4V-1

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

石坂 勇樹† 木村 成伴‡ 海老原 義彦‡

†筑波大学 情報学群情報科学類 ‡筑波大学大学院 システム情報工学研究科

1 はじめに

近年，環境や施設などの情報を計測するセンサネットワークが注目されている．しかし，攻撃者が悪意のあるセンサノードを追加することで，センサネットワークの通信を傍受したり，妨害したりする攻撃が問題となっており，その中で代表的な攻撃方法としてワームホール攻撃がある．

ワームホール攻撃では，図 1 のように，攻撃者がセンサネットワーク内に出力の高い電波を発するセンサノード(以下では攻撃ノードと呼ぶ)を設置する．攻撃ノードは，通常のルートと同じかそれ以下のホップ数で，宛先ノードまでの通信を行うことができる．これにより，たくさんの通常ノードに，短いホップ数で通信が可能な攻撃ノードにパケットを中継するよう誘導することで，通信データの内容を傍受，あるいは成りすましを行う．

ワームホール攻撃の検出方式として現在提案されているものの多くは，特別なハードウェアを全てのノードに設置する必要がある[1][2]．

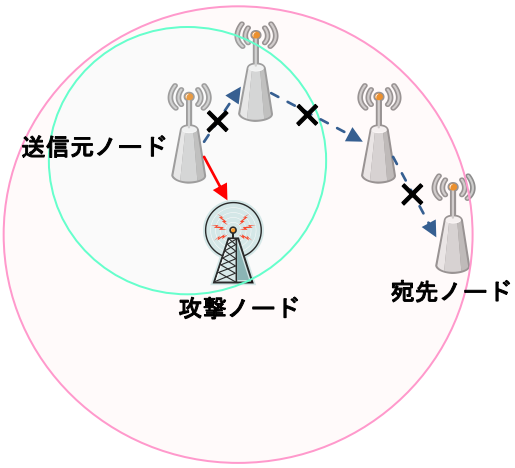

図 1 ワームホール攻撃

しかし，センサノードは多数必要であり，再利用もできないことから，それらのハードウェアを追加することはコスト的に問題がある．

また，特別なハードウェアを用いず，RTT (Round Trip Time)を利用する方式[3]も提案されているが，この方式では，全てのノードで時刻の同期を取り，それらの結果から，それぞれのノードで攻撃ノードを検出する必要があるため，その検出方式は非常に複雑になる．

2 提案方式

前章の問題点を踏まえ，本論文では，ハードウェアの追加を必要とせず，より簡単な方法で攻撃ノードの検出を行う方式を提案する．

まず，攻撃ノードは，広範囲の通信を行うため，通常ノードに比べて，強い出力で信号を送信する必要がある．従って，攻撃ノード付近に設置されているノードは，攻撃ノードの信号が，明らかに強い出力で送信されたということに気付く．この異常な強度で通信を行っているノードを異常ノードと呼ぶ．

あるノードが異常ノードを発見すると，そのノードの情報を保持すると同時に，隣接ノードに，異常ノードを発見したことを示す異常強度信号通知をブロードキャストする．この通知には，異常ノードの識別子，発見ノードの識別子，通知の順序番号，時刻，TTL などを含む．

異常強度信号通知を受信したノードは，その順序番号や時刻から，過去に受信したことがある通知であることが分かれば，これを破棄する．そうでなければ，通知に記された情報を保持するとともに，通知を再びブロードキャストする．これを繰り返すことで，図 2 に示すように，ネットワーク全体で「あるノード(図では B と C)がある異常ノード(図では W)を発見した」という情報が共有される．

なお，受信電波強度の測定は従来のセンサノードでも行われているため，提案方式のためにハードウェアを追加する必要はない．しかし，送受信器の不調のため，通常ノードが一時的に強い出力で信号を出してしまったり，強い出力の信号を観測したと勘違いしたりする可能性が

Wormhole Attack Detection Method Notifying Over-Strong Signals for Sensor Networks
†Yuuki Ishizaka, College of Information Science, School of Informatics, University of Tsukuba
‡Shigetomo Kimura and Yoshihiko Ebihara, Graduate School of Systems and Information Engineering, University of Tsukuba

ある．また，攻撃ノードが，他のノードが攻撃ノードであるとする虚偽の異常強度信号通知を出す可能性もある．

そこで，提案方式では受信電波強度の測定をネットワークに参加している全ノードで行い，他ノードからの通知が一定数以上集まったとき，対象となる異常ノードを攻撃ノードであるとみなす．このように，攻撃ノードの検出を複数のノードの意見に依存させることで，以上の問題を解決している．

攻撃ノード検出後は，この攻撃ノードを含まないルーティングを行う．そのため，攻撃ノードから届いたルーティングの要求メッセージは全て破棄する．さらに，既に構成されているルートでも攻撃ノードを中継するものがあれば，これを除去し，攻撃ノードを含まないルートを再構成する．

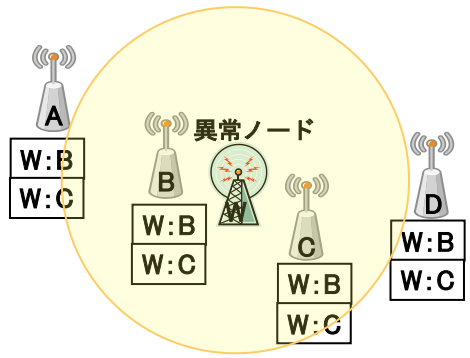

図 2 異常ノードの共有

3 シミュレーション実験

提案方式の有効性を確かめるために，Network Simulator version 2 を使用して，シミュレーション実験を行った．本実験で用いた条件を表 1 に示す．センサノードは実験領域にほぼ等間隔に設置し，攻撃ノードは実験領域の中央に配置する．そして，最も左下のセンサノードから最も右上のセンサノードに無限のサイズのファイルを FTP で転送させ，その間に，異常ノードを発見した通常ノードに異常強度信号通知を送信させた。それぞれの閾値(異常ノードを攻撃ノードと見なすまでに受け取る通知の数)について，この試行を 10 回繰り返し，FTP 通信開始時から全てのノードが攻撃ノードを検出するまでの平均時間と信頼係数 95%のときの信頼区間を表 2 に示す．いずれの閾値の場合でも，2 秒以内に全てのノードが異常ノードを検出しており，提案方式の有効性が確認された．なお，閾値が 4 の場合の平均時間が最小になっているが，その原因については現在調査中である．

表 1 実験条件

Channel Type	WirelessChannel
Radio-Propagation Model	TwoRayGround
Network Interface Type	WirelessPhy
MAC Type	802_11
Interface Queue Type	PriQueue
Link Layer Type	LL
Antenna Type	OmniAntenna
Max Packet in Ifq	50
Routing Protocol	AODV
Number of Mobilenodes	900
Number of Wormholes	1
Network Scope	1km^2
Communication Radius of Mobilenode	50m
Communication Radius of Wormhole	100m
Communication Radius of Anormalynode	70m

表 2 全ノードが攻撃ノードを検出する平均時間

閾値	2	3	4	5
平均時間[s]	1.88±0.06	1.75±0.12	1.68±0.11	1.97±0.10

4 まとめ

本論文では，攻撃ノードの異常強度信号を全てのセンサノードが通知しあうことにより，ワームホール攻撃を検出する方式を提案した．そして，シミュレーション実験により，その有効性を確認した．

今後の課題としては，複数の異常ノードがあった場合でも提案方式が有効に働くことを確認することや，全てのセンサノードがシンクノードに定期的にデータを送信している際に，提案方式によるオーバヘッドが与える影響を調べることなどが挙げられる．

参考文献

[1] L. Hu and D. Evans, Using Directional Antennas to Prevent Wormhole Attacks, Proceedings of the Eleventh Network and Distributed System Security Symposium, pp. 131-141, 2004.

[2] L. Lazos and R. Poovendran, SeRLoc: Robust Localization for Wireless Sensor Networks, ACM Transactions on Sensor Networks, Vol. 1, No. 1, pp. 73-100, 2005.

[3] B. Prasannajit, Venkatesh, S. Anupama, K. Vindhykumari, S. R. Subhashini, and G. Vinitha, An Approach towards Detection of Wormhole Attack in Sensor Networks, Proceedings of 2010 First International Conference on Integrated Intelligent Computing, pp. 283-289, 2010.