社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2003－ＣＳＥＣ－22　(27)
2003／7／18

ユビキタスネットワークにおけるプライバシー保護：アドホックネットワークにおける匿名通信方式の提案

大塚　卓哉†　　小野澤　晃†

ユビキタス環境の研究が盛んに行われている。多くの場面で、環境がユーザのコンテキスト情報を取得する事が想定されており、ユーザのプライバシー確保が問題となる。本稿では、ユビキタス環境がユーザのコンテキスト情報を利用する場面を分析し、大量に発生する探索メッセージに紛れる事でモニタリングによる攻撃に対してユーザの匿名性を実現する手法を提案する。

Users Privacy in Ubiquitous Network: Anonymous Communication Technique for Ad Hoc Network

Takuya Otsuka† and Akira Onozawa†

As it is a common assumption in most of the research on the ubiquitous computing environment that the computing environment retrieves user context information to adapt its behavior to user demands, the issues on user privacy draws more attention. In this paper, we analyze the typical procedure of user context retrieval by the ubiquitous computing environment and propose the anonymous communication technique that hides communication messages amongst query messages. The sender can anonymously provide his context information under the traffic analysis by a attacker monitoring the sender.

1. はじめに

ユビキタス環境の実現に向けた研究が盛んに行われており、多くの研究で、ユーザの行動履歴や現在の状況等のコンテキスト情報を利用してユーザにサービスを提供する事が想定されている。環境がユーザの振る舞いを認識する事は、ユーザに適応した環境を構築する為には不可欠であるが、ユーザの振る舞いを追跡する事によるプライバシーの問題を伴う。一方、インターネットにおけるユーザのプライバシ保護を技術的に保護する検討が多数行われてきた。そして、プライバシの保護には、ユーザの匿名性と、情報開示先の限定を実現する技術が必要であるとの立場から、多数の匿名通信方式が提案されてきた[11)~15)]。一般的に、匿名性を実現する為には、想定する攻撃者に応じた暗号処理コストと通信量コストを必要とする。よって、必要とされる匿名性と、許容されるコストを、匿名通信を利用する場面（シナリオ）に即して設計する事が重要である。

† NTT マイクロシステムインテグレーション研究所
NTT Microsystem Integration Laboratories

1.1 想定するシナリオと課題

本稿では、不特定多数が出入りする街中において、その場に居合わせたユーザが所持する携帯端末群がアドホックネットワーク[1)]を構築し、幾つかの端末がゲートウェイとして固定網へ接続しているネットワーク環境[2)]を想定している。多くのアドホックルーティングプロトコルで既にそのようなゲートウェイ機能が検討されている[3)~5)]。そのような環境で、店舗等のサービス提供者が、今現在近く（マルチホップのアドホックネットワークで到達可能な範囲）に居るユーザのコンテキスト情報を取得し、その情報に基いてなんらかのサービスを提供するというシナリオは、今後頻繁に発生するだろう。

このシナリオにおけるユーザのプライバシを保護する為には、ユーザが意図したサービス提供者に対してのみコンテキスト情報を開示し、かつ、開示した相手に対してユーザが匿名である事を実現すればよい。匿名である事により、ユーザが追跡されずプライバシが保護される。また、不特定多数の信頼できない第三者がユーザの通信を中継する為、ユーザとあるサービス提供者が通信した事を第三者に知られない事が、ユーザの匿名性を保障する為には重要である。一方、サービ

ス提供者は一般的に企業であると想定される為、サービス提供者の匿名性を確保する必要性は少ないと考えられる。以上を、コンテキスト情報を提供するユーザをSender、それを受信するサービス提供者をReceiverとしてまとめると、SenderのReceiver、及び、第三者に対する匿名性が必要とされる一方、Receiverの匿名性は不要である。

次に、どの程度強力な攻撃者を想定するべきか検討する。アドホックネットワークは、無線ネットワークである為、物理的近傍に居る端末が出すパケットを取得し、ヘッダ情報からどの端末へ宛てた通信か容易に知る事が可能である。また、近傍の端末を中継端末として遠隔の端末と通信する為、中継端末はどの二端末が通信しているか知る事が出来る。一方、端末間の通信は暗号化され、通信を行っている二端末以外はその内容は知る事はできないと想定される。よって、物理的近傍でパケットの送受信の発生をモニタできる攻撃者（局所傍受者）を想定するべきである。しかし、各攻撃者が単独でモニタできる物理的範囲は極めて限定されており、広範囲をモニタする為には、多くの端末を配置するか、それなりの見返りを支払って多数の端末を結託させなければならない。この為の経済的負担は大きく、広範囲をモニタする攻撃の十分な抑止力となると考えられる。まとめると、結託により広範囲をモニタ可能な強力な攻撃者（広域傍受者）を想定せずに、単独の局所傍受者に対してSenderの匿名性を実現する手法が必要とされる。

1.2 提案手法の概要

シナリオにおいて、まず初めに、サービス提供者の端末は、近くにいるサービスを提供する対象となるユーザの端末を発見する必要がある。シナリオが想定する環境は、端末が動的に出入りする為、必要がある時に、ユーザ端末の発見が実行されるべきである。また、アドホクネットワークを前提としている為、P2P的な分散探索が発見手法として整合する。近年、多数の分散探索手法が検討されており、ユニークな識別子を付与する事が可能なもの（音楽ファイル等）を一つ発見する目的であれば、分散ハッシュテーブルを用いたCAN[6]やChord[7]等の効率のよい手法が報告されている。しかし、本稿が想定するシナリオで要求されるような、端末が動的に出入りする環境で、複数の潜在的候補を発見する目的では、何らかのルールに基いて候補となるすべての端末へ探索メッセージを送信する必要があり、非常に多くのメッセージ数が必要とされる。ブロードキャストはシステムにとって負荷が高い為[8]、負荷を少なくする複数の手法が検討[9),10)]されているが、未解決の課題である。

提案する匿名通信方式では、ユーザ端末間でやり取りされる大量の探索メッセージに紛れて、他のユーザ端末群からなる環状通信路を構築する。探索メッセージに紛れる事で、ユーザは局所傍受者に対する匿名性を確保する事ができる。環状通信路は、始点、終点の判別が困難である為、ユーザは、構築した環状通信路を利用して、局所傍受者を含む他のユーザ端末に対して匿名で通信を行う事が可能である。

2. 従来手法

2.1 送信者匿名通信方式

一般的に、Receiver匿名性を実現する手法[15)]は、Receiverとなる可能性のあるすべてのユーザ端末に、計算コストのかかる非対称鍵暗号化処理を要求する。Sender匿名性のみを実現する事により匿名通信プロトコルを軽量化できる。ここでは、Senderの匿名性のみを実現する方式を議論する。Crowds[11)]は本提案手法が参考としている低コストなSender匿名な方式であり、各ノード(jondo)が確率的に他のjondo、或いは、Receiverを選択しメッセージを転送する事で、SenderとReciver間を複数のjondoから成る匿名通信路を構築する。crowdsは実装による実用性も検証されている。また、Multicast Groupを用いた低コストな手法としてRivulet[12)]が提案されている。他のMulticast Groupメンバー間でメッセージを分割し、複数のメンバーがReceiverに対し分割したメッセージを送信する事で、Senderの匿名性を実現する。いずれも実用的な方式であるが、局所傍受者に対するSenderの匿名性は考慮されていない。

2.2 通信傍受者を考慮した匿名通信方式

通信を傍受する攻撃者に対してSenderの匿名性を実現する手法の基本的な戦略は、Senderでない時もメッセージを余分に発信する事により、真にSenderある時との動作上の判別を困難にする事である。すべての通信をモニタ可能な広域傍受者を想定した手法として、DC-net[13)]や、より大規模な環境でスケーラブルに動作するように階層化されたBroadcast groupを用いるP5（Peer-to-Peer Personal Privacy Protocol）[14)]等がある。いずれの手法も、広域傍受者に対するSenderの匿名性を維持する為に各ノードは不要なダミーメッセージ（Noise）を定常的に発生させ、システム全体の通信量を増大させる。提案手法では、システムの通信量コストを考慮し、ダミーメッセージを発生させ、それに紛れるのではなく、探索メッセージに紛れることで匿名性を実現する。

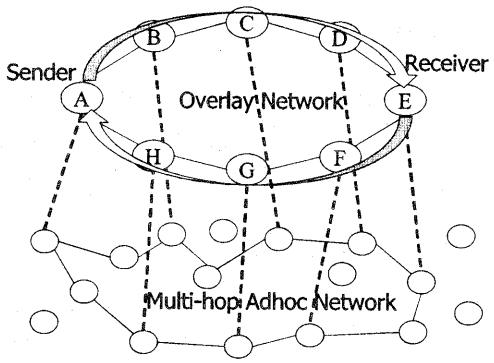

図 1　提案方式の概念図

3. 提案手法

提案方式は、何らかの Ad Hoc Routing Protocol が実装されているものとして、Application 層で Overlay Network としての環状経路を構築する (図 1)。提案手法は、Sender の局所傍受者である攻撃者に対する匿名性を高める為に、探索メッセージに紛れて環状匿名通信路を構築し、Receiver を起点としてその環状通信路上にメッセージを巡回させるプロトコルを特徴とする。以降、本稿では、この Overlay としての環状経路を匿名通信路、或いは、経路と呼ぶ。

3.1 提案プロトコル

ユーザの端末、及び、サービス提供者の端末をまとめてノードとよぶ。提案プロトコルは PKI の存在を前提としており、ノードは認証局により発行された証明書を保持し、ノード間の通信は両端認証の上、アプリケーション層で SSL/TSL 等により保護される（Hello メッセージは除く）。本プロトコルは 5 種類のメッセージ、Hello,Query,RAC,Communication (Comm) ,Dissolution(Diss) からなる。サービス提供者端末（Receiver）は探索メッセージである Query を発行しノード間を伝播させ応答するノードを探索する。Query を受信したノードの中で、匿名で情報を出したいユーザ端末（Sender）は匿名通信路の構築要求である RAC を発行し Receiver との間に環状の匿名通信路を構築する。この匿名通信路上に匿名通信の内容を格納した Comm を流す事で匿名通信を行い、使用後は匿名通信路解体要求である Diss で匿名通信路を解体する。

3.1.1 プロトコルメッセージ詳説

1. 近傍との情報交換 (Hello)

各端末は自身の無線到達範囲に存在する端末に Hello を broadcast する事により、各々の証明書つき公開鍵を定期的に交換する。各ノードは近傍ノードと Hello によって交換した情報を Neighbor Table(NT) に保持、逐次更新して行き、更新されなくなったものから破棄してゆく。よって NT にはそのノードと近い過去に出会った他ノードが登録されている事になる

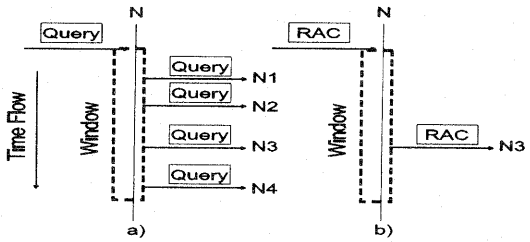

図 2　メッセージ転送の Window

2. ユーザ端末の探索 (Query)

サービス提供者ノードは、コンテキスト情報を提供するノードを探索するために、サービス提供者ノードの証明書 (Receiver-Cert:R-Cert)、Query の転送数 (Qt)、Query の識別子 (Q-ID)、希望するコンテキスト情報種や情報提供の条件 (Req-list) をセットした探索メッセージ (Query) を生成する。自 NT に登録されているノードを転送先ノードとし、転送先ノードとの保護された Query メッセージ：$Enc_{next-node}(Q-ID, Qt, R-Cert, Req-list)$ として送信する。Query を受信したノードは、Qt を 1 減じ自 NT に登録されているノードに転送する。Qt が 0 であれば破棄する。各ノードから発行、及び、転送される Query は、各 Query 毎に、Window 時間以内のランダムな遅延時間が設定される (図 2 a)。図 2 中の縦線は注目しているノードで、時間の経過に伴う動作を表現する。縦線に向かう矢印はメッセージの受信を示し、縦線から出る矢印はノードが発信するメッセージを示す。ここでは、ノード N が Query を受信し、他のノード（N1〜N4）へ転送している。また、余分な Query を減らす為に、同じ Query を受信した場合は Q-ID で識別し破棄し、Query の送信先ノードから既に同じ Q-ID の Query を受けていれば、そのノードへは送信しない

3. 匿名通信路の構築要求（RAC）

本方式では、Query に応答するユーザノードが Sender であり、Query を発行したサービス提供者ノードが Receiver である。Query を受信し、その Query に応答する事を決定した Sender は、Receiver との保護された通信を行う為に、対象秘密鍵 (S-key) を生成し Query メッセージ中の R-Cert の公開鍵で暗号化 ($Enc_{Pub_r}(S-key|pair-bit)$) する。さらに、

ランダムに生成された識別子 (Path-ID) と、最終到達先としての Receiver が設定された匿名通信路構築要求 (RAC:Request for Anonymous Channel) を 1 対生成する ($pair-bit$ には 0 と 1 が、RAC 対のそれぞれに設定され、S-key と連結される)。RAC 対のそれぞれに含まれる Path-ID と $Enc_{Pub_r}(S-key|pair-bit)$ からは、2 つの RAC が対であるとは分らない。Sender は、後に示す拘束条件に従って RAC 発行先ノードを 2 つ決定し、転送先ノードとの保護された RAC メッセージ:$Enc_{next-node}(Receiver, Path-ID, Enc_{Pub_r}(S-key|pair-bit))$ として送信する。RAC を受信したノードは RAC の転送確率 P_{RT} に従い、自 NT から選択したノード、または、Receiver を RAC の転送先に決定する。各ノードは、RAC 受信後、Window 時間以内のランダムな遅延後に RAC を転送する (図 2 b)。各ノードは RAC の転送元ノードと転送先ノード、RAC の Path-ID より RAC テーブル (RACT) を作成する。

4. 匿名通信 (Communication)

Sender と Receiver は RAC 対によって構築された 2 つの経路を環状通信路として利用する。Receiver は対となる RAC を受信し、S-key を取得する。Sender と Receiver は、2 者で共有した S-key で通信内容 (Payload) を暗号化し、転送先ノードとの保護された Comm メッセージ：$Enc_{next-node}(Path-ID, Enc_{s-key}(Payload))$ を生成し、環状通信路上に一方向に流す事で匿名通信を行う。Comm を受信したノードは自 RACT から転送先を決定し、Window 時間以内のランダムな遅延時間後に送信する。Receiver は自身を起点として Comm メッセージを流し、Sender は Payload を更新して環状通信路を巡回させる。

5. 匿名通信路の解体要求 (Dissolution)

Receiver は、匿名通信が終了したら、通信路の解体要求 (Diss) を発行する。Receiver は、S-key で通信内容 (Payload) を暗号化し、転送先ノードとの保護された Diss メッセージ：$Enc_{next-node}(Path-ID, Enc_{s-key}(Payload))$ を生成し、送信する。Diss を受信したノードは該当する匿名通信路の経路情報を RACT から削除し、Window 時間以内のランダムな遅延時間後 Diss を転送する。

3.1.2 Sender の RAC 発行先ノードの拘束条件

Sender である N が生成した対となる RAC を、RAC1、RAC2 とし、それぞれの送信先 Nn と Nm が次の条件を満たすように選択する (図 3)。RAC1 の Nn への送信時から遡ること Window 時間内になんらかのメッセージ (Query、RAC、Comm、Diss)

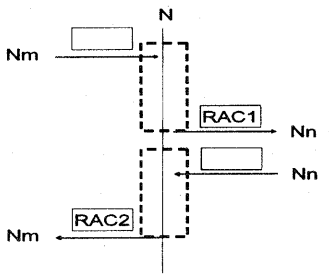

図 3 Sender の RAC 発行先ノード選択の拘束条件

を Nm から受信し、かつ、RAC2 の Nm への送信時から遡ること Window 時間内になんらかのメッセージを Nn から受信している。この条件の理由は次節で述べる。十分な数のメッセージを受信できるように Window 時間が設定されていれば、この拘束条件を満たす以下の手順例は容易に実行できる。Sender は RAC1 の送信先 Nn を NT からランダムに決定し送信する。RAC1 の送信時から遡ること Window 時間内に N にメッセージを送信したノードのリストを作成する。RAC1 の送信の前後、N が Nn から何らかのメッセージを受信後 Window 時間内にリストからランダムに選択した Nm へ RAC2 を送信する。

3.2 提案手法の匿名性

提案方式は、プロトコルの実行時にメッセージの送信に意図的な遅延を作る事で、モニタリング (モニターの対象となったノードの送受信の発生すべてを観測する事が出来る) を行い、後述する Brute-Force-Traffic-Analysis を仕掛ける攻撃者から匿名通信路の経路情報を隠すことで Sender の匿名性を実現する。しかし、同じ匿名通信路上で Comm を繰り返し往復させると、攻撃者が経路情報を知る可能性が高まり、Sender が特定される場合が発生する。そこで、Sender は Comm の送信回数に閾値を設定し、攻撃者が経路を知る前に匿名通信路を再構築する事で匿名性を確保する。以降詳細を記す。

3.2.1 Window 時間の設定

攻撃者から匿名通信路の経路情報を隠し、Sender の匿名性を確保する為に、システムで統一の Window 時間を設定する。サービス提供者により定常的に Query が生成され、各ノードが定常的にメッセージを送受信していると仮定すると、各ノードは、Window 時間内にその NT に登録されている k 個のノードとの間で m 個のメッセージを送信、或いは受信すると期待される。Hello を除くすべてのメッセージはノード間で暗号化され、そのメッセージサイズをシステムで統一する事

により、モニタリングを行う攻撃者がRAC、Comm、Dissを受信した各時点では、その送信元がどのノードから送信されたRAC、Comm、Dissを転送したのか判別できず、攻撃者から匿名通信路の経路情報を隠す事ができる。

3.2.2 攻撃者のモデル

ここでは、匿名通信路上にいない（匿名通信路を構成するノードでない）攻撃者、匿名通信路上にいる（匿名通信路を構成するノードである）がモニタリングできない攻撃者、匿名通信路上にありモニタリングしている攻撃者、の3種類の攻撃者について議論する。本稿が想定するシナリオでは、単独の局所的傍受者による攻撃を想定しているので、ここでは結託による攻撃については議論しない。また、単独の攻撃者がモニタリング可能な範囲は、ノードの密度や下層のアドホックルーティングプロトコルに依存する為、その範囲についての定量的な議論は行わない。

攻撃者が匿名通信路上にいない場合、Query、RAC、Comm、Dissのすべてのメッセージはノード間で暗号化されている為、匿名通信路の存在を知る事は困難である。

攻撃者が匿名通信路上にいるがモニタリングできない場合、RAC、Comm、Dissを順に受信するが、受信したメッセージにはSenderを特定する情報がない為、攻撃者は送り元がSenderであるか判別できない。この場合、RACの平均転送回数をRtとすると、ノード間を送受信されるRACのうち$1/Rt$がSenderから直接送信されたものであるから、攻撃者は、確率$1/Rt$で送り元がSenderであると推測できる。

最後に、攻撃者が匿名通信路上にありモニタリング可能な場合を考える。攻撃者のモニタリング対象ノードに、攻撃者へRACを送信した匿名通信路上1Hop先のノードと、さらにその数Hop先までの匿名通信路上のノードが含まれており、攻撃者が匿名通信路の経路情報を知るために最も有利な状態にいる場合を想定する。攻撃者のモニター対象ノードが、他のノードと繰り返し通信する場合、その通信履歴より匿名通信路の部分的な経路情報を攻撃者が知る可能性がある。攻撃者が経路情報を知る可能性は、同一の匿名通信路上で繰り返しCommを往復させるに従って増加する。次に、本稿が想定するシナリオにおいて、最も強力な上記の攻撃者によるBrute-Force-Traffic-Analysis攻撃について述べ、攻撃者が経路情報を取得する手順を示す。

3.2.3 Brute-Force-Traffic-Analysis 攻撃

攻撃者は、受信したCommの送り元（RACの送り元）をモニタリングする事で、送り元のメッセージ受信歴から、Commを送り元へ送信したノードの候補を知る事が出来る。この候補の中には、現在注目しているComm以外のメッセージを送り元へ送信したノードも含まれるが、Commを送り元へ送信した匿名通信路上の隣接ノード（2Hop先のノード）が必ず含まれている。従って、攻撃者がCommを受信する度に、そのCommの送り元へメッセージ送信したノードを調べ、毎回、候補に含まれているノードを1つに特定する事で、匿名通信路上の隣接ノードを知る事ができる。Brute-Force-Traffic-Analysis攻撃の手順を詳述する。

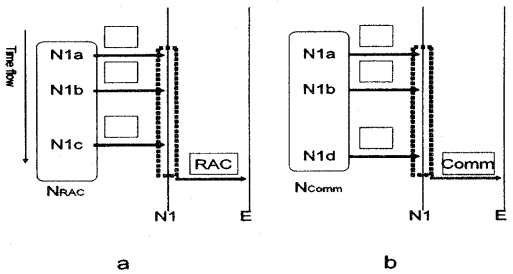

図4 Brute-Force-Traffic-Analysis 攻撃の手順

攻撃者はRAC受信時、RAC受信から遡る事Window時間内に、RACの送信元ノード（N1とする）にメッセージを送信したノードのリスト（N_{RAC}）を作成する（図4a）。図4a中の縦線はそれぞれ、攻撃者（E）、ノードN1（N1）、縦方向に時間経過に伴う動作を表現する。縦線に向かう矢印はメッセージの受信を示し、メッセージの送り元がN_{RAC}である。Eは自身が受信したメッセージがRACである事は知る事ができるが、他のメッセージはノード間通信が暗号化されている為、Query、RAC、Comm、Dissのどれであるかを知る事ができない。さらに、攻撃者は、このRACにより構築された匿名通信路を流れるCommを受信時に、Comm受信から遡る事Window時間内に、N1にメッセージを送信したノードのリスト（N_{Comm}）を作成する（図4b）。次回以降のComm受信時も同様に、Comm受信から遡る事Window時間内に、N1にメッセージを送信したノードのリスト（N'_{Comm}）を作成し、N'_{Comm}に含まれていないN_{Comm}中の要素を消去する。この操作をN_{Comm}の要素が1つになるまで繰り返し☆、最後に残った要素が攻撃者から匿名

☆ Sender の RAC 発行先ノード選択の拘束条件がある為、N_{Comm} の要素数が 1 になるまでこの手順は終了しない。拘束条件が無いと、N_{Comm} の要素が N_{RAC} 中に存在しない要素

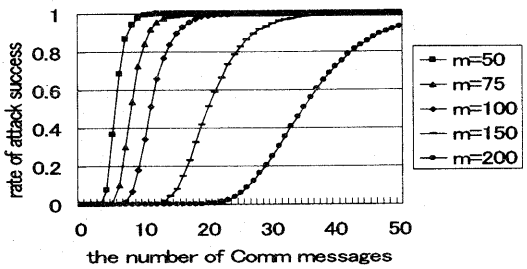

図 5 Brute-Force-Traffic-Analysis 攻撃の成功確率

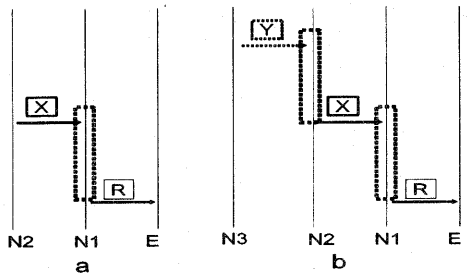

図 6 Brute-Force-Traffic-Analysis 攻撃の手順

通信路上で 2 つ離れた位置にあるノード（N2 とする）である。攻撃者が N2 のモニタリングも可能であった場合、同様の手順で、匿名通信路上で N2 に隣接するノード（N3 とする）を知る事が出来る。

ここでは、攻撃者が N1 から Comm を受信する場合について記したが、攻撃者が、N1 へ Comm を送信する場合は、N1 へ Comm を送信後、Window 時間内に N1 がメッセージを送信したノードのリストを N_{Comm} として、同様の手順が適用される。

この手順により、Comm による匿名通信回数が増加するほど、攻撃者が匿名通信路の経路情報を知る可能性が増加する。各ノードがサイズ k(=100) の NT を持ち、Window 時間に受信するメッセージの期待値が m である場合に、攻撃者が Comm を n 回受信した時点で経路情報を知る事ができる確率を試算した。注目する匿名通信である Comm は毎回同じノードから送信されるが、他のメッセージは各ノードから偏りなく送信されるものとする。図 5 の横軸は Comm の送信回数（n）で、縦軸は攻撃者が上記の手順により経路情報を知る事が出来る確率である。この攻撃手順において、攻撃者のモニター範囲の大きさは、攻撃者が知る経路情報の範囲に影響するが、攻撃者が経路情報を知るまでに要する Comm の送信回数に影響しない☆。

攻撃者が、上記の手順で匿名通信路の経路を知る事ができると、次のようにして Sender を特定できる場合が発生する。攻撃者が、経路情報として、匿名通信路上で 2 ホップ先まで（N1、N2）を知る事ができた場合は、Sender の RAC 発行先ノードの拘束条件により、N1、N2 が Sender であるか否かの判定はできない。何故ならば、攻撃者は、図 6a に示すように、攻撃者が RAC を N1 から受信した時点から遡ること Window 時間に N2 から少なくとも 1 つのメッセージ（X）を受けていた事を知るが、そのメッセージ（X）が RAC である（N1 は Sender ではない）か、拘束条件により存在するその他のメッセージである（N1 は Sender である）か知る事はできないからである。しかし、攻撃者が、経路情報として、匿名通信路上で 2 ホップより先（N1、N2、N3...）を知る事ができた場合は、図 6b に示すように Sender を特定できる場合が発生する。図 6b 中のメッセージ X は必ず存在するが、N1 が Sender である場合、N2 がメッセージ X を送信した時点から遡ること Window 時間に N3 からメッセージ（Y）を受信していたとは限らない。一方、N1 が RAC の中継ノードである場合は、必ずメッセージ（Y）が発生する。よって、攻撃者がメッセージ Y を観測しなかった場合、N1 が Sender であると断定できる。このように攻撃者が経路情報を知る事により、Sender の匿名性が失われる場合が発生する。

従って、Sender は攻撃者に経路情報を知られる前に、匿名通信路を再構築する必要がある。Sender は、図 5 で示したように、k と m より攻撃の成功確率を算出し、Sender が許容できる確率に基いて Comm の送信限界数を決定し、限界数を超えたら Reciever に匿名通信路の解体要求（Diss）の発行を求め、匿名通信路の再構築を行うことで匿名性を確保する。Sender 自身が、攻撃者が実行する手順と同様にして、N_{Comm} を作成し、要素が 1 つになる前に匿名通信路の再構築を行うことも考えられるが、Sender に新たな負荷を要求することになる。Comm 送信回数の閾値に基く匿名通信路の再構築の方が、より簡便で、Sender が求める匿名性に柔軟に対応できる。

3.2.4 Window 時間の設定と通信に要する時間

Window 時間を設定する事で、局所傍受者である攻撃者のモニタリングによる攻撃に対する匿名性を高め

だけになった時点で、N1 が Sender である事が判明し、手順が終了する場合がある。

☆ 攻撃者がモニター対象となっている複数ノードに対し Brute-Force-Traffic-Analysis 攻撃を並行して実行したとしても、各ノードにおいて経路を確定させる為に要する Comm の送信回数は、Comm の送信元において経路を確定させる為に要するそれとほぼ同じである。

られる事を示した。Window 時間を大きくとる（m を大きくとる）と、同一匿名通信路で多数回 Comm を送信しても匿名性を維持できる一方、Sender と Receiver をメッセージが往復するのに要する時間の増大が懸念される。提案手法では、匿名通信路の構築過程で中継ノードに要求される処理は、中継ノード公開鍵で多重に経路情報を暗号化する Onion Routing[15] 等と異なり、非対称鍵暗号処理が無く、負荷が軽い。従って、同一匿名通信路で多数回 Comm を送信する場合に備えて、Window 時間を大きく設定せずに、必要がある場合には匿名通信路を再構築した方が利便性が良い。提案方式は、街中等の公共空間で探索メッセージが大量に発生する場面を想定している為、Sender と Receiver 間のメッセージの往復時間が現実的な範囲になるように Window 時間を設定できると考えられる。反対に、大量の探索メッセージの発生が期待できない場面には適用できない。

4. ま と め

匿名性を実現するには、必要とされる匿名性と、許容されるコストを、匿名通信を利用する場面に即して設計する事が重要である。本稿では、ユビキタス環境が、ユーザのコンテキスト情報を利用する場面を分析し、大量に発生する探索メッセージに紛れて、Sender が匿名でコンテキスト情報を提供する方式を提案した。提案手法では、各ノードはメッセージの転送に意図的な遅延時間（Window）を設け、Sender は同一匿名通信路を利用した匿名通信の回数を制限する事で、モニタリングを行い、Brute-Force-Traffic-Analysis 攻撃を仕掛ける攻撃者から匿名通信路の経路情報を隠し、Sender の匿名性を実現する。一方、Sender と Receiver 間の通信が複数端末を経由する事、意図的な遅延を設ける事により、提案方式は、高い応答速度を要求するアプリケーションには不向きであり、広告、メッセージングサービス等の応答速度を要求しない利用目的へ適用が可能であると考えられる。

参 考 文 献

1) manet http://www.ietf.org/html.charters/manet-charter.html
2) MESHNETWORKS http://www.meshnetworks.com/
3) Ad hoc On-Demand Distance Vector (AODV) Routing http://www1.ietf.org/internet-drafts/draft-ietf-manet-aodv-13.txt
4) The Dynamic Source Routing Protocol http://www1.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt
5) Global connectivity for IPv6 Mobile Ad Hoc Networks http://www1.ietf.org/internet-drafts/draft-wakikawa-manet-globalv6-02.txt
6) S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker,: A scalable content addressable network. in Proc. ACM SIGCOMM (2001).
7) I. Stoica, R. Morris, D. Karger, M. Frans Kaashoek, H. Balakrishnan,: Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications. in Proc. ACM SIGCOMM (2001).
8) S. Ni, Y. Tseng, Y. Chen, J. Sheu,: The broadcast storm problem in a mobile ad hoc network. In Proceedings of the ACM/IEEE international conference on Mobile computing and networking (MOBICOM), pp.151-162, (1999).
9) A. Qayyum, L. Viennot, and A.Laouiti,: Multipoint relaying for flooding broadcast messages in mobile wireless networks, in Proc. 35th Annual Hawaii International Conference on System Sciences (HICSS'02), (2002).
10) Brad Williams, Tracy Camp,: Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks. In Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),pp.194-205, (2002)
11) Reiter,M.K.,and Rubin, A.D,: Crowds: Anonumity for Web transactions. ACM Trans.Info.Sysyt.Security 1(1998)
12) D. Inoue and T.Matsumoto, Rivulet:An Anonymous Communication Method Based on Group Communication, IEICE Trans. Fundamentals, Vol.E85-A, No.1, pp.94-101 (2002)
13) D. Chaum,: The Dining Cryptographers Problem: Unconditional sender and recipient untraceability. Journal of Cryptology, 1(1):pp.65-75, (1988).
14) R. Sherwood, B. Bhattacharjee, A. Srinivasan,: P5: A Protocol for Scalable Anonymous Communication, In Proceedings of the IEEE Symposium on Security and Privacy, (2002).
15) Reed,M.,Syverson,P.,and Goldschlag,D,: Anonymous conections and Onion Routing. IEEE J.Selected Areas in Commun. 16,4,pp.482-494,(1998).