様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　５月１１日現在

機関番号：１１３０１
研究種目：研究活動スタート支援
研究期間：2011～2012
課題番号：23800005
研究課題名（和文）通信の安全性と品質を統合制御可能なセキュリティ技術に関する研究

研究課題名（英文）Combined Control of Quality of Service and Security in Wireless Networks

研究代表者
ファドゥルラ ズバイル　（FADLULLAH ZUBAIR）
東北大学・大学院情報科学研究科・助教
研究者番号：40614011

研究成果の概要（和文）：近年，インターネットが普及する中，無線ネットワークやマルチメディア通信などにおいて通信品質を保証することが大変重要になってきている．一方，ネットワークが複雑化するにつれて，通信の安全性を保証することも求められている．しかしながら，これら２つを同時に達成することは困難が多い．そこで本研究では，通信品質制御及びセキュリティ制御の各パラメータを適切に調節するための仕組みを考案し，アプリケーションが求める性能を実現するための技術を確立した．

研究成果の概要（英文）：Recently, development of wireless network and multimedia communications have led to increasing importance of ensuring guaranteed Quality of Service (QoS). On the other hand, high security is required as the network systems get more complex. However, it is difficult to fill these requirements together. Therefore, in this research, we proposed a system to adjust the parameters to control QoS and security in the networks.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2011 年度	1,000,000	300,000	1,300,000
2012 年度	900,000	270,000	1,170,000
年度			
年度			
年度			
総　計	1,900,000	570,000	2,470,000

研究分野：工学
科研費の分科・細目：計算機システム・ネットワーク
キーワード：ネットワーク，QoS，セキュリティ，

１．研究開始当初の背景

近年のインターネットの爆発的な普及に伴い、通信における通信品質（QoS：Quality of Service）保証とセキュリティ向上の両立が求められている。例えば IEEE802.11 で規定される無線アドホックネットワークなどでは、ユーザが要求するセキュリティレベルと通信遅延の保証がなされている。この規格では、ユーザが要求するセキュリティレベルを保証する暗号鍵長を利用しつつ通信遅延を最小化している。これによって、ネットワーク負荷を調整しつつ遅延とセキュリティのバランスを制御している。しなしながら、未だいくつかの問題点も存在する。特に、帯域を過剰に消費させることでユーザの許容出来る遅延性能を満たしつつ保証できるセキュリティレベルを低減させる攻撃は非常

に大きな問題となっている。この攻撃はセキュリティレベルが低く攻撃がより効果的になるようなタイミングにおいて実行される。既存の研究においても、通信遅延の変化に合わせて暗号鍵長を動的に調節することの重要性が挙げられている。例えば、無線ローカルエリアネットワーク(WLAN:Wireless Local Area Network) 環境における各レイヤーのセキュリティの特徴を統合することで、認証時間や暗号化のオーバヘッド、スループットなどを考慮したシステムモデルを提案しているものが挙げられる。しかしこの研究では、無線のホストと通信中のアクセスポイント間の暗号化プロトコルのみしか考慮しておらず、有線と無線の両方から構成されるネットワークにおけるエンドツーエンドでの暗号化通信を考慮していない。このような問題は近年注目を集めている無線アドホックネットワークや４G ネットワークなどにおいて大きく注目を集めている。そこで本研究では、高いセキュリティを保証しつつエンドツーエンド通信における QoS を考慮したシステムモデルの構築を行う。

２．研究の目的

近年の著しいネットワーク技術の進歩やリアルタイム性を要求するアプリケーションの台頭によって、今後様々な QoS 要求を持ち、異なるセキュリティレベルが必要とされるような通信が必要とされると考えられる。これまでの研究では、QoS 保証とセキュリティ向上についてはそれぞれ別々に取り上げられてきた。そのため、QoS 保証に関する通信制御がその通信におけるセキュリティにどのような影響を与えるか、また同様にセキュリティ制御が通信品質に与える影響について、早急に検討を行う必要がある。例えば、WLAN や WiMax (Worldwide Interoperability for Microwave Access) 上においてユーザが VoIP (Voice over IP) 通信を利用する際、可能な限り通信遅延を小さくする必要がある。この時同時に、ユーザは暗号鍵長を長くしたり、より強固な暗号プロトコルを利用したりするなど、より高いセキュリティレベルを要求する。このように QoS 要求とセキュリティ要求が混在するような環境において、暗号化アルゴリズムや暗号鍵長はエンドツーエンドの遅延に対してどのような影響を与えるのか、ジッターやスループット、パケット損失などのパラメータに対してはどのような影響があるのか、ユーザ間の公平性については影響があるのかなど、検討すべき課題は多数存在する。そこで本研究では、これらの関係性について調査、検討を行い、効率的に QoS の保証とセキュリティの向上を実現するためのシステムモデルを開発することを目的とした。

３．研究の方法

本研究では、近年利用者が急増している WLAN 環境において固定端末やモバイル端末が通信を行うような環境を想定し、システムの開発、評価を行った。システム開発の第一段階としては、QoS 保証に関するパラメータのそれぞれがどのようにしてネットワークにおけるセキュリティに影響を与えるのか調査した。また、この調査に基づき、通信における QoS 保証とセキュリティの関係性について、Quality of Security Services (QoSS) としてモデル化を行った。そして、このモデルを基に新たなネットワークモデル構築のための課題の明確化を行った。次にシステム開発の第二段階として、この課題を解決するためにゲーム理論を用いて QoS を考慮しつつセキュリティを確保するための技術を提案した。

また、提案手法を評価するため提案アルゴリズムの安定性や動作性能について解析を行った。この解析ではまず始めに数学モデルや数値計算などによる評価を行い、設計に問題がないかを確認した。次に、詳細なシミュレーション実験によって提案技術を評価することによって、提案技術の有効性を客観的に示した。以上に示した一連の作業，つまりアルゴリズムの考案，パラメータの調節，ネットワークシミュレータによる実験と性能評価を繰り返し行うことにより，提案システムを完成させた.

４．研究成果

本研究では、初年度である平成２３年度に通信における QoS 保証とセキュリティの関係性について調査するため QoSS のモデル構築を行った。更に平成２４年度にはこの QoSS モデルを基に、ゲーム理論を用いてユーザの QoS を考慮しつつセキュリティを確保するための技術を提案した。以下ではこれらの成果の概要について述べ、その評価を行った結果について紹介する。

(1)QoSS モデルの概要

本研究では IEEE802.11 WLAN 環境における新たな QoSS モデルの構築を行った。まずこの QoSS モデルの概要について説明する。この QoSS モデルでは、WLAN の各アクセスポイントがユーザから要求される QoS やセキュリティに合わせて必要なネットワークパラメータの設定を行う。この時、スループットやエンドツーエンド遅延、帯域利用率、公平性、エラー率などの QoS パラメータに関する要求

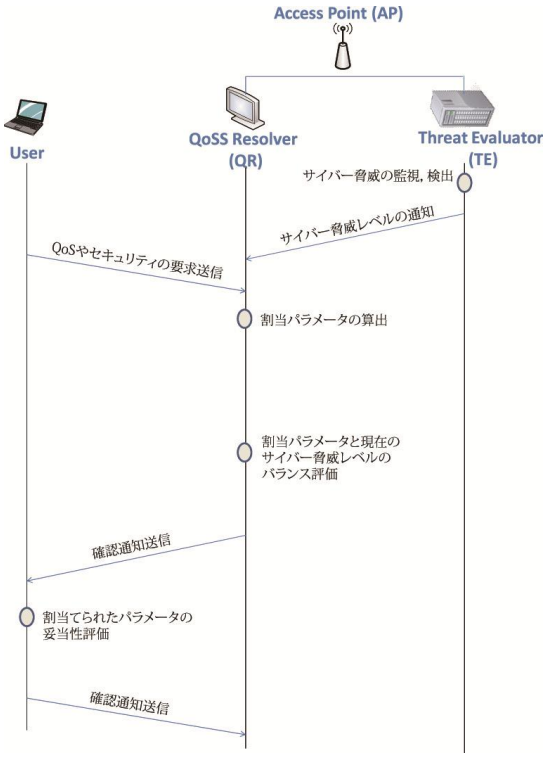

図 1: ユーザーアクセスポイント間の
通信の流れ

を満たしつつ、ユーザ毎に要求されるセキュリティレベルの考慮することによって適切なパラメータの設定を行う。更に、ユーザのネットワークに対する経験度に合わせて設定を容易に行えるよう、設定可能なセキュリティレベルを次のように規定する。まず、ネットワークに不慣れなユーザに対しては、高、中、低、なしの４つの選択肢からセキュリティレベルを選択させる。一方ネットワークに対する知識の豊富なユーザに対しては、セキュリティプロトコルや暗号化方式、暗号鍵長、アクセス制御の許容度、否認不可レベルなどの選択機会を与える。

次に、この QoSS モデルを想定するネットワーク環境において実行するためのシステム構成について説明する。図１は想定ネットワークにおいてユーザとアクセスポイント間で QoS やセキュリティに関する要求についての決定を行うための通信を行なっていく流れの例を示したものである。図に示すように、アクセスポイントは“QoSS Resolver（QR）”と“Threat Evaluator（TE）”の２つの構成要素から成る。QR は各ユーザの特徴に合わせ QoS とセキュリティのバランスを調節するためのものである。一方、TE はネットワークにおけるサイバー脅威を監視、検出し、その脅威レベルを評価する役割を果たす。評価の結果は定期的に QR に対して通知する。QR はユーザからの QoS やセキュリティに関する要求を受け取った際、TE から通知される脅威レベルを考慮しつつ要求があったユーザに対して QoS とセキュリティレベルのバランスを調整して応答を行う。ユーザは与えられた QoS やセキュリティレベルが十分であるか検証し、確認通知を QR に対して送信する。このようにしてユーザとアクセスポイント間で通信を行うことで、各ユーザの QoS やセキュリティレベルの決定が行われる。

(2)提案技術の概要

本稿では、前述した QoSS モデルにおける各ユーザに対して最適な QoS やセキュリティに関するパラメータの割り当てを行うことを目的として、ゲーム理論を用いた技術の提案を行う。なお、用いられるゲーム理論において、ユーザは“プレーヤー”と呼称され、アクセスポイントに接続する全プレーヤーに対して最適な QoS とセキュリティのパラメータを割り当てるために“非協力ゲーム”が実行されるものとする。このゲームでは、各プレーヤーは自身の要求をアクセスポイントに送信し、アクセスポイントは各プレーヤーの要求を基にゲーム理論を用いて戦略的な解を与える。各プレーヤーに与えられた解は互いの要求に対して影響を与え合うものであり、また、新たなプレーヤーが新たにシステムに参加した場合も、そのプレーヤーの要求に従って各ユーザはその戦略を変更し、最適な解を導出するように行動する。この結果、各プレーヤーの解は“ナッシュ均衡”と呼ばれる安定状態に至る。この状態では、どのプレーヤーも自身の戦略を変更することによってより高い利得を得ることができないことが示されている。つまり、このナッシュ均衡に至った状態が各プレーヤーに対して最適な状態であると言え、適切な QoS やセキュリティのパラメータを与えることが可能となっている。

(3)提案技術の評価

ここではコンピュータシミュレーションを用いて行った提案技術の評価結果について述べる。なお、シミュレータには MATLAB を利用した。

① 想定環境

シミュレーションの想定環境として、WLAN 環境においてアクセスポイントが１つあり、そのアクセスポイント下でユーザが２～５人が動的に存在するものとする。また、ネットワークを流れるトラヒックの種類として、ベストエフォート型、音声データ、動画デー

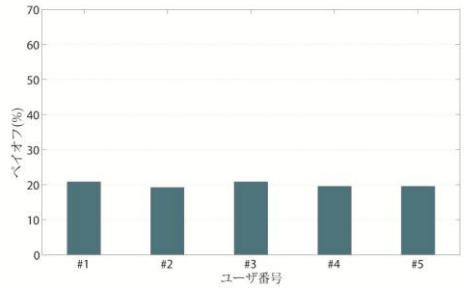

図 2: 各ユーザが得られたペイオフ

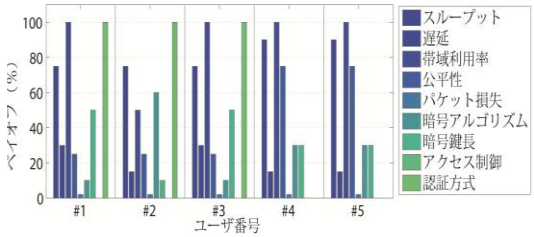

図 3: 各パラメータのペイオフ

タの３種類を想定する。ユーザが選択可能な QoS パラメータとしてはスループット、エンドツーエンド遅延、帯域利用率、公平性、パケット損失の５つ、セキュリティに関するパラメータとしては暗号化アルゴリズム、暗号鍵長、アクセス制御レベル、認証方式の４つを想定する。なお、シミュレーションの試行回数は１００回とし、その平均結果を算出した。

② 実験結果

図２は想定環境において５人のユーザが通信を行い、ゲーム理論を用いた提案技術を利用しナッシュ均衡に至った状態で得られたペイオフを示したものである。結果より、各ユーザはほぼ等しく約２０％のペイオフが得られていることが確認された。これは、提案技術を用いることで各ユーザの QoS やセキュリティに対する要求に対して等しくその要求を満たすことができたことを示している。この結果について、QoS やセキュリティに関するパラメータについて更に詳しく解析を行った結果が図３である。図３より、各ユーザは平等に要求に対して約７０％のスループットを得られていることが分かる。また、遅延に関しては、ユーザ１が約３０％と最も高い結果が得られているが、これは、他ユーザの遅延以外の QoS やセキュリティに関するパラメータとのバランスが考慮されたことによって得られたものである。一方、セキュリティに関しては、ユーザ１，２，３，はそれぞれ要求した認証方式を用いた通信を得ることができたのに対して、ユーザ４、５からは要求がなかったため認証方式を用いた通信は与えられなかったことが分かる。また、ユーザ２が最も強固な暗号化アルゴリズムを与えられていることが確認できる。それぞれの結果より、各ユーザはそれぞれの要求に見合ったセキュリティ方式を利用可能であったことが分かる。また、想定環境において異なる人数のユーザが通信を行った場合、ナッシュ均衡に到達するまでにどれくらいの時間がかかるかについての調査も行った。ユーザが２人の場合、約１０ｍｓであり、ユーザが４人の場合でも収束までの時間は１００ｍｓ以下を保つことができた。一方、ユーザ数が６人、７人、と増加していくと、その必要時間は８００ｍｓ、５ｓとなり、ユーザが１０人の場合は３００ｓとなった。このようにユーザ数が増加するに従ってナッシュ均衡が得られるまでの時間は増加していくが、ユーザから要求される QoS やセキュリティに関するパラメータを適切に制御するためには許容可能な時間であると考えられる。これらの結果より、本提案技術の有効性を確認することができた。

５．主な発表論文等

〔学会発表〕（計１件）

Zubair Md. Fadlullah1, Athanasios V. Vasilakos, Nei Kato, “A Game Theoretic Approach to Integrate Security with Quality of Service” IEEE International Conference on Communications (ICC 2012), 12th, Jun. 2012, Ottawa, Canada.

６．研究組織

(1)研究代表者
ファドゥルラ ズバイル（FADLULLAH ZUBAIR）
東北大学・大学院情報科学研究科・助教
研究者番号：40614011

(2)研究分担者
なし

(3)連携研究者
なし