改ざんの有無の検証が可能となる。他にも、ハッシュ連鎖を用いたSAODV(Secure-AODV)[6]や共通鍵に基づく軽量なプロトコル[7]も提案されている。

しかし、これらの手法の多くは中継パケットに対し電子署名のような、パケットの内容を検証するための情報を追加する必要がある。ホップごとにパケット長が増大する恐れがある他、端末側で都度これらの情報を検証する必要があることから、ネットワークが大規模である場合や端末の計算リソースが限られるシステムに対しては、採用に際して一考の余地がある。

2-2 トラストに基づく手法

これらの方式では各端末に対し過去の行動履歴に応じたトラスト値を付与し、その値に基づいた経路選択を行なうことで、問題を起こす可能性の高い端末の経路への介入を防ぐ。トラストに基づく手法の多くは主としてパケットの破棄のような攻撃への対策を対象とするが、この要因には、意図的な攻撃のみならず端末の通信性能の低さや位置依存の電波伝搬変動に起因する通信失敗を含むこともできる。そのため、攻撃者を仮定しないMANETにおいても通信信頼度向上のため、トラストを用いる検討も多数行われている。トラストに基づく場合、暗号理論に基づく手法と比較してパケット長が短く済む他、端末側での署名検証の手間が省ける(もしくは検証対象のパケットが短く済む)などの理由から、例えば過密な無線センサネットワークのような端末の計算・通信リソースに限りがあるシステムや、車車間通信システムのようなリアルタイム性が要求されるシステムに適しているといえる。

しかし、これらの方式においては原理的に端末側でのトラストの偽装が容易に行なうことができるという問題がある。仮にトラストを実際よりも高い値に偽装した場合、悪意を持った端末による経路に介入およびパケット破棄のような攻撃が可能となる。そこで、近年はトラストの偽装への対策を、外部の信頼できる基地局のような第三者に依頼する手法の検討が行われている。例えば、E-STAR [8]では電子署名に基づいてトラスト改ざんの検知を実現している。証明書の管理およびトラストの更新を外部機関に一任することで、端末側での偽装の一切の対策を行なっている。また、 文献[9]では完全集中制御型のトラストに基づくルーティング手法が提案されている。ここではトラストへの改ざんへの対策および経路選択のため、移動端末が基地局に対しP2P通信を行なう。

これらの手法を用いることでトラストの改ざんを対策できるが、一方でコストの増大も生じる。例えばE-STARではホップごとに電子署名を追加する必要があることから、他の暗号理論に基づく手法と同様、ネットワーク規模に応じてパケット長が増大するといった問題がある。これにより、トラストに基づく手法本来のメリットである通信・演算効率の良さが失われる恐れがある。また、集中制御型の手法では都度基地局を介する必要があることから通常のDSRやAODVと比較して通信回数が増大するほか、そもそもMANETを用いず、送信元端末-基地局-宛先端末間でのやり取りで通信が完結させた方が通信効率面および安全面の両面から優れる可能性もある。

このように、本分野においては複数の議論がなされており、電子署名やトラストのようなツールは揃っているものの、秘匿性と通信・演算効率はトレードオフの関係にあり、いずれの手法も一長一短であるといえる。

3 本研究で検討した基地局補助型のトラスト管理システムの概要

暗号理論に基づくルーティングにおいては、ホップごとに電子署名の検証や付与を行なう必要があることなどから、ネットワーク規模の拡大に応じてルーティングパケットが肥大化し、通信効率が劣化する、移動端末への計算負荷が増大するといった特徴がある。また、従来のトラストに基づくルーティングにおいては、トラストの評価を端末間で行なう場合には観測結果やトラスト値そのものの改ざんへの耐性に難点がある。基地局を介する集中制御型のトラストに基づく方式はこれらへの耐性を有する一方、都度基地局-端末間で

の P2P 通信を行なう必要があることから通信効率が著しく劣化する他、MANET 本来の利点であるネットワーク形態の柔軟性が失われるする恐れがある。このように、従来の方式では安全面、通信面いずれかに問題点がある。これらの背景を踏まえ本研究では、トラスト管理を基地局に一任しつつ、基地局-端末間の P2P 通信は行わず、不正を検知した際に基地局がネットワーク全体へその旨をブロードキャストする方式を考える。

図 1 に、本研究で検討したネットワークアーキテクチャの概要を示す。ここでは、各移動端末は DSR に基づいてマルチホップルーティングを行なう。各端末には過去の行動履歴から算出されるトラストが付与され、これを参考情報としたルーティングを行なう。なお、詳細なルーティングの手順は次章で述べる。また、トラストの管理には移動通信システムの基地局や自前の無線 LAN アクセスポイントのような、信頼できる固定基地局を活用する。これら基地局は MANET が通信を行なう帯域をモニタリングし、受信したルーティングパケットに基づいて各移動端末のトラスト値を更新する。複数基地局がバックボーンネットワークを介して繋がっており、端末 ID とそのトラスト値のリストからなる共通のデータベースにアクセス可能であるとする。また、モニタリングした情報とデータベースに格納されたトラスト値を比較し、もし不正な端末の存在を検知した場合は、ネットワーク上へその旨をブロードキャストする。

このように、本アーキテクチャでは従来の集中制御型の手法で仮定していた移動端末から基地局への P2P 通信を行わない。このような手法と比較して以下のような特徴があるといえる:

- 基地局がネットワークをモニタリングできる場合は不正端末への対策が可能である
- 基地局が存在しない環境においても、不正者の介入を許容してしまう点を除けば移動端末間で従来の DSR とほぼ同様のルーティングを行なうことができる。
- セキュリティを仮定しない通常の DSR と比較した通信効率の劣化が小さい

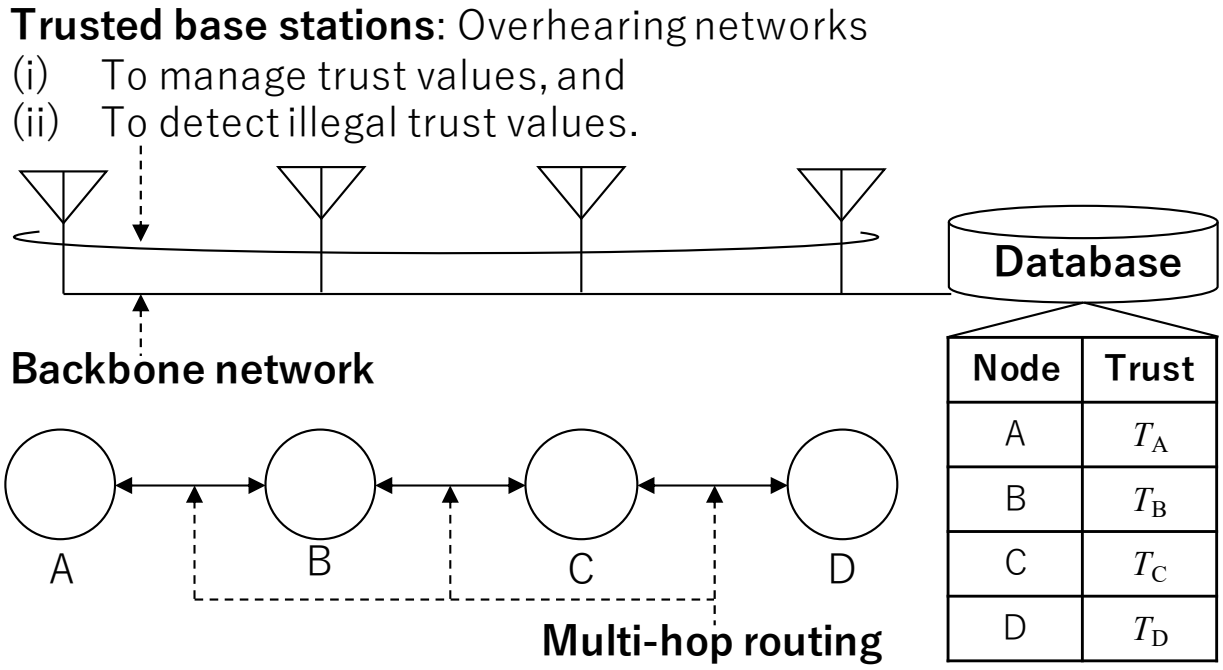

図 1 基地局補助型のトラスト管理システムに基づくマルチホップルーティングの概要。固定設置された基地局群がネットワークをモニタリングし、MANET より受信した経路構築時のパケットをトラスト管理および不正検知に活用する。端末-基地局間の明示的な通信は不正検知時の基地局からのブロードキャストのみである。

4 提案手法

本章では、図 1 に示したアーキテクチャに基づくルーティング手法について述べる。MANET のルーティングにおいては、中継端末によるパケットの破棄や改ざん、ワームホール攻撃など、様々な攻撃が存在する。本研究では、トラストに基づくルーティングの関連検討である文献[8][9]に基づき、パケットの破棄とルーティング時のトラストの改ざんの 2 つに対応可能な手法の設計を行なう。このうち、パケットの破棄は経路構築後の攻撃となる。ルーティング時に予め悪意を持った端末を経路から除外することで対策可能である他、パケットの破棄は文献[10]で提案されているような、複数端末が協調して観測する手法を併用することで検出可能である。検出結果を別途トラストの計算へ反映させることで、攻撃発生以降、攻撃を行なった端末の経路への参加を回避できることから、以下に述べる手法では特にトラストの改ざんへの対策に着目する。

本手法は、代表的なルーティングプロトコルである DSR に基づくものである。各端末には過去の通信履歴に応じたトラスト値が付与されており、本手法におけるルーティング時の経路選択の規範にこれを用いるものとする。トラストには、目的に応じて様々な定義が存在する。本研究では、正しくパケットを中継する割合と定義する。ここで、ネットワークに複数の端末が存在する場合のi番目の端末のトラスト値を考える。評価対象となる通信がn回行われた後の、本端末のトラストを次式で定義する。

$$T_{i,n} = 1 - \frac{y_{i,n}}{x_{i,n}}$$

ここで、$x_{i,n}$は過去に中継を行なった総数、$y_{i,n}$はそのうち正しく中継が行われなかった回数である。定義より、トラストはまた、一度も評価が行われていない場合、$T_{i,n} = 0.5$とする。

ある送信元端末が遠隔に存在する宛先端末と通信を行なうため、経路構築を行なう状況を考える。はじめに、送信元端末は経路要求パケット(RREQ: Route Request)をブロードキャストする。周辺に存在する端末は受信した RREQ を中継する。この RREQ には、通常の DSR における RREQ に加え、経路上の端末のトラスト値から算出されるその経路の信頼度に関する指標を設け、これを経路値Sと表記する。各端末は中継時、自身のトラスト値をもとに、次式に基づいて経路値を更新する。

$$S = \sum_{i \in Route} (1 - T_{i,n})$$

この値が小さいほど経路上に存在する端末の信頼度が高く、不正が発生しにくいといえる。宛先端末は複数経路から RREQ を受け取った場合、この経路値を参考に経路を選択し、その経路に対する返信パケット(RREP: Route Reply)を送信する。

この際、中継端末が自身のトラスト値を実際の値よりも高く偽った場合、対策なしでは自身が経路上の中継端末として選択されるよう仕向けることができる。そこで、図 1 に示した基地局群は RREP をモニタリングする。RREP に記載された端末と自身のデータベースに格納されたトラスト値より経路値を計算し、受信した経路値と比較する。この際、受信値と真の値に差があれば経路上に不正端末が存在するものとして取り扱い、その経路の使用を避けるようネットワーク上にブロードキャストする。また、もし経路値が一致する場合は経路上に存在する端末全てが適切に中継を行なったものとしてトラスト値の更新を行なう。これにより、トラスト管理を信頼できる基地局群に一任しつつ、トラスト管理に関する通信を不正検知時のブロードキャストのみに抑えることができる。

以下に、詳細な手順を記す。

1. 送信元端末: 以下に示すフォーマットに従う RREQ をブロードキャストする。
   $$RREQ = (RREQ_{DSR}, S)$$
   ここで、$RREQ_{DSR}$は通常の DSR における RREQ である。また、この時点では$S = 0$とする。
2. 中継端末: 経路値を更新しながら RREQ を中継する。
3. 宛先端末: 複数経路から RREQ を受信した場合、これらのうち経路値が最小である経路を選択し、この経路値をS'とする。
4. 宛先端末: 以下に示すフォーマットに従う RREP パケットを生成し、ブロードキャストする。
   $$RREP = (RREP_{DSR}, S')$$
   ここで、$RREP_{DSR}$は通常の DSR における RREP である。
5. $RREP_{DSR}$上に記載された中継端末: $RREP_{DSR}$を中継する。

6. 基地局群: 上記 RREP を受信した際、RREP に記載された中継端末と自身のデータベース情報を照合し、真の経路値を計算する。また、この経路上に記載された全てのノードに対し次式を適用し、総通信回数に関する情報を更新する。

$$x_{i,n} = x_{i,n-1} + 1$$

7. 基地局群: もし真の経路値と RREP 上に記載された経路値を比較し$S \neq S'$となった場合、この経路上に存在するすべての端末に対し次式を適用する。

$$y_{i,n} = y_{i,n-1} + 1$$

さらに、この経路の使用を停止する旨をネットワーク上にブロードキャストする。

8. 宛先端末: 基地局群からステップ 7 におけるブロードキャストパケットを受信した場合(すなわち、不正が検知された場合)、ステップ 3 の経路選択からやり直す。
9. 基地局群: 全ノードのトラスト値を更新する。
10. 基地局群: (一定期間ごと)最新のトラスト情報を端末に配布する。

なお、関連する基地局補助型のプロトコルと異なり、トラストの改ざんを許容する点を除けば周辺に基地局が存在しない場合であっても従来の DSR とほぼ同様のルーティングを実施できる。

5 性能評価

ここでは、提案手法の性能について述べる。本研究では、トラスト算出に関する計算機シミュレーションによる評価と、ルーティング時にネットワークに送信されるパケットの総量の最小値の理論評価の 2 つを通して提案手法を用いることで効率的なセキュアルーティングを実施できること示した。以下に、各評価結果の詳細を述べる。

5-1 計算機シミュレーション

まず、計算機シミュレーションにより、不正検知およびトラストの更新の挙動に関する確認を行なった。ここでは 1000m 四方の二次元エリアを仮定し、送信元端末および宛先端末をそれぞれ(200m, 500m)および(800m, 500m)の位置に固定設置した。また、N台の中継端末をランダムに配置し、このうちN_{m}台の端末は悪意を持ったユーザであると仮定した。これらの悪意を持った端末は、確率p_fで自身のトラストを 0.9 と偽るものとする。加えて、全ての通信は送受信者間の距離d[m]がある閾値d_{th}[m]を下回った際に成功するものとした。なお、マルチパスフェージングやシャドウイングといった受信電力値の確率的変動は考慮していない。最後に、ネットワークのモニタリングを行なう基地局群は評価エリア全体をモニタリングできるように配備し、トラストは更新のたびに各端末へ配布されるものとした。

本評価では、以下の手順を複数回繰り返した:

1. 中継端末をシミュレーションエリアへ一様分布に従ってランダムに配置する。
2. 送信元端末-宛先端末間のルーティングを実施する
3. ルーティングの結果に基づいてトラスト値を更新する

なお、パラメータはそれぞれ$d_{\mathrm{th}} = 200$[m], $N = 50$, $N_{\mathrm{m}} = 5$, $p_f = 0.6$としている。図 2 に、経路構築の回数に応じた各端末のトラストの推移を示す。この図では、横軸が端末番号を、縦軸が端末番号に対応するトラスト値を表わす。このうち 1-5 番目の端末が悪意を持った端末であり、試行回数を 100 回、1000 回、10000 回と増やした際のトラスト値の推移を評価した。図より、経路構築を行なうごと、悪意を持った端末のトラストが下がり、一方で攻撃を行なわない端末のトラストは 0.9 を越える高い値に収束することがわかる。これは提案手法に基づく不正検知が成功した結果であり、基地局を補助的に活用することで悪意を持った端末とそうでない端末を振り分けられることが確認できた。

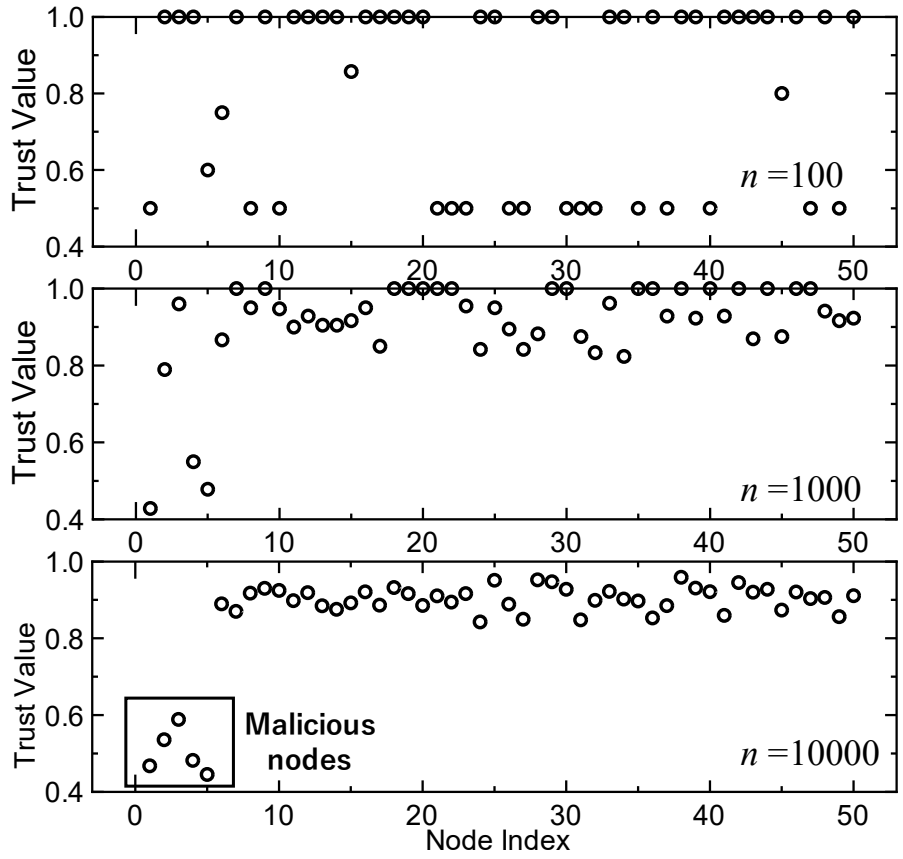

図 2　ノードごとのトラスト値の推移の数値例. 端末番号 1-5 は悪意を持った端末(malicious nodes)である。経路構築を行なうごと、悪意を持った端末のトラストが下がり、一方で攻撃を行なわない端末のトラストは 0.9 を越える高い値に収束することがわかる。

5-2 通信効率特性

次に、提案手法の通信効率特性を評価した。通信効率にはパケット到達率や送信回数など、様々な指標が考えられる。ここで、本研究での提案手法も含めたセキュアなルーティング手法の多くは AODV や DSR といったプロトコルにおけるパケットフォーマットに電子署名やトラストといった追加の情報を付与することで各種攻撃への耐性を持たせている。そのため、ネットワーク規模に応じて RREQ や RREP のパケット長が長くなるケースが殆どである。このような背景を鑑み本研究では、ルーティングを行なう際にネットワーク上に流れるパケットの総長の最小値をルーティングオーバヘッド(RO: Routing Overhead)と定義し、これを評価指標とした。また、ここでは比較のため、以下に示す関連手法の同特性をあわせて評価した(カッコ内のテキストは図 3 中での表記を意味する):

- 通常の DSR (Pure DSR)
- E-STAR [8]: DSR をベースとした､電子署名とトラストのハイブリッド型のルーティング手法である。基本的には本研究における提案手法と同様、ルーティングパケットに付与されたトラスト値に基づいて経路の質の評価を行なう。また、トラストを含むルーティングパケットへの改ざんを端末間で検知するため、ホップごとに中継パケットに電子署名を付与している。これにより、第三者によるパケットの正当性の検証が可能となる。ただし、ホップごとに電子署名を新規に付与するため、ネットワーク規模の拡大に応じてパケット長が増大するといった問題点がある。
- 完全集中制御型のトラストに基づくルーティング手法(Centralized method) [9]: トラストに基づくルーティング手法である。ここではトラストへの改ざんへの対策として、信頼できる基地局を活用している。本手法では移動端末が基地局に対し P2P 通信を行なう必要があるため、通常の DSR と比較して通信回数が増大するという問題がある。

これらの手法の RO 特性を評価するため、送信元端末-宛先端末間の直線上にt台の中継端末が並び、これら全ての端末によって経路が構築される環境を考える。このような環境において、提案手法における RO は次式で表せる。

$$\mathrm{RO} = \sum_{i=0}^{t} Size\big(RREQ(i)\big) + \sum_{j=0}^{t} Size\big(RREP(j)\big)\ [\mathrm{byte}]$$

ここで、$\mathrm{Size}(\cdot)$はカッコ内に記されたパケットの長さ、$RREQ(i)$は送信元端末による送信を基準としたi番目のホップにおける RREQ、$RREP(j)$は送信元端末による送信を基準としたj番目のホップにおける RREP である。ここで、通常の DSR におけるパケット長は格納される ID の長さなどに依存する。ここでは、文献[11]におけるセキュアルーティングに関する議論に基づき、$Size\big(RREQ_{DSR(i)}\big) = 12 + 4i$，$Size\big(RREP_{DSR}(j)\big) = 12 + 4t$とした。また、経路値の長さを$Size(S) = Size(S') = 4$[byte]とすることで、提案手法における RO を次式のように計算できる。

$$\mathrm{RO} = \sum_{i=0}^{t} (4i + 16) + (t + 1)(4t + 16)$$

また、比較手法における RO 特性も同様の手順で導出した。図 3 に、中継端末の台数に対する RO 特性を示す。この図において縦軸が RO に相当し、この値が小さいほど効率よくルーティングが実施できる。なお、E-STAR においては電子署名 1 つ辺りの長さを 4byte と仮定した。代表的な暗号学的ハッシュ関数である SHA-2 における出力が最小で 28byte であることなどからもわかるように、4byte/電子署名は短い設定である。そのような仮定を置いた上であっても通常の DSR と比べて著しく RO 特性が増大しており、その差は中継端末が増えるに従い開く。また、完全集中制御型の手法においてはパケット長の増大こそ抑えられるものの、都度基地局と通信を行なう必要がある。そのため、本手法も RO 特性の劣化が確認できる。一方、提案手法は通常の DSR に対する追加情報が経路値 1 つのみである。加えて完全集中制御型の手法と比較して基地局との P2P 通信を行なわないため、通常の DSR とほぼ同等の通信効率でルーティングを実施できる。

これらの比較を通し、提案手法を用いることで、通信効率の劣化を抑制しつつトラスト改ざんへの耐性を持たせたルーティングを実施できることが確認できた。

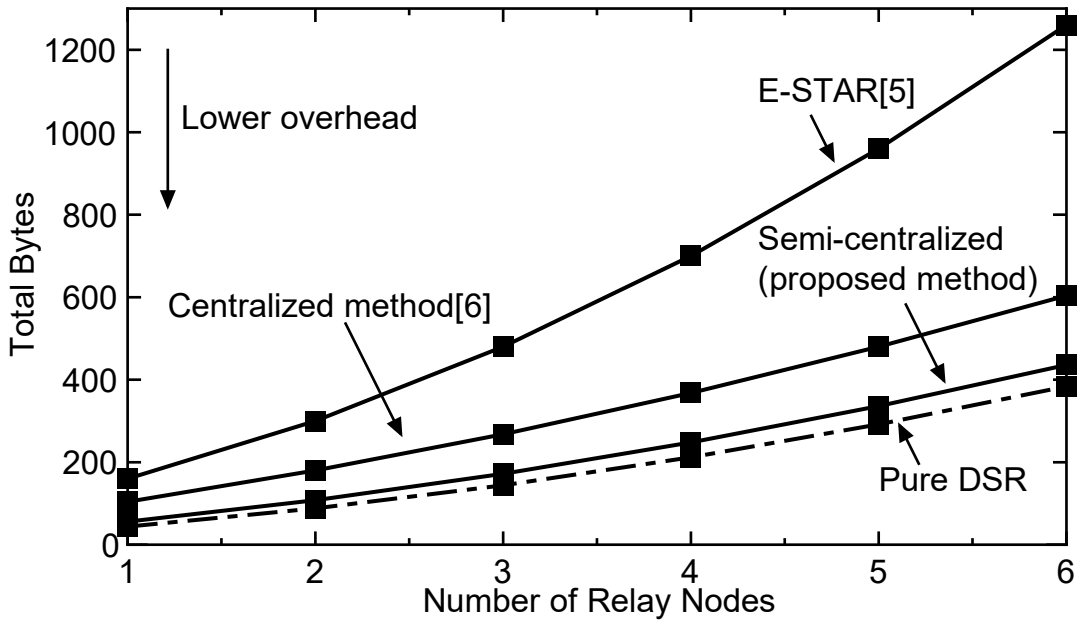

図 3　ルーティング時のオーバヘッド特性。提案手法を用いることで、通常の DSR と比べても遜色のない通信効率で悪意を持つ端末への耐性を持ったルーティングが実現できる。

6 おわりに

本研究では、MANET におけるセキュアかつ効率的なルーティングプロトコルの実現を目的とし、基地局をトラスト管理システムとして補助的に活用する手法の検討を行なった。トラストの更新およびトラスト改ざんの不正検知を基地局に一任し、かつ基地局−移動端末間の通信を、不正検知時の基地局からのブロードキャストのみに制限することで、通信効率と不正検知を両立したルーティングが実現できる。計算機シミュレーションおよび理論評価により、基地局側でトラストの改ざんを検知可能であり、かつ関連手法と比較してルーティング時のオーバヘッド特性に優れることを確認した。提案手法を用いることで、自動運転のような低遅延性が要求されるシステムや、IoT ネットワークのような端末の計算能力の制約から電子署名の搭載を避けたいシステムの安全な運用が期待できる。

本研究で提案した手法は、基地局が利用可能な場合トラストの管理が可能であり、かつ周辺に基地局が存在しない場合であっても移動端末間でルーティングが実施できる点に特徴がある。しかし、周辺に基地局が存在しない場合は、トラストの改ざんのような攻撃を許容してしまう。集約署名のような、署名の総長が署名回数に依存しない電子署名方式[12][13]を併用することで通信効率を維持しつつこのような攻撃への耐性を持たせられる可能性が高い。今後はアプリケーションごとのセキュリティの要件に応じた、このようなオプションの設計を進めたい。また、アプリケーションの新規開拓も進める予定である。次世代移動通信システムの議論においては、分散端末間で協調的に機械学習を行なう手法が注目されているが、このようなアプリケーションも従来の MANET と同様のセキュリティの問題を抱えている可能性が高い。本研究の成果の活用によって、最新の無線システム安全かつ効率的な運用の実現に貢献したい。

【参考文献】

[1] H. G. Seif and X. Hu, “Autonomous driving in the iCity - HD maps as a key challenge of the automotive industry, Engineering, ” Engineering, vol.2, no.2, pp.159-162, 2016.

[2] H. Harada et al., “IEEE 802.15.4g based Wi-SUN communication systems, ” IEICE Trans. Commun., vol.E100-B, no.7, pp. 1032-1043, 2017.

[3] B. Kannhavong et al., “A survey of routing attacks in mobile ad hoc networks, ” IEEE Wireless Commun., vol.14, no.5, pp.85-91, 2007.

[4] D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for Internet of things: A survey, ” Journal of Network and Computer Applications, vol.66, pp.198-213, 2016.

[5] K. Sanzgiri et al., “Authenticated routing for ad hoc networks, ” IEEE J. Sel. Areas Commun., Vol. 23, No. 3, pp.598–610, 2005.

[6] M. Guerrero Zapata and N. Asokan, “Securing ad hoc routing protocols, ” Proc. ACM WiSE ’02, pp.1–10, 2002.

[7] Y-C. Hu and A. Perrig, “Ariadne: A secure on-demand routing protocol for ad hoc networks, ” Wireless Networks, vol. 11, pp.21-38, 2005.

[8] M.M.E.A. Mahmoud, X. Lin, and X. Shen, “Secure and reliable routing protocols for heterogeneous multihop wireless networks, ” IEEE Trans. Parallel Distrib. Syst., vol.26, no.4, pp. 1140-1153, 2015.

[9] J. Yun, S. Seo, and J. Chung, “Centralized trust-based secure routing in wireless networks, “ IEEE Wireless Commun. Lett., vol. 7, no.6, pp.1066-1069, 2018.

[10] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, “Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning, ” IEEE Trans. Veh. Technol., vol. 63, no.9, 4647-4658, 2014.

[11] Y. Shibasaki et al., “An AODV-based communication-efficient secure routing protocol for large scale ad-hoc networks, ” Proc. IEEE CCNC 2020, Jan. 2020.

[12] A. Boldyreva et al., “Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing, ” Proc. ACM CCS ’07, pp.276–285, 2007.

[13] K. G. Paterson, “ID-based signatures from pairings on elliptic curves, ” Electron. Lett., Vol. 38, No. 18, pp.1025–1026, 2002.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
大規模モバイルアドホックネットワークにおけるAODVに基づく効率的かつセキュアなルーティングプロトコルの提案	電子情報通信学会センサネットワークとモバイルインテリジェンス(SeMI)研究会	2019年7月
An AODV-Based Communication-Efficient Secure Routing Protocol for Large Scale Ad-Hoc Networks	IEEE Consumer Communications & Networking Conference (IEEE CCNC 2020)	2020年1月
Network-Density-Controlled Decentralized Parallel Stochastic Gradient Descent in Wireless Systems	IEEE International Conference on Communications (IEEE ICC 2020)	2020年6月

(その他、学術論文1編を査読付き国際学術論文誌へ投稿中)