様式3

論 文 内 容 の 要 旨

氏 名 （ 北 健太朗 ）	
論文題名	Anonymity and Privacy in Named Data Networking based on Onion Routing and K-anonymity （ 名前ベースネットワーキングにおけるオニオンルーティングとK-匿名性にもとづく匿名性とプライバシー）

論文内容の要旨

効率的なコンテンツ配布の実現する新たなネットワークアーキテクチャとして、名前ベースネットワーキング(NDN)が提案されている。一方、NDNの課題として、十分な強度の匿名性とプライバシーが提供されないことが挙げられる。これは、各コンテンツに割り当てられるコンテンツ名がプロデューサの識別子であるプロデューサ名とコンテンツの種類を示すコンテンツIDを含み、かつ、各コンテンツにプロデューサの署名が付与されるというNDNの特徴によるものである。近年、政府や企業による個人情報の収集が深刻な脅威となっており、この課題はNDNの普及を妨げる要因の一つである。本稿では、コンテンツ名と署名からの情報漏洩を防ぐことで、NDNにおいて匿名性とプライバシーを提供するシステムをそれぞれ設計する。まず、本稿の前半では、プロデューサが複数個の匿名化ルータを経由することで、身元を隠蔽しつつコンテンツを提供することを可能にする、匿名化システムを設計する。この設計方針は既存の秘匿サービスに基づくものであるが、設計システムではさらに、NDNのパケットが送信元の情報を持たないことを利用し、プロデューサの身元を、隣接する匿名化ルータからも隠蔽する。これにより、秘匿サービスと同等の匿名性を一つ少ない匿名化ルータで達成でき、コンテンツ提供にかかる通信遅延を削減できる。次に、本稿の後半では、コンシューマが各地のInternet-of-Things(IoT)デバイスが収集したデータを検索する際に、コンシューマの興味のある位置をK-匿名性により隠蔽する、位置プライバシー保護システムを設計する。K-匿名性に関する既存研究では、オネストなアノニマイザがコンシューマの興味のある位置を含むK個の位置からなる匿名位置集合を生成し、そこに含まれる全位置のコンテンツを検索することで、興味のある位置を第三者から隠蔽するシステムが提案されている。設計システムはこのような既存システムに対して以下の優位性がある。第一に、興味のある位置に関する情報漏洩を最小化するために匿名位置集合が満たすべき要件をK-匿名性とT-近傍性を用いて定義した点、第二に、既存システムのアノニマイザがオネストであるのに対して、本システムはセミオネストなアノニマイザに対するプライバシーを達成する点である。したがって、本システムはより現実的なシナリオに対して強力な位置プライバシーを提供できる。以上のように、本研究はNDNの課題であった匿名性とプライバシーの不足に対する解法を示すものであり、NDNの一層の普及に貢献するものと考えられる。

様式 7

論文審査の結果の要旨及び担当者

氏　名　（　北　健太朗　）		
	（職）	氏　名
論文審査担当者		
主 査	教授	長谷川　亨
副 査	教授	村田　正幸
副 査	教授	山口　弘純
副 査	教授	下西　英之
副 査	教授	渡辺　尚

論文審査の結果の要旨

Named Data Networking(NDN)は，次世代インターネットアーキテクチャの一つであり，従来の提供できなかったマルチキャスト，移動，キャッシュを提供する有用なアーキテクチャである．ただし，NDNでは宛先として，データの名前を用いるため，宛先の名前からプライバシーが漏洩する脆弱性が課題となっている．

本博士論文では，この脆弱性に対して，NDN網において，データを提供するプロデューサ，およびデータを要求するコンシューマのプライバシーを保護する手法を提案している．提案と貢献は以下の通りである．

第一に，プロデューサのプライバシー保護に対して，IPで受信者匿名性を提供するTorの秘匿サービスをベースに，プロデューサ匿名性を提供するプロトコルを設計した．本プロトコルの設計における理論面と実践面の貢献は以下の通りである．まず，理論面では，プロデューサ匿名性をコンフィギュレーションの概念を用いて厳密に定義し，設計したプロトコルがプロデューサ匿名性を満たすことを証明している．IPの受信者匿名性と異なるプロデューサ匿名性を定義した点が画期的である．次に，実践面では，プロトコルを詳細に設計，実装して性能を評価するとともに，攻撃に対する耐性について，IPの秘匿サービスと評価し，その優位性を明らかにした．まず，IPの秘匿サービスでは，最低でも3台の匿名ルータを経由する必要があるのに対して，本プロトコルでは2台の匿名ルータを経由するだけでよく、通信遅延を削減している．次に，プロデューサから1ホップ目のルータが乗っ取られると，プロデューサ匿名性も受信者匿名性も破られる脆弱性があるのに対して，双方のプロトコルで乗っ取られる確率を評価した．この結果，第1ホップに匿名ルータでなく，IPルータを用いる本プロトコルが乗っ取られる確率が低く，攻撃耐性が高いことを明らかにした．

第二に，コンシューマのプライバシー保護に対しては，コンシューマが目的位置のデータを取得する位置ベースサービスを対象として，コンシューマが要求したデータの目的位置の匿名性を提供するプロトコルを設計した．本プロトコル設計における理論面と実践面の貢献は以下の通りである．まず，理論面では，目的位置のプライバシーを，K匿名性とT近似性を用いて目的位置匿名性を厳密に定義した．実践面では，実用的な位置ベースサービスを想定して，位置サービスで提供される全体の位置から，目的位置匿名性を満たす位置の集合を求めるアルゴリズムを設計した．さらに，コンシューマ匿名性を満たすアノニマイザを導入し，アノニマイザが提供するコンシューマ匿名性と組み合わせることで，NDN網で目的位置匿名性を提供するプロトコルを設計した．設計したプロトコルを実際の都市のデータをベースにシミュレーションで評価することで，定義した目的位置匿名性を提供できることを明らかにした．

本博士論文で取り扱う技術は，NDNなどの次世代インターネットだけでなく，現在のIPにおけるプライバシー漏洩という本質的な課題に挑戦するものである．本博士論文では，コンシューマとプロデューサ，すなわち情報にアクセスするユーザと，情報を提供するユーザと情報を紐づけらないようにする手法を提案し，NDN網において課題を解決している．今後，NDNの普及を妨げるプライバシー漏洩に対して，一つの解を示したことで，NDNの普及に貢献することが期待できる．さらに，提案した手法は，現在のIPベースのインターネットにも応用可能である，インターネットにおけるプライバシー向上に対して，基礎的な成果を出している．以上のような理由から，本論文は博士（情報科学）の学位論文として価値のあるものと認める．