アドホックネットワークにおける経験情報の共有方式

3G−04

大塚　卓哉　　小野澤　晃
NTT生活環境研究所
〒180-8585 東京都武蔵野市緑町 3-9-11, Email:otsuka@ma.onlab.ntt.co.jp

1　はじめに

人が身につける通信能力を持つデバイスが、人や環境に関する様々な情報をリアルタイムに取得し、相互にやり取りすることにより、我々の生活の場である実空間とネットワークの仮想空間の融合したユビキタスネットワークの世界の実現が目前に迫っている。その世界においてやりとりされる実空間の情報は個人の生活に直結する経験情報であり、そのようなプライベートな情報の利用形態に関する問題は、現在のネットワークプライバシーの問題よりはるかに重大な問題である。我々はユビキタスネットワークの世界においても、個人のプライバシーコントロールが保障される経験情報共有の方式について検討を行った。

2　要求条件

2.1　前提とするネットワーク

我々が想定するネットワークは、ユーザが保持するPDA等の携帯端末や、生体情報を取得する微小デバイス等でアドホックに構成されるアドホックネットワーク[1]を前提とする。よって、必ずしもインターネットに繋がる状態にあるとは限らず、物理的に限定された範囲で局所的に出来上がるネットワークを想定する。そのようなネットワークにおいて2つのデバイスが互いを発見し、双方向に情報のやり取りを行う必要がある。

2.2　プライバシーコントロール

ユビキタスネットワークにおいてもデバイスが持つ情報の流通をデバイスの所持する個人が完全にコントロールできる(プライバシーコントロール)方式を規定する必要がある。これを、sender anonymityの確保と通信内容の秘匿により実現する。認証のためのCAの存在は必要と考えるが、情報の仲介を行う第三者信頼機関は、権限の集中やシステムのスケーラビリティの観点から排除する。また、プライベートな情報の利用にあたって、情報の利用者の匿名性は必要ないと考えreceiver anonymityはサポートしない。
P2Pネットワークは元来匿名性が高く、Freenet[2]では匿名の情報発信、情報受信を実現しているが、この方式はFile Sharing向けの方式になっており、我々が必要とする、実世界のリアルタイム情報を双方向に共有することには向かない。

3　検討方式

前節の要求条件を満たす方式の検討を行った。デバイス(以降Nodeと呼ぶ)が保持する情報の利用に際し、ソースを特定できないように、Nodeを複数中継する一時的な匿名通信路を構築し、その通信路を介して2Node間は双方向の通信を行う。
提案方式は、何らかのAd-hoc Routing Protocolの実装を前提としており、その上で動作するプロトコルである。また各NodeにNodeの証明書を発行するCAの存在を仮定し、提案プロトコルのレイヤで各Node間の通信は両端認証の上、SSL等で保護される。

3.1　環状通信路

情報提供者(Sender Node)と情報利用者(Receiver Node)間に双方向の通信がある場合、直線状の通信路を用いると、終端部分の通信の折り返しのために匿名性を確保するのが困難である。通信路を環状[3]にし、一方向にメッセージが流れるようにすると、通信の両端(Sender NodeとReceiver Node)を判別する事ができず、問題を回避できる。

3.2　探索

各Nodeは直接通信できる近傍のNodeと周期的に提供可能な情報種について情報交換(Hello Message)し、Nodeアドレス及びNodeの証明書と共にして管理する(Neighbor Table:NTと以降呼ぶ)。NTには上限があり、更新されない古いエントリーから削除されるため、直接通信できないまでも大体近傍にいるNodeが互い

の NT に記録されている。
情報の利用をしたい Node は、利用したい情報種を記述したメッセージ (Query Message) を作成し、自身の NT から適合する相手 Node を選択し探索メッセージを送信する。Query Message には、探索メッセージの作成者の Node アドレス、公開鍵が含まれる。
Query Message を受信した Node は自身の NT から、メッセージ中の、利用したい情報種に適合する Node を選択し Forward する。メッセージには転送上限が設定されており適当な Hop 数 Forward されたら破棄される。図 1 は、Node Z が Query Message を発行し複数の中継 Node を経由し Node A に達する過程である。

3.3 匿名通信路構築

各 Node は、Query Message に応答する形で情報提供を行う場合と、自発的に情報提供を行う場合がある。情報提供を行う Node(Sender Node) は、匿名通信路構築要求メッセージ (request for an Anonymous Connection:RAC) を自身の NT から選択した 2Node に対して送信する。RAC には Receiver Node と共有する秘密鍵の情報、Receiver Node のアドレス、RAC の転送の上限が含まれる。RAC を受信した Node は、RAC が転送上限に達するまで、自 NT から RAC に記された Receiver Node 以外の転送先を選択し RAC を転送する。各 Node は RAC の転送元の Node アドレスと転送先の Node アドレスを保持する (RAC Table:RACT)。転送上限の RAC は Receiver Node へ転送される。匿名通信路は RAC が転送された Node の RACT によってネットワーク上に存在する。図 1 では Query を受信した Node A が RAC を発行する場合を記している。Node A は自 NT から 2 つの転送先 Node(Node B と Node C) を選択し RAC を送信する。RAC を受信した Node はそれぞれの NT から転送 Node を選択し RAC を転送する。どの Node も RAC が Node Z へ向けられたものであることはわかるが、Node A が RAC を発行したことは分からない。
2 つの RAC が転送される過程でできる匿名通信路上の中継 Node が、RACT をもとに Receiver Node と Sender Node 間で共有された秘密鍵で保護されたメッセージを転送することにより、Receiver Node と Sender Node 間の匿名通信 (Sender Anonymity) が行われる。

3.4 考察

本稿では RAC の転送論理について触れていないため、匿名通信路の実際の経路長 (メッセージが実際に転送される Node 数) が必要以上に長くなり、ネットワークに負荷がかかる。提案方式の拡張として、匿名通信路のより効率のよい構築方法を検討しており、それぞれの方式の評価を行っている。

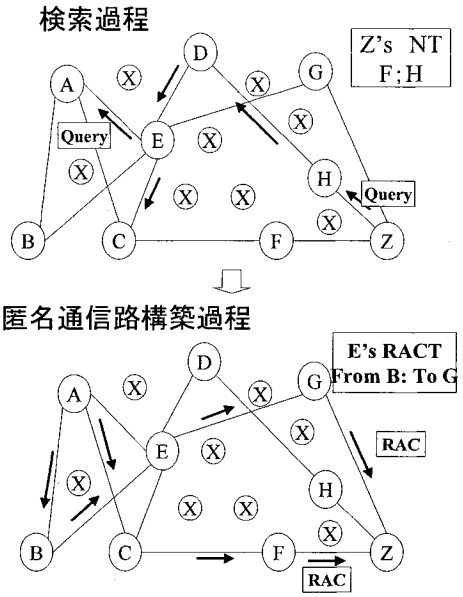

図 1: 検索・匿名通信路構築過程

4 まとめ

様々なデバイス群で構成されるアドホックなネットワークを前提として、デバイス間で一時的な匿名通信路を構築し、情報のやり取りを行う提案方式の骨子を述べた。現在、提案方式に加え、匿名通信路の通信路長を最適化しネットワークにかかる負荷を削減するための追加方式を評価中である。

参考文献

[1] manet http://www.ietf.org/html.charters/manet-charter.html

[2] Freenet http://freenet.sourceforge.net

[3] NETWORKS WITHOUT USER OBSERVABILITY http://www.semper.org/sirene/publ/PfWa_86anonyNetze.html