論 文 内 容 の 要 旨

氏 名 （ 高 博奇 Boqi GAO ）	
論文題名	Research on Detecting Malicious Nodes in Wireless Sensor Networks (無線センサネットワークにおける攻撃端末の検出に関する研究)

論文内容の要旨

With the rapid advances in wireless communication and digital electronics, wireless sensor networks (WSNs) have demonstrated their feasibility for monitoring events and environments. For example, WSNs can be deployed to monitor air conditions, water flows, and temperatures. People can obtain useful information from the gathered data from WSNs. A WSN is comprised of solely of sensor nodes, and no special infrastructure is required. Due to such characteristics, malicious nodes can easily join a WSN. That is, WSNs are inherently vulnerable to malicious nodes. The malicious nodes execute inappropriate actions (e.g., dropping packets and sending redundant packets) to destruct the network reliability and functionality, which triggers event losses. Even worse, such malicious nodes may lead to severe risks, particularly for real-time and safety-critical monitoring WSN applications, such as extreme weather monitoring, water quality monitoring, and forest fire alarming. Therefore, methods to detect malicious nodes in WSNs are strongly required.

Recently, with the development of machine learning technologies, many studies have proposed machine learning-based approaches to detect malicious nodes in WSNs. Generally, machine learning-based approaches train classifiers, which are based on observation of behaviors of nodes, to classify the category of nodes. However, existing methods ignore three main challenges. (i) Since general machine learning methods rely on training data, trained classifiers do not work well in test environments that are different from training environments. (ii) From the perspective of malicious nodes, malicious nodes can also learn from the detection methods to avoid being detected. Therefore, a fixed classifier cannot detect malicious nodes with learning ability. (iii) Energy harvesting cooperative (EHC) schemes are studied a lot recently. Nodes are allowed to share energy in EHC-WSNs, and some malicious nodes utilize this scheme to deprive energy from other nodes. Since the residual energy storage is private data, which could be fabricated by malicious nodes, regular machine learning-based methods do not work well because learning from fabricated data is meaningless.

In this thesis, we focus on detecting malicious nodes in WSNs with machine learning-based methods, and tackle the above-mentioned challenges. In Chapter 1, we introduce the research background and issues. In Chapter 2, we propose an ensemble learning method to detect malicious nodes in unknown network environments. We first prepare weak malicious node detectors trained in diverse environments, and then construct a strong ensemble malicious node detector, which is tailored to a given test environment, by fusing weak detectors whose performances are estimated to be high in the test environment.

In Chapter 3, we construct a framework where the malicious and normal nodes can learn by competition. In our framework, malicious nodes learn to avoid being detected and normal nodes learn to detect malicious nodes with high accuracy. We design reinforcement learning-based malicious nodes, and define a novel observation space and sparse reward function for the reinforcement learning. A malicious node thus can utilize this method to learn from existing detection methods. We also design an adaptive learning method to detect these smart malicious nodes. We construct a robust classifier, which is frequently updated, to detect these smart malicious nodes.

In Chapter 4, we propose an unsupervised learning-based method for detecting energy depriving malicious nodes in an EHC-WSN. In EHC-WSNs, nodes wirelessly transfer a portion of their energy to their neighboring nodes if their neighboring nodes lack energy. An energy depriving malicious node may forge that it has little energy, thus it can deprive energy from its neighboring nodes. Detecting energy depriving malicious nodes is not a trivial task because the real energy storage is a private data of each node. For detecting such malicious nodes, we utilize an unsupervised approach because it is impossible to prepare labeled data in a WSN in the real world. In our method, each node first observes energy of its neighboring nodes, then it utilizes this information to obtain data points for clustering.

Finally, in Chapter 5, we summarize this thesis and discuss our future work.

様式 7

論文審査の結果の要旨及び担当者

氏　名	（　　高　博奇　　）	
	（職）	氏　名
最終試験担当者	主 査　教授	原　隆浩
	副 査　教授	藤原　融
	副 査　教授	下條　真司
	副 査　教授	鬼塚　真
	副 査　教授	松下　康之

論文審査の結果の要旨

無線通信技術の向上により、無線センサネットワークにおけるイベント検出や環境モニタリングの実践化が進んでいる。無線センサネットワークはセンサ端末のみで構成されるため、特別なインフラを必要としない。一方で、攻撃端末が容易に介入できるという弱点もある。攻撃端末とは、パケットドロップや無駄なパケット送信などの不適切な行動を取る端末を指し、ネットワークの安定性や機能を破壊する目的を持つ。これにより、無線センサネットワークにおけるイベント検出が正常に行われない等の不具合が生じてしまう。そのため、無線センサネットワークにおける攻撃端末の検出は重要な課題である。本研究では、機械学習を用いたアプローチにより無線センサネットワーク内の攻撃端末を検出することを目的としており、具体的には以下の3つの問題に取り組んだ。

(1) 端末数やネットワークサイズが不明な無線センサネットワークに対する攻撃端末の検出問題に取り組んだ。無線センサネットワークにおいて分類器を用いた手法は過去に提案されているが、訓練環境とテスト環境を同一と想定したものだけであり、実践性に乏しい。本研究では、テスト環境が不明な場合にも対応できるアンサンブル学習器を提案している。提案手法は、様々なネットワーク環境において弱検出器を作成しする。そして、テスト環境で収集したデータを用いて、テスト環境おいて高性能と推測される弱検出器を統合した検出器を作成する。シミュレーション実験により、提案手法は既存手法を上回る性能を持つことを示した。

(2) 攻撃端末も機械学習により検出を避ける環境を想定した攻撃端末の検出問題に取り組んだ。特に、攻撃端末が強化学習を用いてネットワークに攻撃しつつ検出を避ける状態を学習することを想定した。また、通常の端末は、深層学習を用いて現在の攻撃端末の状態に適応するように学習し、学習能力を持つ攻撃端末を検出する。シミュレーション実験により、学習能力を持つ攻撃端末は、既存の攻撃手法よりも検出されにくいことを確認している。また、提案手法は、このような攻撃端末に対しても既存手法よりも高精度で検出できることも確認している。

(3) ハードウェア技術の発展により、端末のバッテリを無線通信で他の端末にシェアすることが可能となっている。この技術は無線センサネットワークの寿命を長くする効果を持つが、攻撃端末が存在する場合、バッテリを奪われるリスクもある。このような攻撃を行う端末を検出する問題に取り組んだ。提案手法は、隣接端末のバッテリをモニタリングし、その情報から機械学習ベースのクラスタリングを用いて通常の端末か攻撃端末かを分類する。シミュレーション実験から、提案手法は既存のクラスタリング手法よりも高精度で攻撃端末を検出できることを確認した。

以上のように、本論文は無線センサネットワークにおける攻撃端末の特定に関する先駆的な研究として、情報科学に寄与するところが大きい。よって本論文は博士（情報科学）の学位論文として価値のあるものと認める。