様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２８　日現在

機関番号：　１４６０３
研究種目：　若手研究(B)
研究期間：　2015～2017
課題番号：　１５Ｋ１５９８１

研究課題名（和文）Endorsement Based Offline Mobile Payment System for Disaster Areas

研究課題名（英文）Endorsement Based Offline Mobile Payment System for Disaster Areas

研究代表者
高　俊涛（Gao, Juntao）

奈良先端科学技術大学院大学・情報科学研究科・助教

研究者番号：３０７３２９６１

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：災害地域の人々は商人から救援物資を購入する必要がある。しかし、通信インフラを利用できないため、銀行サーバでの取引と支払いを行うことができない。このプロジェクトでは、ユーザが災害地域での電子取引を行うことを可能にするため、裏書きに基づくモバイル決済システムを提案している。このシステムは、スマートフォンを利用してモバイルアドホックネットワークを組み立てることで通信を実現させるから、速やかに構築できるし、地震の余震によるネットワークノードの故障に対してロバスト性を付けさせる功能も持っている。また、ユーザを認証できるスキーム、結託攻撃と二重支払い攻撃を防ぐスキームも提案している。

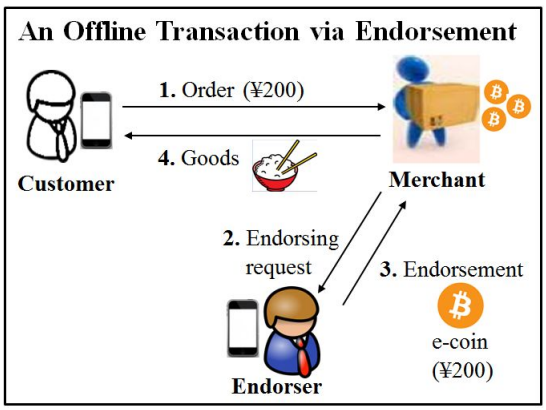
研究成果の概要（英文）：This project aims at proposing an endorsement based mobile payment system that can be used by people in disaster areas to buy goods from merchants even without online connection to bank servers. This payment system utilizes mobile ad hoc networks formed from smart phones for communication, thus could be rapidly constructed and robust to node failures in aftershock of earthquakes. Specifically, we proposed schemes for user authentication, preventing collusion and double-spending attacks. We also proposed a monitoring scheme to secure packets route against Byzantine attacks in mobile payment systems and an adaptive packet transmission algorithm that saves battery power of smart phones. We verified by simulations that 1) our endorsement based mobile payment system achieves high transaction completion ratio, 2) our monitoring based link state routing protocol can guarantee secure transactions in mobile payment system.

研究分野：　network protocol

キーワード：　mobile payment system　endorsement　electronic money　secure routing　byzantine attack　traffic scheduling　Q-learning

１．研究開始当初の背景

Nowadays people in a disaster area could use smart phones to buy goods, like clothing, food and medicine. However, most mobile payment systems (MPSs) via smart phones rely on online banking services, which is unavailable in disasters due to the lack of communication infrastructures. By now, no offline MPSs for disaster areas via smart phones have been developed.



２．研究の目的

As endorsers could provide offline payment guarantees, this project aims at developing an offline MPS based on endorsement (called EMPS) for people in a disaster area using smart phones to buy goods (see the figure below). We will also propose schemes to secure transactions in our EMPS and develop mathematical models to evaluate message delay performance.

(1) Overall Design of Offline EMPS: We will design the overall architecture and components of EMPS, including participants, endorsing mechanism and authentication. In our EMPS, an endorser guarantees the transaction between a customer and a merchant via electronic money, with which the merchant could change for real money from banks some days later.

(2) Preventing Colluding Attack: Since there is no online banking service, it is possible for an endorser and a customer to collude to defraud a merchant if both of them do not have money in their bank accounts. Thus, we will use e-coins for balance checking to prevent such colluding.

(3) Preventing Double-Spending Attack: An endorser may double spend the same electronic money with merchants. Existing solutions to prevent double-spending require great computation power and battery energy, thus not suitable for smart phones in disaster areas. We will propose a lightweight scheme based on transaction chain and monitoring to prevent double-spending attacks.

(4) Experiment: We will do simulations to test the usability and security of our proposed system.

３．研究の方法

(1) Endorsement: One major novelty of this project is to introduce another type of participants, endorsers, who guarantee to pay merchants in case customers do not have enough money. The offline electronic transaction procedures of EMPS are as follows.

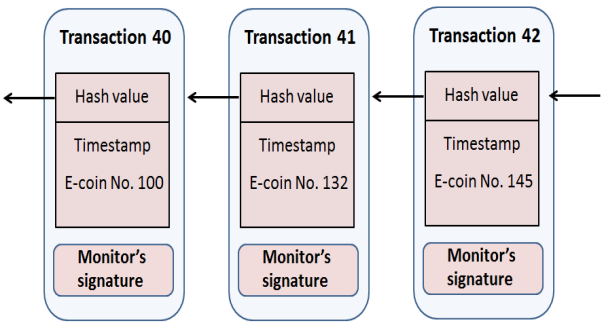
① A customer sends transaction order message to a merchant; ② The merchant creates billing message and requests an endorser to endorse it; ③ The endorser creates an endorsement message with e-coins and forwards it to the merchant; ④ The merchant supplies required goods to the customer and changes for

real money from a bank with obtained e-coins when he accesses bank services several days later.

(2) Privacy and Authentication: We use nickname to provide user anonymity, blind signature technique to protect transaction messages and digital signature to authenticate participants.

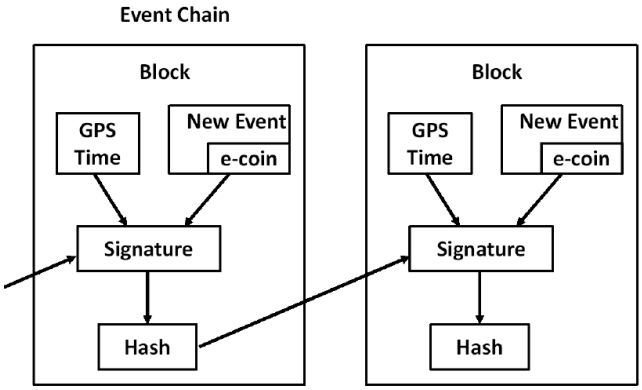
(3) Preventing Collusion: Endorsers will deposit in advance real money in banks in exchange for e-coins, each with a unique identifier. During a disaster, an endorser will attach enough e-coins to guarantee the payment of a transaction. Otherwise the merchant will reject the transaction. In this way, collusion is avoided.

(4) Preventing Double-Spending: To prevent an endorser from double spending e-coins with merchants, we propose a scheme of transaction chain for merchants to check the log of e-coin transactions associated to the endorser (see the figure below). To create the transaction chain, an endorser requests a monitoring participant to sign (with their digital signature) each of his/her new e-coin transaction. Any merchant could check this chain of e-coin usage history to detect double spending.

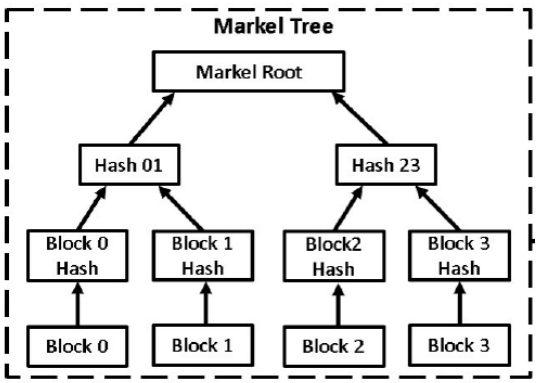


4．研究成果

(1) We proposed a new mobile payment system utilizing 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 an event chain mechanism to prevent double spending attacks.



(2) We also proposed a multilevel endorsement mechanism with a lightweight scheme based on Bloom filter and Merkle tree to reduce communication overheads.

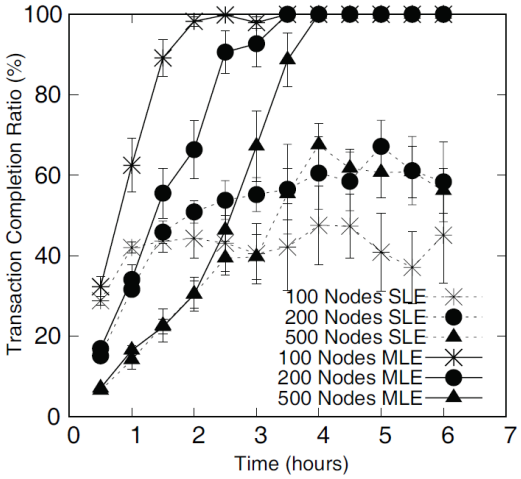


(a) Transaction Block in Markel Tree

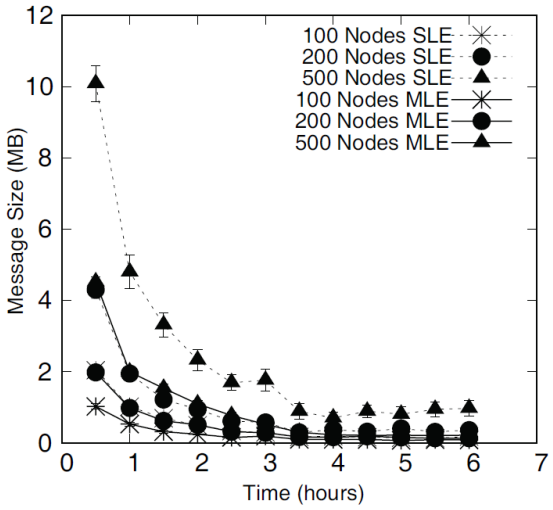
Our mobile payment system achieves secure transaction by adopting various schemes such as location-based mutual monitoring scheme and blind signature.

(3) As validated by simulations, the

proposed mobile payment system is useful in a disaster area, achieving high transaction completion ratio and is storage efficient for mobile devices.

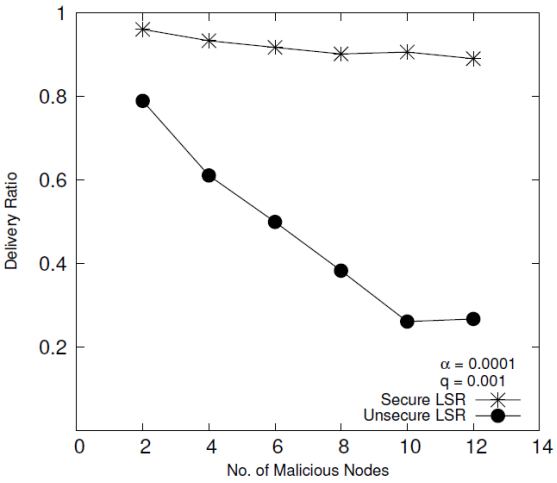


(a) Transaction completion ratio



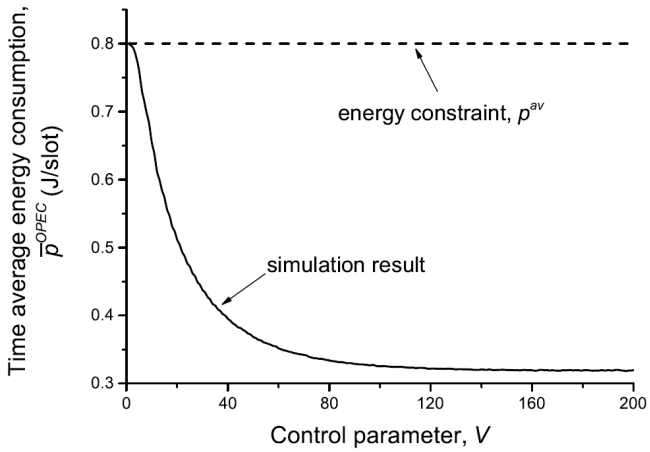
(b) Merchant message size

(5) To secure packets route against Byzantine attacks in mobile payment systems, we proposed a monitoring based link state routing protocol, which guarantees communication among connected benign nodes in the network. As verified by simulations, the proposed routing protocol achieves an average of 89% to 96% packet delivery ratio when 11% to 21% active malicious links are excluded from the network.



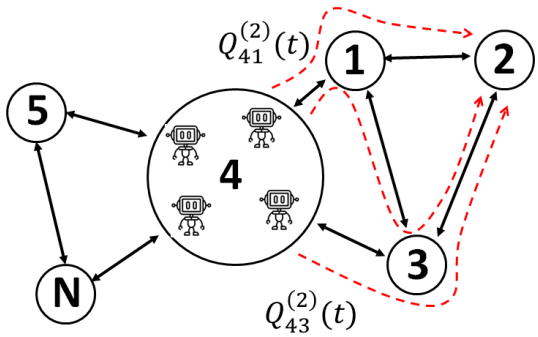
(a) Packet delivery ratio

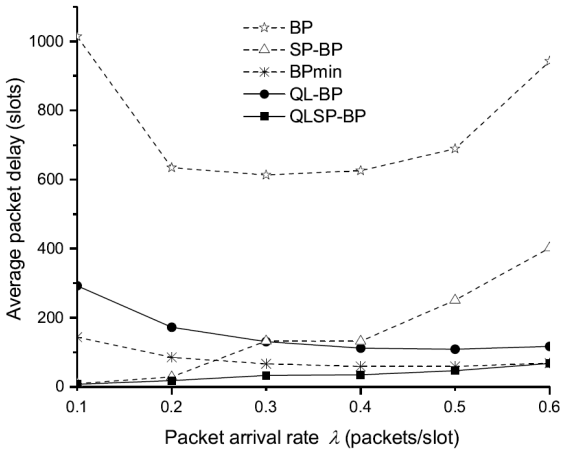
(6) To save battery power of smart phones, we proposed an adaptive packet transmission algorithm which only transmits packets when wireless channel condition is good and does not transmit packets when wireless channel condition is bad. As verified by simulations, our algorithm can effectively reduce enery consumption and thus enlong battery lifetime, which is critical for users in disaster areas.



(7) To reduce communication delay in our mobile payment system, we proposed multi-agent Q-learning aided backpressure routing algorithm, where

each node estimates route congestion using only local information of neighboring nodes. Simulation results show that our algorithm reduces average packet delay by 95% for light traffic loads and by 41% for moderate traffic loads when compared to state-of-the-art BPmin algorithm.





5．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　2 件）査読あり

① Babatunde Ojetunde, Naoki Shibata, and Juntao Gao, Monitoring-Based Method for Securing Link State Routing against Byzantine Attacks in Wireless Networks, Journal of Information Processing, pp.98-110, 15 Feb. 2018.
DOI: https://doi.org/10.2197/ipsjjip.26.98

② Babatunde Ojetunde, Naoki Shibata and Juntao Gao, “ Secure Payment System Utilizing MANET for Disaster Areas, IEEE Transactions on Systems, Man and Cybernetics: Systems, Early Access, pp.1-18, Sep. 2017.
https://ieeexplore.ieee.org/document/8053463/

〔学会発表〕（計　12 件）査読あり

① Juntao Gao, Yulong Shen, Minoru Ito and Norio Shiratori, Bias Based General Framework for Delay Reduction in Backpressure Routing Algorithm, International Workshop on Computing, Networking and Communications, March 2018.

② Ying Liu, Juntao Gao, Yishan Lin and Minoru Ito, Application of Back-Pressure Algorithm to Traffic Signal Control in Road Networks of Finite Road Capacity, 第 25 回マルチメディア通信と分散処理ワークショップ (DPSWS 2017), 11 Oct. 2017.

③ Juntao Gao and Minoru Ito, Consideration on Applying Q-Learning to Backpressure Routing Algorithm to Improve Delay Performance, 第25回 マルチメディア通信と分散処理ワークショップ (DPSWS2017), 11 Oct. 2017.

④ Babatunde Ojetunde, Naoki Shibata and Juntao Gao, Securing Link State Routing for Wireless Networks against Byzantine Attacks: A Monitoring Approach, IEEE Computer Society International Conference on Computers, Software & Applications, pp591-601, 4 Jul. 2017.

⑤ Ojetunde Babatunde, Noki Shibata and Juntao Gao, A Proposed

Monitoring Scheme to Prevent Byzantine Attacks on Link State Routing in MANETs, 第 171 回 DPS・第 83 回 MBL・第 69 回 ITS 合同研究発表会, Jun. 2017.
⑥ Lin Yi Shan, Liu Ying, Juntao Gao and Minoru Ito, Back-Pressure Based Traffic Scheduling Algorithm for Urban Vehicular Networks with Self-Driving Vehicles, 第112回数理モデル化と問題解決研究発表会 (MPS2017), 2017年02月.
⑦ Juntao Gao, Minoru Ito and Norio Shiratori, Optimal Scheduling for Incentive WiFi Offloading under Energy Constraint, IEEE 27th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp1906-1911, 4 Sep. 2016.
⑧ Babatunde Ojetunde, Naoki Shibata, Juntao Gao, and Minoru Ito, Consideration on Monitoring Scheme to Secure Link State Routing against Byzantine Attacks, 第24回 マルチメディア通信と分散処理ワークショップ (DPSWS2016), 2016年10月.
⑨ Babatunde Ojetunde, Naoki Shibata, Juntao Gao, and Minoru Ito , An Enhanced Endorsement Chain using Endorsement Delegation on MANETs Based Mobile Payment System in a Disaster Area, 第166回マルチメディア通信と分散処理研究会 (DPS), 2016年03月.
⑩ Babatunde Ojetunde, Naoki Shibata, Juntao Gao, and Minoru Ito, Simulation Based Evaluation of a Mobile Payment System Utilizing MANETs for a Disaster Area, マルチメディア、分散、協調とモバイル(DICOMO2015)シンポジウム, 2015年07月.
⑪ Juntao Gao and Minoru Ito , A Study for Residual Inter-Contact Time in Homogeneous Opportunistic Networks, マルチメディア、分散、協調とモバイル(DICOMO2015)シンポジウム, 2015年07月.
⑫ Juntao Gao and Minoru Ito , Residual Inter-Contact Time for Opportunistic Networks with Pareto Inter-Contact Time: Two Nodes Case, The 21st International Conference on Parallel and Distributed Processing Techniques and Applications, 2015年07月.

６．研究組織

(1)研究代表者

高　俊涛（Gao Juntao）
奈良先端科学技術大学院大学・情報科学研究科・助教
研究者番号：30732961