| | |
|---|---|
| Title | 高信頼性を有するIoTの実現に向けたセキュアアクセス制御方式に関する研究 |
| Sub Title | Research of secure access control schemes for realization of IoT with high reliability |
| Author | 笹瀬, 巌(Sasase, Iwao)<br>豊田, 健太郎(Toyoda, Kentaro) |
| Publisher | |
| Publication year | 2017 |
| Jtitle | 科学研究費補助金研究成果報告書 (2016. ) |
| JaLC DOI | |
| Abstract | デバイス同士がネットワークを自動的に構築するIoT(Internet of Things)は, 構造物モニタリング, 災害検知, 自動検針, 在庫管理といったアプリケーションを実現する基盤技術であり, 省電力, リアルタイム, 高信頼, 高セキュリティが求められる。しかしながら, これらのアプリケーションを想定した場合の省電力, 高信頼性, および高セキュリティに関する検討は十分ではない。本研究では, 上記IoTにおける次世代アプリケーションを想定した際の省電力, 高信頼性, および高セキュリティを満たすルーティング, メディアアクセス制御および攻撃防御について検討を行い, 特性改善を図る方式を提案した。<br>IoT (Internet of Things), which builds a network between the devices automatically, is the important technology which achieves the realization of useful applications such as a monitoring of a structure, an accident detection, the automatic meter reading and inventory control, and thus, power-saving, real time, high reliability and security are required. However the consideration about power-saving, high reliability and security is not enough. In this research, we considered the routing, media access control and aggressive defense with power-saving, high reliability and high security when assuming the next generation application in the above-mentioned IoT. |
| Notes | 研究種目 : 基盤研究(C)(一般)<br>研究期間 : 2014 ~ 2016<br>課題番号 : 26420369<br>研究分野 : 情報通信工学 |
| Genre | Research Paper |
| URL | https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KAKEN_26420369seika |

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　２９　年　　５　月　１７　日現在

機関番号：　３２６１２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６４２０３６９

研究課題名（和文）高信頼性を有するＩｏＴの実現に向けたセキュアアクセス制御方式に関する研究

研究課題名（英文）Research of Secure Access Control Schemes for Realization of IoT with High Reliability

研究代表者

笹瀬　巌（SASASE, IWAO）

慶應義塾大学・理工学部（矢上）・教授

研究者番号：００１８７１３９

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：デバイス同士がネットワークを自動的に構築するIoT（Internet of Things)は，構造物モニタリング，災害検知，自動検針，在庫管理といったアプリケーションを実現する基盤技術であり，省電力，リアルタイム，高信頼，高セキュリティが求められる．しかしながら，これらのアプリケーションを想定した場合の省電力，高信頼性，および高セキュリティに関する検討は十分ではない．
本研究では，上記IoTにおける次世代アプリケーションを想定した際の省電力，高信頼性，および高セキュリティを満たすルーティング，メディアアクセス制御および攻撃防御について検討を行い，特性改善を図る方式を提案した．

研究成果の概要（英文）：IoT (Internet of Things), which builds a network between the devices automatically, is the important technology which achieves the realization of useful applications such as a monitoring of a structure, an accident detection, the automatic meter reading and inventory control, and thus, power-saving, real time, high reliability and security are required. However the consideration about power-saving, high reliability and security is not enough.
In this research, we considered the routing, media access control and aggressive defense with power-saving, high reliability and high security when assuming the next generation application in the above-mentioned IoT.

研究分野：　情報通信工学

キーワード：　メディアアクセス制御　セキュアネットワーク　IoT

１．研究開始当初の背景

デバイス同士がネットワークを構築することで自動化する IoT (Internet of Things) は，構造物のモニタリング，災害検知システム，電気使用量を収集する自動検針システム，在庫管理システムといったアプリケーションを実現する基盤技術であり，省電力，リアルタイム性，高信頼性，高いセキュリティが求められる．しかしながら，橋梁モニタリング，自動検針システム，RFID を用いた在庫管理システム等のアプリケーションを想定した場合の省電力，高信頼性，および高いセキュリティに関する検討は十分ではない．そこで本研究では，上記の IoT における次世代アプリケーションを想定した際の省電力，高信頼性，および高いセキュリティを満たすルーティング，メディアアクセス制御方式および攻撃防御システムについて検討を行う．

２．研究の目的

近年，ユビキタス社会を実現する技術として，これまで人の手によって行われてきた自動検針，物流管理，環境計測，健康管理支援といったアプリケーションを，デバイス同士がネットワークを構築することで自動化する IoT が注目されている．IoT を実現する基盤技術として，無線ネットワーク機能を有するデバイスで IPv6 を用いたネットワークを構成する 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks)および RFID (Radio Frequency IDentification)があるが，特定のアプリケーションを想定した場合の省電力，高信頼性，および高いセキュリティに関する検討は十分ではない．そこで本研究では，以下に示す IoT による次世代アプリケーションを想定した際の省電力，リアルタイム性，高信頼性，および高いセキュリティを満たすルーティング，メディアアクセス制御方式および攻撃防御システムについて検討を行う．本研究における具体的な課題と研究目的を以下に示す．

(1) WSNs (Wireless Sensor Networks) は，森林火災検知および橋梁モニタリングといったアプリケーションへの応用が期待されているが，故障端末が発生した際に所望のセンシングエリアをカバーする手法の検討，太陽光などのエナジーハーベスティングを利用して駆動する EH-WSNs での省電力なルーティングおよびメディアアクセス制御が必要である．

(2) IoT を構成するスマートフォン，無線センサ端末，RFID といったデバイスを用いたシステムおよびサービスのセキュリティ・プライバシに関する研究は急務である．具体的には，スマートフォンを利用した安全な認証方式，位置情報検索サービスのプライバシ，SNS におけるセキュリティ， IP 電話における迷惑電話発信者検知，スマートメータにおけるプライバシ保護を目的とした消費電力量制御手法，RPL におけるセキュア・ネットワーク・プロトコル，安全な RFID サプライチェーンの実現を目指す．

３．研究の方法

提案方式の有効性を明らかにするために，理論解析および C/C++，MATLAB，Contiki OS，R 等を用いたシミュレーションを行う．提案方式の理論解析・計算機シミュレーションプログラムの作成などに関しては，本研究課題のサブテーマに密接に関わる研究を行っている研究代表者の研究室に所属する大学院・学部学生と共に研究を推進する．研究成果は速やかに国内研究会や国際会議で発表し，内外の研究者との討論を積極的に行い，研究レベルと内容を充実させ，学術論文誌への投稿を行う．

４．研究成果

(1) 机上のスマート端末間における振動を用いた鍵共有方式（雑誌論文①，学会発表②)

スマートフォンの近距離無線通信技術を用いた電子決済および端末間でのデータ共有アプリケーションにおいて中間者攻撃が問題となっている．通信の安全を保つために Diffie-Hellman の鍵共有が広く用いられているが，中間者攻撃は攻撃者が無線信号を傍受し通信を行う端末と近接していると見せかけることで可能となるため，無線を使用せずに秘密鍵の交換を行う技術が求められている．そこで提案方式では，無線を使用せずにバイブレーション機能を用いて．机の上に存在する複数の端末間での鍵交換方式を提案する．提案方式では秘密鍵の交換を行いたい複数の端末を同一の机の上に置き，端末をランダムなパターンで振動させ，そのときの加速度情報を他の端末で測定することで，各端末が測定した加速度をもとに秘密鍵の生成を行う．Android 端末を用いて実環境での実験を行い．本研究の有効性を示した．

(2) 走行時の加速度情報を用いたスマート自転車鍵の検討（学会発表④)

近距離無線通信および加速度情報を用いたスマート自転車錠の鍵認証システムについての検討を行う．従来の古典的な自転車錠である物理鍵方式は紛失しやすく，またシリンダ錠は鍵長が 4 桁程度で安全性に問題がある．そこで提案方式では，近距離無線通信および加速度情報を計測可能な自転車錠の存在を想定し，自転車に乗車中に錠および，鍵となるユーザのスマートフォンのそれぞれで加速度情報を測定し，得られた加速度情報を元に自転車錠の開閉を行う認証鍵を生成する方式を提案する．実際に自転車に搭乗し，計測した加速度情報を基に提案方式の有効性を示した．

(3) 複数世帯で共有する蓄電池を用いたスマートメータ電力使用量の秘匿化手法（雑誌論文 ②，学会発表⑩)

通信機能を活用してリアルタイムに自動検針 (AMI: Advanced Meter Infrastructure) を行うスマートメータの普及によって，電力消費量の見える化，およびエネルギーの効率化が期待されている．一方，計測した各世帯のリアルタイムな電力使用量から顧客のライフスタイルを推定する NILM (Non-Intrusive Load Monitoring) と呼ばれる手法が提案されているが，プライバシを侵害する可能性が問題となっている．そこで従来，家庭用蓄電池を用いて家電を使用していない時に充電を行い，家電の使用時には充電した蓄電池を使用することによりNILMによるライフスタイルの推定を困難にして，プライバシ保護を行う方式(BLH: Battery-based Load Hiding)が検討されてきた．しかしながら，従来のいずれの方式も１軒に１つの高価な家庭用蓄電池を配置したモデルを想定しており，複数世帯に１つの蓄電池を配置する方式の検討がなされていない．複数世帯に１つの蓄電池を配置方式では，蓄電池の配置コストの低減が期待されるが，同時に各世帯の電気使用料の負担の公平性を維持することが課題となる．そこで本論文では，各世帯の電気使用料の負担の公平性を考慮しつつ，まず 2 世帯の使用電力量を同時に制御して電力使用量を秘匿化する手法を提案する．提案方式では，各世帯の電気使用料の負担額が実際の世帯内での電気使用料から一定額以上逸脱した場合に，差の大きな世帯が優先的に放電を行い，差の小さな世帯は優先的に充電を行うことで世帯間の電気使用料の負担の公平性を実現する．その後，2 世帯以上の複数世帯数に拡張した方式を提案し，実際の電力消費量のデータセットを用いて計算機シミュレーションを行い，本方式の有効性を示した．

(4) グラフ剪定および頑強な代表ノードによる SNS の Sybil ノード検知手法（雑誌論文③，学会発表⑤)

SNS (Social Networking Service) において，スパムを配信する等の行為を行う不正アカウントの検出が急務である．その検出法として，友人数の多いシードと呼ばれる代表アカウントを起点にその友人に信頼値を分配し，信頼値の低い者を不正アカウントとして検知する PI (Power Iteration) 法及び，不正アカウントに流入する信頼値を抑制するため，共通の友人が少ない者同士の友人関係を不正アカウント-正規アカウント間の友人関係と見なして関係を剪定する GP (Graph Pruning) 法が存在する．しかし,PI 法においては，一般に友人数の多いアカウントは同一コミュニティに属す傾向があるため，選択されるシードが偏り，信頼値が均一に分配されない問題がある．また攻撃者が複数の不正アカウントを用いることで共通の友人数を増大し，GP 法における剪定を回避できる問題がある．そこで正規アカウントに対してより均一に信頼値を割り当てるため,SNS 全体に対してコミュニティ検出を行い，検出された各コミュニティの中から友人数の多いアカウントをシードとして選択する方式を提案する.さらに選択したシードを起点に信頼できるアカウントの領域を求めることで複数の不正アカウントを用いた場合に対してもロバストな剪定方式を提案する．これら 2 つの提案により，正規アカウントに分配される信頼値を増大し，不正アカウントに分配される信頼値を低減することを可能とする．実データを用いた特性評価を行い，提案方式は従来方式と比較して各アカウントの正規性をより正確に判別可能であることを示した．

(5) RFID サプライチェーンにおける安全な鍵共有手法（雑誌論文④⑨，学会発表①⑨⑫⑬)

製品識別コード (EPC: Electronic Product Code)を RFID タグに付加することで，サプライチェーンの円滑化が期待されている．しかしながら，商品に付加されたタグが輸送中に攻撃者に読み取られた場合，製造者はそれに気付くことができない．そこで提案方式では，製造者が EPCIS (EPC Information Service) サーバ上でタグが不正に読み取られたことを検知できる方式を提案する．製造者は EPC に乱数を加えた状態で出荷し，その乱数を製造者が管理する EPCIS サーバに配置する．EPCIS サーバ上で正しいアクセスコードを入力できたパーティのみが乱数を得られるような認証システムを構築し，そのアクセスコードを閾値秘密分散法により複数のシェアに分割し，商品のタグに書き込む．さらに偽のシェアが書き込まれたダミーのタグを同梱する．これにより，攻撃者は膨大な数のアクセスコード候補を EPCIS サーバ上で試す必要があり，製造者は攻撃を検知することが可能となる．安全性証明および実装により提案方式の有効性を示した．

(6) RPL ネットワークのセキュア・ルーティングプロトコルの研究（雑誌論文⑥⑧，学会発表⑦⑱)

RPL はツリー構造のルーティング・プロトコルであり，マルチホップ IoT ネットワークの標準プロトコルとして注目されている．しかしながら，RPL ネットワークでは悪意のある中継ノードによって伝送パケットの中断，破棄，改竄といっ

た攻撃を受ける可能性がある．そこでネットワーク上での振舞をスコア化し，それを RPL におけるルーティング先決定に用いるランク値に反映することで悪意のある中継ノードをルーティング対象から除外する方式を提案する．Contiki OS および Cooja によるネットワーク・シミュレーションにより，その有効性を示した．

(7) 準同型暗号を用いた安全な位置情報検索手法（雑誌論文⑤，学会発表⑮）

近年，ユーザの所在地をサーバに明かすことなく，近傍のロケーション（POIs: Points of Interest）を検索する位置情報検索サービスが注目されている．従来，準同型暗号を用いることでユーザの位置をサーバから秘匿し，POI を検索可能な方式が提案されているが，サーバが所有する全ての POI に対して行列演算を行うため，サーバの計算量が増大する問題がある．そこで POI テーブルを分割し，準同型性を用いて統合することで，計算量を低減する POI 検索方式を提案する．特性評価により，提案方式は，従来方式の安全性と検索精度を保ちつつ，サーバの計算量を大幅に削減できることを示した．

(8) IP 電話における迷惑電話発信者検知に関する研究（雑誌論文⑦⑩，学会発表⑧⑳）

近年，格安な通話料金で利用できる IP 電話が普及し始めている．格安で通話が容易になった一方，販売促進および宣伝といった音声スパム（SPIT : SPam over Internet Telephony）の出現が問題視されている．電子メールにおける広告であるスパムの対策においては，受信者がメールを受信する前にサーバ側でメールの内容を確認することでスパムメールを判定することができるが，IP 電話の場合は受話者が実際に電話に出るまで内容を把握することができないため，その通話が音声スパムであるかを判定することが困難である．そこで，発信者の通話の特徴を基に迷惑電話発信者検知する手法を提案し，その有効性を確認した．

(9) WSNs における高伝送効率を達成するデータ転送手法（学会発表③⑪⑭⑯⑰）

EH-WSNs において現在の電力変換技術では，環境電力の変換効率が低く充電レートが低くなるため，低充電レートにおいても高スループットで通信可能な技術が重要である．そこで本論文では低充電レートにおいても高スループットな通信を実現するために，平均充電レートを考慮することで，適応的に中継端末を選択する方式を提案する．本方式は，各 EH 端末が平均充電レートに応じて適応的にスループットの基準を決定する．計算機シミュレーションを用いて，提案方式が従来方式と比較し，現実な環境である低充電レートにおいて，高スループットを実現することを示した．また，EH-WSN を橋梁モニタリング・アプリケーションに応用した際に，高パケット到達率を達成する方式の検討の提案を行い，その有効性を示した．

(10) 火災検知データを優先してシンクに伝達する森林火災検知手法（雑誌論文⑪，学会発表⑲）

無線センサネットワークを用いた森林火災の監視システムが注目されている．従来，通常観測されるデータに対し，火災検知データの優先度を考慮することによりシンクに火災検知を早く伝達する手法が検討されている．しかしながら火災発生時には，複数のノードが火災を検知するため，高優先度の火災検知データが衝突しやすくなる問題がある．そこで本論文では，火災検知直後および焼失寸前のみに高優先度を指定することで，高優先度データの損失率を低減する森林火災監視システムを提案した．提案方式では，高優先度のデータのみを，焼失の可能性の低いノードに伝送することにより，高優先度データがシンクへの到達時間を低減した．計算機シミュレーションを用いた特性評価により，提案方式は，焼失するノードの送受信回数を従来と同程度に保ちつつ，高優先度データの低損失率および高優先度データのシンクまでの到達時間の低減を達成できることを示した．

## 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 11 件）


①. Alisa Arno, Kentaroh Toyoda, Yuji Watanabe, Iwao Sasase and P. Takis Mathiopoulos, “Vibration-based key exchange among multiple smart devices on the desk,” International Journal of Image Processing & Communications, 査読有, Vol.16, No.3-4, pp.1-8, Mar. 2017. DOI: 10.1515/ipc-2016-0009

②. Ryota Negishi, Shuichiro Haruta, Chihiro Inamura, Kentaroh Toyoda, and Iwao Sasase, “Monetary Fair Battery-based Load Hiding Scheme for Multiple Households in Automatic Meter Reading System,” Journal of Telecommunications and Information Technology, 査読有, No. 1, pp.110-119, Apr. 2016. http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-1966cc26-3491-4f6d-96c2-f3e3a2f90c23/c/JTIT_2016_1_Negishi.pdf

③. Shuichiro Haruta, Kentaroh Toyoda and Iwao Sasase, “Trust-based Sybil Nodes Detection with Robust Seed Selection

and Graph Pruning on SNS," IEICE Transactions on Communications, 査読有, Vol.E99-B, No.5, pp.1002-1011, May 2016.
DOI: 10.1587/transcom.2015AMP0004

④. Kentaroh Toyoda and Iwao Sasase, "Illegal interrogation detectable products distribution scheme in RFID-enabled supply chains," IEICE Transactions on Communications, 査読有, Vol. E99-B, No. 4, pp.820-829, Apr. 2016. DOI: 10.1587/transcom.2015ADP0008

⑤. Yasuhito Utsunomiya, Kentaroh Toyoda and Iwao Sasase, "LPCQP: Lightweight private circular query protocol with divided POI-table and somewhat homomorphic encryption for privacy-preserving k-NN search," Journal of Information Processing Information Processing Society of Japan (IPSJ), 査読有, Vol. 24, No.1, pp.109-122, Jan. 2016.
DOI: 10.2197/ipsjjip.24.109

⑥. Kenji Iuchi, Takumi Matsunaga, Kentaroh Toyoda and Iwao Sasase, "Secure Parent Node Selection Scheme in Route Construction to Exclude Attacking Nodes from RPL Network," IEICE Communications Express (ComEX), 査読有, Vol.4, No.11, pp.340-345, Nov. 2015.
DOI: 10.1587/comex.4.340

⑦. Miho Kurata, Kentaroh Toyoda and Iwao Sasase, "Two-stage SPIT detection scheme with betweenness centrality and social trust" IEICE Communications Express (ComEX), 査読有, Vol.4, No.7, pp.239-244, July 2015.
DOI: 10.1587/comex.4.239

⑧. Takumi Matsunaga, Kentaroh Toyoda and Iwao Sasase, "Low false alarm attackers detection in RPL by considering timing inconstancy between the rank measurements," IEICE Communications Express (ComEX), 査読有, Vol.4, No.2, pp.44-49, Feb. 2015.
DOI: 10.1587/comex.4.44

⑨. Ryo Hattori, Kentaroh Toyoda and Iwao Sasase, "Deterministic blocker tag detection scheme by comparing slot status in UHF RFID inventory management system," IEICE Communications Express (ComEX), 査読有, Vol.4, No.1, pp.26-30, Jan. 2015.
DOI: 10.1587/comex.4.26

⑩. Kentaroh Toyoda and Iwao Sasase, "Unsupervised clustering-based SPITters detection scheme," Journal of Information Processing, Information Processing Society of Japan (IPSJ), 査読有, Vol.23, No.1, pp.81-92, Jan. 2015.
DOI: 10.2197/ipsjjip.23.81

⑪. Takuma Koga, Kentaroh Toyoda and Iwao Sasase, "Priority based routing for forest fire monitoring in wireless sensor network," The Journal of Telecommunications and Information Technology (JTIT), 査読有, Vol. 3, pp.90-97, Sep. 2014.
http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-e1668d38-61ba-4cf4-857b-cc06b153506a/JTiT_3_2014_Koga.pdf

〔学会発表〕(計 47 件)

①. Tatsuaki Sato, Kentaroh Toyoda and Iwao Sasase, "Practical Key Distribution Scheme with Less Dummy Tags in RFID-enabled Supply Chains," Asia-Pacific Conference on Communications (APCC), 査読有, Yogjakarta (Indonesia), Aug. 25-27, 2016.

②. Alisa Arno, Kentaroh Toyoda, Yuji Watanabe, and Iwao Sasase, "Vibration-based Key Exchange between Two Smart Devices on the Desk," IEICE Information and Communication Technology Forum (ICTF), 査読有, Patras (Greece), July 6-8, 2016.

③. Yuya Tamura, Kentaroh Toyoda and Iwao Sasase, "Closer destination selection scheme for mobile sink and charger enabled WRSNs," IEEE Consumer Communications and Networking Conference (CCNC), 査読有, pp.132-137, Las Vegas (USA), Jan. 8-11, 2016.

④. Alisa Arno, Kentaroh Toyoda, and Iwao Sasase, "Accelerometer Assisted Authentication Scheme for Smart Bicycle Lock," IEEE World Forum on Internet of Things (WF-IoT), 査読有, Milan (Italy), Dec. 14-16 2015.

⑤. Shuichiro Haruta, Kentaroh Toyoda, and Iwao Sasase, "Trust-based Sybil Nodes Detection with Robust Seed Selection and Graph Pruning on SNS," IEEE Workshop on Information Forensics and Security (WIFS), 査読有, Rome (Italy), Nov.16-19, 2015.

⑥. Takayuki Hirayama, Kentaroh Toyoda, and Iwao Sasase, "Fast Target Link Flooding Attack Detection Scheme by Analyzing Traceroute Packets Flow," IEEE Workshop on Information Forensics and Security (WIFS), 査読有, Rome

(Italy), Nov. 16-19, 2015.

⑦. Kenji Iuchi, Takumi Matsunaga, Kentaroh Toyoda and Iwao Sasase, "Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network," Asia-pacific Conference on Communications (APCC), 査読有, Kyoto (Japan), Oct. 13-16, 2015.

⑧. Miho Kurata, Kentaroh Toyoda, and Iwao Sasase, "Two stage SPIT detection scheme with betweenness centrality and social trust," Asia-pacific Conference on Communications (APCC), 査読有, Kyoto (Japan), Oct. 13-16, 2015.

⑨. Kentaroh Toyoda and Iwao Sasase, "Illegal Interrogation Detectable EPC Distribution Scheme in RFID-enabled Supply Chains," IEEE International Conference on RFID Technology and Applications (RFID-TA), 査読有, Tokyo (Japan), Sep.16-18 2015.

⑩. Chihiro Inamura, Kentaroh Toyoda, and Iwao Sasase, "Monetary Fair Battery-based Load Hiding Scheme for Two Households with One Battery in Automatic Meter Reading System," IEICE Information and Communication Technology Forum (ICTF), 査読有, Manchester (UK), June 2-5, 2015.

⑪. Yu Usami, Kentaroh Toyoda and Iwao Sasase, "Reliable EH-WSN based Bridge Monitoring System by Adjusting Sleep Timing with Beacon Signal," IEICE Information and Communication Technology Forum (ICTF), 査読有, Manchester (UK), June 2-5, 2015.

⑫. Kentaroh Toyoda and Iwao Sasase, "Secure and Fast Missing RFID Tags Identification with Lightweight MAC and Rateless Coding," IEEE International Conference on Communications Workshops), 査読有, London (UK), June 8-12 2015.

⑬. Kentaroh Toyoda and Iwao Sasase, "Secret Sharing Based Unidirectional Key Distribution with Dummy Tags in Gen2v2 RFID-enabled Supply Chains," IEEE International Conference on RFID, 査読有, San Diego (USA), Apr.15-17 2015.

⑭. Takuma Koga, Kentaroh Toyoda and Iwao Sasase, "Adaptive Relay Selection with Energy and Channel Information in Energy Harvesting WSNs," IEEE Consumer Communications and Networking Conference (CCNC), 査読有, Las Vegas, (USA), Jan.9-12 2015.

⑮. Yasuhito Utsunomiya, Kentaroh Toyoda and Iwao Sasase, "LPCQP: Lightweight Private Circular Query Protocol for Privacy-Preserving k-NN Search," IEEE Consumer Communications and Networking Conference (CCNC), 査読有, Las Vegas (USA), Jan.9-12 2015.

⑯. Ryota Negishi, Kentaroh Toyoda and Iwao Sasase, "Opportunistic routing protocol with grid-based relay slot selection in energy harvesting WSNs," Asia and Pacific Conference on Communications (APCC), 査読有, Pattaya (Thailand), Oct,1-3. 2014.

⑰. Aye Mon Htun, Maung Sann Maw and Iwao Sasase, "Reduced complexity on mobile sensor deployment and coverage hole healing by using adaptive threshold distance in hybrid wireless sensor networks," IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE PIMRC), 査読有, Washington D.C. (USA), Sep. 2-5, 2014.

⑱. Takumi Matsunaga, Kentaroh Toyoda and Iwao Sasase, "Low false alarm rate RPL network monitoring system by considering timing inconstancy between the rank measurements," International Symposium on Wireless Communication Systems (ISWCS), 査読有, Barcelona (Spain), Aug.26-29 2014.

⑲. Takuma Koga, Shinichiro Hara, Kentaroh Toyoda and Iwao Sasase, "Priority based routing for forest fire monitoring in wireless sensor network," IEICE Information and Communication Technology Forum (ICTF), 査読有, Poznan (Poland), May 28-30 2014.

⑳. Kentaroh Toyoda, "Unsupervised Clustering-based SPITters Detection Scheme (invited talk)," in IEICE Information and Communication Technology Forum (ICTF), 査読無, Poznan (Poland), May 28-30 2014.

他 27 件

〔その他〕
ホームページ等
http://www.sasase.ics.keio.ac.jp

## ６．研究組織

(1)研究代表者
笹瀬 巌 (SASASE IWAO)
慶應義塾大学・理工学部・教授
研究者番号：00187139

(2)研究分担者
豊田 健太郎 (TOYODA KENTAROH)
慶應義塾大学大学院・理工学研究科・助教
研究者番号： 60723476
平成 27 年度のみ研究分担者