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

令和　５ 年　 ６ 月 ２０ 日現在

機関番号：６２６１５
研究種目：若手研究
研究期間：2020～2022
課題番号：２０Ｋ１４７４２

研究課題名（和文）A New PLS-aware Incentive Routing Protocol Targeting Secure and Efficient Data Delivery in D2D Communication-based IoT Systems

研究課題名（英文）A New PLS-aware Incentive Routing Protocol Targeting Secure and Efficient Data Delivery in D2D Communication-based IoT Systems

研究代表者
劉　佳（LIU, JIA）

国立情報学研究所・ストラテジックサイバーレジリエンス研究開発センター・特任助教

研究者番号：１０８１３４２０

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：物理層セキュリティ技術に基づいたインセンティブルーティング設計フレームワークを開発しました。一般的なエンドツーエンド（E2E）パスのセキュリティパフォーマンスを定量化し、セキュリティとサービス品質の最適なトレードオフを調査しました。構築されたセキュアなルーティングスキームは、多項式時間でルーティング計算を実行することができ、分散型IoTシステムにおけるE2Eのセキュアなデータ配信に対する軽量なソリューションを提供します。

研究成果の学術的意義や社会的意義
研究成果の学術的意義や社会的意義は次のように反映されます：1. 物理層セキュリティ技術のIoTシステムへの適用を容易にします。2. 新興の物理層セキュリティ技術の普及に貢献します。3. IoTシステムにおける物理層セキュリティとサービス品質のパフォーマンスについて包括的な理解を提供します。4. Society 5.0において、国と市民の安全性を向上させます。

研究成果の概要（英文）：We have developed an incentive routing design framework based on physical layer security techniques. We have quantified the security performance of general end-to-end (E2E) paths and investigated the optimal tradeoff between security and quality of service. The constructed secure routing scheme can perform routing calculations in polynomial time, providing a lightweight solution for E2E secure data delivery in decentralized IoT systems.

研究分野：通信工学

キーワード：物理層セキュリティー　IoT　セキュアルーティング　激励メカニズム　サービス品質

１．研究開始当初の背景

D2D communication-based IoT systems have been recognized as a critical element of Society 5.0 to implement ubiquitous, high-speed, and low-latency data delivery in the 5G era. However, numerous sensitive data delivery poses great challenges to the security of such systems. This is because the open wireless medium makes data easy to be wiretapped by malicious eavesdroppers, whereas IoT devices usually do not have enough computing resources to implement complex cryptographic schemes. Therefore, without a lightweight yet powerful security solution, the safety of the nation and citizens in Society 5.0 will be at great risk. PLS technology is an information-theoretic approach that exploits the inherent physical characteristics of wireless medium (such as fading, path loss, noise, and interference) to achieve transmission security. Due to the advantages of easy implementation and no requirement of distributing/managing secret keys, PLS technology is very promising to be applied in the design of IoT systems, as is evident from some influential academic papers and ongoing JSPS projects.

２．研究の目的

The goal of this research is to develop a novel routing framework that integrates PLS technology with upper-layer routing techniques, for secure and efficient data delivery in D2D communication-based IoT systems. The proposed PLSI routing protocol is expected to be individually rational, stable, distributed, and computationally efficient.

３．研究の方法

(1) Performance Evaluation Framework: Our approach utilizes Stochastic Geometry to model the system topology dynamically. By employing Laplace Transform, Contour Integration, and Probability Theory, we derive the exact secrecy outage probability of the route. Additionally, Queueing Theory is employed to model the data delivery process, enabling us to derive closed-form expressions for throughput, delay, and secrecy throughput using the refined QBD-based analytical framework.

(2) Incentive Mechanism Design: As illustrated in Fig. 1, we model the incentive mechanism as a two-stage Stackelberg game. At Stage I, the source determines the optimal value of the reward to maximize its utility. At Stage II, each jammer strategizes its jamming power to maximize its utility, which is modeled as a non-cooperative game.

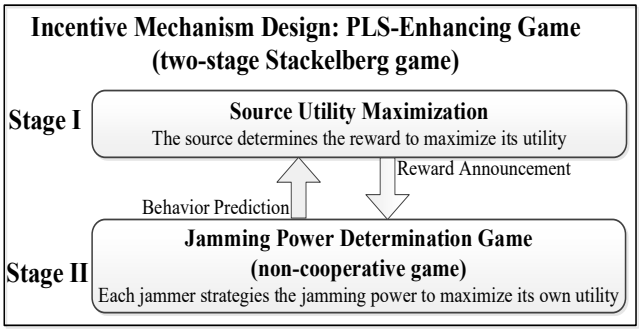

Fig. 1 Incentive mechanism design.

(3) PLS-QoS Tradeoffs: Based on the performance evaluation and incentive mechanism, we formulate the tradeoff issues as mathematical optimization problems, which are usually non-linear and non-convex. To address these problems, we propose efficient algorithms by employing the techniques of alternative optimization, Zoutendijk's method, fractional programming, semi-definite programming, DC programming, and so on.

(4) Routing Protocol Design: As illustrated in Fig. 2, the PLS-aware incentive routing protocol is designed in a backward induction manner. We convert the problem of optimal route selection to finding the "shortest weighted path". As a result, we integrate all information related to a link as its weight and employ the classical Bellman-Ford algorithm to establish the optimal route for secure data delivery while ensuring QoS performance.

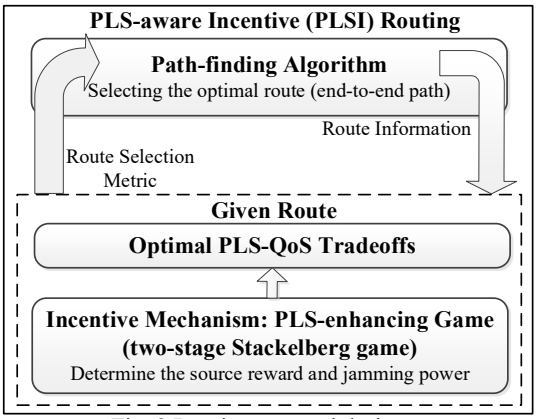

Fig. 2 Routing protocol design.

４．研究成果

Overall, we have successfully completed all the research tasks outlined in the project plan and have published 9 journal papers and 9 conference papers. The specific research achievements are summarized as follows:

(1) We design an incentive jamming-based secure routing scheme for decentralized IoT

In a typical decentralized IoT scenario, comprising legitimate devices, unauthorized eavesdroppers, and self-interested jammers, we present an innovative secure routing scheme based on incentive jamming. For a specific source and destination pair, we begin by developing a theoretical model that elucidates the relationship between the security performance of a given route and the jamming power exerted by jammers in the IoT network. Subsequently, we introduce an incentive mechanism whereby the source provides rewards to incentivize selfish jammers to engage in artificial jamming. To determine the optimal source rewards and jamming power, we devise a two-stage Stackelberg game framework. Leveraging the theoretical model, source rewards, and jamming power settings, we formulate a shortest-weighted path-finding problem to identify the optimal route for secure data delivery between the source and destination. This problem can be efficiently solved using the Bellman-Ford algorithm. Importantly, we demonstrate that the proposed routing scheme is individually rational, stable, distributed, and computationally efficient.

(2) We design a QoS-aware secure routing scheme for decentralized IoT

We still focus on a general multi-hop decentralized IoT system consisting of legitimate nodes, malicious eavesdroppers, and selfish jammers. Initially, we establish a theoretical model that examines the

relationship between the end-to-end security and quality of service (QoS) performance of a given route, taking into account the transmitting power of legitimate nodes and the jamming power exerted by the network's jammers. Subsequently, we devise an incentive mechanism aimed at motivating jammers to generate artificial jamming, thereby enhancing security. We also develop a non-cooperative game framework to address the challenge of setting jamming power. By leveraging the security and QoS performance modeling of the route, along with the jamming power configuration, we propose a theoretical framework to determine the optimal transmitting power for nodes along the route. This approach ensures optimal transmission security while adhering to QoS constraints. Finally, leveraging the power configuration results obtained for the given route, we formulate a problem of finding the shortest-weighted path to identify the optimal route for data delivery within the network. This problem can be effectively solved using algorithms such as Bellman-Ford or Dijkstra's algorithm. The routing scheme we propose is demonstrated to be individually rational, stable, distributed, and computationally efficient.

(3) We design an incentive routing scheme to achieve covert communication in multi-hop decentralized IoT

We further focus on a multi-hop decentralized IoT system consisting of legitimate nodes, adversary wardens, and friendly yet self-interested jammers. Our investigation revolves around designing a routing scheme that enables covert communication within this network. Initially, we conduct a theoretical analysis of a given route between a pair of source and destination nodes to uncover the relationship between the level of jamming power exerted by jammers and the performance of covertness. Subsequently, we develop an incentive mechanism that encourages selfish jammers to provide deliberate jamming to safeguard the secrecy of communication by offering them rewards from the source. To analyze the strategic interactions between the source and the jammers and determine the optimal configuration of rewards and jamming power, we establish a two-stage Stackelberg game framework. Leveraging these findings, we formulate a problem of finding the shortest-weighted path, aiming to identify the optimal route for covert communication between the source and destination nodes.

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9件／うち国際共著　9件／うちオープンアクセス　3件）

１．著者名 Liu Jia、Xu Yang、Shen Yulong、Takakura Hiroki、Jiang Xiaohong、Taleb Tarik	４．巻 9
２．論文標題 Buffer Space Management in Intermittently Connected Internet of Things: Sharing or Allocation?	５．発行年 2022年
３．雑誌名 IEEE Internet of Things Journal	６．最初と最後の頁 10961～10977
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JIOT.2021.3128523	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Xu Yang、Liu Jia、Shen Yulong、Jiang Xiaohong、Ji Yusheng、Shiratori Norio	４．巻 20
２．論文標題 QoS-Aware Secure Routing Design for Wireless Networks With Selfish Jammers	５．発行年 2021年
３．雑誌名 IEEE Transactions on Wireless Communications	６．最初と最後の頁 4902～4916
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TWC.2021.3062885	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Zhao Shuangrui、Liu Jia、Shen Yulong、Jiang Xiaohong、Shiratori Norio	４．巻 16
２．論文標題 Secure and Energy-Efficient Precoding for MIMO Two-Way Untrusted Relay Systems	５．発行年 2021年
３．雑誌名 IEEE Transactions on Information Forensics and Security	６．最初と最後の頁 3371～3386
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2021.3080088	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Xu Yang、Liu Jia、Shen Yulong、Liu Jun、Jiang Xiaohong、Taleb Tarik	４．巻 8
２．論文標題 Incentive Jamming-Based Secure Routing in Decentralized Internet of Things	５．発行年 2021年
３．雑誌名 IEEE Internet of Things Journal	６．最初と最後の頁 3000～3013
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JIOT.2020.3025151	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Zhao Shuangrui、Liu Jia、Shen Yulong、Jiang Xiaohong、Shiratori Norio	4．巻 15
2．論文標題 Secure Beamforming for Full-Duplex MIMO Two-Way Untrusted Relay Systems	5．発行年 2020年
3．雑誌名 IEEE Transactions on Information Forensics and Security	6．最初と最後の頁 3775～3790
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2020.3001733	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Xu Yang、He Honggang、Liu Jia、Shen Yulong、Taleb Tarik、Shiratori Norio	4．巻 10
2．論文標題 IDADET: Iterative Double-Sided Auction-Based Data-Energy Transaction Ecosystem in Internet of Vehicles	5．発行年 2023年
3．雑誌名 IEEE Internet of Things Journal	6．最初と最後の頁 10113～10130
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JIOT.2023.3236968	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Dong Xuewen、You Zhichao、Shen Yulong、Lu Di、Xu Yang、Liu Jia	4．巻 Early Access
2．論文標題 A Two-Dimensional Sybil-Proof Mechanism for Dynamic Spectrum Access	5．発行年 2022年
3．雑誌名 IEEE Transactions on Mobile Computing	6．最初と最後の頁 1～15
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TMC.2022.3200044	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Zheng Kechen、Sun Wendi、Liu Xiaoying、Zhao Dongdong、Xu Yang、Liu Jia	4．巻 16
2．論文標題 Throughput maximisation for multi‐channel energy harvesting cognitive radio networks with hybrid overlay/underlay transmission	5．発行年 2022年
3．雑誌名 IET Communications	6．最初と最後の頁 274～290
掲載論文のDOI（デジタルオブジェクト識別子） 10.1049/cmu2.12347	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Qu Zheng、Jia Qingyao、Lyu Chen、Liu Jia、Liu Xiaoying、Zheng Kechen	4．巻 2022
2．論文標題 Detecting Fake Reviews with Generative Adversarial Networks for Mobile Social Networks	5．発行年 2022年
3．雑誌名 Security and Communication Networks	6．最初と最後の頁 1〜11
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2022/1164125	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

〔学会発表〕　計9件（うち招待講演　0件／うち国際学会　9件）

1．発表者名 Shanshan Zhang, Yang Xu, Jia Liu, Hiroki Takakura, Chen Lyu, Norio Shiratori
2．発表標題 Bandwidth Allocation for Low-Latency Wireless Federated Learning: An Evolutionary Game Approach
3．学会等名 2023 IEEE International Conference on Communications (ICC)（国際学会）
4．発表年 2023年

1．発表者名 Meng Xie, Jia Liu, Hiroki Takakura, Yang Xu, Zhao Li, Norio Shiratori
2．発表標題 Incentive Routing Design for Covert Communication in Multi-hop Decentralized Wireless Networks
3．学会等名 2022 IEEE Global Communications Conference (GLOBECOM)（国際学会）
4．発表年 2022年

1．発表者名 Yang Xu, Jia Liu, Hiroki Takakura, Zhao Li, Yusheng Ji, and Norio Shiratori
2．発表標題 Stackelberg Game-based Secure Communication in SWIPT-enabled Relaying Systems
3．学会等名 2022 IEEE International Conference on Communications (ICC)（国際学会）
4．発表年 2022年

１．発表者名
Honggang He, Yang Xu, Jia Liu, Hiroki Takakura, Zhao Li, Norio Shiratori

２．発表標題
Double-Sided Auction based Data-Energy Trading Architecture in Internet of Vehicles

３．学会等名
2022 IEEE Wireless Communications and Networking Conference (WCNC)（国際学会）

４．発表年
2022年

１．発表者名
Jianbo Shao, Yang Xu, Jia Liu, Hiroki Takakura, Zhao Li, Xuewen Dong

２．発表標題
On Strategic Interactions in Blockchain Markets: A Three-stage Stackelberg Game Approach

３．学会等名
2021 IEEE Global Communications Conference (GLOBECOM)（国際学会）

４．発表年
2021年

１．発表者名
Wendi Sun, Xiaoying Liu, Kechen Zheng, Yang Xu, Jia Liu

２．発表標題
Spectrum Utilization Improvement for Multi-Channel Cognitive Radio Networks with Energy Harvesting

３．学会等名
2021 International Conference on Networking and Network Applications（国際学会）

４．発表年
2021年

１．発表者名
Shuangrui Zhao, Jia Liu, Yulong Shen and Xiaohong Jiang

２．発表標題
Covert Outage Analysis for Random Wireless Networks Under Warden Collusion

３．学会等名
International Conference on Networking and Network Applications（国際学会）

４．発表年
2020年

１．発表者名 Yang Xu, Kehan Yang, Yu Wang, Zhao Li, Tao Zhang, Jia Liu
２．発表標題 On Jamming Power Optimization for Secure and QoS-Aware Routing in Ad Hoc Networks
３．学会等名 International Conference on Networking and Network Applications（国際学会）
４．発表年 2020年

１．発表者名 Yuyu Hu, Zhao Li, Jingling Li, Zhixian Chang, Yang Xu, Jia Liu
２．発表標題 Incremental-Compensation based Robust Topology Control for Micro/Nano Satellite Network
３．学会等名 International Conference on Networking and Network Applications（国際学会）
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関