

研究成果報告書

研 究 題 目		国際連携による高信頼の大規模無線 LAN システム に関する研究	実 施 年 度
			H26・27 年度
代 表 研 究 者	所 属	広島大学 大学院工学研究院 情報部門	
	氏 名	中西 透	印
1. 研究の目的・背景 ホスト（コンピュータ）・アクセスポイント（AP）間配線の不要な無線 LAN は、低い導入・運用コスト、設置場所の柔軟性、通信範囲の広域性などの点で優れており、近年、その普及が目覚ましい。この無線 LAN において、AP を複数設置し、その間のマルチホップ通信により通信範囲を拡大することで、従来の屋内利用に加え、屋外でも利用するための研究が現在、盛んにおこなわれている。大規模無線 LAN における、このマルチホップ通信では、中継ノード前後の無線リンク間の干渉電波により発生する通信速度の低下やリンク切断が問題となっており、その対策が不可欠である。 本研究では、DTN（遅延耐性ネットワーク）における「蓄積転送」の手法を採用することで本問題に対処する。すなわち、中継ノードで一旦、転送データを蓄積・保存しておき、次の送信先とのリンクが確立できた時点で、その転送を行う。また、各ノードで保存されるデータを、Web 技術により管理することで、システム内に分散配置されるデータへのアクセスを容易とする。更に、通信状況に応じて、動作する（電源 ON とする）AP を集約し、現時点では不要となる AP を停止することで、省エネルギーを実現する。 本システムでは、データがシステム内の複数のノードに分散配置されることから、データの安全性の実現が重要な課題となる。特に、無線 LAN 環境において機密情報のやりとりが発生するため、送信コンテンツの暗号化が不可欠となるが、想定している蓄積転送では、従来の SSL のようなエンド・エンド間通信路ベースの暗号化が容易でない。そのため、本研究では、受信者の ID や属性を用いてコンテンツ毎に個別に暗号化することで、大量のデータに対する鍵管理の問題を解決しながら、セキュリティを確保する。 本研究は、以上の高信頼・高性能・省エネルギーのセキュアな大規模無線 LAN システムの構築を目的としている。ASEAN の中核であるインドネシアの研究者を含めた国際連携を行うことで、汎用性の高い、適用範囲の広いシステムの構築を目指す。本研究での成果は、日本と同様、通信インフラの整備が不十分なインドネシアでは低コストの広域 LAN としての利用が期待される。			

2. 研究成果及び考察（申請時の計画に対する達成度合を織込む）

本研究の成果および研究実施計画に対する到達度合は以下の通りである。

- 1) AP 構成の最適化 本研究の無線 LAN システムで利用する無線アクセスポイント（AP）構成の最適化を目的として、まず、本システムに採用する高速無線プロトコル IEEE802.11ac について、屋内外、部屋数・フロア数、ホスト数、AP 数といった測定環境を変えながらスループット測定を行い、そのモデル化を行った。また、11ac で採用されている高速化技術のモデル化を行い、本グループで開発しているシミュレータに組み込んだ。それらの結果を元に、従来研究で提案している AP 配置アルゴリズム、動作 AP 選択アルゴリズム、経路アルゴリズムの拡張を行い、シミュレータを用いたシミュレーションで評価してきた。現在、これらのアルゴリズムを実際のネットワーク環境で実行可能とするシステムの開発を進めており、Linux-PC を用いたプロトタイプの実装を終えている。
- 2) データ管理の最適化 本研究のデータ管理システムとして、扱う全データの一括管理・バックアップと、停電などによる通信リンク切断時の必要データへのアクセス性を実現するため、全データの管理を行うインデックスサーバと、セクション毎に必要なデータのみを管理するセクションサーバの 2 階層で構成し、それぞれを Web サーバ化することでユーザからのアクセス性を向上することとした。その際、ハイブリッド型ピアツーピアネットワークのコンテンツ配置手法を応用することで、セクションサーバにおける必要データのコピー、不要データの除去の自動化・最適化を実現する。これにより、ユーザからのアクセスの高速化を実現する。現在、本システムの開発を進めている。
- 3) コンテンツの暗号化 DTN では鍵サーバへデータ受信時に安定してアクセスできないため、各ユーザに事前に鍵が配布されているモデルが必要となる。そこで本研究では、属性毎に鍵を付与でき、属性に基づいて復号ユーザグループを指定可能な属性ベース暗号（ABE）を採用して、コンテンツを暗号化するデータ共有システムの構築を行なった。また、中継ノードの不正に対応するため、通信経路を決定するために必要なルーティング情報も ABE を用いて暗号化している。初年度において、プロトタイプ実装として、3 ノードにおいて Linux-PC 上で実装を行ない、国際会議 CANDAR2014 で発表した。また、次年度においては、マルチホップでの検証を行なうために、4 ノードで動作するように拡張して実装を行ない、国際会議 CANDAR2015 で発表している。マルチホップでのセキュア通信は実現できているが、Web ベースシステムでの実装や蓄積転送管理システムとの統合は今後の課題である。

3. 経費の使用状況（申請時の計画に対する実績を記述）

交付申請時の計画通りに下記のように経費を使用している。

最新の研究成果を調査するため、消耗品として、主要な国際会議(PKC,EUROCRYPT)などの論文集を購入した。また、マルチホップネットワークにおけるセキュリティの状況についてサーベイするための研究資料も購入している。

国内で開催された研究集会として、国際会議 ASIACCS, 電子情報通信学会ソサイエティ大会・総合大会, 情報処理学会全国大会, コンピュータセキュリティシンポジウムに参加し、セキュリティ, 暗号, ネットワークの最新研究について調査を行ない, その旅費および参加費に経費を使用した。また, 共同研究者間や関連研究者との研究打合せを行ない, その旅費に経費を使用した。

研究成果発表として, 国際会議 CANDAR2014 および CANDAR2015 のワークショップにおいて論文が採録されており, その発表のため, 旅費および参加費に経費を使用した。また, 国内研究会においても成果発表を行ない, その旅費に経費を使用した。

4. 将来展望（今後の発展性、実用化の見込み等について記述）

まず, AP 構成の最適化については, 本研究で提案したアルゴリズムをオンラインで実行し, その結果を AP およびホストにフィードバックする実機システムの実装を行っていく。現在, Linux-PC を用いたプロトタイプの実装を終えており, それを用いた評価実験を実施する。また, この実装でボトルネックとなるホストの操作権限の管理サーバへの委譲を緩めるための種々の改善を図る。更には, ホストとして, Windows-PC も利用可能とするための拡張も行う。

次に, データ管理の最適化については, 上述の実機システムへの実装を進める。まず, 本システムで管理・保存可能なデータ量に制限があることから, 管理すべきデータの区別を行い, それらへのインデックス付与方法についての検討を行い, 実装を行う。また, サーバにおける必要データのコピーおよび不要データの除去機能の実装を行う。その上で, 実機システムを用いた評価実験を行う。更には, 本システムの利用環境やマニュアル類の整備を行い, インドネシアを含む, 様々な場所での利用を可能としていく予定である。

DTN のセキュリティについては, IoT におけるセキュリティの重要性が高まっており, 今後もホットな研究分野であると考えられる。モバイル分散環境においては, 各ノードの信頼性が高くないためデータの秘匿性・完全性の確保が不可欠であるが, DTN 環境ではエンド・エンド間での通信を確保できないため, 本研究の属性ベース暗号・認証の必要性は高い。現在はコンテンツデータとルーティング情報の暗号化を行なっているが, ノード間認証や DOS 攻撃への対策も必要であり, 今後の課題と考えている。

5. 成果の発表（学会での発表、学術誌への投稿等を記載。予定を含む）

学術雑誌：

[1] Chang Choon Chew, Nobuo Funabiki, Wataru Maruyama, and Sho Fujita, "An extended active access-point selection algorithm for link speed changes in wireless mesh networks," International Journal Space-Based and Situated Computing, vol. 4, nos. 3/4, pp. 184-193, November 2014.

査読付き国際会議：

[2] Amang Sudarsono, Toru Nakanishi, "An Implementation of Secure Data Exchange in Wireless Delay Tolerant Network Using Attribute-Based Encryption," CANDAR WICS 2014: (First International Workshop on Information and Communication Security), pp.536-542, 2014.

[3] Chang Choon Chew, Nobuo Funabiki, Sho Fujita, "Extensions of Active Access-Point Selection Algorithm for Wireless Mesh Networks Using IEEE802.11ac Protocol," CANDAR PDAA 2014: (Sixth International Workshop on Parallel and Distributed Algorithms and Applications), pp.310-314, 2014.

[4] Nobuo Funabiki, Yuuma Tani, Shigeto Tajima, "A Frame Aggregation Extension of Routing Algorithm for Wireless Mesh Networks," CANDAR ASON 2014: (Seventh International Workshop on Autonomous Self-Organizing Networks), pp.238-242, 2014.

[5] Amang Sudarsono, Toru Nakanishi, "An Implementation of Secure Data Exchange System with Multi-hop Routing in Wireless Delay Tolerant Network Using Attribute-Based Encryption," CANDAR WICS 2015: (Second International Workshop on Information, Communication Security), pp.470-476, 2015.

[6] Md. Selim Al Mamun, Md. Ezharul Islam, Nobuo Funabiki, I.-Wei Lai, "Active Access-Point Configuration Algorithm with Dynamic Mobile Router Placement for Elastic WLAN System," CANDAR ASON 2015: (Eighth International Workshop on Autonomous Self-Organizing Networks), pp. 246-252, 2015.

国内研究会：

[7] 藤田 翔, 舩曳信生, "大規模無線メッシュネットワークのための動作アクセスポイント選択アルゴリズム," 電子情報通信学会 NS 研究会, NS2014-250, pp.427-432, 2015.

[8] 青柳有輝, 舩曳信生, 福士 将, "ユーザ PC コンピューティングシステムのジョブスケジューリング法の実装と評価," 電子情報通信学会 NS 研究会, NS2014-271, pp.553-558, 2015.