論 文 内 容 の 要 旨

博士論文題目　MANETを用いた商取引システムのための安全なプロトコル

氏　　名 BABATUNDE OJETUNDE

(論文内容の要旨)

（１，２００字程度）

Commerce system in a disaster area has the potential to provide electronic transactions for people purchasing recovery goods like foodstuffs, clothes, and medicine. However, to enable transactions in a disaster area, current payment systems need communication infrastructures (such as wired networks and cellular networks) which may be ruined during such disasters as large-scale earthquakes and flooding and thus cannot be depended on in a disaster area. In such a situation where the communication infrastructure is damaged, it is practically impossible to secure the commerce system or the routing protocol that may be adopted to route transactions against attacks. Furthermore, most existing secure routing protocols adopt a cryptography-based approach, trust-based approach, or incentive-based approach to detect and prevent such attacks. However, such protocols still have drawbacks, such as difficulty in maintaining secure key, or leaving routes unsecured against Byzantine attacks. Therefore, to address the shortcomings of the existing systems, a secure MANET-based commerce system is proposed.

In the first part of this dissertation, we introduce a new mobile payment system utilizing infrastructureless MANETs to enable transactions that permit users to shop in disaster areas. Specifically, we introduce an endorsement-based mechanism to provide payment guarantees for a customer-to-merchant transaction and a multilevel endorsement mechanism with a lightweight scheme based on Bloom filter and Merkle tree to reduce communication overheads.

In the second part of this dissertation, we introduce a monitoring-based method in the link state routing protocol to secure the packets' route against Byzantine attacks. The goal of our proposed scheme is to guarantee communication among connected benign nodes in the network. Specifically, each node monitors the action of neighboring nodes and compares the optimal packet route against the packet route history. The proposed scheme provides protection against colluding attacks and other Byzantine attacks.

氏　名	Babatunde Ojetunde

（論文審査結果の要旨）

災害発生時には必ずしも十分な現金を所持しているとは限らず、緊急に必要な品を購入するために電子的な商取引システムを利用することが考えられる。しかし、大災害などにより通信インフラが機能しない状況下ではサーバに接続できないため，オンラインによる電子商取引を行うことは困難である。不正な利用者を検出・排除した安全な電子商取引を行うため、現状のシステムは、暗号、信頼できる利用者、報酬などに基づくプロトコルを用いているが、通信インフラが機能しない状況では、このようなプロトコルを利用することは事実上不可能である。以上のことから、災害時にも安全な電子商取引が行えるようなシステムを構築することは重要な問題である。本研究では、通信インフラに依存しない MANET を利用したモバイル決済手法を用いた災害時でも安全な電子商取引を実現するシステムを提案する。具体的には、多段階の裏書による支払い保証メカニズムを導入し、携帯端末の電力消費を抑えるために Bloom フィルタと Merkle 木に基づいた通信量の削減を図る。次に、隣接ノードの動作を監視し、最適なパケット経路とパケット経路履歴とを比較することで、結託攻撃やビザンチン攻撃等を行う不正な利用者を排除した MANET を構成する手法を提案する。本研究の学術的貢献は以下の通りである。

(1) 通信インフラに依存しない携帯端末に適した安全な電子商取引の手法を提案している。
(2) 様々なノードから構成される MANET において、不正なノードを検出・排除し、結託攻撃やビザンチン攻撃から耐性のある手法を提案し、既存の手法との比較で優位性を確認している。

従来の携帯端末を用いた電子商取引システムに関する研究はオンラインシステムの存在を前提としており、災害などで通信インフラが機能しない場合の電子商取引の具体的な手法を提案している例はない。その際、MANET を利用するが、不正なノードを検出・排除し、安全な通信を行うことは重要な問題である。本研究では、これらの問題に対する具体的な解決手法を提示しており、大きな貢献があると評価する。

以上のことから、本論文は博士（工学）の学位論文として価値あるものと認める。