5V-09

センサネットワークのための異常強度信号通知を用いたワームホール攻撃検出方式における通知送信範囲制限の改良

松井　和也†　　木村　成伴‡

筑波大学情報学群情報メディア創成学類†　　筑波大学システム情報系情報工学域‡

1. はじめに

無線センサネットワーク（WSN: Wireless Sensor Network）は，周囲の環境などの情報を測定して上位システムへ送るためにセンサノードで構築されるネットワークである．

WSN におけるデータ送受信では，データを計測したノードが WSN 内の他のノードを中継して上位システムへつながるシンクノードと呼ばれるノードに伝えるマルチホップ通信が用いられる．しかし，センサノードは処理能力が低く，また，電池容量も制限されることから，通信の暗号化などの処理が省略されることが想定される．このため，WSN に対する攻撃の対策が重要な課題となる．

そのような攻撃のひとつにワームホール攻撃がある．この攻撃では周囲のノードより高出力な信号強度を発するノードを WSN 内に設置する．このノードは，より遠くのノードと通信でき，通常の経路よりも短いホップ数でシンクノードに到達することができるので，結果として，攻撃ノードを通る経路が選択されやすくなる．これを利用して，攻撃者はパケットの盗聴や改ざん，破棄などの攻撃を行うことができる．

この問題を解決するため，著者らは異常強度信号通知を用いたワームホール攻撃検出方式[1]を提案している．本論文では，本方式に通知送信範囲制限に改良を施すことを提案する．

2. 異常強度信号通知

攻撃ノードの付近にいるノードは，通常よりも強度の強い信号を受信する．これを利用し，異常強度信号通知を用いたワームホール攻撃検出方式[1]では，異常な信号強度を検出した周辺ノードが異常強度信号通知をブロードキャストして情報を他のノードに伝える．

An Improvement of Notification Transmission Range Restriction in Wormhole Attack Detection Method Using Abnormal Signal Strength Notification for Sensor Networks

†Kazuya MATSUI, College of Media Arts, Science and Technology of Informatics, University of Tsukuba

‡ Shigetomo KIMURA, Faculty of Engineering, Information and Systems, Tsukuba University

通知を受け取ったノードは，異常強度信号を出している異常ノードのアドレスと検知したノードのアドレスを保存し，一定数の発見ノードが集まれば，異常ノードを攻撃ノードとみなして，これを中継先から排除する．しかし，文献[1]における異常強度信号通知は，ホップカウントを用いて通知が届く範囲を制限しているため，攻撃ノードの通信範囲から，予め，適切なホップ数を決めておかなければ，通知が必要なノードに届かないという問題があった．例えば，図 1 は，中央の攻撃ノード（通信範囲を円で示す）を付近の検出ノード D が発見し通知した例である．但し，異常強度信号通知の検出ノードから 3 ホップ先まで届くように制限している．

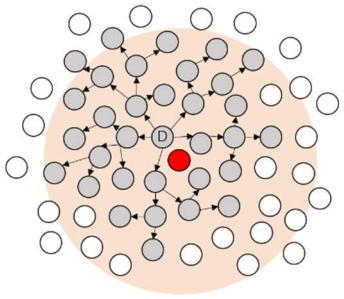

図 1　通知受信範囲

図の右下のノードは通信半径内にあるにも関わらず通知が届いていない．通知が届くホップ数を増やすと，この問題は解消さえるが，図左上のノードの一部は，攻撃ノードの通信範囲外であるにも関わらず，通知が届いており，ホップ数を増やすとこのような通知を受け取らなくても良いノードが増えることになる．以上の問題は，攻撃ノードの通信領域と検出ノードから一定のホップで到達する領域の間に乖離があるために起きる．

3. 提案方式

前章の問題点を解決するため，本章では，通知送信範囲制限を改良することを提案する．

通知範囲は，任意の攻撃ノード通信半径に対して図 2 のようになることが理想である．この要件は通知を受け取る条件を「異常信号強度が通知されたノードの隣接ノードであること」とす

れば達成できる．

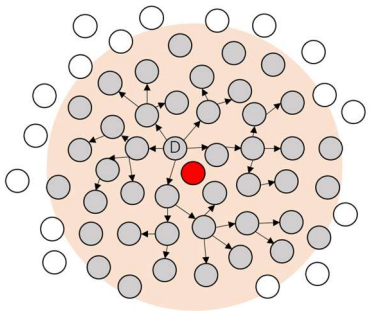

図 2　理想的な通知受信範囲

攻撃ノードの隣接ノードであることは，使用しているルーティングアルゴリズムにも依存するが，AODV などの場合は，Route Reply メッセージを受け取っているかどうかで判断できる．なお，隣接ノードが攻撃ノードに中継しないように経路を修正すれば，隣接しないノードからのパケットも，攻撃ノードに中継されなくなる．

4. 実験

提案方式の有効性を評価するため，0.09km^2 四方の正方形の領域の中央に攻撃ノードを，10×10 の 30m 間隔の格子状に通常ノードを置き，表 1 に示す条件で実験を行った．シミュレーションは NS3.30 を用いた．

表 1　実験環境

通常ノード数	100
攻撃ノード数	1
通常ノード通信半径	40m
攻撃ノード通信半径	50m，100m，150m
ルーティング プロトコル	AODV
データレート	16kbps
シミュレーション 時間	60s
文献[1]の通知を送 るホップ数	3

5 秒おきに実験領域内のランダムな通常ノードから実験領域右下端に位置する通常ノードに UDP で CBR トラフィックを送る．攻撃ノードは AODV のコントロールパケット以外の UDP パケットを破棄する．この条件下で(A)何も防御しない，(B)異常強度信号通知を用いたワームホール攻撃検出方式[1]，(C)提案方式のそれぞれを用いた場合において実験を 10 回行い，その平均値と信頼レベル 95%の信頼区間を求めた．攻撃ノードの通信半径を変更したときの，攻撃ノードが破棄したパケット数を図 3 に，(B)と(C)における，異常強度信号通知を受信した数を図 4 に示す．

図 3 より，攻撃ノードの通信半径が小さいうち

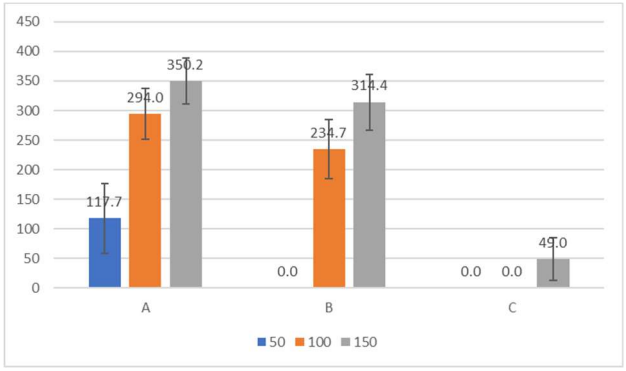

図 3　攻撃ノードが破棄したパケット数

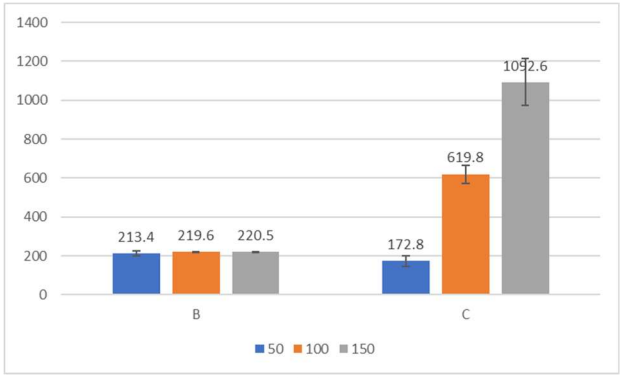

図 4　異常強度信号通知受信数

は B も C も機能しているが，通信半径が大きくなると，B では破棄したパケット数が A よりも 10～20%しか削減できなかった．これは，通知を送るホップ数が少なく，通知を受信できなかったノードが攻撃ノードに中継してしまったためである．一方，C は通信半径が 100m でも攻撃ノードを排除できているが，150m の場合は完全には排除できなかった．これは，攻撃ノードを認識する数だけ通知を受け取る前に攻撃ノードに中継したためであり，この遅延は攻撃ノードの通信半径が大きいほど，顕著に表れると考えられる．

図 4 より，C では B と比べて，異常強度信号通知受信数が 2.8～5.0 倍に増えている．これは，B では必要なノードに通知が届いていないことを示している．

5. まとめ

本論文では，異常強度信号通知を用いたワームホール攻撃検出方式の通知配布範囲を改良した．今後，攻撃ノードが複数の場合に機能することの確認や，信号の受信強度のみで攻撃ノード検出方式自体の改善することを検討している．

参考文献

[1] 石坂勇樹，木村成伴，海老原義彦，センサネットワークのためのホップカウント付き異常強度信号通知を用いたワームホール攻撃検出方式，信学技報，Vol. 111, No. 344, pp. 143-148, 2011.