2004－DPS－118　(9)
2004／6／4

安全性を尺度としたアドホックルーティングプロトコル (Extended Abstract)

東京電機大学理工学部情報システム工学科
吉田 圭佑　桧垣 博章
E-mail: {kei,hig}@higlab.k.dendai.ac.jp

モバイルコンピュータ間の無線マルチホップ配送を通信基盤とするモバイルアドホックネットワークにおいては、有線ネットワーク環境と比較して、配送メッセージ群を盗聴することが容易であるという問題がある。暗号通信を用いることが考えられるが、計算オーバヘッド、通信オーバヘッドが大きくなるという問題は避けられない。そこで、配送に用いる経路を探索する際に、可能性のある複数の経路のうち、最も盗聴される可能性の低い経路を選択する手法を用いることを提案し、その実現プロトコルの枠組を提示する。

Secure Ad Hoc Routing based on Probability of Wiretapping (Extended Abstract)

Keisuke Yoshida and Hiroaki Higaki
Department of Computers and Systems Engineering
Tokyo Denki University
E-mail: {kei,hig}@higlab.k.dendai.ac.jp

In a mobile ad hoc network (MANET) based on wireless multihop message transmission, wiretapping is more easily possible than in wired networks. Encription of messages is a candidate to solve this problem. However, it requires additional computation and communication overhead. In this paper, we propose a method to select a message transmission route on which probability of wiretapping during transmission is the lowest among possible routes from a source mobile computer to a destination one.

1　背景と目的

近年、ノート型 PC や PDA(Personal Digital Assistance) などのモバイルコンピュータの普及にともない、IEEE802.11 [9] や HIPERLAN [7]、Bluetooth [8] などの無線 LAN 技術の研究開発が行なわれている。従来のコンピュータネットワークは、有線ネットワークに接続されたルータのみがメッセージの配送を行なうインフラストラクチャネットワーク (Infrastructured Networks) であった。モバイルコンピュータは、有線ネットワークに接続されたアクセスポイントを経由して、他のモバイルコンピュータとの通信を可能としている。しかし、インフラストラクチャネットワークの構築と運用に要する金銭的、時間的コストは大きい。そのため、イベント会場などで利用者の要求を充足するために一時的に構築されるネットワークや、工事現場、災害現場、戦場のように要求の変化に応じて構成が変化する必要のあるネットワーク、さらに航空機や乗用車などに搭載されたコンピュータを相互接続するネットワークなどに適用することは困難である。そこで、有線ネットワークとそれに接続するアクセスポイントを用いず、無線通信するモバイルコンピュータがメッセージをマルチホップで配送するモバイルアドホックネットワーク (MANET) が注目されている。

モバイルアドホックネットワークでは、移動コンピュータは無線通信によって互いにメッセージを交換する。ある移動コンピュータから送信された無線信号は、その信号到達範囲内に位置するすべての移動コンピュータが受信可能である。そのため、有線ネットワークと比較して、盗聴者がより容易に配送中のメッセージを入手可能な環境であるといえる。そこで、アドホックネットワークにおいて盗聴に対して頑強な通信を実現するために、WEP [9] や WPA [10] といった暗号通信技術が研究開発されている。しかし、暗号通信を用いる場合、通信開始時の暗号鍵交換手続き、暗号化と復号化に要する計算オーバヘッド、平文に対する暗号文のデータ長の拡大による通信オーバヘッドなどを要する。各移動コンピュータの計算資源が限られており、電磁波ノイズや複数の無線信号の衝突、通信帯域の競合等のために大きな通信コストを要するアドホックネットワークにおいては、暗号化による安全性の確保は必ずしも有効な手法とはならない。アドホックネットワークでは、任意の移動コンピュータ対が常にメッセージを直接交換できるとは限らないことから、マルチホップのメッセージ配送が用いられる。また、移動コンピュータが位置を時々刻々変化させることから、その配送経路を通信開始時に、すなわちオンデマンドに決定する手法が広く用いられている。そこで、本論文では、この経路決定時に複数の経路を探索、検出し、それぞれの安全性を評価して、最も安全な経路を選択することで安全な通信を実現することを提案し、その実現ルーティングプロトコルを設計する。

2　従来手法

DSR [1] や AODV [2] といった従来提案されている多くのアドホックルーティングプロトコルは、送信元移動コンピュータから送信先移動コンピュータまでのホップ数が最小となる経路を検出している。この方法は、有線ネットワークで広く用いられているが、有限容量のバッテリで駆動し、移動しながら通信するコンピュータで構成され、移動コンピュータ間のメッセージ交換が無線通信によってなされるアドホックネットワークでは、必ずしも有効な方法とはならない。[5] では、複数の経路を探索、検出し、RTT の小さな経路を選択する手法を提案している。ABR [4] では、各通信リンクにおけるビーコンの紛失率からそれぞれのリンクの安定性を評価し、より安定なリンクから構成される経路を選択し、データの配送を行なう。また、[6] では、他の通信との競合、衝突を回避できる経路を選択するとともに、送信電力を制御することで高スループットを実現している。さらに [3] では、検出された経路上にある各移動コンピュータがメッセージを配送するために必要な最小の電力で通信することによって、消費電力を低減する方法が提案されている。このように、ホップ数以外の尺度によって、送信元移動コンピュータから送信先移動コンピュータへの経路を決定する手法が提案されているが、盗聴に対する安全性を尺度として経路決定するアドホックルーティングプロトコルは、提案されていない。

3 提案手法

安全性に基づいて、送信元移動コンピュータから送信先移動コンピュータまでの配送経路を決定するためには、安全性の評価方法を定めることと、これを用いた複数経路探索プロトコルを設計することが必要である。本論文では、各移動コンピュータが自身の位置 (座標 (x, y)) を GPS 等を用いて入手可能であるとする。また、任意の座標 (x, y) における盗聴危険度 $d(x, y)(\geq 0)$ は、あらかじめ評価されているものとする。このとき、移動コンピュータ M_i が自身の無線信号到達範囲内にメッセージを送信した場合、このメッセージが盗聴される危険度は $\iint_{S(M_i)} d(x, y)dxdy$ で与えられる。ただし、$S(M_i)$ は、M_i からの無線信号到達範囲の全体を表している。これに基づくと、経路 $R = \langle M_0(= M_s), \ldots, M_n(= M_d)\rangle$ に沿ってメッセージをマルチホップ配送した場合、このメッセージが盗聴される危険度は $\sum_{M_i \in R} \iint_{S(M_i)} d(x, y)dxdy$ で与えることができる。ここで $(x', y') \in S(M_i) \cap S(M_{i+1})$ については、危険度を二重に加算しているが、マルチホップ配送により M_i と M_{i+1} がともにメッセージを自身の無線信号到達範囲内に送信することから、妥当な評価方法であるといえる。

送信元移動コンピュータは、複数経路検出可能なアドホックルーティングプロトコルを用い、検出した経路のうち盗聴危険度がもっとも小さい経路を選択する。本論文では、ABR [4] で用いられている $Rreq$ (経路探索要求メッセージ) の配送方法を応用して、SBR(Security Based Routing) プロトコルを設計する。ここでは、$Rreq$ を転送した移動コンピュータは、自身のアドレスを $Rreq$ に格納する。$Rreq$ を受信した移動コンピュータは、この $Rreq$ に自身のアドレスが含まれない場合には、受信した $Rreq$ をブロードキャスト送信し、含まれる場合にはこれを破棄する。これによって、送信元移動コンピュータから送信先移動コンピュータに至るループを含まないすべての経路を検出することができる。ただし、各移動コンピュータは複数回のブロードキャスト送信を行なうことがあることから、通信オーバヘッドが大きいという特徴がある。本論文で提案する盗聴危険度は、累積的であり、経路長の増加に対して単調増加することから、送信元移動コンピュータが許容盗聴危険度を定めて $Rreq$ にピギーバックし、また、検出途中の経路についての盗聴危険度を評価する ($Rreq$ 配送中に危険度を評価する) ことによって、評価危険度が許容危険度をこえた時点で $Rreq$ の配送を中止することとする。これによって、メッセージ数の削減等、通信オーバヘッドの削減が可能となる。

[SBR プロトコル]

1) 送信元移動コンピュータ M_s は、送信先移動コンピュータを M_d、配送経路上にある移動コンピュータのアドレス列を $\langle M_s\rangle$、累積危険度を $\iint_{S(M_s)} d(x, y)dxdy$、許容危険度閾値を D_{th} とする経路探索要求メッセージ $Rreq$ を自身の無線信号到達範囲内に位置するすべての移動コンピュータにブロードキャスト送信する。すなわち、$Rreq.src := M_s$、$Rreq.dst := M_d$、$Rreq.seq := \langle M_s\rangle$、$Rreq.danger := \iint_{S(M_s)} d(x, y)dxdy$、$Rreq.threshold := D_{th}$ とする。
2) 中継移動コンピュータ M_i は、$Rreq$ を受信すると、以下の処理を行なう。
   2-1) $M_i \in Rreq.seq$ であるならば、M_i はこの $Rreq$ を破棄する。
   2-2) $Rreq.danger + \iint_{S(M_i)} d(x, y)dxdy > Rreq.threshold$ であるならば、M_i はこの $Rreq$ を破棄する。
   2-3) それ以外の場合、$Rreq.seq$ の末尾に M_i を追加し、$Rreq.danger := Rreq.danger + \iint_{S(M_i)} d(x, y)dxdy$ と更新した $Rreq$ を自身の無線信号到達範囲内に位置するすべての移動コンピュータにブロードキャスト送信する。
3) 送信先移動コンピュータ M_d は、$Rreq.dst = M_d$ を満たす $Rreq$ を受信したならば、$Rrep.src := M_d$、$Rrep.dst := M_s$、$Rreq.seq$ の末尾に M_d を追加したアドレス列を検出経路 $Rrep.route$、$Rrep.danger := Rreq.danger$ とした経路探索応答メッセージ $Rrep$ を $Rrep.route$ で M_d の直前にアドレスが含まれている移動コンピュータにユニキャスト送信する。

4) 中継移動コンピュータ M_i は、$Rrep$ を受信すると、$Rrep.route$ で M_i の直前にアドレスが含まれている移動コンピュータにこの $Rrep$ をユニキャスト送信する。

5) 送信元移動コンピュータ M_s は、タイマを用い、タイムアウト以前に受信した $Rrep.dst = M_s$ を満たす複数の $Rrep$ のうち、$Rrep.danger$ が最小である $Rrep$ に含まれる経路 $Rrep.route$ をアプリケーションメッセージの配送経路として採用する。アプリケーションメッセージは、この経路を用いてソースルーティングされる。□

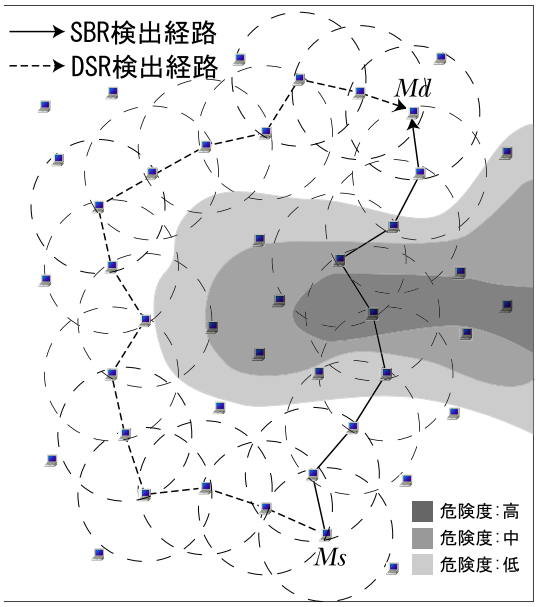

図 1: SBR と DSR による検出経路

4 まとめと今後の課題

本論文では、盗聴が容易な無線通信を用いるアドホックネットワークにおいて、盗聴の危険度が小さな経路を用いた通信を実現するために、安全性を尺度として経路を決定するルーティングプロトコル SBR を提案した。今後は、検出される経路の安全性を従来プロトコルと比較評価することによって有効性を示すとともに、送信電力を変化させることでより安全性の高い通信路を提供できるプロトコルへと拡張する。

参考文献

[1] Johnson, D.B., Maltz, D.A., Hu, Y.C. and Jetcheva, J.G., “The Dynamic Source Routing Protocol for Mobile Ad hoc Networks,” Internet Draft, draft–ietf–manet–dsr–09.txt (2003).

[2] Perkins, C., Belding-Royer, E. and Das, S., “Ad–hoc On–Demand Distance Vector Routing,” RFC 3561 (2003).

[3] Stojmenovic, I. and Lin, X., “Power Aware Localized Routing in Wireless Networks,” Proceedings of the IEEE International Parallel and Distributed Processing Symposium, pp. 371–376 (2000).

[4] Toh, C.K., “Associativity-Based Routing for Ad Hoc Mobile Networks,” Wireless Personal Communications Journal, Vol. 4, No. 2, pp. 103–139 (1997).

[5] Wang, L., Shu, Y., Dong, M., Zhang, L. and Yang, W.W., “Adaptive Multipath Source Routing in Ad Hoc Networks,” Proceedings of the IEEE International Canference on Communications, Vol. 3, pp. 867–871 (2001).

[6] 梅島, 桧垣, “電力制御による競合解消を適用したアドホックルーティングプロトコル,” 電子情報通信学会ネットワークシステム研究会, 信学技報, Vol. 103, No. 443, pp. 57–60 (2003).

[7] “Radio Equipment and Systems (RES); HIPERLAN,” ETSI, Functional Specifications (1995).

[8] “The Official Bluetooth Wireless Info Site,” http://www.bluetooth.com .

[9] “Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) spcifications” IEEE Std 802.11–1997 (1997).

[10] “Wi–Fi Protected Access: Strong, standards–based, interoperable security for today’s Wi–Fi networks,” Wi–Fi Alliance (2003).