Vol.2010-CSEC-49 No.6
2010/5/11

MANET における匿名通信のための経路構築を必要としない Onion Routing

上口　優太[††]　井上　慎一郎[†]　菅谷　直史[†]
石井　方邦[†]　笹瀬　巌[†]

概要:本論文では，MANET(Mobile Ad-hoc NETwork)の匿名通信において，中継ノードが多重暗号化することで，経路構築が不必要であり，また送信ノードの暗号化による負荷を分散する Onion Routing を提案する．提案方式では，中継ノードが確率的に暗号化を行うことで経路が自動的に構築され，匿名性を保証しつつ宛先へパケットを届けることが可能となる．また，中継ノードの暗号化回数を規制することによりホップ数の増大及びパケットドロップ率の低減が可能となる．計算機シミュレーションにより，パケットの到達時間，および宛先ノードがメッセージを入手できる確率を評価する．

Path Designless Onion Routing in MANET for Anonymous Communication

Yuta Kamiguchi[††]　Shinichiro Inoue[†]
Naofumi Sugaya[†]　Masakuni Ishii[†]
and Iwao Sasase[†]

In this paper, we propose Onion Routing that need not path design, and can load dispersion by relay nodes encrypt multiply in MANET(Mobile Ad-hoc NETwork) for anonymous communication. In this proposition, route is built automatically, and can send packet to destination node with secure anonymity by relay nodes encrypt stochastically. The number of hops and drop rate of packet can be reduced by controlling encryption of relay node. Performance evaluation by simulation show the time of packet arrival, and probability that destination node can get messages.

1. はじめに

近年，ユビキタス社会を支える技術として，ノード同士が協調しあい自律分散的に柔軟なネットワークを構築する無線アドホックネットワーク(MANET:Mobile Ad-Hoc NETwork)が注目されている 1)2)．自立分散制御に基づく MANET は，拡散性や耐障害性に優れ，例えばノード数が常時変化している場合においてもネットワークの維持が可能であり，また，中継ノードとして選択されていたノードが電力不足で使用できなくなる場合においても，他のノードが新たな中継ノードとなることにより通信の再開が可能である，といった特徴を持つ．これらの特徴を生かし，MANET は基地局などのインフラがない災害現場やイベント会場において，ノード同士が即興でネットワークを構築し，情報の収集や管理を行う，といった使用方法が期待されている．

また，インターネットの普及に伴い，近年個人情報の流出などプライバシーの確保が重要となりネットワークユーザの匿名性を保護するために様々な匿名通信の研究が行われている 3)．匿名通信は，電子投票やネット上でのアンケートなどにおいて利用が期待されており，様々な暗号技術やルーティング方式を組み合わせることで実現されている．

MANET は教室やイベント会場でも即興で構築されるネットワークであり，MANET を用いてその場でアンケートを取るといった使用方法も十分に考えられる．しかしながら，MANET はノード同士が協調し合うことで構築されるネットワークであるがために，他のノードによるアンケート結果の盗聴やアンケートの送信者がどのノードであるか分かってしまう恐れがある．そこで，近年暗号化やルーティングにより上記の問題を解決する MANET における匿名通信が注目されている． MANET における匿名通信では，経路匿名性，送信元匿名性，宛先匿名性の 3 つの匿名性の保証が重要である．ここで，経路匿名性とはどのような経路で通信が行われているかを秘匿にすること，送信元匿名性とはどのノードが送信元ノードであるかを秘匿にすること，そして宛先匿名性とはどのノードが宛先ノードであるかを秘匿にすることである．

MANET はインターネットとは様々な点で異なるため，MANET に適した形で匿名通信方式を考える必要がある．従来の MANET における匿名通信では，暗号化技術や特殊なルーティング技術により匿名通信方式を確立しようとしてきた．従来,4)の方式ではグループ署名を利用した方式が研究されており，5)ではネットワークエリアを分割する方式，3)6)7)では Onion Routing を用いた方式の研究が行われている．4)の方式では，ノード間での協調が必要となるため，宛先が送信元を特定できないという送信元匿名性のみを保証するのみであり，全ての匿名性を満足に保証することはできないという問題がある．一方で 5)の方式では全ての匿名性を保証することは可能ではある

† 慶應義塾大学理工学部情報工学科
†† kamiguchi@sasase.ics.keio.ac.jp

Vol.2010-CSEC-49 No.6
2010/5/11

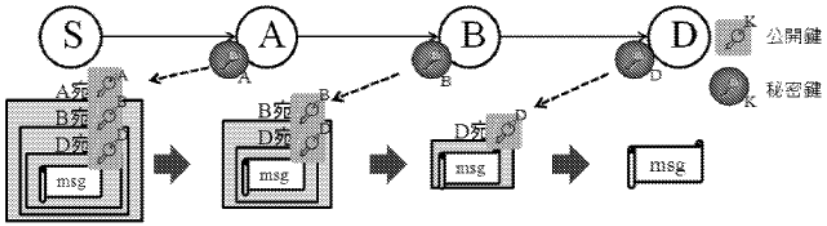

図 1　Onion Routing の動作例

が，前提として GPS が必要不可欠であり，また RF(Rondom Forworder)という特殊なノードの設定が必要となる．3)6)7)の研究では，通信に先立って予め経路構築行うためにを宛先匿名性および経路匿名性が保証されず，また送信元ノードがホップ数分の暗号化処理を強いられるため，負荷が集中するといった問題がある．

そこで本論文では，経路匿名性，送信元匿名性，宛先匿名性の全ての匿名性を保証し，また特殊な条件を必要とせず，更に送信元ノードの負荷を分散することが可能な Onion Routing を提案する．本方式では，初めに経路匿名性を保証するために中継ノードが確率的に暗号化を行う．これにより，通信に先立って予め経路を構築する必要がなくなり，暗号化次第で次ホップノードが変化することで通信経路に対して匿名性を保証することが可能となる．更に，経路を予め構築する必要がないために，宛先匿名性を保証することが可能となる．次に送信元匿名性を保証するために，送信ノードはメッセージに対して多重暗号化を行う．これにより，他のノードからは送信ノードの特定が困難となり，送信元匿名性を保証することが可能となる．以上により，3 つの匿名性を全て保証することが可能となる．また，中継ノードが随時確率的に暗号化を行うため，送信元ノードのみが多重暗号化を行っていた従来と比較して送信元ノードにおける多重暗号化による負荷の分散が可能となる．

以降，2 章では Onion Routing の動作について説明する．3 章では従来の MANET における Onion Routing を取り上げ、その問題点について述べる．4 章では提案方式について述べる．5 章では提案方式の評価を行い，最後に 6 章で本稿をまとめる．

2. Onion Routing

本章では，一般的な Onion Routing についての概要を説明する．元々Onion Routing はインターネット上で匿名通信を行うために開発されたものである．Onion Routing は多重暗号化を用いた方式で，この多重暗号化によりメッセージの内容，送信元，宛先を秘匿にすることが可能となる．以下，図 1 を用い，Onion Routing の動作を示す．

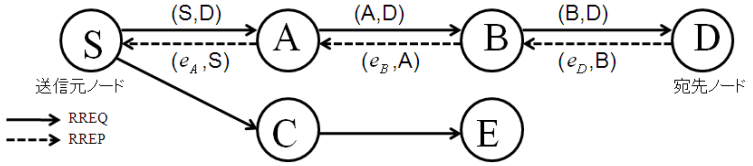

図 2AODV における経路構築の例

1. 送信者 S は宛先 D に対するメッセージを作成する．
2. S は D までの経路上全てのノードの公開鍵を入手する．
3. S はメッセージに対して，D の公開鍵，B の公開鍵，A の公開鍵の順で多重暗号化を行う．
4. S は多重暗号化されたメッセージを A に向けて送信する．
5. A は受け取ったパケットを自身の秘密鍵を用いて復号し, B に向けて送信する．
6. B は A 同様に復号処理を行い，D に送信する．
7. D が自身の秘密鍵で復号すると，メッセージを取り出すことができる．

以上が Onion Routing の動作である．ノード A にとって送信元は S, 宛先は B となり，ノード B にとって送信元は A，宛先は D となっている．しかし，多重暗号化が何重に施されているかが未知であるため，A から見た場合 S は単なる中継ノードであり，S の前にも送信者がいたと考えることが可能となる．したがって，S が送信元であると特定されることはなく，送信元匿名性が保証される．また，B からみた場合，D は単なる中継ノードであり，D の先にも宛先があると考えることが可能であるため，D が宛先であると特定されることはなく，宛先匿名性が保証される．したがって，インターネット上では Onion Routing を用いることで送信元匿名性および宛先匿名性を保証する匿名通信を実現することが可能となる．

3. 関連研究 3)

本章では，MANET における Onion Routing の関連研究とその問題点ついて述べる．

3.1 MANET における Onion Routing

従来の MANET における Onion Routing では，経路構築を行い，その後に 2 章で述べたような方式を用いて通信を行う．従来の MANET における Onion Routing ではルーティングプロトコルとして AODV を用いているものが多く，ここでは AODV を用いた場合について述べることとする．図 2 に AODV における経路構築の例を示し，以下経路構築について述べる．

1. 送信元ノード S は宛先ノード D までの経路を見つけるために，近隣ノードへ RREQ パケットを送信する．

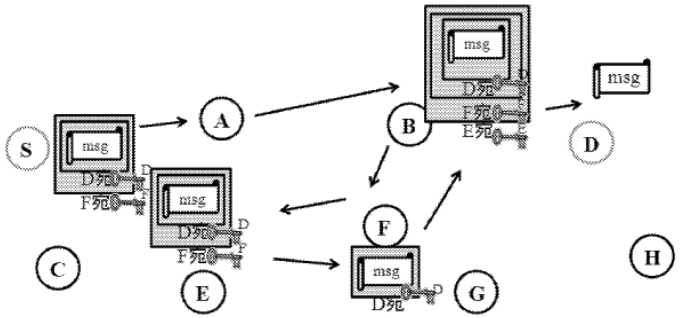

図 3 提案方式の動作例 1

2. RREQ パケットを受け取ったノード A および C は，自身が宛先ノードでないため，自身の近隣ノードへ RREQ パケットを送信する．

3. 同様にノード B は宛先ノードでないため RREQ パケットを送信する．

4. RREQ パケットを受け取ったノード D は宛先ノードであるため，送信元ノード S に向けて RREP パケットを返信する．

5. RREP パケットには中継するノードの情報などが記載されており，送信元ノードがこの RREP パケットを受け取ることで経路を構築することが可能となる．

以上が AODV の基本的な動作である．基本的な AODV の RREQ パケットには送信元ノードの情報も含まれているため，送信元匿名性が保証されない．そこで，従来の MANET における Onion Routing では送信元ノードの情報を入れずに，1 つ前のノードの情報を入れることで RREQ パケット，RREP パケット共に自身の前後のノードの情報しか手に入らないようにしている．図 2 の RREQ パケットでは(1 つ前のノード情報，宛先ノードの情報)となっており，例としてノード A とノード B の間では(ノード A の情報，ノード D の情報)となっている．また，RREP パケットでは(鍵を取得するための情報，RREQ を送ってきた元のノードの情報)となっており，例としてノード A とノード B の間では(ノード B による鍵を取得するための情報，ノード A の情報)となっている．これにより送信元匿名性を保証することが可能となる．

3.2 問題点

従来方式 3)の MANET における Onion Routing では送信元から宛先までの経路を最初に構築した上でインターネットにおける Onion Routing と同様の手順で多重暗号化し，通信を行う．しかしながら，この方法では以下の 2 つの問題があると考えることができる．1 つ目の問題は，経路構築の段階で RREQ パケットおよび RREP パケットをやりとりするために宛先匿名性と経路匿名性が保証されないことである．RREQ パケットには「宛先 D までの経路を知りたい」といった内容の情報が入っているため，宛先ノードの情報は秘匿とはならず，宛先匿名性が保証されない．また，最短経路でパケットのやり取りを行うことおよび RREP パケットの中継により，経路が把握されやすくなり，経路匿名性も保証されないという問題がある．2 つ目の問題は，送信元ノードの多重暗号化による負荷である．2 章で述べたように，送信元ノードは中継ノードの数だけ公開鍵を入手し多重暗号化する必要がある．これは中継ノードの数が少ないときには大きな負荷とはならないが，中継ノードの数が増えるに連れて，送信元ノードの多重暗号化による負荷が莫大になるという問題が考えられる．

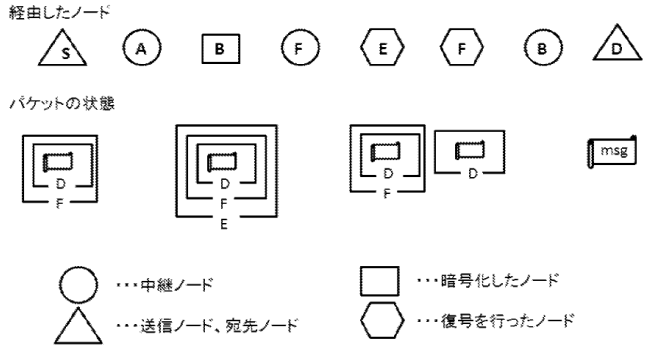

図 4 提案方式の動作例 2

4. 経路構築を必要としない Onion Routing

本章では 3.2 で述べた宛先匿名性と経路匿名性が保証されない問題，および送信元ノードの負荷が莫大になる問題の 2 つの問題を解決するために，経路構築を必要とせず，送信元ノードの負荷分散を可能とする Onion Routing について述べる．

4.1 経路構築を必要としない方式

本論文では，中継ノードが暗号化することでパケットの次ホップ先ノードが変化し，最短ルートを通ることなくメッセージを送信する方式を提案する．本方式を用いることにより，経路匿名性，送信元匿名性，宛先匿名性の 3 つの匿名性全てを保証することが可能となり，また送信元ノードの多重暗号化による負荷を低減することが可能となる．以下，図 3 および図 4 を用いメッセージの作成から宛先がメッセージを入手するまでの流れを示す．前提として全てのノードの公開鍵が入手可能であるとする．また，何の暗号化も施されていないものをメッセージとし，暗号化されたものをパケットという呼び方で統一する．

1. 送信者 S は宛先 D 宛のメッセージを作成する．

2. S は D の公開鍵および任意のノードの公開鍵を入手する．

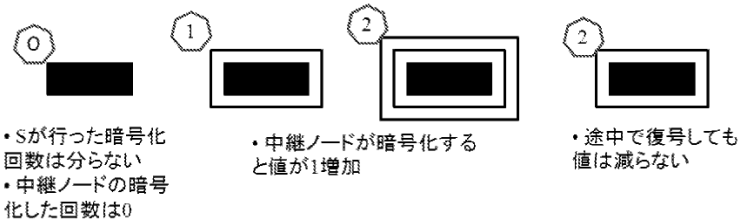

図 5 暗号化回数の規制例

3. S はメッセージを D の公開鍵，任意のノードの公開鍵の順で多重暗号化する．
4. S は最初の宛先(ここでは 2 で手に入れた任意のノードが最初の宛先となる)に向けて送信する．
5. 中継ノードはこのパケットに対し，自身宛のパケットであれば復号して次の宛先へ送信．自身宛でない場合，記載されている宛先へ送信するか，もしくは暗号化して宛先を変えて送信するかを確率的に決定する．
6. 5 の操作を繰り返し，最後に D が自身の秘密鍵で復号することで，メッセージを取り出すことが可能となる．

以上が提案方式の動作である．これにより，通信に先立って最短経路を構築せずにメッセージをやりとりできるため経路匿名性が保証される．また中継ノードは入手したパケットに記載されている宛先が最終宛先であるかどうかが分からないため，宛先匿名性が保証されることとなる．また，従来の方式では送信元ノードが中継ノードの数だけ多重暗号化する必要があったが，この方式では中継ノードの数が増えても送信元ノードの暗号化負荷はある一定の水準で抑えることが可能となるため，送信元ノードの暗号化負荷が莫大になることはなく，送信元ノードの暗号化負荷の低減が可能となる．

4.2 暗号化回数の規制方法

1 つのメッセージに対する暗号化回数を規制しない場合，中継ノードの暗号化回数が多くなり，宛先ノードに到達するまでのホップ数の増大，パケットドロップ率の増加が問題となる．そこで，1 つのメッセージに対する暗号化回数の規制が重要となる．図 5 に暗号化回数の規制例を示す．図 5 に示すように，本方式では以下の方法で暗号化回数を規制することとする．

- 中継ノードの行った暗号化回数をヘッダに記載する．
- 途中で復号したとしても，値は不変．
- 暗号化回数が少ない場合には高確率，多い場合には低確率で暗号化処理を行う．

この方法を取ることで，ホップ数の増大およびパケットドロップ率の増加といった問題を解決することが可能となる．この方法では一見，記載されている暗号化回数の値が 0 と表記してある場合に匿名性が保証されないように見えるが，送信元ノードが行った暗号化回数は送信元ノード以外のノードにとっては未知であり，復号しても記載されている暗号化回数の値が減らないため，各種匿名性を保証することが可能となる．また，要求される匿名性に応じて値の限界値を定めることで，その要求に応じた高い匿名性を確保することが可能となる．

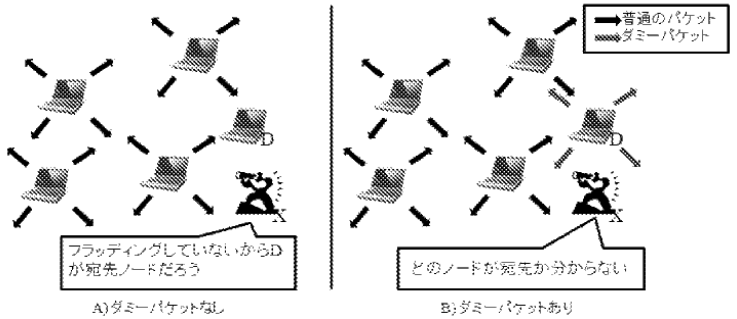

図 6 ダミーパケットの例

4.3 ダミーパケット

MANET では，パケットを送信する際フラッディングを用いる．そのため，宛先ノードがパケットを入手した後にフラッディングを行わないと近隣ノードから宛先であると特定される危険性がある．そこで提案方式では，宛先ノードはパケットを受け取った後にダミーパケットを送信することとする．この方式により，宛先ノードの特定を防ぐことが可能となる．図 6 にダミーパケットの例を示す．図 6 に示すように宛先がダミーパケットをフラッディングすることで，宛先であると特定される危険性がなくなる．しかし，このダミーパケットによってネットワーク全体の負担が増加することが考えられる．そこで，ダミーパケットの TTL を短くすることでネットワーク全体の負担を軽減することとする．

5. 特性評価

計算機シミュレーションにより，パケットの到達時間および宛先ノードがメッセージを入手できる確率の評価を行う．ここで，宛先ノードがメッセージを入手できる確率とは宛先ノードにパケットが届き，尚且つ復号できる状態であることを示す．表 1 にシミュレーション諸元を示す．また，ルーティングプロトコルには AODV を用いることとする．

表 1 シミュレーション諸元

シミュレータ	NS-2(ver.2.34)
ノード数	50
シミュレーション範囲	800m×800m
パケットサイズ	256byte,512byte
MAC	IEEE 802.11
ノードの配置	ランダム
初期暗号化回数	2

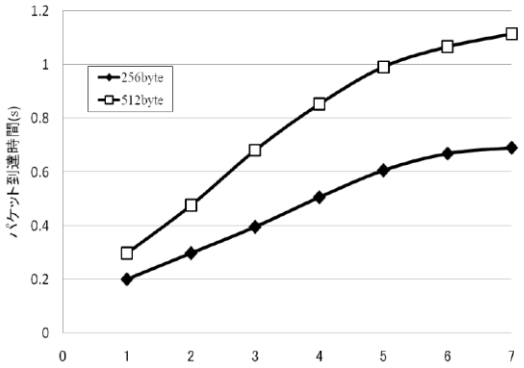

図 7 中継ノードの最大暗号化回数に対するパケットの到達時間

5.1 中継ノードの暗号化回数に対するパケット到達時間

図 7 に中継ノードの最大暗号化回数に対するパケットの到達時間を示す．横軸を中継ノードの最大暗号回数とし，縦軸をパケット到達時間とする．図 7 を見て分かるように，中継ノードの最大暗号化回数が増えるに連れて，ホップ数が増加し到達時間が増加することが分かる．また，4.2 章で述べたように，中継ノードの暗号化回数が少ない時は高確率，多い時には低確率で暗号化するという規約を設けているため，中継ノードの暗号化回数が増加するに連れてパケット到達時間の上がり幅が減少していることが分かる．したがって，中継ノードの暗号化回数を増やすことによる匿名性の強化とパケット到達時間はトレードオフの関係にあると言える．

5.2 中継ノードの暗号化回数に対する宛先ノードがメッセージを入手できる確率

図 8 に中継ノードの最大暗号化回数に対する宛先ノードがメッセージを入手できる

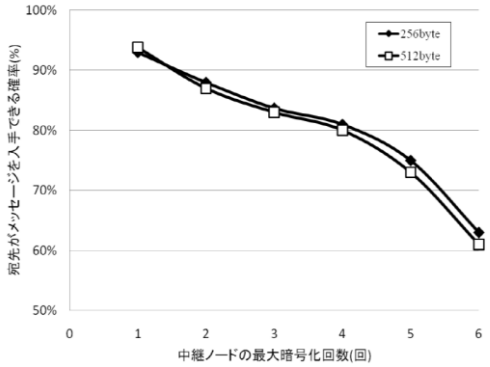

図 8 中継ノードの暗号化回数に対する宛先ノードがメッセージを入手できる確率

確率を示す．横軸を中継ノードの最大暗号化回数とし，縦軸を宛先ノードがメッセージを入手できる確率とする．中継ノードの最大暗号化回数が増加するに連れて宛先ノードがメッセージを入手できる確率は減少している．これはノードの配置をランダムにしているため，途中の宛先ノードが 1 つでも電波範囲から外れている場合に届かなくなるためだと考えられる．また，中継ノードの最大暗号化回数が 4 回以降では宛先ノードがメッセージを入手できる確率が急激に減少していることが分かる．これは，宛先ノードにパケットが届いたとしても，復号不可能な状態であることが多くなるためだと考えられる．以上より中継ノードの暗号化回数と宛先がメッセージを入手できる確率にもトレードオフの関係があり，中継ノードの暗号化回数が 3 回までは実用可能な範囲であると言える．

以上の評価により，匿名性とパケット到達時間および宛先がメッセージを入手できる確率にはトレードオフの関係が成り立っており，要求する匿名性に応じて中継ノードの暗号化回数の上限を設定することで有効な方式に成り得ると言える．

6. 結論

本論文では，MANET における匿名通信で，中継ノードが暗号化することにより，経路構築が不必要となり，また送信元ノードの負担を軽減する Onion Routing を提案した．中継ノードによる暗号化により次ホップの宛先ノードが自動的に更新されるため，経路匿名性が保証され，経路構築をしないことから宛先匿名性も保証される．また，送信元匿名性は従来と同様に多重暗号化することで保証している．さらに，多重暗号化の回数を規制することで，多重暗号化の回数が過多になることを防ぎ，ダミーパケットの導入により更なる匿名性の向上を図った．計算機シミュレーションにより，パ

ケットの到達時間および宛先がパケットを入手できる確率を示した．今後の課題として，宛先ノードがパケットを入手できる確率を向上するために再送方法や Ack の送信方法などを検討する予定である．

謝辞　本論文の一部はグローバル COE プログラム[アクセス空間支援基盤技術の高度国際連携]により行われた．

参考文献

1) S. Corson, J. Macker,“Mobile ad hoc networking(MANET): Routing protocol performance issues and evaluation consideration ”, IET-FRFC25010, January 1999.
2) Bangnan Xu, Hischke S and Walke B, “The role of ad hoc networking in future wireless communications” Communication Technology Proceedings, 2003, ICCT 2003, Vol 2, pp.1353-1358, Apr. 2003
3) Lui Yang, Markus Jakobsson and Susanne Wetzel, “Discount Anonymous On Demand Routing for Mobile Ad hoc Networks” Securecomm and Workshops, pp.1-10, Aug. 2006
4) Lianyu Zhao and Haiying Shen, “A Low-cost Anonymous Routing Protocol in MANETs” , Computer Communications and Networks, pp.1-6, Aug, 2009
5) Jung Ha Paik, Bum Han Kim and Dong Hoon Lee, “A3RP:Anonymous and Authenticated Ad Hoc Routing Protocol” , International Conference on Information Security and Assurance, pp.67-72, Apr. 2008
6) Xiaoqing Li, Hui Li, Jianfeng Ma and Weidong Zhang, “An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks” , Fifth International Conference on Information Assurance and Security, Vol 2, pp.287-290, Aug, 2009
7) Imad Aad, Claude Castelluccia and Jean-Perre Hubaux “Packet Coding for Strong Anonymity in Ad Hoc Networks”, Securecomm and Workshops, pp.1-10, Sept, 2006