ISSN 2186-5647

秘密分散法に基づく DTN 耐攻撃ルーティングに関する一考察

日大生産工(院)　○荒井　裕典
日大生産工　　新井　雅之

1.　まえがき

現在，継続的なネットワーク接続が不可能な極限的環境や移動環境での技術問題の解決策として遅延耐性ネットワーク(DTN: Delay Tolerant Networking)が提案されている[1]．DTN ではデータ転送は中継ノードに依存しており，中継ノードへの攻撃，盗聴や中継ノード自身の障害によってデータの損失や大きな遅延が発生する可能性がある[2].

本報告では，データの安全性と到達可能性の向上のために，DTN における危険ノードの存在を考慮した，マルチパスと秘密分散法による冗長性の付加に基づく接触回避ルーティングを提案する．シミュレーションを行い，提案手法の転送成功確率，平均遅延時間について評価する．

2.　関連研究

2-1.　遅延耐性ネットワーク

遅延耐性ネットワークとはエンドツーエンドで送信者から受信者まで常時繋がっている通信ではなく，ストアアンドフォワード方式で転送を行うネットワークである．図1にDTNにおけるデータ転送の例を示す．図中の実線は現在繋がっているリンクを，点線は繋がっていないリンクを示す．まず，送信者と接触したノードにデータが渡される．データを受け取ったノードは次に他のノードとリンクが繋がるまでデータを保持する．そしてまたリンクが繋がったノードにデータを渡す．この繰り返しで送信者から受信者まで通信をするものである．

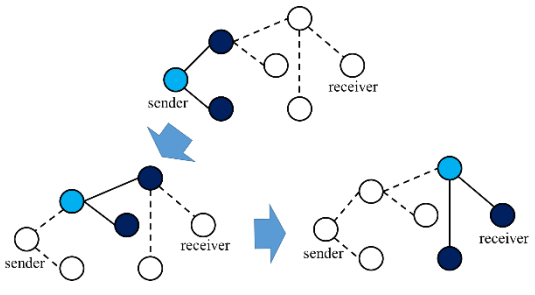

図 1.　DNT におけるデータ転送例

2-2.　DTNにおける接触回避ルーティング

小薄らは攻撃ノードが存在するDTNを想定し，接触回避ルーティングを提案している[2]．各ノードのネットワーク内での位置，他の中継ノードとの接触の有無や接触確率は既知であるとする．これらの情報はコンタクトグラフで表現可能である．図2にコンタクトグラフの一例を示す．図2中の実線エッジはリンクが繋がる可能性があることを示す．λ_{ab}，λ_{bc}，λ_{bd}はノードaとb, bとc, bとdの接触確率を示している．小薄らの提案手法では，データの複製および分割は行わず，危険ノードと接触する頻度の高いノードを識別し，回避して転送を行う．

2-3.　(*k*, *n*)閾値法

(*k*, *n*)閾値法は秘密分散法の一種であり，データの可用性，機密性を両立させる技術である[3]．秘密情報を *n* 個の分散情報に分割し，*n* 個の中から *k* 個集めると元の秘密情報が復元できる．(*k*, *n*)閾値法では情報論的安全性が保証されており，*k* 個未満の分散情報を紛失しても機密情報が流出しないので機密性が保証される．また，全体量の *k*/*n* から秘密情報が復元できることから可用性が向上する．(*k*, *n*)閾値法は冗長性を付加するため，総データ量が増加する．分散，復号処理の高速化や総データ量の縮小が可能な排他的論理和を用いた(*k*, *n*)閾値分散法が提案されている[4, 5].

3.　提案手法

本報告では DTN における危険ノードの存在を考慮し，秘密分散法と 3 種類の戦略を組み合わせた転送プロトコルに基づくルーティングを提案する．提案手法では，(*k*, *n*)閾値法を用いて元データに冗長データを付加し，任意の個数 *n* に分割して *n* 個の分散データを作成する．本モデルでは攻撃ノードはデータを盗聴するのみで，盗まれたデータは消失しないものとする．また，攻撃ノード自身も他の中継ノードと同様にデータの転送を行うものとする．

(*k*, *n*)閾値法(C)をベースに，以下の3種類の戦略を組み合わせた転送プロトコルを提案する．

Note on DTN Anti-Attack Routing Based on Secret Sharing

Hironori ARAI,　Masayuki ARAI

1)危険隣接ノード回避(L):
危険ノードと接触する可能性のあるノードへの転送の回避
2)危険ノード回避(A):
危険ノードへの転送の回避
3)遠回り回避(D):
転送ホップ数が増加する転送の回避

4. 実験結果

シミュレーションにより，提案手法の評価を行った．コンタクトグラフの生成に際して，各ノードの接触の有無を確率 0.4 で設定した．ノード(i, j)の接触確率λ_{ij}は，接触する可能性がある場合，平均 10，標準偏差 5 の正規分布に基づいて設定した．ノード(i, j)の接触時間間隔はλ_{ij}の逆数を平均とする指数分布となる．また，繰り返し回数は 100 回で行っている．送信者が送信を開始してから期限内で k 個の分散データが受信できた場合を送信成功とする．任意の時間内に k 個受信できなかった，あるいは k 個受信する前に攻撃ノードに k 個収集された場合は失敗とする．また，転送プロトコルによっては転送可能ルートが存在しない場合があり，これも失敗とする．

図 3 に総ノード数 100，(4, 8)閾値法において攻撃ノード数を変化させた場合の転送成功確率を示す．また，図 4 に同条件での成功時の平均遅延時間を示す．図中のラベルの C，D，A，L は上の(C)，(D)，(A)，(L)を示す．ラベル(A+D)は危険ノードとそれに接触する可能性のあるノードへの転送の回避を示している．図 3 は(C), (D), (A), (L)の全てを組み合わせた転送プロトコルが，最も成功確率が高いことを示している．また，転送ホップ数が増加する転送の回避が受信成功率の向上に寄与することが分かる．図 4 から，受信成功率が高い転送プロトコルは平均遅延時間が長いことがわかる．

5. まとめ

本報告ではDTNにおいて，(k, n)閾値法による冗長性の付加と，危険ノードの回避を考慮した上での適切なルーティングについての提案，比較を行った．データ受信成功率を上げるには，攻撃ノードに接触する可能性があるノードに転送しないことと，ホップ数が増加しない転送が必要だという結果を得た．また，受信成功率と平均到達時間・平均失敗時間はトレードオフの関係であることが分かった．これは転送条件が厳しいほど，次に転送な中継ノードと接触するまでのデータ保持時間が伸びるためと考えられる．

(k, n)閾値法は冗長性を付加するため，総データ量が増加する．今後の課題として排他的論理和に基づく(k, n)閾値法を用いた場合でのデータ量の評価が挙げられる．

参考文献

[1]鶴正人，他． “DTN技術の現状と展望”，通信ソサイエティマガジン No. 16, pp. 57-68, 2011年.
[2]小薄 他, “遅延耐性ネットワークにおける接触回避ルーティング”，電子情報通信学会IN研究会技術研究報告，IN2015-57, pp. 25-28, 2015年.
[3]保坂 他, “秘密分散法とその応用”，東芝レビュー, Vol.62 No.7, pp. 23-26, 2007年.
[4]藤井 他, “高速な(2,n)閾値法の構成とシステムへの応用”，コンピュータセキュリティシンポジウム2005予稿集 ，pp. 631-636, 2005年.
[5]多田 他, “閾値3の秘密分散法の構成法”，コンピュータセキュリティシンポジウム2005予稿集, pp. 637-642, 2011年.

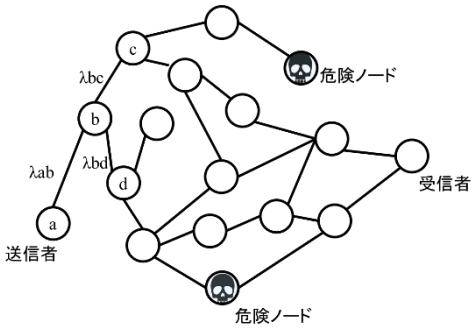

図 2. コンタクトグラフ例

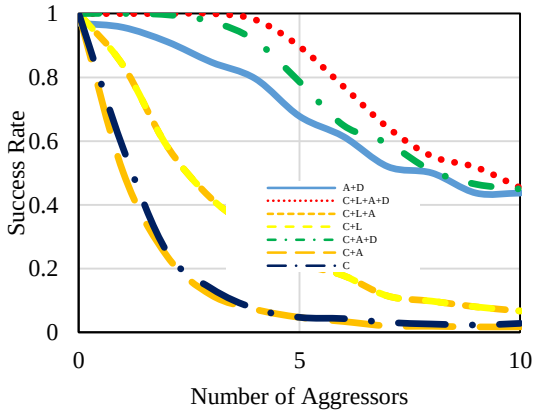

図 3. 攻撃ノード数による受信成功率の変化

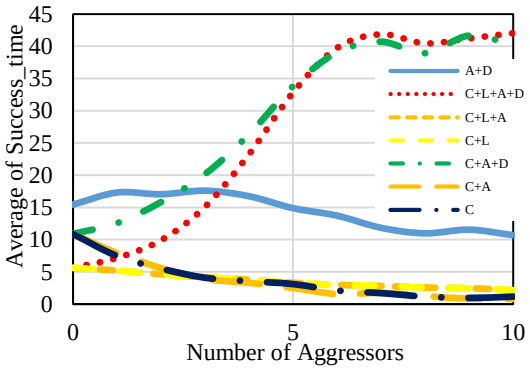

図 4. 攻撃ノード数による成功時の平均遅延時間の変化