審 査 の 結 果 の 要 旨

氏　名　清　　雄一

本学位請求論文では、無線センサーネットワークにおける高いセキュリティを構築するために必要となるメッセージ通信妨害攻撃の検知手法に関して新しい手法を提案している。無線センサーネットワークは、多数のセンサーノードから構成され、侵入者等のイベント検知に用いられる。無線ネットワークでは攻撃者が物理的にノードを取得、鍵等の情報を全て抽出し、悪意のあるプログラムを実行する不正ノードを作成可能である。

無線ネットワークの目的が犯罪検知の場合、攻撃者は、セキュリティの三要素である機密性・完全性・可用性のうち、特に可用性に対する攻撃を行うことが考えられる。そこで本論文では、可用性に対する攻撃として、イベントを通知するメッセージがユーザに届くことを妨げる攻撃の検知を目的としている。特にメッセージ通信の上位レイヤーに注目し、不正メッセージを多数作成することによりネットワークの輻輳を引き起こす攻撃の検知を対象としている。

このような無線ネットワークのセキュリティに対する要件として、正しいメッセージを不正メッセージであると誤検知しない、多数のノードの不正取得への耐性がある、多数のノードの故障に耐性があることが要求される。だが、これらの三つの要件を同時に満たす既存研究は存在しない。すなわち、正しいメッセージが失われたり、数個～数十個のノードの不正取得や故障により、不正メッセージやその発生元ノードの検知が不可能となる。

本論文では、センサーノードの物理的な位置を利用して正しい鍵の組み合わせ情報を全ノードへ配備することにより、全てのメッセージ転送ノードが不正メッセージの検知をできる可能性を与えた。また、正しい鍵の組み合わせ情報をそのまま保持させずノードへ配備する際に別のデータ構造に変化させた。これにより、正しいメッセージを不正メッセージであると誤検知せず、かつ多数のノードの不正取得攻撃に対しても耐性を持たせることを可能とした。

また本論文では、メッセージを転送する各ノードにノード ID と短いビット（たとえば 1 ビット）のメッセージ認証コードを付加させた。いくつかの不正メッセージがユーザに届くことにより、統計学的手法を用いることで、不正メッセージを発生させた可能性が高いノードを特定できる。本論文では、2/3 以下の任意の精度において、不正ノードを検知できる手法を考案し、それを数学的に証明した。

無線ネットワークでは、攻撃者が一つのノードを不正取得し、その情報を用いることで多数の不正ノードを作成する、複製ノード攻撃が存在する。複製ノードを分散的に検知する既存手法では、ノードの不正取得や故障により急激に検知率が低下する。本論文では、複製ノードを検知するための鍵を全ノードに分散して配備させ、同時に、実際に検知に必要な情報を持つノードをごく少数のノードのみに設定した。またこれらのノードが故障した場合は、自動的に別のノードが持つ情報が検知に必要な情報となる仕組みを与えた。これらにより、ノードの故障や不正取得に耐性があり、高い検知率を維持できることを数学的に証明した。

本論文で提案された手法は無線ネットワークにおいてネットワークの輻輳を引き起こす攻撃の検知を目的とし、正しいメッセージを不正メッセージであると誤検知せず、かつ、数十個以上の多くのノードが不正取得または故障した状況においても、不正メッセージやその発生元ノード、または複製ノードの検知を行えることができる、初めての手法であり、無線ネットワーク研究分野に顕著なる貢献を与えた。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。