一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
CPSY2018-119,DC2018-101 (2019-03)

無線センサーネットワークのセキュリティ対策の最適化

蓑原　　隆

拓殖大学工学部情報工学科
〒193–0985 東京都八王子市館町 815–1
E-mail: minohara@cs.takushoku-u.ac.jp

あらまし　無線センサーネットワーク (以下 WSN) には，屋外や遠隔地など管理が困難な場所に設置されることや，無線通信の開放性に起因する脆弱性などの様々なセキュリティ上の懸念が存在する．このような複数のセキュリティ問題に対して，多数の対策が研究され報告されているが，一般にセキュリティ対策は特定の問題に特化されており，WSN の設計者にとって，どのような対策をどれだけ実装すればよいかを判断することが困難になっている．一方，無線センサーノードにおける計算能力，記憶容量，電源容量などの制約から実装できる対策は限定されてしまう．本研究では，WSN のセキュリティ対策の最適化という課題を解決するために，WSN の様々なセキュリティ対策の効果と，実装に必要なコストを数量化し，総合的な評価を定量的に行えるようにすることで，対象とする WSN の仕様に基づく実装上の制約を満たしたうえで，WSN の利用者のセキュリティ要求に対する効果を最大にする対策の組合せを探索するという方法を提案する．
キーワード　無線センサーネットワーク セキュリティ評価 攻撃/防御グラフ

Optimization of Security Methods for Wireless Sensor Networks

Takashi MINOHARA

Department of Computer Science, Faculty of Engineering, Takushoku University
815–1 Tatemachi, Hachioji, Tokyo, 193–0985 Japan
E-mail: minohara@cs.takushoku-u.ac.jp

Abstract　Wireless sensor networks(WSNs) will face various security issues because they are utilized in poorly controled environment such as outdoors or remote places. There are a number of counter measures proposed against attacks to the WSNs, but it is hard to select appropriate measures since they are specialized to a certain problem. Furthermore WSN's limited capacity of calcuration, memory and power source make deployment of counter measures restricted. In this paper, a method to optimize selection of counter measures against attack to the WSN is presented. Relation between attacks and couter measures are analysed quantitatively and optimal combination of couter measures will be found with considering limited resources of the target WSN.
Key words　Wireless sensor networks, Security Assesment, Attack/Defence graph

1. はじめに

大規模なデータを収集し解析するためのデータ収集技術として，センサーを持つ小型無線ノードを多数配置し，それらが自律的にネットワークを構成してデータを収集する無線センサーネットワーク (WSN) が，環境，農業，建築構造物などのモニタリングといった様々な分野で注目されている．

WSN は測定の対象となる環境や利用者と直接的な関係を持っているため，その安全に深刻な影響を与える可能性があるにもかかわらず，以下のような本質的な脆弱性を抱えている．

（1） 屋内外のオープンな場所に設置されることが多く物理的な攻撃を受けやすい．

（2） 遠隔地で連続運転することが多く，管理者が異変に気付きにくい．

（3） 無線通信の開放性から，通信の妨害，傍受，介入が比較的容易である．

これらの問題に対して，様々な攻撃が想定され，多数の対策が報告されている [1]．しかし，一般にこれらの攻撃対策は想定された攻撃に特化されており，WSN の利用者の機密性，可用性，完全性に関する要求と直接対応していないことから，

This article is a technical report without peer review, and its polished and/or extended version may be published elsewhere.
Copyright ©2019　by　IEICE

どのようなセキュリティ対策を実装すれば十分であるのか判断することが困難になっている．

一方，WSN には，多数のノードを使用するためにノード 1 台あたりのコストを下げたいという要求や，電源設備を持たない場所で使うために消費電力を下げたいという要求が存在し，ノードに使用されるデバイスの電力，計算能力，通信能力などが制限されている．したがってどのようなセキュリティ対策を実装できるか，特に複数の対策を共存させることが可能かどうかは，実際に使用する WSN の能力に依存し，実装上の制約を満した上で，利用者のセキュリティ要求を満たす対策，あるいは対策の組合せを選択することは困難であり，WSN のセキュリティ対策の効果を定量的に評価して選択を行う方法を確立することが重要な課題となっている．

本研究の目的は，実装上の制約を満した上で，利用者のセキュリティ要求を満たすセキュリティ対策の組合せを，対策の効果を定量的に評価して選択を行う方法を確立することである．WSN に対する攻撃は，複数のネットワーク階層において様々な攻撃が想定されている [1]．したがって，特定の階層の攻撃対策は他の階層の攻撃によって無効化されてしまう可能性があり，利用者のセキュリティ要求を満足させる WSN を設計するには複数の対策を組み合わせて実装する必要がある．しかし，WSN のセキュリティ対策を定量的に評価しようとする試みは極めて少なく，存在するものも複数のセキュリティ対策の組み合せを選択するものではない．例えば，定量的評価の 1 つである Anand らの研究 [2] では，盗聴攻撃に対する WSN 通信プロトコルの強さを確率的に評価するモデルが提案されている．しかし，対象とする攻撃の種類が限定されており，対策の選択には向いていない．また，有線ネットワークのセキュリティ対策の評価手法が報告されている攻撃グラフ [3]〜[5] について，Sen らは確率的に取り扱うことで WSN の複数の階層の攻撃を考慮したリスク評価を行っている [6] が，セキュリティ対策の組み合せの選択を目的とはしていない．一方，Thakore らの研究 [7] は，ネットワーク上に複数のセキュリティモニタを配置する際の最適な配置を求めるものである，配置を評価する複数の評価尺度を結合した目的関数と配置コストの評価関数を使って最適な組み合せを機械的に探索する方法であるが，この研究の研究対象が有線ネットワークの監視であることから，WSN にはそのまま適用することが困難である．

本研究では，まず，WSN に対する攻撃と防御の関係を考慮して，攻撃グラフによる WSN のセキュリティ評価を拡張して，攻撃に対する防御の影響を考慮した攻撃/ 防御グラフを作成する．次に攻撃対策の選択を攻撃/防御グラフにマッピングする方法を定める．最後に，攻撃対策を実装するための条件から，対策の組合せを実装可能であるという制約のもとで，機密性，完全性，可用性を量的に比較して最適な組合せを求められるようにする．

2. 攻撃対策の組合せの最適化

2.1 攻撃/防御グラフを用いた攻撃対策効果の数量的評価

WSN に対する攻撃を分類したものを表 1 に示す [6]．これらの攻撃はそれぞれ独立したものではなく，ある攻撃を実行されるために，他の攻撃が使われるような攻撃の前提となる条件や，ある攻撃を影響によって他の攻撃が引き起こされるような後続の攻撃の条件などによって，関連づけられている．Sen らは，想定される攻撃者の最終目的に到達する攻撃間の関係をグラフにし，攻撃が成功する確率を計算することで，WSN のリスク評価を行う方法を提案している．

一方，WSN の攻撃に対する対策は，最終的な危険に到達す

表 1　WSN に対する攻撃の定義
Table 1　Definition of Attacks to the WSN

攻撃	定義
盗聴 (Eavesdropping)	ノード間の通信を傍受する攻撃
通信妨害 (Jamming)，DoS	ネットワーク通信を無線妨害または多数のパケットの送信によって妨害する攻撃
ノード置換 (Node Subversion)	攻撃者が正常なノードに取って代わる攻撃
シビル (Sybil)	攻撃者のノードが偽の ID を作って，それを正常なノードに見せかける攻撃
スプーフィング (Spoofing)	攻撃者が正常なノードのふりをする攻撃
経路変更 (Altering)，リプレイ (Replay)	通信経路を継続的に変更したり，同じパケットを繰り返し送ったりする攻撃
ワームホール (Wormhole)，シンクホール (Sinkhole)，ブラックホール (Blackhole) 攻撃	攻撃者が偽の有利な経路情報を広告することで通信経路を変更させ通信が攻撃者のノードを通過するようにする攻撃，このとき攻撃者はパケットを破棄することもできる．
選択的転送 (Selective Forwarding)	攻撃者のノードを通過するように経路を変更させたあとで，選択的にパケットを転送する攻撃
確認応答偽装 (Acknowledgment Spoofing)	隣接ノードの特定や認証の過程で偽装した確認応答を送信する攻撃
ノードの不正動作 (Node Malfunction)	マルウェアを実行させるなどして正常なノードに不正な動作をさせる攻撃
ノードの複製 (Node Replication)	攻撃者が正常なノードを元にして偽のノードを作成する攻撃
不正データの挿入 (False Data Injection)	攻撃者が正常な通信に誤った内容のパケットを紛れ込ませる攻撃
ノード停止 (Node outage)	正常なノードが動作できないようにする攻撃
物理的攻撃 (Directed Physical Attack)	ノードに物理的なダメージを与える攻撃
ハロー攻撃 (Hello Flood)	Hello メッセージを連続的に送りつけることで正常なノードが他のメッセージを扱えなくする攻撃
同期妨害 (Desynchronization)	センサーノードによる通信の再確立が連続的に妨害される攻撃
マルウェア攻撃 (Malware Attack)	正常なノードの上で不正なプログラムを実行させる攻撃

表 2　攻撃の対策
Table 2　Countermeasures against Attacks

攻撃	対策の例
盗聴 (Eavesdropping)	通信の暗号化
通信妨害 (Jamming), DoS	周波数拡散通信，優先メッセージ，デューティサイクルの低下，リージョンマッピング，通信モードの変更
シビル (Sybil)	認証，プロービング
スプーフィング (Spoofing)	認証
経路変更 (Altering)，リプレイ (Replay)	イグレスフィルタリング，認証，モニタリング
ワームホール (Wormhole)，シンクホール (Sinkhole)，ブラックホール (Blackhole) 攻撃	認証，地理または時間情報に基づくパケットの抑制
選択的転送 (Selective Forwarding)	パケット多重化，プロービング
確認応答偽装 (Acknowledgment Spoofing)	署名，認証
ノードの複製 (Node Replication)	認証
不正データの挿入 (False Data Injection)	署名，認証
ハロー攻撃 (Hello Flood)	認証，通信経路の確認
同期妨害 (Desynchronization)	認証

る前に，攻撃の影響を排除することを目的として実現されている．各攻撃に対する防御をまとめたものを表 2 に示す．

ここで，攻撃対策が行なわれていないときに攻撃グラフ上の攻撃の影響が伝搬するという条件を攻撃グラフに付加すると，攻撃対策を考慮したグラフを作成することができる．図 1，2，3 に，それぞれ，攻撃者の最終目的を機密性，完全性，可用性の喪失としたときのグラフを示す．

例えば，図 1 の機密性のグラフにおいて，ワームホール攻撃では，あたかも有利な経路があるかのように経路制御パケットの偽装が行われるが，ワームホール攻撃自身を防御するのではなく，偽装パケットの影響を排除するために，電子署名によるパケットの認証を行うか，地理または時間情報利用して疑わしいパケットを排除することで偽装を失敗させ，さらにはワームホール攻撃を防ぐことができ，最終的な機密性の喪失の可能性を下げることができることがわかる．同様にして，図 2 の完全性の評価では，マルウェアによってノードに不正な動作をさせようとい試みの成功の可能性を多重化によって軽減できることがわかる．

攻撃/防御グラフを用いた，攻撃対策の量的評価の計算は，攻撃グラフを用いたリスク評価の計算と同様にして行う．すなわち，実際の WS の使用環境などから，各攻撃の可能性を数値としてグラフ上に割り当てる．このとき攻撃の可能性の数値を割り当てられていない攻撃については，近隣の攻撃の情報から逆算して求める．

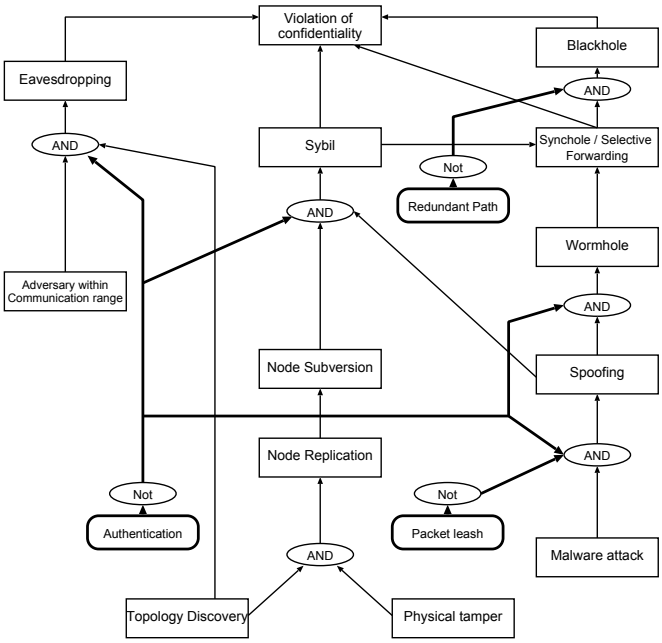

図 1　機密性の評価のための攻撃/防御グラフの例
Fig. 1　Attack/defence graph for evaluation of confidentiality

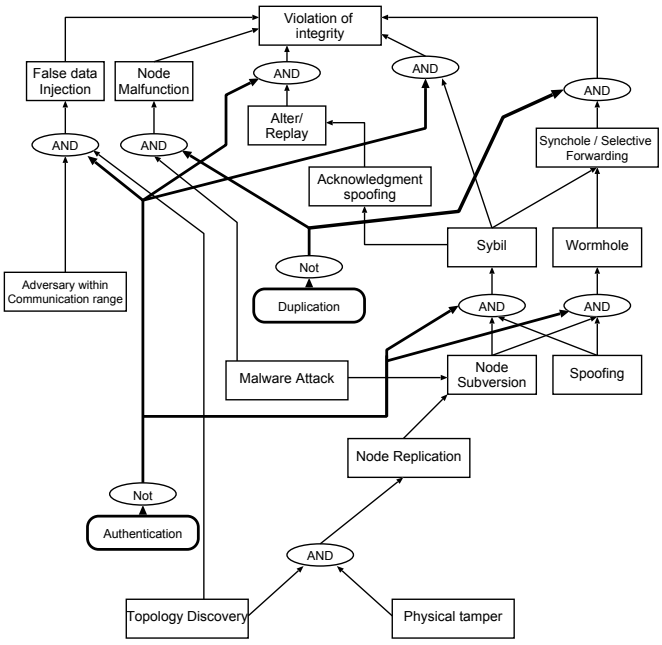

図 2　完全性の評価のための攻撃/防御グラフの例
Fig. 2　Attack/defence graph for evaluation of integrity

グラフの順方向の計算では，ある攻撃が，ただ 1 つの親の攻撃の結果として起こる場合には，親の成功確率をそのまま子の成功確率とする．複数の親が存在する場合には，それらの親の攻撃全てが成功したときに子の攻撃が成功すると考え，親の攻撃の成功確率の積を子の成功確率とする．成功確率を子から親の方向に計算する必要があるときは，グラフをベイジアンネットワークであると考え，事後確率から事前確率を推定する．

図が煩雑になることを防ぐために，例えば「認証 (Authentication)」が複数の攻撃影響の経路を制御しているように表現

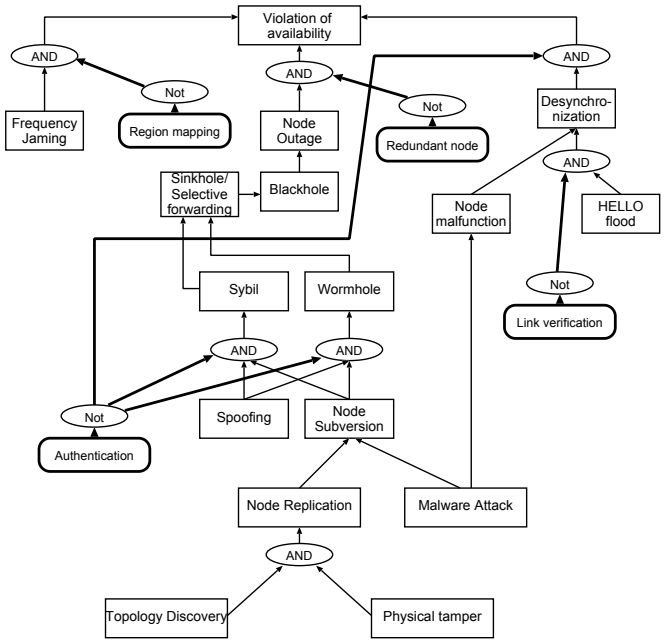

図 3　可用性の評価のための攻撃/防御グラフの例
Fig. 3　Attack/defence graph for evaluation of availability

したが，実際に実装されるセキュリティ対策は，経路制御時の認証であるのか，データそのものの認証であるのかなど，セキュリティ対策によって，特定の経路だけに影響を与えるものも少くない．本研究においても，グラフを使ってセキュリティを量的に評価するときは，それぞれのセキュリティ対策が対象としている部分だけを計算に入れるようにする．

すなわち，全ての攻撃対策の集合 C の部分集合として，攻撃対策の集合 C_d が選択されたとき，対象とする WSN に対する全攻撃の集合 Φ の任意の要素 ϕ についての防御確率 $d(\phi, C_d)$ が求められるものとし，このときの攻撃 ϕ の成功確率 $p(\phi)$ は，対策がされていないときの成功確率 $p_{nocm}(\phi)$ を使って，$p(\phi) = p_{nocm}(\phi) \cdot d(\phi, C_d)$ のように求められるものとする．

2.2　攻撃対策の実装上の制約を光量した対策選択の最適化

前節で説明した，攻撃/対策グラフを用いた評価方法によって，対象となる WSN に対して，セキュリティ対策の組合せが選択されたときに，機密性，完全性，可用性の推定を行うことができる．しかし，実際に選択を行う際には利用者の要求を反映させる必要がある．WSN の利用者によって機密性を重視する場合もあれば，完全性や可用性が満たされれば機密性はそれほど重要でないという場合もある．

また，WSN に使用されるデバイスの CPU 性能，メモリ容量，電源容量などの制約から，選択できるセキュリティ対策の組合せは制限される．例えば，各対策を実装するには，表 3 に示すような暗号計算などの機能が必要とされる場合があり，それらの要求を同時に満すことが困難なことがある．

さらに，それらの対策を実装したときのメモリ使用量，消費電力などが，システムの容量を越えないようにしなければならない．本研究では，事前に各対策について実装時に必要な資源の量を表 4 に示すように求めておき，その結果を利用して必要な資源の合計が，対象とするシステムの容量を越えないように制約を定める．

表 3　攻撃実装要件の例
Table 3　example prerequisite of couter measures

	暗号計算	鍵管理	多重通信	...
対策 1	AES-128	分散管理	無	
対策 2	RSA-1024	集中管理	二重化	

表 4　対策実装オーバヘッドの例
Table 4　example overhead of counter measures

	処理時間	電力消費	記憶容量
対策 1	2.3ms	25.9mJ	2.1kB
対策 2	0.64s	304mJ	50kB

まず，各パラメータを次のように定義する．

w_c　：機密性に対する要求の重み $(0 \leq w_c \leq 1)$
w_i　：完全性に対する要求の重み $(0 \leq w_i \leq 1)$
w_a　：可用性に対する要求の重み $(0 \leq w_a \leq 1)$
$Conf(\Phi, C_d)$　：セキュリティ対策の集合 C_dが適用された WSN において，想定される全攻撃Φによって，機密性が損なわれる確率
$Int(\Phi, C_d)$　：セキュリティ対策の集合 C_dが適用された WSN において，想定される全攻撃Φによって，完全性が損なわれる確率
$Avail(\Phi, C_d)$　：セキュリティ対策の集合 C_dが適用された WSN において，想定される全攻撃Φによって，可用性が損なわれる確率
$Impl(C_d)$　：$\{0,1\}$ 対象とする WSN での C_dの実装の可否
$Cost_t(c)$　：対策 $c(c \in C_d)$ を実装したときに必要な処理時間
$Cost_m(c)$　：対策 $c(c \in C_d)$ を実装したときに必要なメモリ容量
$Cost_p(c)$　：対策 $c(c \in C_d)$ を実装したときに必要な電力量
max_t　：対象とする WSN の余剰処理時間の最大値
max_m　：対象とする WSN の余剰メモリの最大値
max_p　：対象とする WSN の余剰電力量の最大値

これらのパラメータを用いて，セキュリティ対策の組合せの最適化の問題は次のように定義される．

$$\min_{C_d} w_c Conf(\Phi, C_d) + w_i Int(\Phi, C_d) + w_a Avail(\Phi, C_d)$$

s.t.

$$Impl(C_d) = 1$$

$$\sum_{c \in C_d} Cost_t(c) < max_t$$

$$\sum_{c \in C_d} Cost_m(c) < max_m$$

$$\sum_{c \in C_d} Cost_p(c) < max_p$$

3. おわりに

本研究では，攻撃間，攻撃と対策間の関係をグラフにして，セキュリティ対策の効果を数量的に評価することで，WSN のセキュリティ対策の実装上のコストを考慮した上で，最適な対策の組合せを求める方法を提案した．

具体的な WSN のフレームワークとして Contiki-NG を対象としたセキュリティ対策の最適化のシステムを実装中であるため，提案手法の評価は今後の課題としたい．

文　献

[1] Y. Wang, G. Attebury and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, Vol. 8, No.2, pp.2–23 (2006)

[2] M. Anand, Z. Ives, and I. Lee, “Quantifying Eavesdropping Vulnerability in Sensor Networks,” ACM International Workshop on Data Management for Sensor Networks, pp. 3–9 (2005)

[3] I. Ray and N. Poolsapassit, “Using attack trees to identify malicious attaks from authorized insiders,” in Proc. 10 th Eur. Conf. Res. Comput. Security, pp. 231-246 (2005)

[4] J. Dawkins, C. Campbell, and J. Hale, “Modeling network attaks: Extending the attack tree paradigm,” in Proc. Workshop Statist. Mach. Learn. Techn. Comput. Intrusion Detection, pp.75-86 (2002)

[5] N. Poolsappasit, R. Dewri, and I. Ray, “Dynamic security risk management using Bayesian attack graphs,” IEEE Trans. Dependable Security Comput., vol. 9 no.1, pp.61-74 (2012)

[6] A. Sen, S. Madria, “Risk Assessment in a Sensor Cloud Framework using Attack Graphs,” IEEE Transactions on Services Computing, Vol. 10, No. 6, pp.942–955 (2017)

[7] U. Thakore, G. A. Weaver and W. H. Sanders, “A Quantitative Methodology for Security Monitor Deployment,” IEEE/IFIP International Conference on Dependable System & Networks, pp.1–12 (2016)

[8] A. Ramos, B. Aquino, M. Lazar, R. H. Filho, and J. J. P. C. Rodrigues, “A Quantitative Model for Dynamic Security Analysis of Wireless Sennsor Networks,” IEEE Global Communications Conference, pp. 1–6 (2017)