ブロックチェーン技術に基づいた ポテンシャルルーティングに向けた攻撃検知・防御

和歌山大学 システム工学部
久世 尚美

1. はじめに

ネットワーク技術の発展に伴い,ネットワークを利用した様々なサービスやアプリケーションが普及し,我々の生活を支えている.特に近年では,Internet of Things（IoT）の発展に伴い,パソコンやスマートフォンなどの通信機器に留まらず,自動車や家電製品など,あらゆる「モノ（Things)」に通信機能が具備され,ネットワークを形成している.その結果,ネットワークは大規模化・複雑化の一途を辿っており,管理者が一元的にネットワーク全体の収集,管理,制御を行う従来の中央集中制御は限界を迎えている.そのため,ネットワークの規模や複雑さの持続的な増加に対して対応可能な,分散的なネットワーク制御の仕組みが必要となっており,「自己組織化」の仕組みが注目を集めている[1-3].

「自己組織化」は自然界で見られる現象で,ここの構成要素の局所的な相互作用により全体の機能が創発される.このような自己組織化の仕組みは,高い拡張性,適応性,耐故障性を有することから,大規模,複雑なネットワーク制御との親和性が高く,自己組織型ネットワーク制御が注目を集めており,アリの採餌行動に基づいたルーティングやホタルの発光同期に基づいたノードの同期制御など,様々な研究が取り組まれている[1,3].

一方で,ネットワークを利用したサービスやアプリケーションの普及に伴い,ネットワークを対象としたサイバー攻撃が大きな問題となっている.しかしながら,自己組織型ネットワーク制御を対象としたセキュリティに関しては十分に検討が行われていないのが現状である.特に,自己組織型ネットワーク制御においては,個々のノードが自律分散的に動作を行うため,各ノードの得られる局所的な情報をいかに集約して攻撃の検知を行うか,また集約した情報の信頼性をどのように確保するかが重要となる.そこで,分散型台帳管理技術であるブロックチェーン[4]を自己組織型ネットワーク制御へと応用し,集約された情報をブロックチェーンの形式で管理することでその信頼性を確保し,攻撃の検知･防御へと活用する.特に本研究では,無線センサネットワークを対象とした自己組織型のルーティング手法であるポテンシャルルーティング[5]を題材とし,ブロックチェーンに基づいた悪性ノード検知・防御手法の提案を行い,その有効性を示す.

2. ポテンシャルルーティング

ポテンシャルルーティング[5]は,無線センサネットワークを対象とした自己組織型のルーティング手法である.ポテンシャルルーティングにおいては,各ノードが「ポテンシャル」と呼ばれるスカラー値を持つ.送信すべきデータがあるときには,「自身より低いポテンシャルを持つ隣接ノードへデータパケットを送信する」というルールに従ってデータの転送を行う.一般に,無線センサネットワークでは,センサノードがセンシングした情報をシンクノードへ集約するため,シンクノードに近いノードほど低いポテン

シャルを持つようにポテンシャル場を構築する．これにより，ポテンシャルに基づいた分散的なデータ転送が行われ，データパケットがシンクノードへと到達可能となる．

3． ブロックチェーン技術に基づいた悪性ノードの検知･防御手法

ポテンシャルルーティングを対象とした，ブロックチェーンに基づいた悪性ノード検知・防御手法の提案を行う．

本研究では，無線センサネットワーク内において，データ送信を阻害する悪性ノードが存在する状況を想定し，その検知・防御について考える．本研究の問題設定の概要を図 1 に示す．

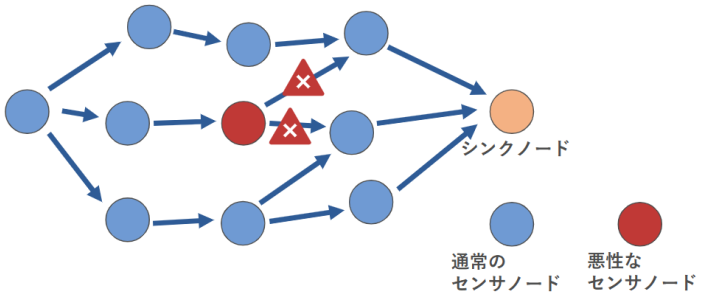

図 1 悪性ノードによるデータ送信の阻害

対象とする無線センサネットワークにおいては，図 1 に示すように，センサノードがセンシングした情報を，センサノードが中継しシンクノードへ集約を行う．本研究では，センサノードの一部がマルウェア感染などにより悪性ノードとなっている場合を想定する．悪性ノードでない通常のセンサノードは，隣接するセンサノードからデータパケットを受け取った際，ポテンシャルに基づいて適切に中継を行う．一方で悪性ノードは，隣接するセンサノードからデータパケットを受け取った際，その情報を不正に詐取するとともに，次のセンサノードへの中継を行わず，その結果，センサノードがセンシングした情報が適切にシンクノードに集約されず，ネットワーク機能の低下を招く．そのため，悪性ノードを早期に検知し，攻撃の影響を抑えることが重要となる．

提案手法は大きく攻撃検知機構と攻撃防御機構から構成される．

攻撃検知機構においては，各センサノードにおいて隣接ノードから送られるデータパケットの数を観測し，隣接ノードの信頼度の判定を行う（図 2）．ポテンシャルルーティングにおいては，隣接ノード間のポテンシャルの関係に基づいてデータパケットの送信先が決定されるため，ポテンシャルとフローとの整合性が保たれている場合には「正常」，そうでない場合には「不審」と判定を行う．各ノードが自身の隣接ノードに対して判定を行った結果はシンクノードに集約され，多くのノードから「不審」と判定されたノードに関しては「悪性」と判定する．

攻撃防御機構においては，攻撃検知機構で「悪性」と判定されたノードを避けるようポテンシャル場を再構築することにより，攻撃の影響を抑える．

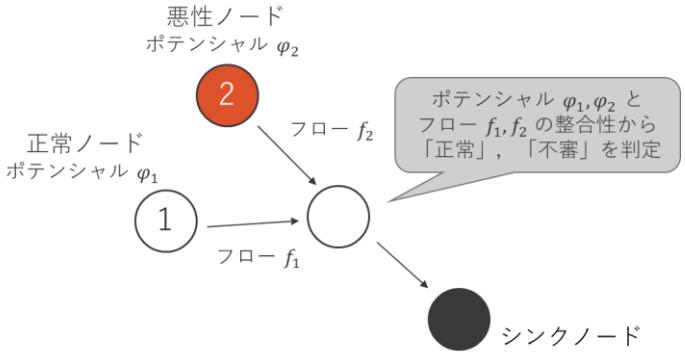

図 2 ノードの信頼度の判定

攻撃検知機構においては，センサノードが持つ情報をネットワーク内に複数存在するシンクノードに集約して悪性ノードの検知を行う．一方で，自己組織型のネットワークにおいては，個々のノードが自律分散的に動作を行うため，各シンクノードに集約された情報の信頼性を保証・検証する仕組みが必要となる．そこで，高い改ざん耐性，透明性を有するブロックチェーン技術を利用し，各ノードに集約された情報をブロックチェーンの形式で保管する（図 3）．

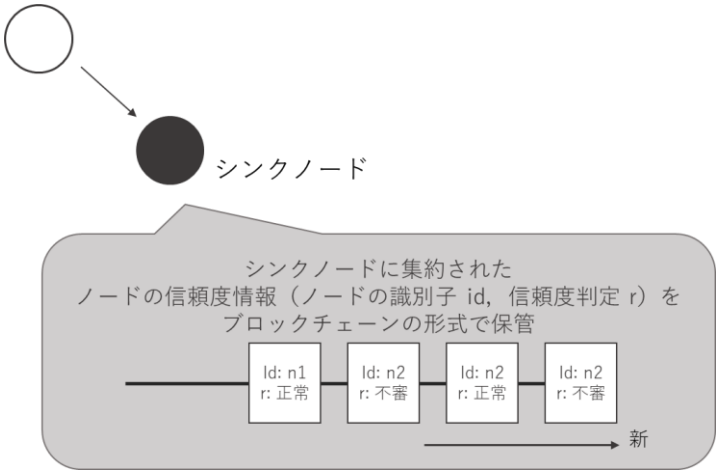

図 3 ブロックチェーンに基づいた情報の管理

ブロックチェーンにおいては，情報をブロックとして保存し，ブロック同士を鎖状に連結したブロックチェーンの形式でデータが保管される．ブロックチェーンは高い改ざん耐性，透明性を持つことが知られており，この特性を活用することで，シンクノードに集約された情報の信頼性を保証し，自己組織型ネットワーク制御における悪性ノードの検知・防御を実現する．

4． シミュレーション実験

提案手法の有効性を示すため，シミュレーション評価を行った．本評価では，4×4 の格子状ネットワークを用いた．16 個のノードのうち，2 個をシンクノード，残りをセンサノ

ードに設定し，シミュレーション開始から 100～200 秒においてセンサノードのうち 2 個が悪性ノードとして，データパケットの送信の阻害を行っている環境を想定する．

図 4 に，シンクノードに到達したデータパケットの数の時間変化を示す．

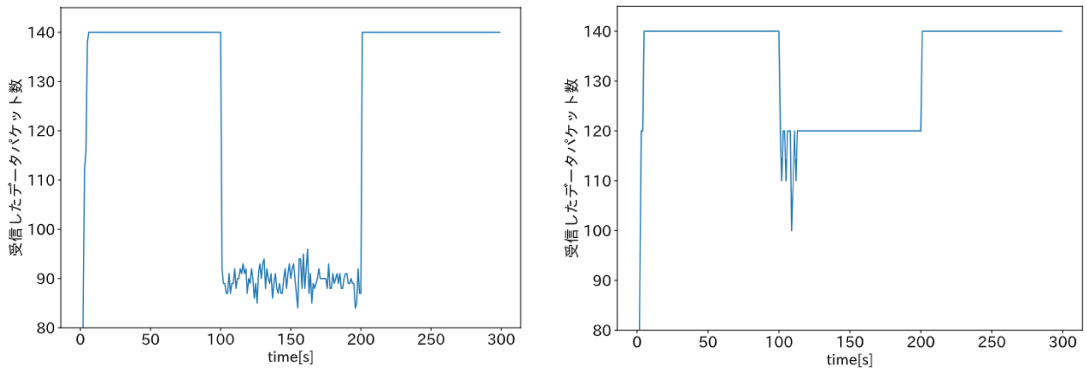

図 4 シンクノードに到達したデータパケット数
（左：攻撃検知・防御なし，右：提案手法）

図 4 において，左のグラフは攻撃検知・防御機構を導入していない通常のポテンシャルルーティングの結果，右のグラフは提案手法を導入した場合の結果を示す．図より，攻撃が発生している 100～200 秒において，攻撃検知・防御機構なしの場合にはシンクノードにおけるデータパケットの受信数が 3 割以上減少している一方で，提案手法を導入した場合においては，データパケット受信数の減少が抑えられていることが確認できる．これは，提案手法において，悪性ノードの検知を早期に行い，ポテンシャル場の制御を行うことで攻撃の影響を抑えられているからであると考えられる（提案手法においてもデータパケット受信数の減少が見られるのは，悪性ノード自身がセンシングした情報が転送されないためである）．

5． まとめ

本研究では，大規模・複雑なネットワークへ向けた自己組織型ネットワーク制御におけるセキュリティに着目し，自己組織型のルーティング手法であるポテンシャルルーティングを対象とし，ブロックチェーン技術に基づいた悪性ノード検知・防御手法の提案を行った．評価実験を通して，提案手法を用いることで，データを不正に棄却する悪性ノードを検知し，攻撃の影響を抑えられることを示した．

謝辞

本研究を遂行するにあたり，公益財団法人天野工業技術研究所から多大なご支援を頂きました．ここに記して謝意を示します．

参考文献

1） F. Dressler and O. B. Akan, “A survey on bio-inspired networking,” Computer Networks, vol. 54, no. 6, pp. 881–900, Apr. 2010.

2） C. Muller-Schloer, H. Schmeck, and T. Ungerer, Eds., Organic computing - A paradigm shift for complex systems. Basel, Switzerland: Springer, 2011.

3） C.-M. Pintea, Advances in bio-inspired computing for combinatorial optimization problems, 2014th ed. Berlin, Germany: Springer, 2013.

4） S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Decentralized Business Review, pp. 1–9, 2008.

5） N. Kuze, D. Kominami, K. Kashima, T. Hashimoto, and M. Masayuki, “Controlling large-scale self-organized networks with lightweight cost for fast adaptation to changing environments,” ACM Transactions on Autonomous and Adaptive Systems, vol. 11, no. 2, p. 9:1-9:26, Jun. 2016.