(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6662267号
(P6662267)
(45)発行日　令和2年3月11日(2020.3.11)　(24)登録日　令和2年2月17日(2020.2.17)

(51)Int.Cl.　　F I
G06F 21/55 (2013.01)　G06F 21/55
H04B 7/24 (2006.01)　H04B 7/24
H04W 12/12 (2009.01)　H04W 12/12

請求項の数 11　(全 14 頁)

(21)出願番号　特願2016-209860(P2016-209860)
(22)出願日　平成28年10月26日(2016.10.26)
(65)公開番号　特開2018-73004(P2018-73004A)
(43)公開日　平成30年5月10日(2018.5.10)
審査請求日　平成30年11月15日(2018.11.15)

(73)特許権者　000003207
トヨタ自動車株式会社
愛知県豊田市トヨタ町１番地
(74)代理人　100100549
弁理士　川口　嘉之
(74)代理人　100085006
弁理士　世良　和信
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100123319
弁理士　関根　武彦
(74)代理人　100123098
弁理士　今堀　克彦
(74)代理人　100143797
弁理士　宮下　文徳

最終頁に続く

(54)【発明の名称】攻撃通知システムおよび攻撃通知方法

(57)【特許請求の範囲】
【請求項１】
第１の無線通信網と第２の無線通信網のいずれを用いてもサーバ装置と通信可能なユーザ装置に対して攻撃されていることまたは攻撃されかけていることを通知する攻撃通知システムであって、
ユーザ装置に関する情報を管理する管理手段と、
第１の無線通信網のトラフィックを監視して攻撃を検知する監視手段と、
前記監視手段によって検知された攻撃の対象のユーザ装置を特定する解析手段と、
前記解析手段によって特定されたユーザ装置または当該ユーザ装置に関連する装置に対して、前記第２の無線通信網を介した通信によって通知を行う通知手段と、
を備え、
前記監視手段は、攻撃対象の前記第１の無線通信網の基地局を含む攻撃検知情報を前記解析手段に送信し、
前記解析手段は、前記攻撃検知情報に含まれている基地局を利用して通信を行っているユーザ装置を攻撃対象のユーザ装置として特定する、
攻撃通知システム。
【請求項２】
前記第１の無線通信網は、公衆無線ＬＡＮであり、
前記第２の無線通信網は、携帯電話網である、
請求項１に記載の攻撃通知システム。

【請求項３】
前記管理手段は、ユーザ装置ごとに当該ユーザ装置の前記第１の無線通信網における識別子を記憶しており、
前記解析手段は、前記管理手段を参照して前記攻撃検知情報から攻撃対象のユーザ装置を特定する、
請求項１または２に記載の攻撃通知システム。
【請求項４】
前記管理手段は、ユーザ装置ごとに、当該ユーザ装置の前記第２の無線通信網における識別子を記憶しており、
前記通知手段は、攻撃対象として特定されたユーザ装置に対して、前記第２の無線通信網を介した通信によって前記通知を行う、
請求項１から３のいずれか１項に記載の攻撃通知システム。
【請求項５】
前記管理手段は、ユーザ装置ごとに、当該ユーザ装置に関連する装置の前記第２の無線通信網における識別子を記憶しており、
前記通知手段は、攻撃対象として特定されたユーザ装置に関連する装置に対して、前記第２の無線通信網を介した通信によって前記通知を行う、
請求項１から３のいずれか１項に記載の攻撃通知システム。
【請求項６】
前記ユーザ装置に関連する装置は、前記通知手段からの通知を受けると、当該通知を受けた旨を前記ユーザ装置に対して無線通信によって知らせる、
請求項５に記載の攻撃通知システム。
【請求項７】
前記解析手段は、前記監視手段によって検知された攻撃が、同じ地域の複数台のユーザ装置を対象とする攻撃であるか否か判定し、
前記通知手段は、前記攻撃が同じ地域の複数台のユーザ装置を対象とする攻撃である場合には、通知を転送すべきことを表す情報を含めて前記通知を行い、
前記ユーザ装置または前記ユーザ装置に関連付けられた装置は、通知を転送すべきことを表す情報を含む通知を受信した場合は、当該通知を周囲のユーザ装置またはユーザ装置に関連付けられた装置に転送する、
請求項１から６のいずれか１項に記載の攻撃通知システム。
【請求項８】
前記ユーザ装置は、車両に備え付けられた車載装置である、
請求項１から７のいずれか１項に記載の攻撃通知システム。
【請求項９】
前記ユーザ装置に関連する装置は、前記車両内に存在する携帯情報端末である、
請求項８に記載の攻撃通知システム。
【請求項１０】
第１の無線通信網と第２の無線通信網のいずれを用いてもサーバ装置と通信可能なユーザ装置に対して攻撃されていることまたは攻撃されかけていることを通知する攻撃通知システムが行う攻撃通知方法であって、
第１の無線通信網のトラフィックを監視して攻撃を検知する監視ステップと、
前記監視ステップにおいて検知された攻撃の対象のユーザ装置を特定する解析ステップと、
前記解析ステップにおいて特定されたユーザ装置または当該ユーザ装置に関連する装置に対して、前記第２の無線通信網を介した通信によって通知を行う通知ステップと、
を含み、
前記監視ステップにおいては、攻撃対象の前記第１の無線通信網の基地局を検知し、
前記解析ステップにおいて、前記監視ステップによって検知された、攻撃対象の前記第１の無線通信網の基地局を利用して通信を行っているユーザ装置を攻撃対象のユーザ装置

として特定する、
攻撃通知方法。
【請求項１１】
請求項１０に記載の方法の各ステップをコンピュータに実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、攻撃通知システムに関し、特に無線通信網を介して攻撃を検知した際の通知方法に関する。
【背景技術】
【０００２】
近年、車両に無線通信機能を持たせサーバ装置や他の車両との間で無線通信を行って各種のサービスを提供することが検討されている。無線通信網として、携帯電話網や公衆無線ＬＡＮを利用することが想定される。車両がインターネットに接続されることにより、外部ネットワークから車載機等を介して車両内のＣＡＮやＥＣＵへの攻撃が行われるおそれがある。このような車両への攻撃は、特定の車両を対象とする攻撃と、特定エリアにいる複数の車両を対象とする攻撃があり得る。
【０００３】
また、車両への直接的な攻撃だけでなく、サーバ装置と車両間の通信を妨げることを目的とした、ネットワークに対するＤＤＯＳ攻撃もありうる。
【０００４】
従来は、このようなカーテレマティクス環境の車両への攻撃に対しては、車載機側で認証を実行して通信元の信頼性を担保したり、データの送受信時に暗号化を施したりする対策が提案されている（特許文献１，２）。これらの手法は、個々の車両を対象とする攻撃に対しては有効であるが、ネットワーク負荷の増大によるサーバとの通信妨害を目的とする攻撃には対応できず、また、攻撃されていることを通知できない。
【０００５】
特許文献３は、偽の情報による攻撃を通知タイミングに基づいて検知した後、偽情報を受信できないように擬似乱数により生成されたデータによる妨害信号を送信して、他の端末も偽情報を受信できないようにすることを提案する。この手法は、個々の車両への偽情報による攻撃に対しては有効と考えられるが、通信負荷をかける攻撃に対しては、逆に通信負荷を増長してしまう。また、周辺の車両は擬似データを受信して処理を試みようとすることで余計な負荷がかかるほか、攻撃兆候を伝達することができない。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２０１３－１５７６９３号公報
【特許文献２】特開２０１３－９８７１９号公報
【特許文献３】特開２０１５－２０７９１２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
上記のような問題点を考慮して、本発明は、個々の車両を対象とした攻撃とネットワーク全体を対象とした攻撃の両方について、攻撃を防ぎ、かつ、攻撃されていることを通知可能とすることを目的とする。
【課題を解決するための手段】
【０００８】
本発明の第一の態様は、第１の無線通信網と第２の無線通信網のいずれを用いてもサーバ装置と通信可能なユーザ装置に対して攻撃されていることまたは攻撃されかけていることを通知する攻撃通知システムである。第１の無線通信網と第２の無線通信網はどのよう

な通信網であってもかまわないが、第２の無線通信網は第１の無線通信網よりもセキュリティが確保されていることが好ましい。また、ユーザ装置とサーバ装置の間の通信は、第１の無線通信網または第２の無線通信網のみによって接続される必要はなく、専用網のような第３の無線通信網を介して接続されてもよい。

【０００９】

本態様に係る攻撃検知システムは、ユーザ装置に関する情報を管理する管理手段と、第１の無線通信網のトラフィックを監視して攻撃を検知する監視手段と、前記監視手段によって検知された攻撃の対象のユーザ装置を特定する解析手段と、前記解析手段によって特定されたユーザ装置または当該ユーザ装置に関連する装置に対して、前記第２の無線通信網を介した通信によって通知を行う通知手段と、を備える。これらの各手段は、サーバ装置に設けられてもよいし、サーバ装置とは異なる装置に設けられてもよい。

【００１０】

監視手段は、第１の無線通信網のトラフィックを監視し、トラフィック量や通信データの内容等を解析することによって、ユーザ装置への攻撃を検知する。なお、攻撃の検知には、攻撃が現に行われていることを検知することと、攻撃がこれから行われることを検知することの両方が含まれる。攻撃には、個々のユーザ装置を対象とする攻撃と、ネットワーク全体を対象とする攻撃が含まれうる。攻撃検知の具体的な手法は特に限定されず、既存の任意の手法を採用可能である。監視手段は、攻撃対象のユーザ装置の第１の無線通信網における識別子（モバイルＩＰの気付ＩＰアドレスなど）を把握できる。以下、第１の無線通信網における識別子を、第１識別子とも称する。

【００１１】

解析手段は、監視手段によって検知された攻撃対象のユーザ装置を特定する。例えば、監視手段が攻撃対象の第１の無線通信網における識別子（気付ＩＰアドレスなど）を把握できる場合には、解析手段は、この識別子からユーザ装置の個体識別子や第２の無線通信網における識別子を特定することが好ましい。なお、攻撃がネットワーク全体を対象とする場合、解析手段は、当該攻撃によって影響を受けるユーザ装置を攻撃対象として特定することが好ましい。このような特定を可能とするために、管理手段は、ユーザ装置の第１の無線通信網における識別子と、第２の無線通信網における識別子（携帯電話番号など）あるいは個体識別子を対応付けて記憶することが好ましい。以下、第２の無線通信網における識別子を、第２識別子とも称する。

【００１２】

通知手段は、特定されたユーザ装置またはそのユーザ装置に関連する装置に対して、第２の無線通信網を介して通信によって、攻撃兆候の通知を行う。ここで、ユーザ装置に関連する装置とは、ユーザ装置と同じユーザが使用している装置や、ユーザ装置と通信可能（好ましくは近距離無線通信によって直接通信可能）な装置が該当する。好ましくは、ユーザ装置に関連する装置とは、ここで挙げた両方の条件を満たす装置である。ユーザ装置に関連する装置は、例えば、ユーザが所有するスマートフォンや携帯情報端末である。通知手段は、通知内容に、例えば、攻撃元の第１識別子や、攻撃の種別情報、攻撃履歴などを含ませることが好ましい。

【００１３】

通知を受けたユーザ装置またはユーザ装置に関連する装置の動作は特に限定されない。例えば、ユーザに通知を行うだけでもよいし、攻撃元からの通信をフィルタリングしてもよいし、サーバ装置との通信経路を第２の無線通信網を用いる経路に切り替えてもよい。

【００１４】

上述の構成によれば、個々の車両を対象とした攻撃だけでなくネットワークを対象とする攻撃についても、攻撃によって被害を受けるユーザ装置に対して通知を行うことが可能となる。通知は第２の無線通信網を介した通信によって行っているので、通信負荷をかけるＤＤＯＳ攻撃のような攻撃が第１の無線通信網に対して行われている場合であっても、ユーザ装置に対して通知が行える。また、通知によって第１の無線通信網に対する通信負荷を増大させる事態も避けられる。

【００１５】
本発明において、第２の無線通信網は、第１の無線通信網よりもセキュアな通信網または通信品質が管理された通信網であることが望ましく、セキュアかつ通信品質が管理された通信網であることがさらに望ましい。例えば、第１の無線通信網は公衆無線ＬＡＮであり、第２の無線通信網は携帯電話網とすることができる。携帯電話網は品質管理がされており、攻撃によるリソースの飽和も生じにくいため、携帯網を用いれば確実に通知をユーザ装置に送ることができる。
【００１６】
本発明において、監視手段は、検知した攻撃が個々のユーザ装置を対象とするものである場合、攻撃対象のユーザ端末の第１識別子を含む攻撃検知情報を前記解析手段に送信するように構成できる。解析手段は、攻撃検知情報に基づいて、攻撃対象のユーザ装置を特定するように構成できる。第１識別子は、例えば、ＩＰアドレスや気付ＩＰアドレスである。
【００１７】
このようにすれば、個々のユーザ装置に対する攻撃を検知したときに、攻撃対象のユーザ装置を特定し、第２の無線通信網を介して通知を送れるようになる。
【００１８】
また、本発明において、監視手段は、検知した攻撃がある基地局（アクセスポイントとも呼ばれる）および当該基地局配下のネットワークを対象とする攻撃である場合、攻撃対象の基地局を特定する情報を含む攻撃検知情報を解析手段に送信するように構成できる。解析手段は、攻撃検知情報に含まれている基地局を利用して通信を行っているユーザ装置を攻撃対象のユーザ装置として特定するように構成できる。
【００１９】
このようにすれば、基地局または基地局配下のネットワークに対する攻撃（例えば、ＤＤＯＳ攻撃）を検知したときに、攻撃によって影響を受けるユーザ装置を特定し、特定されたユーザ装置に対して第２の無線通信網を介して通知を送れるようになる。
【００２０】
本発明において、管理手段は、ユーザ装置ごとに当該ユーザ装置の第１の無線通信網における識別子（ＩＰアドレスなどの第１識別子）を記憶しており、解析手段は、管理手段を参照して攻撃検知情報から攻撃対象のユーザ装置を特定する、ことが好ましい。監視装置が攻撃対象のユーザ装置の第１識別子を解析手段に送信する場合、解析手段は第１識別子からユーザ装置を特定できる。
【００２１】
また、本発明において、管理手段は、ユーザ装置ごとに、ユーザ装置の第２の無線通信網における識別子（携帯電話番号などの第２識別子）を記憶しており、通知手段は、攻撃対象として特定されたユーザ装置に対して、第２の無線通信網を介した通信によって通知を行う、ことが好ましい。このようにすれば、解析手段によって特定されたユーザ装置に対して、第２の無線通信網を介して通知を送れる。なお、第２識別子が、携帯電話網における携帯電話番号のように、ほぼ固定のものである場合には、管理手段は、第２識別子によってユーザ装置を特定することができる。したがって、管理手段は、第１識別子と第２識別子とを関連付けて記憶するようにしてもよい。
【００２２】
また、本発明において、管理手段は、ユーザ装置ごとに、当該ユーザ装置に関連する装置の第２識別子を記憶しており、通知手段は、攻撃対象として特定されたユーザ装置に関連する装置（以下、関連装置と称する）に対して、第２の無線通信網を介した通信によって通知を行う、ことも好ましい。このようにすれば、解析手段によって特定されたユーザ装置に対して、第２の無線通信網を介して通知を送れる。
【００２３】
関連装置は、通知手段からの通知を受けると、当該通知を受けた旨をユーザ装置に対して無線通信によって知らせることが好ましい。このようにすれば、関連装置を介してユー

ザ装置に攻撃の通知を行える。あるいは、関連装置は、それ自身がユーザに対して通知を行うように構成されてもよい。

【００２４】

本発明において、解析手段は、監視手段によって検知された攻撃が、同じ地域の複数台のユーザ装置を対象とする攻撃であるか否か判定してもよい。この場合、通知手段は、攻撃が同じ地域の複数台のユーザ装置を対象とする攻撃である場合には、通知を転送すべきことを表す情報を含めて通知を行うことが好ましい。ユーザ装置または関連装置は、通知を転送すべきことを表す情報を含む通知を受信した場合は、この通知を周囲のユーザ装置または関連装置に転送することが好ましい。ユーザ装置が車載装置である場合には、車車間通信を用いて通知を周囲のユーザ装置（車載装置）に送信することができる。

【００２５】

このようにすれば、通知手段から通知を受けたユーザ装置が周囲のユーザ装置に攻撃の通知を行える。したがって、通知手段と直接に通信が行えないユーザ装置にも通知を行えるようになる。

【００２６】

なお、この場合に、通知手段が通知を送るユーザ装置は、現に攻撃を受けているユーザ装置、すなわち攻撃対象地域に位置するユーザ装置に限る必要はなく、その周囲に位置するユーザ装置に通知を行ってもよい。攻撃を受ける前に通知を送ることで、対象エリアに進入する前あるいは進入した直後から攻撃に対する対策を取ることができるようになる。

【００２７】

本発明において、ユーザ装置は、車両に備え付けられた車載装置とすることができる。また、ユーザ装置に関連する装置（関連装置）は、同じ車両内に存在する携帯情報端末とすることができる。同じ車両内に存在すれば、この車両の車載装置や運転者に対して通知を行うことができる。

【００２８】

なお、本発明は、上記手段の少なくとも一部を備える攻撃通知システムとして捉えることもできる。本発明は、また、上記処理の少なくとも一部を実行する攻撃通知方法として捉えることができる。また、本発明は、この方法をコンピュータに実行させるためのコンピュータプログラム、あるいはこのコンピュータプログラムを非一時的に記憶したコンピュータ可読記憶媒体として捉えることもできる。上記手段および処理の各々は可能な限り互いに組み合わせて本発明を構成することができる。

【００２９】

例えば、本発明の一態様は、第１の無線通信網と第２の無線通信網のいずれを用いてもサーバ装置と通信可能なユーザ装置に対して攻撃されていることまたは攻撃されかけていることを通知する攻撃通知システムが行う攻撃通知方法であって、

第１の無線通信網のトラフィックを監視して攻撃を検知する監視ステップと、

前記監視ステップにおいて検知された攻撃の対象のユーザ装置を特定する解析ステップと、

前記解析ステップにおいて特定されたユーザ装置または当該ユーザ装置に関連する装置に対して、前記第２の無線通信網を介した通信によって通知を行う通知ステップと、

を含むことを特徴とする。

【発明の効果】

【００３０】

本発明によれば、個々の車両を対象とした攻撃だけでなく、ネットワーク全体を対象とした攻撃についても、攻撃を防ぎ、かつ、攻撃されていることを通知することができる。

【図面の簡単な説明】

【００３１】

【図１】第１の実施形態に係る攻撃検知システムの構成を示す図。

【図２】第１の実施形態における車載機の認証に関する処理を示すフローチャート。

【図３】第１の実施形態における認証データ記憶部のテーブル構成を示す図。

【図４】第１の実施形態におけるトラフィック監視装置が攻撃を検知したときの処理を示すフローチャート。
【図５】第２の実施形態に係る攻撃検知システムの構成を示す図。
【図６】第２の実施形態における認証データ記憶部のテーブル構成を示す図。
【図７】第２の実施形態におけるトラフィック監視装置が攻撃を検知したときの処理を示すフローチャート。
【図８】第３の実施形態に係る攻撃検知システムの構成を示す図。
【発明を実施するための形態】
【００３２】
（第１の実施形態）
図１は、本発明の第１の実施形態に係る攻撃検知システムの構成を示す。攻撃検知システムは、サーバ装置１０と、車両２０に搭載された車載機（車載無線通信装置）２１から構成される。車載機２１は、無線ＬＡＮ通信機と携帯電話通信機（いずれも不図示）を有し、公衆無線ＬＡＮ３１を介しても、携帯電話網３２を介してもサーバ装置１０と通信可能である。車載機２１は、公衆無線ＬＡＮ３１を利用する場合には無線基地局（アクセスポイント）３１ａを介してサーバ装置１０と通信し、携帯電話網３２を利用する場合には携帯基地局３２ａを介してサーバ装置１０と通信する。公衆無線ＬＡＮ３１および携帯電話網３２のいずれを用いた通信も、その中間に専用網３３が介在する。
【００３３】
なお、以下の説明では、記載の簡略化のために、車両２０とそれに搭載されている車載機２１とを区別せずに交換可能な意味で用いることもある。例えば、車両２０が通信すると表現したり、車載機２１が移動すると表現したりすることがある。
【００３４】
ここで、公衆無線ＬＡＮ３１は、比較的攻撃対象となりやすく、悪意のある攻撃者４０は公衆無線ＬＡＮ３１を介して個々の車載機２１を対象として攻撃したり、公衆無線ＬＡＮ３１全体を対象として攻撃をすることが想定される。本実施形態は、このような攻撃を検知して確実に車載機２１に通知することで、車載機２１が攻撃に対して対処できるようにする。
【００３５】
サーバ装置１０は、ＣＰＵなどの演算プロセッサ、ＲＡＭなどの主記憶装置、ＨＤＤやＳＳＤやＤＶＤ－ＲＯＭ等の補助記憶装置、有線あるいは無線の通信装置、キーボードやマウスなどの入力装置、ディスプレイなどの表示装置を含むコンピュータとして構成することができる。サーバ装置１０は、必ずしも１台のコンピュータから構成される必要はなく、複数台のコンピュータが連携することによって以下で説明する機能が実現されてもよい。
【００３６】
サーバ装置１０は、図１に示すように、クライアント管理部１１、認証データ記憶部１２、データ解析部１３、監視結果通知部１４として機能する。これらの各機能は、サーバ装置１０の演算プロセッサがオペレーティングシステム（ＯＳ）やアプリケーションプログラムを実行することによって実現される。また、サーバ装置１０は、公衆無線ＬＡＮ３１を介した車載機２１あるいはネットワーク全体を対象とする攻撃を検知するトラフィック監視装置１５から監視結果を取得可能に構成される。
【００３７】
これらの各機能部の一部は、異なるコンピュータによって実現されても構わない。例えば、クライアント管理部１１の実質的な機能は、サーバ装置１０とは異なるサーバ（ホームエージェント）によって実現され、サーバ装置１０はホームエージェント等からクライアント装置に関する情報を取得するように構成してもよい。
【００３８】
トラフィック監視装置１５は、公衆無線ＬＡＮ３１を介した車載機２１あるいはネットワーク全体を対象とする攻撃を検知する装置である。トラフィック監視装置１５は、無線

基地局３１ａあるいはその上位のネットワーク中継機器に設けられる。トラフィック監視装置１５は、例えば、トラフィック負荷の計測や通信パケットの中身を解析することによって、攻撃を検知できる。ただし、本実施形態では攻撃の検知手法は特に限定されず、既存の任意の手法を利用することができる。

【００３９】

以下、図２～図４を参照して、各機能部によって行われる処理を、より詳細に説明する。

【００４０】

図２は、車載機２１の認証に関する処理を示すフローチャートである。ステップＳ１１において、車載機２１は、公衆無線ＬＡＮ３１や携帯電話網３２の基地局を跨がって走行すると、接続している基地局の情報（ＩＤ）、自端末の情報をサーバ装置１０のクライアント管理部１１に送信する。ここで、車載機２１の情報には、動的に割り当てられたＩＰアドレス、ＭＡＣアドレス、車体識別番号、パスワードなどが含まれる。

【００４１】

クライアント管理部１１は、ステップＳ１２において、車載機２１から送信された情報を受信し、ステップＳ１３において、受信した情報に基づいて車載機２１の認証を行う。認証に成功した場合（Ｓ１４－ＹＥＳ）には、クライアント管理部１１は、車載機２１に対して認証完了を通知すると共に、車載機２１に関するデータを認証データ記憶部１２に蓄積する（Ｓ１５）。認証完了通知を受けた車載機２１は、ハンドオーバー（収容基地局の変更）が発生する度に、自端末の情報をサーバ装置１０のクライアント管理部１１に送信する。この際、認証処理は既に完了しているので、車載機２１は、ハンドオーバー前の基地局情報および気付ＩＰアドレスと、ハンドオーバー後（現在）の基地局情報および気付ＩＰアドレスを送信すればよい。

【００４２】

一方、ステップＳ１３において認証に失敗した場合（Ｓ１４－ＮＯ）は、クライアント管理部１１は、車載機２１に対して認証失敗を通知する（Ｓ１６）。認証に失敗した場合には、ステップＳ１１に戻って認証処理を再度行う。認証の失敗回数が所定回数を超えた場合には、サーバ装置１０は認証処理を終了する。上記の所定回数は１以上の任意の値としてよい。

【００４３】

図３は、本実施形態における認証データ記憶部１２のテーブル構成を示す図である。認証データ記憶部１２は、車体識別番号１２１、無線基地局ＩＤ１２２、無線ＬＡＮ気付ＩＰアドレス１２３、携帯基地局ＩＤ１２４、車載機電話番号１２５を記憶する。車体識別番号１２１は、車両を識別するための情報であり、車両ごとにユニーク（一意）なものである。無線基地局ＩＤ１２２は、車載機２１が収容されている無線ＬＡＮ基地局３１ａのＩＤである。無線ＬＡＮ気付ＩＰアドレス１２３は、車載機２１が収容されている無線ＬＡＮ３１において車載機２１に動的に割り当てられているＩＰアドレスである。携帯基地局ＩＤ１２４は、車載機２１が収容されている携帯基地局３２ａのＩＤである。車載機電話番号１２５は、車載機２１の携帯電話番号である。

【００４４】

認証データ記憶部１２に記憶される無線基地局ＩＤ１２２、無線ＬＡＮ気付ＩＰアドレス１２３、携帯基地局ＩＤ１２４は、車両２０の移動に伴い更新される。一方、車体識別版後１２１および車載機電話番号１２５は固定である。

【００４５】

図４は、トラフィック監視装置１５が攻撃を検知したときの処理を示すフローチャートである。トラフィック監視装置１５は、無線ＬＡＮ３１のトラフィックを監視して、攻撃を検知する（Ｓ２１）。ここで、攻撃の検知には、攻撃が現に行われていることを検知することと、攻撃がこれから行われることを検知することの両方が含まれる。また、トラフィック監視装置１５は、個々のユーザ装置を対象とする攻撃と、ネットワーク全体を対象とする攻撃のいずれも検知可能である。上述したように、トラフィック監視装置１５によ

る、攻撃検知手法は特に限定されない。

【００４６】

攻撃を検知すると、トラフィック監視装置１５は、攻撃検知情報をサーバ装置１０のデータ解析部１３に送信する（Ｓ２２）。送信される攻撃検知情報には、攻撃対象の車載機２１の気付ＩＰアドレス、無線基地局のＩＤ、攻撃元装置のＩＰアドレス、攻撃の種別、攻撃の履歴などが含まれる。攻撃対象が個々の車両である場合には、攻撃検知情報には攻撃対象の車両の気付ＩＰアドレスがあればよく、当該車両を収容している無線基地局のＩＤは省略可能である。また、攻撃対象がネットワーク全体である場合には、攻撃検知情報には攻撃されている無線基地局のＩＤがあればよく、攻撃によって影響を受ける車載機２１（攻撃対象の無線基地局が収容している車載機２１）の気付ＩＰアドレスは省略可能である。

【００４７】

サーバ装置１０のデータ解析部１３は、トラフィック監視装置１５から攻撃検知情報を受信すると（Ｓ２３）、攻撃対象車両の車体識別番号を特定する（Ｓ２４）。攻撃対象車両の車体識別番号は、攻撃検知情報に含まれる気付ＩＰアドレスを用いて認証データ記憶部１２を検索することによって取得可能である。なお、攻撃対象がネットワーク全体である場合には、ここで特定する車体識別番号は、攻撃によって影響を受ける車両のものとすればよい。例えば、データ解析部１３は、攻撃されている無線基地局に収容されている車両の車体識別番号を取得する。

【００４８】

次に、攻撃対象の車両に対して、監視結果通知部１４が、攻撃されているという警告を通知する（Ｓ２５）。この通知は、公衆無線ＬＡＮ３１経由ではなく、比較的セキュアな携帯電話網３２を経由してプッシュ通知によって行う。そのため、監視結果通知部１４は、認証データ記憶部１２を参照して、通知対象車両が使用している携帯電話網３２の基地局のＩＤや車載機２１のアドレス（携帯電話番号）を取得する。監視結果通知部１４が送信する情報には、攻撃元のＩＰアドレスや、攻撃の種別、攻撃の履歴などが含まれる。

【００４９】

なお、サーバ装置１０は、プッシュ通知を送るために必ずしも車載機２１の携帯電話番号を知っている必要はなく、デバイストークンや登録ＩＤなどのプッシュ通知を行うための車載機２１の識別子を知っていればよい。

【００５０】

車載機２１は、携帯電話網３２のプッシュ通知によって攻撃通知を受信すると（Ｓ２６）、攻撃に対する対策を実施する（Ｓ２７）。攻撃に対する対策は、攻撃による悪影響を回避できるものであれば特に限定されないが、例えば、攻撃元（ＩＰアドレス）からのパケットをフィルタリングしたり、サーバ装置１０との通信経路を公衆無線ＬＡＮ３１から携帯電話網３２のみに切り替えたりすることが考えられる。

【００５１】

本実施形態によれば、個々の車両を対象とした攻撃であっても公衆無線ＬＡＮ全体を対象とした攻撃であっても、攻撃の影響を受ける車両（車載機）に対して攻撃を受けていることを通知できる。専用網３３および携帯電話網３２はいずれも通信品質管理がされており、攻撃によるリソース飽和等がおきにくく、サーバ装置１０から車載機２１に確実に通知が行えるためである。さらに、車載機２１は、攻撃の通知を受けて、フィルタリングや通信路切替などの対策を取って、攻撃による悪影響を防止できる。

【００５２】

（第２の実施形態）

本発明の第２の実施形態は、基本的に第１の実施形態と同様であるが、車両２０のユーザが有するスマートフォン端末２２を介して攻撃通知を送る点で異なる。以下、主に第１の実施形態と異なる点について説明する。

【００５３】

図５は、本発明の第２の実施形態に係る攻撃検知システムの構成を示す図である。スマ

ートフォン端末２２は、車載機２１とＢｌｕｅｔｏｏｈ（登録商標）やＢＬＥ通信などによって接続可能である。なおここでは、スマートフォン端末を利用する例を説明するが、スマートフォン端末の代わりに、ウェアラブル端末やタブレット型コンピュータを利用してもかまわない。

【００５４】

図６は、本実施形態における認証データ記憶部１２のテーブル構成を示す図である。本実施形態では、スマートフォン端末２２を介して攻撃通知を送るために、スマートフォン気付ＩＰアドレス１２６とスマートフォン電話番号１２７が認証データ記憶部１２に格納される。これらの情報は、認証処理（図２）の際に車載機２１からクライアント管理部１１に送信されてもよいし、その他のタイミングで送信されてもよい。車載機２１と接続されているスマートフォン端末２２の電話番号およびステータス情報（接続中・切断中など）は、認証処理以外の任意のタイミングで車載機２１からクライアント管理部１１に通知することも好ましい。

【００５５】

図７は、本実施形態における、トラフィック監視装置１５が攻撃を検知したときの処理を示すフローチャートである。トラフィック監視装置１５が攻撃を検知してからサーバ装置１０が攻撃対象車両の車体識別番号を特定するまでの処理（Ｓ２１～Ｓ２４）は、第１の実施形態と同様である。

【００５６】

本実施形態では、データ解析部１３は、攻撃対象の車両と接続中のスマートフォン端末（関連端末）２２を、認証データ記憶部１２を参照して特定する（Ｓ３１）。そして、特定されたスマートフォン端末２２に対して、監視結果通知部１４が、攻撃されているという警告を通知する（Ｓ３２）。

【００５７】

スマートフォン端末２２は、攻撃通知を受信すると（Ｓ３３）、ＢＬＥ通信などによりその旨を車載機２１に対して通知（転送）する。車載機２１が攻撃通知を受信した後の処理（Ｓ２６およびＳ２７）は第１の実施形態と同様である。

【００５８】

本実施形態によれば、スマートフォン端末２２を経由して攻撃通知を送信しているので、車載機２１に負荷がかかっている場合でも通知を行える。例えば、攻撃者が公衆無線ＬＡＮ３１を介して攻撃によって車載機２１の無線ＬＡＮ通信処理部に対して負荷をかける攻撃をした場合でも、車載機２１はＢＬＥ等の通信によってスマートフォン端末２２から通知を受けることができるので、確実な攻撃通知が行える。

【００５９】

なお、上記の説明では、スマートフォン端末２２が車載機２１に攻撃通知をしているが、その代わりにあるいはそれと同時に、スマートフォン端末２２がユーザに対して攻撃通知をするようにしてもよい。攻撃通知に気がついたユーザが、車載機２１の通信経路を公衆無線ＬＡＮ３１から携帯電話網３２のみに切り替えるなどを対処をとることができる。

【００６０】

また、サーバ装置１０が通知を行う対象のスマートフォン端末２２は、車載機２１と必ずしも通信が接続していなくてもかまわない。例えば、車両２０の運転者が所有しているスマートフォン端末に対して、車載機２１との接続確立に関係なく通知を行ってもよい。この際、車両２０（車載機２１）の位置とスマートフォン端末２２の位置が同一であるということを条件として、スマートフォン端末２２に攻撃通知を送信してもよい。

【００６１】

（第３の実施形態）

本発明の第３の実施形態は、基本的に第１の実施形態あるいは第２の実施形態と同様であるが、車載機２１が周囲の車両５０に対して攻撃通知を転送する点で異なる。以下、主に第１，２の実施形態と異なる点について説明する。

【００６２】

図５は、本発明の第２の実施形態に係る攻撃検知システムの構成を示す図である。車載機２０は、サーバ装置１０から直接あるいはスマートフォン端末２２を介して攻撃通知を受け取ると、車車間通信によって攻撃通知をブロードキャスト送信する。

【００６３】

この際、車載機２１は、攻撃通知を受信した際に常にブロードキャスト送信によって攻撃通知を送信してもよいし、所定の条件を満たす場合のみに攻撃通知を送信してもよい。例えば、攻撃通知の内容から、特定のエリアを走行する多数の車両が攻撃対象であると判断できる場合に、ブロードキャスト送信することが考えられる。あるいは、この判断はサーバ装置１０で行って、ブロードキャスト送信が必要であるか否かという情報を攻撃通知に含めて送信するようにしてもよい。また、車載機２１は、攻撃元装置が含まれる公衆無線ＬＡＮ３１の基地局と接続が維持されている間（該当エリアを走行中のとき）あるいは該当エリアの近傍を走行しているときのみブロードキャスト送信したり、攻撃対象車両を検知したときのみブロードキャスト送信したりするようにしてもよい。

【００６４】

本実施形態によれば、車車間通信を活用して、広範囲に攻撃兆候を通知することができる。また、携帯電話通信機能を有していない車載機に対しても攻撃予兆を通知することができる。

【００６５】

（変形例）

上記の説明では、公衆無線ＬＡＮ３１と携帯電話網３２の２つの無線通信網を介して車載機２１がサーバ装置１０と通信可能としたが、本発明において利用可能な無線通信網はこれらに限られず、任意の無線通信網を利用してかまわない。ただし、第１の無線通信網は、攻撃対象となりやすい無線通信網であり、第２の無線通信網は、攻撃を受けにくく通信品質が確保された無線通信網であることが望ましい。もっとも、第１の無線通信網および第２の無線通信網の両方が攻撃を受けやすい無線通信網であっても、攻撃通知が車載機２１まで到達できる確実性が向上するという効果が得られる。

【００６６】

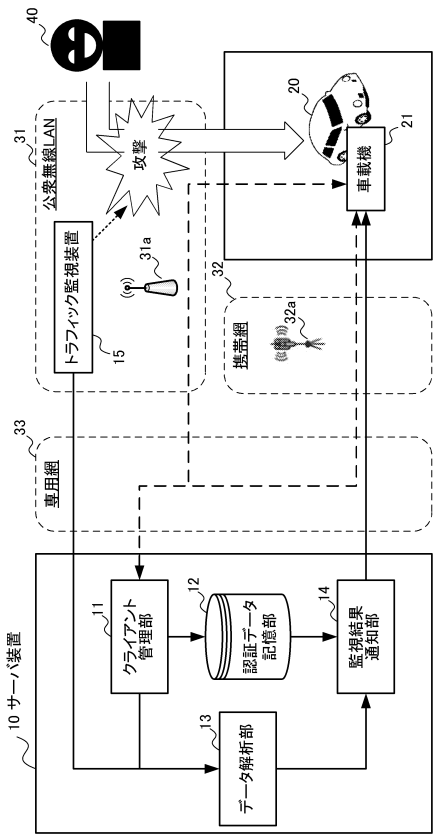
また、上記の説明では車両無線ネットワークを例に挙げているが、車両あるいは車載機以外の無線通信装置を用いてもかまわない。例えば、スマートフォン端末、移動型ロボット、ＩｏＴ（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇｓ）機器、ドローン（無人航空機）などを対象として攻撃検知を通知するようにしてもかまわない。

【符号の説明】

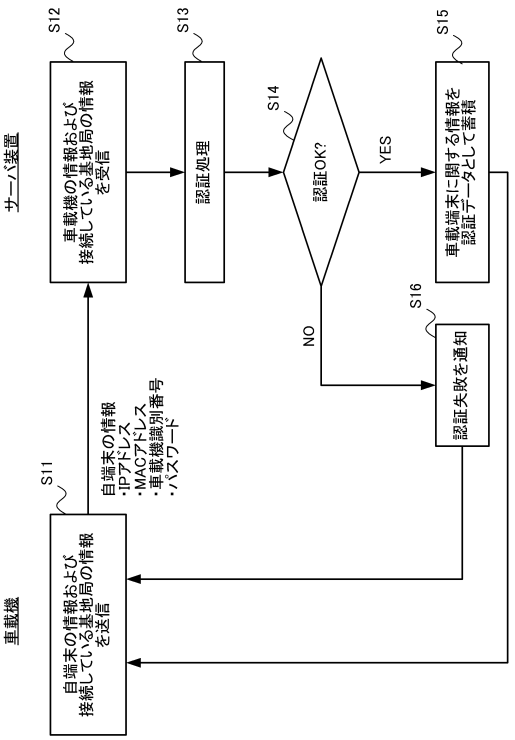
【００６７】

１０：サーバ装置
１１：クライアント管理部
１２：認証データ記憶部
１３：データ解析部
１４：監視結果通知部
１５：トラフィック監視装置
２０：車両
２１：車載機
２２：スマートフォン端末

【図１】



【図２】

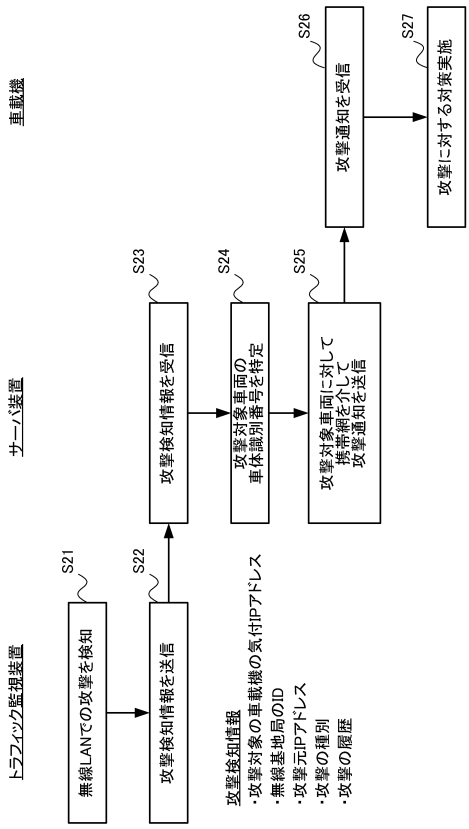


【図３】

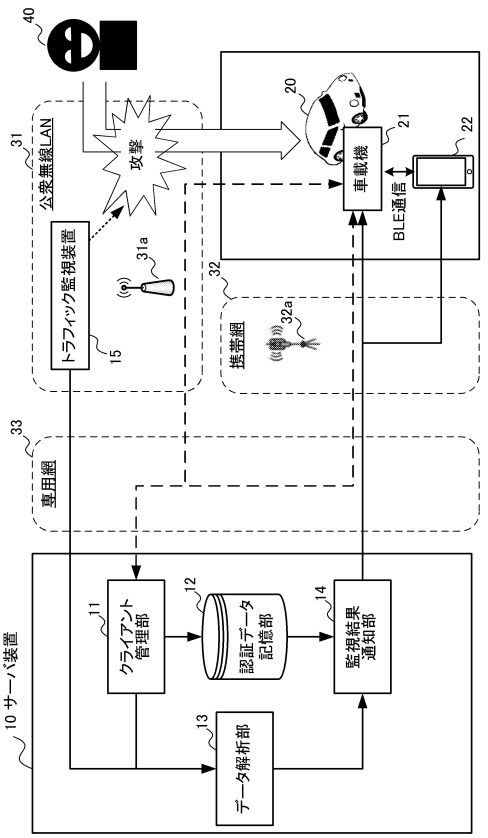
	項目	詳細
121	車体識別番号	車両の識別子。車両ごとにユニーク。
122	無線基地局ID	車両が収容されている無線LAN基地局のID。移動中に変化する。
123	無線LAN気付IPアドレス	車両が収容されている無線LANで動的に割り当てられているIPアドレス。移動中に変化する。
124	携帯網基地局ID	車両が収容されている携帯基地局のID。移動中に変化する。
125	車載機電話番号	車載機の携帯電話番号。

12

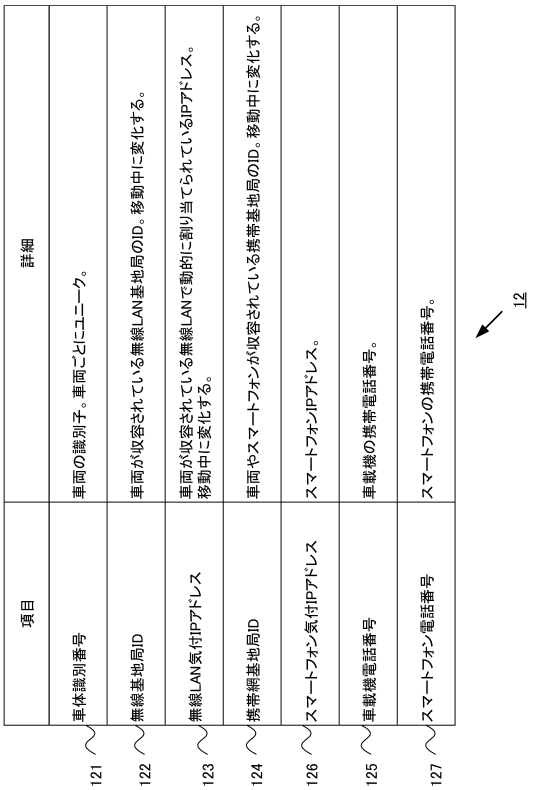
【図４】



【図５】



【図６】

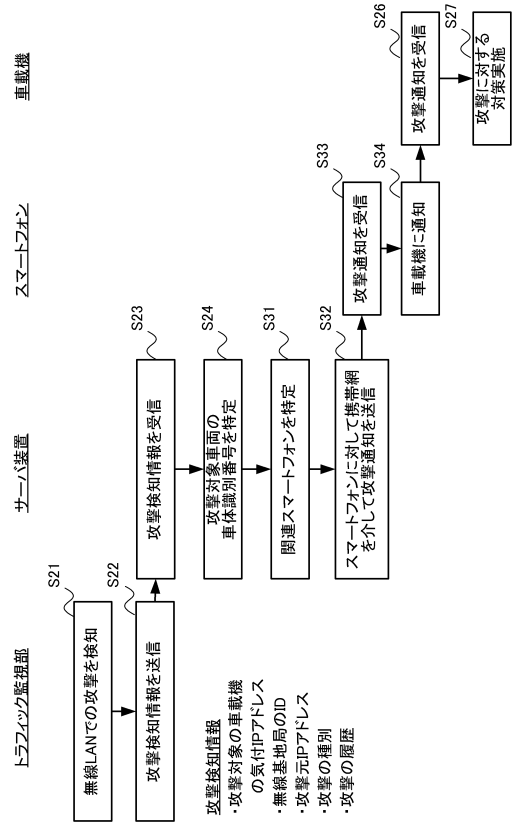


項目	詳細
車体識別番号	車両の識別子。車両ごとにユニーク。
無線基地局ID	車両が収容されている無線LAN基地局のID。移動中に変化する。
無線LAN気付IPアドレス	車両が収容されている無線LANで動的に割り当てられているIPアドレス。移動中に変化する。
携帯網基地局ID	車両やスマートフォンが収容されている携帯基地局のID。移動中に変化する。
スマートフォン気付IPアドレス	スマートフォンIPアドレス。
車載機電話番号	車載機の携帯電話番号。
スマートフォン電話番号	スマートフォンの携帯電話番号。

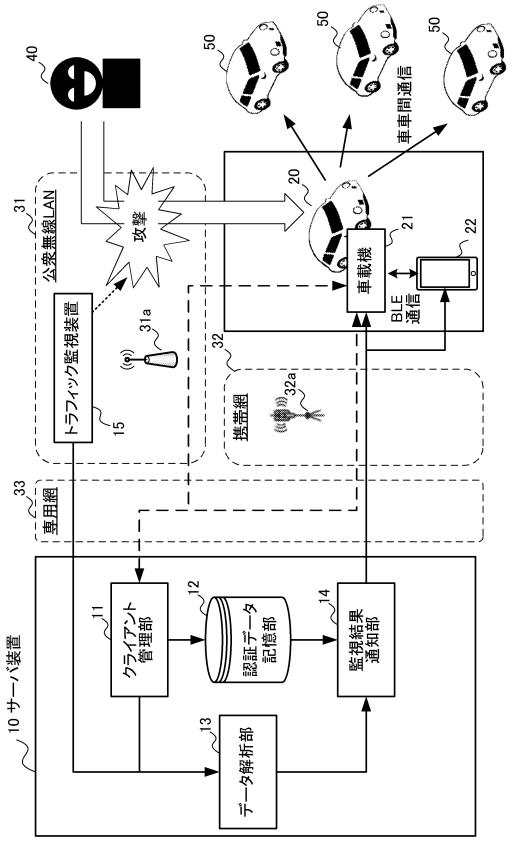
121 122 123 124 126 125 127

12

【図７】



【図８】



フロントページの続き

(74)代理人 100138357
弁理士 矢澤 広伸
(74)代理人 100176201
弁理士 小久保 篤史
(72)発明者 遠藤 俊樹
東京都港区赤坂６丁目６番２０号 株式会社トヨタＩＴ開発センター内
(72)発明者 西山 隆文
愛知県豊田市トヨタ町１番地 トヨタ自動車株式会社内

審査官 宮司 卓佳

(56)参考文献 特開２００４－３５６９１５（ＪＰ，Ａ）
国際公開第２０１６／０３１３８４（WO，Ａ１）
特開２０１５－１３６１０７（ＪＰ，Ａ）
特開平０９－１８００９８（ＪＰ，Ａ）
特開２０１６－１３４１７０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／５５
Ｈ０４Ｂ ７／２４
Ｈ０４Ｗ １２／１２