伝染型ネットワークにおける信用度評価に基づく不正ノードの自律的回避

岸本 一希*, 松本 倫子（九州産業大学）

Autonomous Malicious Node Avoidance with Trust Evaluation in Epidemic Networks

Ikki Kishimoto, Noriko Matsumoto (Kyushu Sangyo University)

1. はじめに

不安定・不確実な通信環境でできるだけ定常的なネットワークを構成するのは、災害時の応急ネットワークや野外の IoT ネットワークなどで重要な意義を持つ。有望な方策として人工衛星ネットワークが期待されているが、現状ではまだコストや普及度などから、簡便とは言い難い。このような状況に対処するための技術の一つとして、伝染型ネットワーク（Epidemic Networks）があり、メッセージをネットワーク内に拡散して宛先まで到達することを期待する [(1)]。しかし、ネットワーク内に不正なノード（ホストやデバイス）が存在してメッセージを破棄したりすると、適切な経路での到達が阻害されるとともに、ネットワーク資源が浪費される。そこで、本研究ではネットワーク内の信用度に基づく防御として、不正ノードの所在を推定して自律的に迂回・回避する経路制御の方式を提案する。

2. 伝染型ネットワーク

インターネットの TCP/IP は、長い通信遅延，頻繁なパケット損，間欠的な通信リンクなどを想定しておらず、そのような劣悪な通信環境ではネットワークを構成できない [(2)]。通信が間欠的に断続するような時間的な不安定さに対しては、切断時にはメッセージを一時的に保持しておき、接続時に送出する蓄積型転送通信が考案され、宇宙探査機や惑星探査機から地球への通信などで実用化されている。通信経路が不定になる空間的な不安定さに対しては、通信可能な領域までメッセージを運搬していく Message Ferry という手法なども考案されている。無線通信のネットワークでは、構成ノードが移動することでも、同様の不安定さが生じる。

別方向からの方策として、伝染型ネットワークでは、メッセージを保持するノードは、他ノードとすれ違うなど無線通信可能な範囲に入ると（接触すると）、そのノードにメッセージの複製を転送する。これを他ノードと接触する度に繰り返すことで、メッセージを拡散していく。ただし、ネットワーク全体の中にメッセージの複製が充満してしまい、通信量が過大になる。これを抑制するために複製数に上限を設けたのが、Spray and Wait である [(3)]。また、過去の接触履歴に基づいて配達予測確率を算出し、宛先ノードへの確率がより高いノードへメッセージを転送するのが PRoPHET であり [(4)]、インターネットの RFC にもなっている [(5)]。

3. 伝染型ネットワークへの攻撃

伝染型ネットワークのように不特定多数の中継ノードで転送していくネットワークは、全てのノードが正しく中継するという性善説で成り立っているが、全体の監視や管理がないこともあり、不正ノードの侵入や次のような様々な攻撃に対して脆弱である。

- メッセージの盗聴、改ざん
- フリーライダー（自己に有利なメッセージのみ中継する）
- ブラックホール攻撃（不正ノードが自分に届いたメッセージを全て破棄して中継しない）

特にブラックホール攻撃は伝染的ネットワークに特有であり、ブラックホールの不正ノードを推定して回避する必要がある。

4. 信用度に基づく防御

不正ノードを推定するためには、各ノードの「信用度」(Trust) を指標として活用する手法が有力である。簡単な例で説明すると、あるノードから別のノードの挙動を観察して、頻繁にメッセージを渡してくるようなら、そのノードの信用度を上げていく。信用度が初期値のままなら（メッセージを渡してくることがないなら）、ブラックホール候補とみなす。

Al Hinai らはこの方式をほぼそのまま Spray and Wait に適用した [(6)]。PRoPHET を対象とした Gupta らの研究は [(7)]、人間社会を模した信用度を最初からノードに割り振るなど、方向性が異なる。最近の研究は Blockchain の活用が活発だが、処理が重い。

5. 本研究の目的

本研究では、以上のような関連研究を踏まえ、P2P ネットワークの分野で提唱されて研究が進んでいる分散協調型の信用度管理の手法 [(8)] なども一部参考にして、PRoPHET におけるブラックホール攻撃の防御を目指した。特に災害時や避難時を想定して、方式を考案・設計し、NetLogo [(9)] でシミュレータを作成して、効果を検証した [(10)]。

6. 信用度に基づく不正ブラックホール・ノードの回避

第 1 の要点として、信用度の評価を次のように行う。

(1) あるノードから見た他ノードの信用度は、初期値ゼロ。

(2) ノード N_I は他ノード N_X からメッセージを渡されたら、N_X への信用度を増やす。これは関連研究 [(6)] と同様。

(3) 伝染型ネットワークではノードどうしが接触すると、保持しているメッセージ一覧（Summary Vector）を互いに交換して、自らが持たないメッセージを相手にリクエストして相手から受け取る。したがって、通常のノードは同じメッセージを改めてリクエストすることはない。一方、ブラックホール・ノードはメッセージを破棄するので、改めてリクエストしてくることがある。そこで、N_I は N_X から同じメッセージのリクエストを改めて受けたら、N_X への信用度を減らす。これを新規に考案して導入した。

第 2 の要点として、配達予測確率を次のように扱う。自らの配達予測確率を P_S、接触した相手が持つ確率を P_R とする。なお、配達予測確率の更新手順は、PRoPHET のままである。

(1) 相手ノードの信用度が負なら、その不審な相手にはメッセージを渡さない。

(2) 信用度が正なら、元の PRoPHET に従い、条件 $P_S < P_R$ が成り立つ場合にメッセージを渡す。

(3) 信用度がゼロなら、この条件を $(1 + d / 100)\, P_S < P_R$ とする。つまり、d が大きいほど渡しにくくなる。これを新しく導入した。

ノードが疎な場合は接触が稀なため、自ノードの P_S は小さい。したがって d の効果は小さく、素性が不明でも P_R が大きい（と自称する）相手に渡しがちになる。相手がブラックホールだと通信が途絶するが、ただでさえ途絶しがちなので、危険を冒してでも渡したほうがいい。ノードが密な場合は接触が頻繁に起き、P_S は大きくなる。したがって d の効果も大きくなり、素性の不明な相手には P_R が大きくても渡さないようになる。迂回路が幾つもありえるので、あえて危険を冒す必要はない。

7. シミュレーション実験と考察

平面空間内を多数のノードが、あちこちランダムに動き回っては互いに接触を繰り返しながら、メッセージを転送していく、というシミュレーション環境を NetLogo (Ver.6.4.0) で作成した。災害時の避難所という状況を想定し、その内部は密、外部は疎な配置にしている。ランダムに選出された一定割合のノードがブラックホールであり、ただし、メッセージの最初の発信源や最終的な宛先にはならない。

以下、d を変えながら実験した結果を示す。いずれも 10 回の試行の平均値である。図 1 は、ブラックホール・ノード数の全ノード数に対する比率（横軸）と、配信率、つまり宛先まで届いたメッセージ数の全メッセージ数に対する比率（縦軸）との関係を示している。提案手法のほうが概ね少し劣っているが、どのノードも信用度の初期値がゼロなことから、元の PRoPHET よりも d だけメッセージを渡しにくくなっており、それが原因と思われる。

図 2 はブラックホール率（横軸）と総転送回数（横軸）との関係を示しており、ブラックホールが存在する場合、提案手法が元の PRoPHET より大きく優れており、ネットワーク帯域やリソース浪費を抑制できていることが見て取れる。図 1、2 から、ブラックホール率が半数を越えると転送が全体的に阻害され、到達率の悪化と変動、転送回数の減少といった様子もうかがえる。

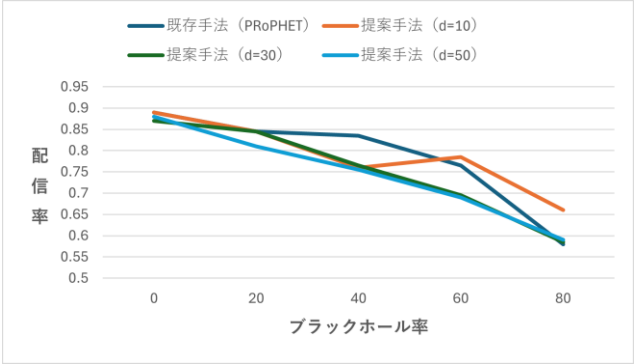

図 1. ブラックホール率 vs. 配信率

Fig.1. Blackhole node ratio vs. delivery ratio.

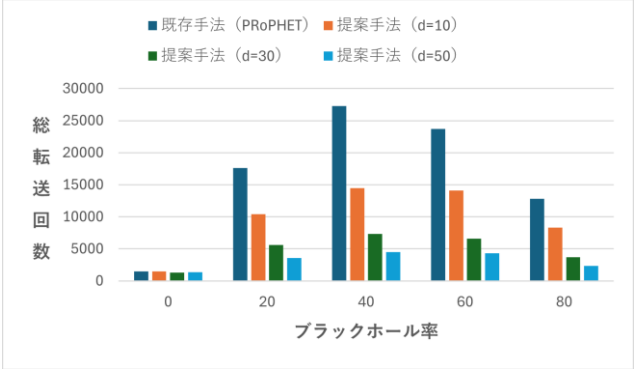

図 2. ブラックホール率 vs. 総転送回数

Fig.2. Blackhole node ratio vs. whole hop counts.

8. おわりに

本研究の Trust_PRoPHET は、計算量も元の PRoPHET と同程度の軽量と見積もっており、ネットワーク帯域の浪費を抑制できたことと併せて、バッテリー電力が貴重となる災害時はもとより、非力な IoT デバイスのネットワークなどにも有利と考えられる。また、故障などによって結果としてブラックホール化したノードにも対応できるものと考えている。

謝辞 貴重なご助言を頂いた吉田紀彦先生（埼玉大学名誉教授・立正大学研究員）に深謝する。本研究は科研費 23K11071、25K15086 の助成を受けている。

文 献

(1) A. Vahdat, et al.: Duke Univ. Tech. Rep., CS-200006 (2000)
(2) 鶴, 他: 信学会 通信ソサイエティマガジン, 16, 57-68 (2014)
(3) T. Spyropoulos, et al.: Proc. ACM WDTN, 252-259 (2005)
(4) A. Lindgren, et al.: Springer LNCS, 3126, 239-254 (2004)
(5) A. Lindgren, et al.: RFC 6693 (2012)
(6) A. Al Hinai, et al.: Proc. IEEE PDCAT, 6 pages (2012)
(7) S. Gupta, et al.: Proc. IEEE WiMob, 724-729 (2013)
(8) N. Matsumoto, et al.: JCM, 12(3), 1-12 (2022)
(9) https://www.netlogo.org/ (2025 閲覧)
(10) 岸本: 九州産業大学 卒業論文 (2026)