(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2010-536221
(P2010-536221A)
(43)公表日　平成22年11月25日(2010.11.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 29/06	(2006.01)	H04L	13/00	305A	5K030
H04L 12/56	(2006.01)	H04L	12/56	A	5K034

審査請求 有　予備審査請求 未請求　（全 18 頁）

(21)出願番号　特願2010-519844 (P2010-519844)
(86)(22)出願日　平成19年9月14日 (2007.9.14)
(85)翻訳文提出日　平成22年2月26日 (2010.2.26)
(86)国際出願番号　PCT/KR2007/004440
(87)国際公開番号　WO2009/020255
(87)国際公開日　平成21年2月12日 (2009.2.12)
(31)優先権主張番号　10-2007-0079637
(32)優先日　平成19年8月8日 (2007.8.8)
(33)優先権主張国　韓国 (KR)

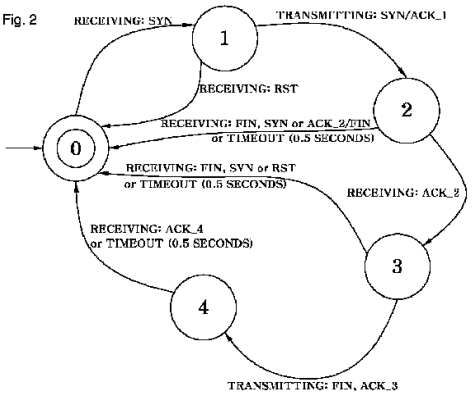
(71)出願人　509103808
サムスン　エスディーエス　シーオー．エルティディ．
大韓民国　１３５－９１８　ソウル　ガンナング　ヨクサム　２ドン　７０７－１９　イロク・ビルディング
(74)代理人　100082072
弁理士　清原　義博
(72)発明者　ヨー，イン　セオン
大韓民国　４６３－８１０　京幾道　セオングナム－シ　ブンダング－グ　グミ－ドング　１８７－２　セジョング・グランシア　１／７３１

Fターム(参考)　5K030 GA13 GA15 HC09 JT09 LB01 LC16

最終頁に続く

(54)【発明の名称】モバイルデバイスに対するＴＣＰベースのサービス拒否攻撃の遮断方法

(57)【要約】
モバイルデバイスに対するＴＣＰ（Transmission Control Protocol）ベースのサービス拒否（Denial of Service;DoS）攻撃の遮断方法が提供される。無線上でＴＣＰプロトコルを利用してモバイルデバイスに絶え間なくＴＣＰパケットを伝送し、無線ネットワークのリソース及びバッテリーに依存するモバイルデバイスのバッテリー電源を浪費するモバイルデバイスに対するサービス拒否攻撃を本発明は効果的に遮断する。ＴＣＰベースのスリーウェイハンドシェーキング（Three-way handshaking）を悪用して有線ネットワークで行われる従来の攻撃は、モバイルデバイスの有線ネットワークにおいてさらに致命的である。このようなモバイルデバイスに対する攻撃を遮断するために、スリーウェイハンドシェーキング及び各々の遷移動作を確認することができる方法により、モバイルデバイスは、受信されるＴＣＰパケットが有効であるか否かを確認することができる。したがって、ＤｏＳ攻撃が無線リソース及びモバイルデバイスのバッテリー電源を消耗することを効果的に防止することができる。



【特許請求の範囲】
【請求項１】
ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法であって、
前記方法は、
前記基地局が前記モバイルデバイスにＴＣＰ接続のための接続要求ＳＹＮパケットを伝送した後、前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記モバイルデバイス側で接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送する段階と、
前記伝送された接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットが受信されると、前記基地局側で前記接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットに対応する確認応答ＡＣＫ＿２パケットを前記モバイルデバイスに伝送する段階と、
前記モバイルデバイスが前記伝送された確認応答ＡＣＫ＿２パケットを受信すると、前記ＴＣＰ接続を完了する段階と、
前記ＴＣＰ接続が完了した後、前記モバイルデバイスが前記基地局からリセットＲＳＴまたは接続要求ＳＹＮフラグが設定されたパケットを受信すると、前記完了したＴＣＰ接続を終了する段階を含むサービス拒否攻撃の遮断方法。
【請求項２】
前記ＴＣＰ接続が完了した後、前記モバイルデバイスがあらかじめ設定されたタイムアウト期間に何らかのパケットを受信しなければ、前記基地局により前記ＴＣＰ接続を不正に終了したものと決定され、前記モバイルデバイスは、前記ＴＣＰ接続を安全に終了させることを特徴とする請求項１に記載のサービス拒否攻撃の遮断方法。
【請求項３】
前記タイムアウト期間は、０．５秒に設定されることを特徴とする請求項２に記載のサービス拒否攻撃の遮断方法。
【請求項４】
ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法であって、
前記方法は、
前記基地局が前記モバイルデバイスにＴＣＰ接続のための接続要求ＳＹＮパケットを伝送した後、前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記モバイルデバイス側で接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送する段階と、
前記基地局側で、前記伝送された接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを受信した後、終了ＦＩＮパケットを前記モバイルデバイスに伝送する段階と、
前記モバイルデバイスが前記伝送された終了ＦＩＮパケットを受信すると、前記ＴＣＰ接続を終了する段階を含むサービス拒否攻撃の遮断方法。
【請求項５】
ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法であって、
前記方法は、
前記基地局が前記モバイルデバイスにＴＣＰ接続のための接続要求ＳＹＮパケットを伝送した後、前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記モバイルデバイス側で接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送する段階と、
前記基地局側で前記伝送された接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを受信した後、前記接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットに対応する確認応答ＡＣＫ＿２フ

ラグ及びＦＩＮフラグが設定された確認応答終了ＡＣＫ＿２／ＦＩＮパケットを前記モバイルデバイスに伝送する段階と、
前記モバイルデバイスが前記伝送された確認応答終了ＡＣＫ＿２／ＦＩＮパケットを受信すると、前記ＴＣＰ接続を終了する段階を含むサービス拒否攻撃の遮断方法。
【請求項６】
ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法であって、
前記方法は、
前記基地局が前記モバイルデバイスにＴＣＰ接続のための接続要求ＳＹＮパケットを伝送した後、前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記モバイルデバイス側で接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送する段階と、
前記基地局側で前記伝送された接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを受信した後、前記接続要求ＳＹＮパケットを前記モバイルデバイスに伝送する段階と、
前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記ＴＣＰ接続を終了する段階を含むサービス拒否攻撃の遮断方法。
【請求項７】
前記モバイルデバイスが前記接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送した後、あらかじめ設定されたタイムアウト期間に何らかのパケットを受信しなければ、前記基地局により前記ＴＣＰ接続を不正に終了したものと決定し、前記モバイルデバイスは、前記ＴＣＰ接続を安全に終了させることを特徴とする請求項４乃至６のいずれかに記載のサービス拒否攻撃の遮断方法。
【請求項８】
前記タイムアウト期間は、０．５秒に設定されることを特徴とする請求項７に記載のサービス拒否攻撃の遮断方法。
【請求項９】
ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法であって、
前記方法は、
ＴＣＰ接続が前記基地局と前記モバイルデバイスとの間に完了後に、前記モバイルデバイスが前記基地局にＴＣＰ接続を正常に終了するための終了／確認応答ＳＹＮ／ＡＣＫパケットを伝送した後、あらかじめ設定されたタイムアウト期間に前記基地局から確認応答ＡＣＫ＿３パケットを受信しなければ、前記ＴＣＰ接続を安全に終了させる段階を含むサービス拒否攻撃の遮断方法。
【請求項１０】
前記タイムアウト期間は、０．５秒に設定されることを特徴とする請求項９に記載のサービス拒否攻撃の遮断方法。
【請求項１１】
コンピュータで読み取り可能な記録媒体であって、請求項１乃至１０のいずれかに記載の方法を実行するためのプログラムが記録されていることを特徴とする記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、モバイルデバイスに対するＴＣＰベースのサービス拒否攻撃の遮断方法に関する。より詳細には、無線上でＴＣＰプロトコルを利用してモバイルデバイス側に絶え間なくＴＣＰパケットを伝送し、無線ネットワーク上のリソースを消費しつつ、バッテリーに依存するモバイルデバイスのバッテリー電源を消耗させるサービス拒否（Denial of Service；ＤｏＳ）攻撃に対して効果的に防御することができるようにしたモバイルデバイス

に対するＴＣＰベースのサービス拒否攻撃の遮断方法に関する。
【背景技術】
【０００２】
一般的に、インターネットサービスは有線サービスから無線サービスに拡大され、モバイルデバイスの形態及びサービスが多様化している。それに伴い、ユーザはどこでもモバイルデバイスを通じてインターネットサービスにアクセスすることが可能になっている。
【０００３】
これにより、有線ネットワークで発生したサービス攻撃は無線サービスに徐々に拡大されることが予想される。特に無線ネットワーク上では、 有線ネットワークのリソースの制限によってその攻撃による被害がさらに致命的になる。
【０００４】
図１は、一般的な状態遷移動作を説明するための全体的な概念図であって、ＴＣＰ接続を完了(establish)し終了するためのＴＣＰプロトコルをさらに詳しく説明するために使用された全体標準有限状態機械（Finite State Machine）を示しており、正確性のためにすべての状態及び遷移が図示されている。
【０００５】
まず、ＴＣＰ接続状態は、下記のように定義される。
ＬＩＳＴＥＮ：サーバのデーモンが実行され、接続要求を待つ状態である。
ＳＹＮ＿ＳＥＮＴ：ローカルのクライアントアプリケーションが遠隔ホストに接続を要求した状態である。
ＳＹＮ＿ＲＣＶＤ：サーバが遠隔クライアントから接続要求を受信し、クライアントに応答したが、まだ確認メッセージを受信していない状態である。
ＥＳＴＡＢＬＩＳＨＥＤ：スリーウェイハンドシェーキングが完了した後、サーバとクライアントが互いに接続された状態である。
ＦＩＮ＿ＷＡＩＴ＿１、ＣＬＯＳＥ－ＷＡＩＴ、ＦＩＮ＿ＷＡＩＴ＿２：サーバがクライアントに接続を終了することを要求し、回答を受信し終了する状態である。
ＣＬＯＳＩＮＧ：通常は生じないが、確認メッセージが伝送途中に紛失された状態である。
ＴＩＭＥ－ＷＡＩＴ：接続は終了したが、紛失された可能性のある遅いセグメントのためにしばらくソケットをオープンする状態である。
ＣＬＯＳＥＤ：接続が完全に終了した状態である。
【０００６】
先行文献（例えば、Transmission Control Protocol, RFC 793, Jon Postel, DARPA Internet Program Protocol Specification, September 1981.）に定義されているようなＴＣＰ接続を完了し終了するＴＣＰ通信の接続原理によると、クライアントとサーバ間のＴＣＰ接続（ＴＣＰ connection）を行うためには、スリーウェイハンドシェーキング（Three-way handshaking）手続を行わなければならない。
【０００７】
より具体的に、クライアントがサーバとＴＣＰ通信を行うためには、接続要求（Synchronous ＳＹＮ）、接続要求／確認応答（Synchronous/Acknowledge ＳＹＮ／ＡＣＫ）及び確認応答（Acknowledge、ＡＣＫ）パケットを送受信する手続が必ず必要である。
【０００８】
ここで、接続要求ＳＹＮ、接続要求／確認応答ＳＹＮ／ＡＣＫ及び確認応答（ＡＣＫ）のスリーウェイハンドシェーキング手続が首尾よく行われる場合、クライアントとサーバ間のＴＣＰ接続が達成される。これは、クライアントが要求したサーバのＴＣＰ通信ポートが通信のためにオープンされることを意味する。
【０００９】
このような従来のＴＣＰの状態遷移（State Transition）において、ＴＣＰ状態遷移は、パケットのフラグによって、どんなＴＣＰスタック状態であるかを示す。しかし、従来のＴＣＰ状態遷移によって、入ってくるパケットは、徹底的に検証されず、従って、このよ

うな脆弱性を悪用する事例が多く発生する。
【００１０】
すなわち、インターネットを通じてスリーウェイハンドシェーキング手続を悪用した攻撃、例えば、ＳＹＮフローディング（Flooding）攻撃のようなサービス拒否（Denial of Service；ＤｏＳ）攻撃を受けている。
【００１１】
一方、モバイルデバイスにインストールされたオペレーティングシステム（ＯＳ）に応じて、前述したＴＣＰ状態遷移（State Transition）のすべてがサポートされたり、されなかったりする。スリーウェイハンドシェーキングの初期段階では、ＴＣＰ仕様で提示される全てのＴＣＰ状態遷移を確認する過程がない。エネルギーを節約するために大部分の時間を休止（Dormant）状態にあるモバイルデバイスにおいて、ＴＣＰベースのサービス拒否（ＤｏＳ）攻撃として多く用いられるが、ＳＹＮフローディング攻撃は、ネットワーク接続が、ＳＹＮフローディング攻撃によって、試みられると、モバイルデバイスは、作動状態（ＡＷＡＫＥ）となり、エネルギーを消費する。
【００１２】
また、モバイルデバイスに伝送されたパケットが特定用途に利用されなくても、当該パケットは、継続的にモバイルデバイスへの接続を試み、モバイルデバイスを作動させる。この場合、無線回線のリソースも、モバイルデバイスのバッテリー電源も消費される。
【００１３】
【非特許文献１】Transmission Control Protocol, RFC 793, Jon Postel, DARPA Internet Program Protocol Specification, September 1981.
【発明の概要】
【発明が解決しようとする課題】
【００１４】
本発明は、モバイルデバイスに対するサービス拒否（Denial of Service；ＤｏＳ）攻撃を効率的に遮断する方法を提供する。該攻撃は、無線上でＴＣＰプロトコルを利用してモバイルデバイスに絶え間なくＴＣＰパケットを伝送し、これにより、無線ネットワークのリソース及びバッテリーに依存するモバイルデバイスのバッテリー電源を浪費させる。
【課題を解決するための手段】
【００１５】
本発明の第１の態様は、ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法において、前記基地局が前記モバイルデバイスにＴＣＰ接続のための接続要求ＳＹＮパケットを伝送した後、前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記モバイルデバイス側で接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送する段階と、前記伝送された接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットが受信されると、前記基地局側で前記接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットに対応する確認応答ＡＣＫ＿２パケットを前記モバイルデバイスに伝送する段階と、前記モバイルデバイスが前記伝送された確認応答ＡＣＫ＿２パケットを受信すると、前記ＴＣＰ接続を完了する段階と、前記ＴＣＰ接続が完了した後、前記モバイルデバイスが前記基地局からリセットＲＳＴまたは接続要求ＳＹＮフラグが設定されたパケットを受信すると、前記完了したＴＣＰ接続を終了する段階を含むサービス拒否攻撃の遮断方法を提供する。
【００１６】
ここで、前記ＴＣＰ接続が完了した後、前記モバイルデバイスがあらかじめ設定されたタイムアウト期間に何らかのパケットをも受信しなければ、前記基地局により前記ＴＣＰ接続を不正に終了したものと決定されることができ、前記モバイルデバイスは、前記ＴＣＰ接続を安全に終了させることができる。
【００１７】
前記タイムアウト期間は、０．５秒に設定されることができる。

【００１８】
本発明の第２の態様は、ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法において、前記基地局が前記モバイルデバイスにＴＣＰ接続のための接続要求ＳＹＮパケットを伝送した後、前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記モバイルデバイス側で接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送する段階と、前記基地局側で、前記伝送された接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを受信した後、終了ＦＩＮパケットを前記モバイルデバイスに伝送する段階と、前記モバイルデバイスが前記伝送された終了ＦＩＮパケットを受信すると、前記ＴＣＰ接続を終了する段階を含むサービス拒否攻撃の遮断方法を提供する。

【００１９】
本発明の第３の態様は、ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法において、前記基地局が前記モバイルデバイスにＴＣＰ接続のための接続要求ＳＹＮパケットを伝送した後、前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記モバイルデバイス側で接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送する段階と、前記基地局側で前記伝送された接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを受信した後、前記接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットに対応する確認応答ＡＣＫ＿２フラグ及びＦＩＮフラグが設定された確認応答終了ＡＣＫ＿２／ＦＩＮパケットを前記モバイルデバイスに伝送する段階と、前記モバイルデバイスが前記伝送された確認応答終了ＡＣＫ＿２／ＦＩＮパケットを受信すると、前記ＴＣＰ接続を終了する段階を含むサービス拒否攻撃の遮断方法を提供する。

【００２０】
本発明の第４の態様は、ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法において、前記基地局が前記モバイルデバイスにＴＣＰ接続のための接続要求ＳＹＮパケットを伝送した後、前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記モバイルデバイス側で接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送する段階と、前記基地局側で前記伝送された接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを受信した後、前記接続要求ＳＹＮパケットを前記モバイルデバイスに伝送する段階と、前記モバイルデバイスが前記伝送された接続要求ＳＹＮパケットを受信すると、前記ＴＣＰ接続を終了する段階を含むサービス拒否攻撃の遮断方法を提供する。

【００２１】
ここで、前記モバイルデバイスが前記接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを前記基地局に伝送した後、あらかじめ設定されたタイムアウト期間に何らかのパケットをも受信しなければ、前記基地局により前記ＴＣＰ接続を不正に終了したものと決定されることができ、前記モバイルデバイスは、前記ＴＣＰ接続を安全に終了させることができる。

【００２２】
前記タイムアウト期間は、０．５秒に設定されることができる。

【００２３】
本発明の第５の態様は、ＴＣＰプロトコルを利用して基地局とモバイルデバイスとの間に伝送されるパケットの流れを確認することによって、サービス拒否（ＤｏＳ）攻撃を遮断するための方法において、ＴＣＰ接続が前記基地局と前記モバイルデバイスとの間に完了後に、前記モバイルデバイスが前記基地局にＴＣＰ接続を正常に終了するための終了／確認応答ＳＹＮ／ＡＣＫパケットを伝送した後、あらかじめ設定されたタイムアウト期間に前記基地局から確認応答ＡＣＫ＿３パケットを受信しなければ、前記ＴＣＰ接続を安全に終了させる段階を含むサービス拒否攻撃の遮断方法を提供する。

【００２４】

ここで、前記タイムアウト期間は、０．５秒に設定されることができる。
【００２５】
本発明の第６の態様は、モバイルデバイス上でＴＣＰ基盤のＤｏＳ攻撃を遮断するための前述した方法を実行することができるプログラムを保存した記録媒体を提供する。
【発明の効果】
【００２６】
本発明のモバイルデバイスに対するＴＣＰベースのサービス拒否攻撃の遮断方法により、ＤｏＳ攻撃が無線リソース及びモバイルデバイスのバッテリー電源を浪費することを防止することが可能である。また、無線ネットワークを通じてＤｏＳ攻撃によって接続が試みられるとき、初期段階においてモバイルデバイスを安全に保護することも可能である。
【図面の簡単な説明】
【００２７】
【図１】一般的なＴＣＰ状態遷移動作を説明するための全体的な概念図である。
【図２】本発明の一実施例によるモバイルデバイスに対するＴＣＰベースのサービス拒否攻撃（ＤｏＳ）の遮断方法を具現するためのモデルを示す全体的な概念図である。
【図３】基地局とモバイルデバイスとの間の正常なＴＣＰ接続完了過程においてのパケットの流れ及びＴＣＰ状態遷移動作を説明するための図である。
【図４】基地局とモバイルデバイスとの間の正常なＴＣＰ接続終了過程においてのパケットの流れ及びＴＣＰ状態遷移動作を説明するための図である。
【図５】不正なＴＣＰ接続の第１例においてのパケットの流れ及びＴＣＰ状態遷移動作を説明するための図である。
【図６】不正なＴＣＰ接続の第２例においてのパケットの流れ及びＴＣＰ状態遷移動作を説明するための図である。
【図７】不正なＴＣＰ接続の第３例においてのパケットの流れ及びＴＣＰ状態遷移動作を説明するための図である。
【図８】不正なＴＣＰ接続の第４例においてのパケットの流れ及びＴＣＰ状態遷移動作を説明するための図である。
【図９】不正なＴＣＰ接続の第５例においてのパケットの流れ及びＴＣＰ状態遷移動作を説明するための図である。
【発明を実施するための形態】
【００２８】
以下、添付の図面を参照して本発明の実施例を詳細に説明する。しかし、下記に例示する本発明の実施例は、様々な他の形態に変形することができ、本発明の範囲が下記実施例に限定されるものではない。本発明の実施例は、この技術分野における通常の知識を有する者に本発明をさらに完全に説明するために提供されるものである。
【００２９】
まず、本発明は、無線でＴＣＰパケットを受信しサービスを受ける、バッテリーから電力供給されるモバイルデバイスのあらゆる事例に対して、適用可能である。本発明は、まだプロトコルが定められていないセンサーネットワーク分野を除いた、ＴＣＰサービスを受けることができるＷｅｂＰＤＡ、２Ｇ－ＥＶＤＯセルラーネットワークや３Ｇ／４Ｇデータサービスセルラーネットワークなどを利用したモバイルデバイス、及びスマートフォンなどにすべて適用されることができる防御手段である。
【００３０】
また、本発明は、モバイルデバイスに実装され、リソースを消費するＴＣＰパケットを確認して処理する。したがって、本発明は、無線リソースとモバイルデバイスリソースを効率的に管理する方法であり、また、無線ネットワークを通じてサービス拒否（ＤｏＳ）攻撃により接続が試みられるとき、モバイルデバイスを安全に保護する方法として使用されることができる。
【００３１】
図２は、本発明の一実施例によるモバイルデバイスに対するＴＣＰベースのＤｏＳ攻撃の

遮断方法を具現するためのモデルを示す全体的な概念図である。

【００３２】

図２を参照すれば、本発明の一実施例によるモバイルデバイスに対するＴＣＰベースのＤｏＳ攻撃の遮断方法を具現するための全体的なモデルは、５つの状態（０乃至４）で構成されている。５つの状態は、基地局とモバイルデバイス、例えば、携帯電話、ＰＤＡ、ＷｅｂＰＤＡ、その他ＴＣＰネットワークに対応可能な無線モバイルデバイスなどとの間で送受信されるパケットの流れによって多様な形態の接続状態を示す。

【００３３】

一方、本発明の一実施例に適用されたモデルは、基地局とモバイルデバイスとの間で送受信されるパケットをモニタリングしながら、各ＴＣＰ状態遷移のために送受信されるパケットがＴＣＰ仕様に適合するかどうかを確認及び判断する。

【００３４】

すなわち、本発明は、従来のＴＣＰ状態遷移による確認機能を行う。したがって、送受信されるパケットのフラグによって次がどのような状態であるべきか、現在の状態でどんなフラグが設定されたパケットが入らなければならないかを段階別に確認することができるようになる。

【００３５】

また、モバイルデバイスに入ってくるすべてのパケットにおいて、１つのセッションは、第１状態０から第５状態４までの段階を経てさらに第１状態０に戻る。セッションを構成するパケットのフラグを利用して、段階０乃至段階４の順序、及び入ってはならないパケットが受信されているかを確認することが可能である。ここで、第１状態０は、１つのセッションの開始と終了を意味する。

【００３６】

図３は、基地局とモバイルデバイスとの間の正常なＴＣＰ接続完了過程に対するパケットの流れ及びＴＣＰ状態遷移動作を例示する。

【００３７】

図２及び図３において示すように、最初に基地局１００とモバイルデバイス２００との間にセッションが形成されるとき、モバイルデバイス２００のＴＣＰ状態は、１つのセッションの開始と終了を意味する第１状態０に設定される。

【００３８】

その後、基地局１００は、ＳＹＮフラグが設定された接続要求ＳＹＮパケットを、接続しようとするモバイルデバイス２００の特定のポートに送信する。本発明では、モバイルデバイス２００が基地局１００から送信された接続要求ＳＹＮパケットの受信を確認すれば、モバイルデバイス２００のＴＣＰ状態は、第１状態０から第２状態１に変わる。

【００３９】

次に、モバイルデバイス２００は、接続要求を受信したことを示すために、接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを基地局１００に送信する。この接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットは、モバイルデバイス２００の接続要求ＳＹＮフラグ及び確認応答ＡＣＫ＿１フラグが設定された接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを基地局１００に送信する。本発明において、モバイルデバイス２００が基地局１００への接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットの送信を確認すれば、モバイルデバイス２００のＴＣＰ状態は、第２状態１から第３状態２に変わる。

【００４０】

その後、基地局１００は、モバイルデバイス２００に接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットに対応する確認応答ＡＣＫ＿２パケットを送信する。本発明において、モバイルデバイス２００が基地局１００から送信された確認応答ＡＣＫ＿２パケットの受信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第３状態２から第４状態３に変わり、ＴＣＰ接続を完了する。その後、基地局１００とモバイルデバイス２００との間にデータ伝送が行われる。

【００４１】

最初にＴＣＰ接続が試みられるとき、モバイルデバイス２００により受信されるＴＣＰパケットは、接続要求ＳＹＮパケットでなければならない。スリーウェイハンドシェーキングを経て、ＴＣＰ接続が試みられるノードとのＴＣＰ接続が達成されるようになる。

【００４２】

したがって、モバイルデバイス２００は、接続要求ＳＹＮパケットに応答して接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットを送り、接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットに対する応答として確認応答ＡＣＫ＿２パケットを受信する。この過程が完全に行われるとき、１つのＴＣＰ接続が達成されるようになる。

【００４３】

本発明は、モバイルデバイス２００がＴＣＰ接続を完了する各段階を１つずつ確認することができるように、第１状態０から第４状態３の段階までの段階にポインタを提供する。接続要求ＳＹＮパケットが最初にＴＣＰ接続を試みるときからスリーウェイハンドシェーキングが完了するときまで各段階にポインタが存在するので、その過程が不正に実行される瞬間を直ちに見つけることができ、また、この誤動作に対して適切な措置を取ることができる。

【００４４】

図４は、基地局とモバイルデバイスとの間の正常なＴＣＰ接続終了過程に対するパケットの流れ及びＴＣＰ状態遷移動作を例示する。

【００４５】

図２及び図４において示すように、基地局１００とモバイルデバイス２００との間のＴＣＰ接続が完了した第４状態３で、基地局１００とのＴＣＰ接続を終了するために、モバイルデバイス２００は、ＦＩＮフラグがセットされた終了確認応答ＦＩＮ／ＡＣＫ＿３パケットを基地局１００の特定のポートに送信する。モバイルデバイス２００から送信された終了確認応答ＦＩＮ／ＡＣＫ＿３パケットが受信されれば、基地局１００は、ＴＣＰ接続終了を認識したことを通知するために、終了確認応答ＦＩＮ／ＡＣＫ＿３パケットに対する確認応答ＡＣＫ＿４パケットをモバイルデバイス２００に送信する。

【００４６】

ここで、本発明において、モバイルデバイス２００が基地局１００への終了確認応答ＦＩＮ／ＡＣＫ＿３パケットの送信を確認すれば、モバイルデバイス２００のＴＣＰ状態は、第４状態３から第５状態４に変わる。

【００４７】

その後、基地局１００は、終了確認応答ＦＩＮ／ＡＣＫ＿３パケットに対応する確認応答ＡＣＫ＿４パケットをモバイルデバイス２００に送信する。本発明において、モバイルデバイス２００が基地局１００から送信された確認応答ＡＣＫ＿４パケットの受信を確認すれば、モバイルデバイス２００のＴＣＰ状態は、第５状態４から第１状態０に変わり、ＴＣＰ接続を終了する。

【００４８】

一方、第５状態４で基地局１００が確認応答ＡＣＫ＿４を送信せず、あらかじめ接続を終了した場合、タイムアウトが作動するようになり、モバイルデバイス２００もＴＣＰ接続を終了するために第１状態０に転換する。

【００４９】

すなわち、モバイルデバイス２００があらかじめ設定されたタイムアウト期間（約０．５秒）に確認応答ＡＣＫ＿４パケットを受信しなければ、モバイルデバイス２００のＴＣＰ状態は、第５状態４から第１状態０に変わり、ＴＣＰ接続を安全に終了する。

【００５０】

以下、不正なＴＣＰ接続の様々な例を通じて本発明の一実施形態によるモバイルデバイスに対するＴＣＰベースのＤｏＳ攻撃の遮断方法について詳細に説明する。

【００５１】

すなわち、ＤｏＳ攻撃が発生する際に、本発明が適用されたモデルを利用してどのようにモバイルデバイス２００がＤｏＳ攻撃を確認し対処することができるかについて説明する

。モバイルデバイス２００が対処することができる大部分のＤｏＳ攻撃は、不正なＴＣＰ接続を試みるものである。

【００５２】

図５は、不正なＴＣＰ接続の第１例における、パケットの流れ及びＴＣＰ状態遷移動作を例示する。

【００５３】

図２及び図５において示すように、モバイルデバイス２００が基地局１００から送信された接続要求ＳＹＮパケットの受信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第１状態０から第２状態１に変わる。その後、モバイルデバイス２００が基地局１００への接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットの送信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第２状態１から第３状態２に変わる。

【００５４】

次に、モバイルデバイス２００が基地局１００から送信された、確認応答ＡＣＫ＿２パケットの受信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第３状態２から第４状態３に変わり、ＴＣＰ接続を完了する。

【００５５】

その後、モバイルデバイス２００が基地局１００から送信されたリセットＲＳＴまたは接続要求ＳＹＮフラグが設定されたパケット、すなわち接続要求パケットの受信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第４状態３から直ちに第１状態０に変わり、ＴＣＰ接続を安全に終了させる。

【００５６】

一方、第４状態３で、基地局１００が何らかのパケットを送信せずに、不正に接続を終了した場合、本発明によってタイムアウトが作動するようになって、モバイルデバイス２００もＴＣＰ接続を終了するために直ちに第１状態０に転換する。

【００５７】

すなわち、モバイルデバイス２００があらかじめ設定されたタイムアウト期間（約０．５秒）に何らかのパケットを受信しなければ、モバイルデバイス２００のＴＣＰ状態は、第４状態３から直ちに第１状態０に変わり、ＴＣＰ接続を安全に終了させる。

【００５８】

不正なＴＣＰ接続の第１例における全ての記載を考慮すると、ネットワークでモバイルデバイス２００に継続的に接続要求ＳＹＮパケットを伝送する事例がしばしば生じる。この場合、無線ネットワークのリソースは、無駄に使用され、モバイルデバイス２００は、継続的に作動状態（wakeup）となり、バッテリーを消費するようになる。

【００５９】

従って、スリーウェイハンドシェーキング以後にリセットＲＳＴや接続要求ＳＹＮパケットが入る場合には、パケットは、不正なパケットとして見なされる。次に、モバイルデバイス２００は、前述したように、第１状態０から第４状態３に順次に転換された後、さらに第１状態０に転換され、パケットが受信されない。

【００６０】

図６は、不正なＴＣＰ接続の第２例におけるパケットの流れ及びＴＣＰ状態遷移動作を例示する。

【００６１】

図２及び図６において示すように、モバイルデバイス２００が基地局１００から送信された接続要求ＳＹＮパケットの受信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第１状態０から第２状態１に変わる。その後、モバイルデバイス２００が基地局１００への接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットの送信を確認すれば、モバイルデバイス２００のＴＣＰ状態は、第２状態１から第３状態２に変わる。

【００６２】

次に、モバイルデバイス２００が基地局１００から送信された終了ＦＩＮパケットを受信すると、基地局１００により不正に接続を終了したものと判断され、モバイルデバイス２

００のＴＣＰ状態は、第３状態２から直ちに第１状態０に変わり、ＴＣＰ接続を安全に終了させる。

【００６３】

一方、第３状態２で、基地局１００が何らかのパケットを送信せずに、不正に接続を終了した場合、タイムアウトが作動するようになり、モバイルデバイス２００もＴＣＰ接続を終了するために直ちに第１状態０に転換される。

【００６４】

すなわち、モバイルデバイス２００があらかじめ設定されたタイムアウト期間（約０．５秒）に何らかのパケットを受信しなければ、モバイルデバイス２００のＴＣＰ状態は、第３状態２から直ちに第１状態０に変わり、ＴＣＰ接続を安全に終了させる。

【００６５】

不正なＴＣＰ接続の第２例における全ての記載を考慮すると、スリーウェイハンドシェーキング手続中に終了ＦＩＮパケットが急に受信される事例が生じる。すなわち、モバイルデバイス２００内部のオペレーティングシステム（ＯＳ）は、スリーウェイハンドシェーキング手続を終了するために、確認応答ＡＣＫ＿２パケットを待つ。

【００６６】

しかし、基地局１００から予期しない終了ＦＩＮパケットが受信されれば、モバイルデバイス２００は、継続的に作動状態で待機し、バッテリー電源を消費する。したがって、この場合には、モバイルデバイス２００は、第１状態０から第３状態２に順次に転換され、さらに第１状態０に転換されることによって、ＴＣＰ接続が終了し、リソースが無駄に使用されることを防止することができる。

【００６７】

すなわち、モバイルデバイス２００のＴＣＰ状態が第１状態０から第３状態２に順次に転換され、さらに第１状態０に転換されることを確認してから、ＴＣＰ接続が終了すれば、バッテリー消耗やリソース割当問題を解決することができる。

【００６８】

図７は、不正なＴＣＰ接続の第３例におけるパケットの流れ及びＴＣＰ状態遷移動作を例示する。

【００６９】

図２及び図７は、スリーウェイハンドシェーキングを完了しつつ終了ＦＩＮパケットが伝送される場合が例示されている。まず、モバイルデバイス２００が基地局１００から送信された接続要求ＳＹＮパケットの受信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第１状態０から第２状態１に転換される。その後、モバイルデバイス２００が基地局１００への接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットの送信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第２状態１から第３状態２に転換される。

【００７０】

次に、基地局１００は、モバイルデバイス２００に接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットに対応する確認応答ＡＣＫ＿２フラグ及びＦＩＮフラグが設定された確認応答終了ＡＣＫ＿２／ＦＩＮパケットを送信することがある。本発明において、モバイルデバイス２００が基地局１００から送信された確認応答終了ＡＣＫ＿２／ＦＩＮパケットの受信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第３状態２から直ちに第１状態０に変わり、ＴＣＰ接続を安全に終了させる。

【００７１】

一方、第３状態２で基地局１００が何らかのパケットを送信せずに、不正に接続を終了した場合、本発明によってタイムアウトが作動し、モバイルデバイス２００もＴＣＰ接続を終了するために直ちに第１状態０に転換される。

【００７２】

すなわち、モバイルデバイス２００があらかじめ設定されたタイムアウト期間（約０．５秒）に何らかのパケットを受信しなければ、モバイルデバイス２００のＴＣＰ状態は、第３状態２から直ちに第１状態０に変わり、ＴＣＰ接続を安全に終了させる。

【００７３】
図８は、不正なＴＣＰ接続の第４例におけるパケットの流れ及びＴＣＰ状態遷移動作を例示する。
【００７４】
図２及び図８において示すように、モバイルデバイス２００が基地局１００から送信された接続要求ＳＹＮパケットの受信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第１状態０から第２状態１に転換される。その後、モバイルデバイス２００が基地局１００への接続要求確認応答ＳＹＮ／ＡＣＫ＿１パケットの送信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第２状態１から第３状態２に変わる。
【００７５】
ここで、同一の基地局１００が第３状態２で同一の接続要求ＳＹＮパケットをモバイルデバイス２００に続いて送信することがある。モバイルデバイス２００が同一の基地局１００からの接続要求ＳＹＮパケットの受信を確認すると、モバイルデバイス２００のＴＣＰ状態は、第３状態２から直ちに第１状態０に変わり、ＴＣＰ接続を安全に終了させる。
【００７６】
不正なＴＣＰ接続の第４例における全ての記載を総合的に考慮すると、スリーウェイハンドシェーキングの途中に同一の接続要求ＳＹＮパケットを連続的に送信される事例が生じる。この場合、接続要求ＳＹＮパケットが連続的に送信され、モバイルデバイス２００は作動状態を継続させる。ここで、本発明の方法により、モバイルデバイス２００は、第１状態０から第３状態２に順次に転換された後、同一の接続要求ＳＹＮパケットを受信すると、さらに第１状態０に転換し、ＴＣＰ接続を安全に終了させる。したがって、モバイルデバイス２００のバッテリー消耗と無線リソースの浪費を効果的に防止することができる。
【００７７】
図９は、不正なＴＣＰ接続の第５例におけるパケットの流れ及びＴＣＰ状態遷移動作を例示する。第５例で、タイムアウトが作動する。
【００７８】
図２及び図９において示すように、基地局１００とモバイルデバイス２００との間のＴＣＰ接続が完了した後、すなわち第４状態３で、モバイルデバイス２００がＴＣＰ接続を終了しようとする場合、モバイルデバイス２００は、基地局１００に終了確認応答ＦＩＮ／ＡＣＫ＿１パケットを伝送する。その後、モバイルデバイス２００は、第４状態３から第５状態４に転換し、基地局１００から確認応答ＡＣＫ＿２を待つ。ここで、あらかじめ設定されたタイムアウト期間（約０．５秒）に何らかの応答がなければ、モバイルデバイス２００のＴＣＰ状態は、第５状態４から直ちに第１状態０に変わり、ＴＣＰ接続を安全に終了させる。
【００７９】
一方、本発明の実施例によるモバイルデバイスに対するＴＣＰベースのＤｏＳ攻撃の遮断方法は、コンピュータで読み取り可能な記録媒体にコンピュータが読み取り可能なコード(computer code)として実装可能である。コンピュータが読み取り可能な記録媒体は、コンピュータシステムによって読み取り可能なデータが保存される任意の記録装置を含む。
【００８０】
例えば、コンピュータが読み取り可能な記録媒体として、ＲＯＭ、ＲＡＭ、ＣＤ－ＲＯＭ、磁気テープ、ハードディスク、フロッピーディスク、携帯記憶装置、非揮発性メモリ（フラッシュメモリなど）、光情報記録装置などが挙げられ、また、搬送波（例えば、インターネットを用いた伝送）の形態で具現されるものも含まれる。
【００８１】
また、コンピュータで読み取り可能な記録媒体は、通信網で接続されたコンピュータシステムに分散され、分散方式で読み出すことができるコードの形態で保存され実行されることができる。
【００８２】

本発明は、好ましい実施例を参照して図示及び説明されたが、当業者は、特許請求範囲に定義された趣旨及び範囲内で形態及び詳細事項について様々の変形が行われることができることを理解することができるだろう。

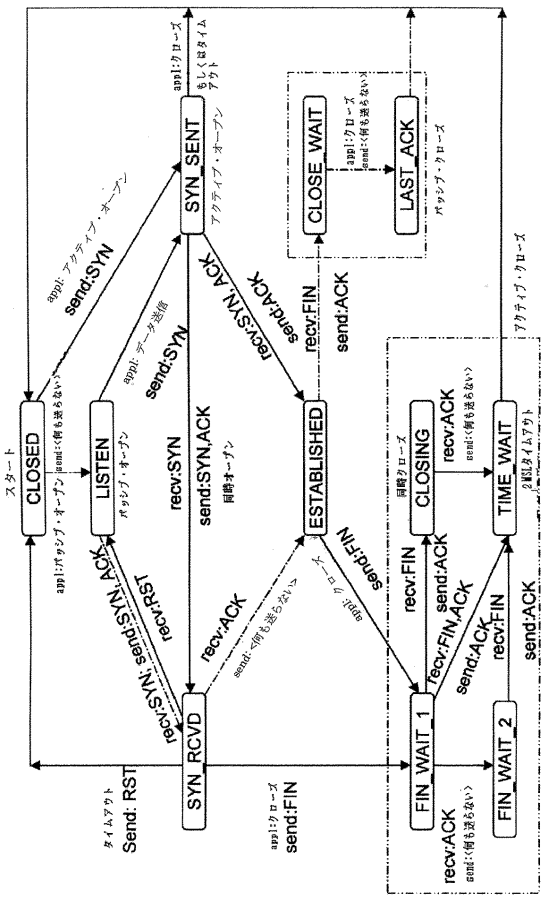
【符号の説明】

【００８３】

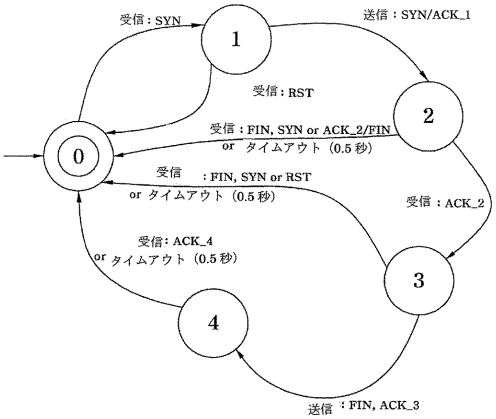
１００　基地局

２００　モバイルデバイス

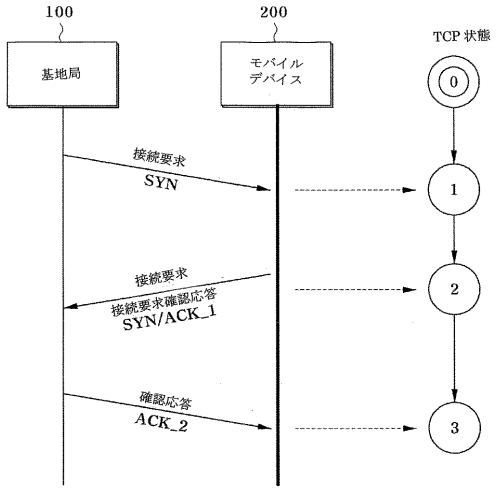
【図１】



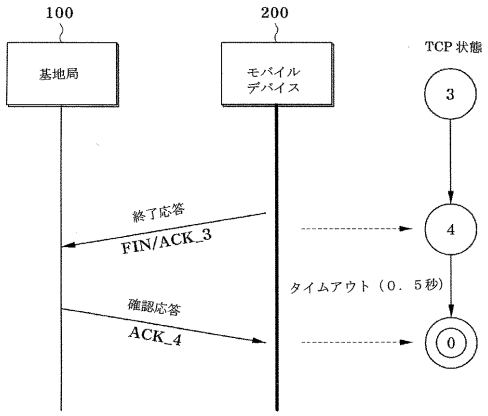
【図２】



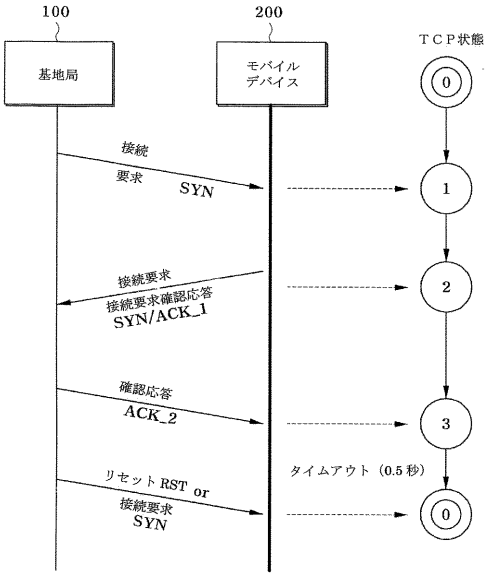
【図３】


100
200
TCP 状態
基地局
モバイル
デバイス
0
接続要求
SYN
1
接続要求
接続要求確認応答
SYN/ACK_1
2
確認応答
ACK_2
3

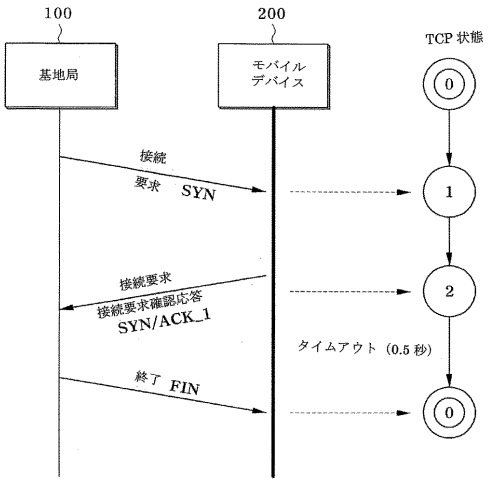
【図４】


100
200
TCP 状態
基地局
モバイル
デバイス
3
終了応答
FIN/ACK_3
4
タイムアウト（0．5秒）
確認応答
ACK_4
0

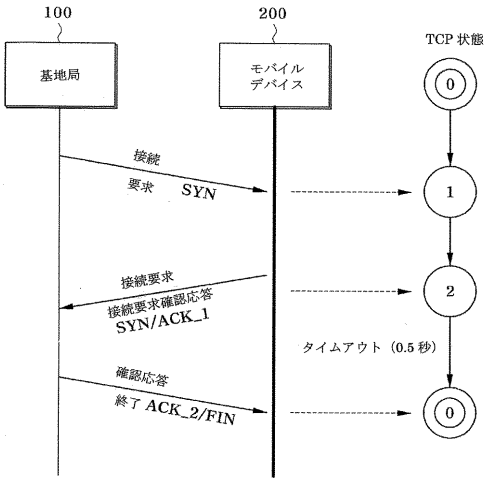
【図５】


100
200
TCP状態
基地局
モバイル
デバイス
0
接続
要求 SYN
1
接続要求
接続要求確認応答
SYN/ACK_1
2
確認応答
ACK_2
3
タイムアウト（0.5秒）
リセット RST or
接続要求
SYN
0

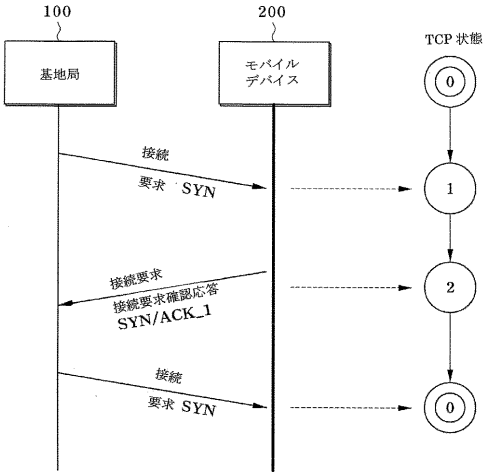
【図６】


100
200
TCP 状態
基地局
モバイル
デバイス
0
接続
要求 SYN
1
接続要求
接続要求確認応答
SYN/ACK_1
2
タイムアウト（0.5秒）
終了 FIN
0

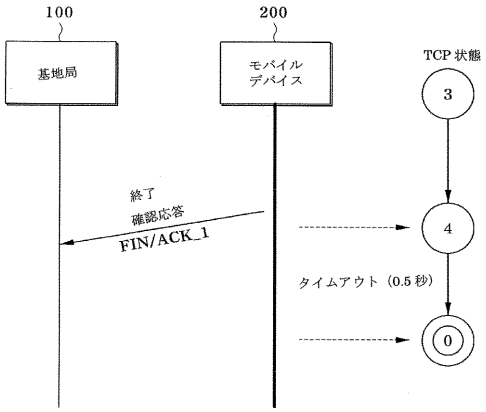
【図７】


100
200
基地局
モバイル
デバイス
TCP 状態
0
接続
要求 SYN
1
接続要求
接続要求確認応答
SYN/ACK_1
2
タイムアウト（0.5 秒）
確認応答
終了 ACK_2/FIN
0

【図８】


100
200
基地局
モバイル
デバイス
TCP 状態
0
接続
要求 SYN
1
接続要求
接続要求確認応答
SYN/ACK_1
2
接続
要求 SYN
0

【図９】


100
200
基地局
モバイル
デバイス
TCP 状態
3
終了
確認応答
FIN/ACK_1
4
タイムアウト（0.5 秒）
0

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/004440

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/22(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 8 : H04L 12/22, 12/24; G06F 12/14, 11/30, 15/173; H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, eKIPASS(KIPO internal)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US20060230129 A1 (YOGESH P. SWAMI et al.) 12 October 2006 See abstract; figures 1A, 2-5; claims 1-4.	1-11
A	US20060229022 A1 (TIAN BU et al.) 12 October 2006 See abstract; figures 2, 3, 4; claims 1, 9, 10.	1, 4, 5, 6, 9, 11
A	US20060230450 A1 (TIAN BU et al.) 12 October 2006 See abstract; claims 13-17, 20.	1, 4, 5, 6, 9, 11
A	US20030084321 A1 (RICHARD PAUL TARQUINI et al.) 1 May 2003 See abstract; claims 1-3.	1, 4, 5, 6, 9, 11

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 APRIL 2008 (29.04.2008)	**29 APRIL 2008 (29.04.2008)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	YANG, CHAN HO Telephone No. 82-42-481-5689

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2007/004440

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US20060230129 A1	12.10.2006	None	
US20060229022 A1	12.10.2006	DE60060001127C0	08.11.2007
		EP01708538A1	04.10.2006
		JP2006295920A2	26.10.2006
		KR2006105590A	11.10.2006
		CN1842087A	04.10.2006
US20060230450 A1	12.10.2006	EP1864471A1	12.12.2007
		KR1020070116612	10.12.2007
		WO2006104752A1	05.10.2006
US20030084321 A1	01.05.2003	GB200224549A0	27.11.2002
		GB200425531A0	22.12.2004
		GB2382755A1	04.06.2003
		GB2405065A1	16.02.2005
		JP2003228552A2	15.08.2003
		SE200202730A0	16.09.2002

Form PCT/ISA/210 (patent family annex) (April 2007)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．フロッピー

Ｆターム(参考) 5K034 AA15 DD02 EE03 HH06 HH11

【要約の続き】
【選択図】 図２