(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6828632号
(P6828632)

(45)発行日　令和3年2月10日(2021.2.10)　(24)登録日　令和3年1月25日(2021.1.25)

(51)Int.Cl.			F I		
H04L	12/28	(2006.01)	H04L	12/28	200M
H04L	9/32	(2006.01)	H04L	9/00	673B
H04L	12/40	(2006.01)	H04L	12/40	M
B60R	16/023	(2006.01)	B60R	16/023	P

請求項の数 6　(全 27 頁)

(21)出願番号　特願2017-150771(P2017-150771)
(22)出願日　平成29年8月3日(2017.8.3)
(65)公開番号　特開2019-29960(P2019-29960A)
(43)公開日　平成31年2月21日(2019.2.21)
審査請求日　令和2年2月21日(2020.2.21)

(73)特許権者　000002130
住友電気工業株式会社
大阪府大阪市中央区北浜四丁目５番３３号
(73)特許権者　000183406
住友電装株式会社
三重県四日市市西末広町１番１４号
(73)特許権者　395011665
株式会社オートネットワーク技術研究所
三重県四日市市西末広町１番１４号
(74)代理人　110000682
特許業務法人ワンディーＩＰパートナーズ
(72)発明者　濱田　芳博
大阪府大阪市中央区北浜四丁目５番３３号
住友電気工業株式会社内

最終頁に続く

(54)【発明の名称】検知装置、検知方法および検知プログラム

(57)【特許請求の範囲】
【請求項１】
差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置であって、
前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、
前記バスにおける通信エラーを監視する監視部と、
前記監視部の監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計する集計部と、
前記集計部の集計結果に基づいて前記攻撃を検知する検知部とを備え、
前記検知部は、前記通信エラーの発生回数の前記識別情報ごとの合計、および前記通信エラーの発生した前記識別情報の数であるエラーＩＤ数に基づいて前記攻撃を検知する、検知装置。
【請求項２】
前記検知部は、前記集計結果における各前記識別情報間での通信エラーの発生状況の偏りに基づいて前記攻撃を検知する、請求項１に記載の検知装置。
【請求項３】
前記検知部は、第１の監視間隔における前記合計と第１のしきい値との第１の比較結果および前記エラーＩＤ数と第２のしきい値との第２の比較結果、ならびに複数の前記第１の監視間隔からなる第２の監視間隔における前記合計と第３のしきい値との第３の比較結果および前記エラーＩＤ数の平均と第４のしきい値との第４の比較結果の少なくともいず

れか一方に基づいて前記攻撃を検知する、請求項１に記載の検知装置。
【請求項４】
前記検知部は、前記第１の比較結果、前記第２の比較結果および前記エラーＩＤ数と前記第２のしきい値より大きい第５のしきい値との比較結果、ならびに前記第３の比較結果、前記第４の比較結果および前記平均と前記第４のしきい値より大きい第６のしきい値との比較結果の少なくともいずれか一方に基づいて前記攻撃を検知する、請求項３に記載の検知装置。
【請求項５】
差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置における検知方法であって、
前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、
前記バスにおける通信エラーを監視するステップと、
監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計するステップと、
集計結果に基づいて前記攻撃を検知するステップとを含み、
前記攻撃を検知するステップでは、前記通信エラーの発生回数の前記識別情報ごとの合計、および前記通信エラーの発生した前記識別情報の数であるエラーＩＤ数に基づいて前記攻撃を検知する、検知方法。
【請求項６】
差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置において用いられる検知プログラムであって、
前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、
コンピュータを、
前記バスにおける通信エラーを監視する監視部と、
前記監視部の監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計する集計部と、
前記集計部の集計結果に基づいて前記攻撃を検知する検知部、
として機能させるためのプログラムであり、
前記検知部は、前記通信エラーの発生回数の前記識別情報ごとの合計、および前記通信エラーの発生した前記識別情報の数であるエラーＩＤ数に基づいて前記攻撃を検知する、検知プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、検知装置、検知方法および検知プログラムに関する。
【背景技術】
【０００２】
従来、車載ネットワークにおけるセキュリティを向上させるための車載ネットワークシステムが開発されている。
【０００３】
たとえば、特許文献１（特開２０１６－１１６０７５号公報）には、以下のような車載通信システムが開示されている。すなわち、車載通信システムは、通信データの送信側が生成するメッセージ認証コードである送信側コードと、前記通信データの受信側が生成するメッセージ認証コードである受信側コードとを使用してメッセージ認証を行う車載通信システムであって、車載ネットワークに接続され、第１の暗号鍵と前記第１の暗号鍵とは異なる第２の暗号鍵のうち前記第１の暗号鍵だけを保持する第１のＥＣＵと、前記車載ネットワークに接続され、前記第１の暗号鍵を少なくとも保持する第２のＥＣＵと、前記車

載ネットワーク及び車外ネットワークに接続され、前記第１の暗号鍵と前記第２の暗号鍵のうち前記第２の暗号鍵だけを保持して、前記第２の暗号鍵を使用して前記車載ネットワークにおける通信時に前記送信側コード又は前記受信側コードを生成する第３のＥＣＵとを備え、前記第２のＥＣＵは、前記第１の暗号鍵を使用して生成した送信側コードを付与した通信データを送信し、前記第１のＥＣＵは、前記通信データを受信した場合に、前記第１の暗号鍵を使用して生成した受信側コードによって、前記受信した通信データに付与された送信側コードの検証を行う。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０１６－１１６０７５号公報

【特許文献２】特開２０１６－９７８７９号公報

【特許文献３】特開２０１５－１３６１０７号公報

【非特許文献】

【０００５】

【非特許文献１】ルネサス　エレクトロニクス株式会社、”ＣＡＮ入門書　Ｒｅｖ．　１．００”、［ｏｎｌｉｎｅ］、［平成２９年６月１７日検索］、インターネット〈ＵＲＬ：ｈｔｔｐｓ：／／ｗｗｗ．ｒｅｎｅｓａｓ．ｃｏｍ／ｊａ－ｊｐ／ｄｏｃ／ｐｒｏｄｕｃｔｓ／ｍｐｕｍｃｕ／ａｐｎ／００３／ｒｊｊ０５ｂ０９３７＿ｃａｎａｐ．ｐｄｆ〉

【非特許文献２】Ｋ．　Ｃｈｏ、外１名、「Ｅｒｒｏｒ　Ｈａｎｄｌｉｎｇ　ｏｆ　Ｉｎ－ｖｅｈｉｃｌｅ　Ｎｅｔｗｏｒｋｓ　Ｍａｋｅｓ　Ｔｈｅｍ　Ｖｕｌｎｅｒａｂｌｅ」、ＣＣＳ　’１６　Ｐｒｏｃｅｅｄｉｎｇｓ　ｏｆ　ｔｈｅ　２０１６　ＡＣＭ　ＳＩＧＳＡＣ　Ｃｏｎｆｅｒｅｎｃｅ　ｏｎ　Ｃｏｍｐｕｔｅｒ　ａｎｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｓｅｃｕｒｉｔｙ、Ｐ．１０４４－１０５５

【非特許文献３】亀岡　良太、外５名、「ラズベリーパイからのスタッフエラー注入によるＣＡＮ　ＥＣＵへのバスオフ攻撃」、２０１７　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｃｒｙｐｔｏｇｒａｐｈｙ　ａｎｄ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ、１Ｅ２－２

【非特許文献４】中山　淑文、外３名、「車載ＣＡＮバスにおける電気的データ改竄の効果」、２０１７　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｃｒｙｐｔｏｇｒａｐｈｙ　ａｎｄ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ、１Ｅ２－３

【発明の概要】

【発明が解決しようとする課題】

【０００６】

特許文献１に記載の車載通信システムでは、車載ネットワークに限定して接続される第１のＥＣＵおよび第２のＥＣＵがメッセージ認証に用いる第１の暗号鍵と、車載ネットワークおよび車外ネットワークの両方に接続される第３のＥＣＵが用いる第２の暗号鍵とが異なることにより、車外ネットワークに接続されない第１のＥＣＵおよび第２のＥＣＵに対する車外ネットワークからのサイバー攻撃を防いでいる。

【０００７】

しかしながら、たとえば、各ＥＣＵ間を接続するバスにおいて伝送される信号を電気的に操作するようなサイバー攻撃に対しては、上記のようなセキュリティ対策が無効化されることがある。

【０００８】

このような攻撃を受けた場合において、車載ネットワークにおける攻撃を精度よく検知するための技術が求められる。

【０００９】

この発明は、上述の課題を解決するためになされたもので、その目的は、車載ネットワークにおける攻撃を精度よく検知することが可能な検知装置、検知方法および検知プログラムを提供することである。

【課題を解決するための手段】

【００１０】
（１）上記課題を解決するために、この発明のある局面に係わる検知装置は、差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置であって、前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、前記バスにおける通信エラーを監視する監視部と、前記監視部の監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計する集計部と、前記集計部の集計結果に基づいて前記攻撃を検知する検知部とを備える。
【００１１】
（６）上記課題を解決するために、この発明のある局面に係わる検知方法は、差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置における検知方法であって、前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、前記バスにおける通信エラーを監視するステップと、監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計するステップと、集計結果に基づいて前記攻撃を検知するステップとを含む。
【００１２】
（７）上記課題を解決するために、この発明のある局面に係わる検知プログラムは、差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置において用いられる検知プログラムであって、前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、コンピュータを、前記バスにおける通信エラーを監視する監視部と、前記監視部の監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計する集計部と、前記集計部の集計結果に基づいて前記攻撃を検知する検知部、として機能させるためのプログラムである。
【００１３】
本発明は、このような特徴的な処理部を備える検知装置として実現することができるだけでなく、検知装置を備える車載通信システムとして実現することができる。また、本発明は、検知装置の一部または全部を実現する半導体集積回路として実現することができる。
【発明の効果】
【００１４】
本発明によれば、車載ネットワークにおける攻撃を精度よく検知することができる。
【図面の簡単な説明】
【００１５】
【図１】図１は、本発明の実施の形態に係る車載通信システムの構成を示す図である。
【図２】図２は、本発明の実施の形態に係る車載通信システムにおける車載ネットワークにおいて伝送されるデータフレームの一例を示す図である。
【図３】図３は、本発明の実施の形態に係る車載通信システムにおける車載ネットワークにおいて伝送されるデータフレームの一例を示す図である。
【図４】図４は、本発明の実施の形態に係る車載通信システムにおけるトランシーバの状態遷移の一例を示す図である。
【図５】図５は、本発明の実施の形態に係る車載ネットワークにおける攻撃を説明するための図である。
【図６】図６は、本発明の実施の形態に係る車載ネットワークにおける電気的データ改ざん攻撃を説明するための図である。
【図７】図７は、本発明の実施の形態に係る車載通信システムにおけるゲートウェイ装置の構成を示す図である。
【図８】図８は、本発明の実施の形態に係るゲートウェイ装置において用いられる長監視間隔期間および短監視間隔期間の一例を示す図である。

【図９】図９は、本発明の実施の形態に係るゲートウェイ装置における集計部が作成する集計表の一例を示す図である。
【図１０】図１０は、本発明の実施の形態に係るゲートウェイ装置における集計部が作成する集計表の一例を示す図である。
【図１１】図１１は、本発明の実施の形態に係るゲートウェイ装置がサイバー攻撃を検知する際の動作手順を定めたフローチャートである。
【図１２】図１２は、本発明の実施の形態に係るゲートウェイ装置がサイバー攻撃を検知する際の動作手順を定めたフローチャートである。
【発明を実施するための形態】
【００１６】
最初に、本発明の実施形態の内容を列記して説明する。
【００１７】
（１）本発明の実施の形態に係る検知装置は、差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置であって、前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、前記バスにおける通信エラーを監視する監視部と、前記監視部の監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計する集計部と、前記集計部の集計結果に基づいて前記攻撃を検知する検知部とを備える。
【００１８】
このような構成により、識別情報ごとの通信エラーの発生状況の集計結果に基づいて、フレームの差出元または宛先の車載装置ごとの通信エラーの発生状況を認識することができるので、たとえば、バスにおいて伝送される信号を電気的に操作するようなサイバー攻撃を受けて通信エラーの発生した車載装置を、特定することができる。したがって、車載ネットワークにおける攻撃を精度よく検知することができる。
【００１９】
（２）好ましくは、前記検知部は、前記集計結果における各前記識別情報間での通信エラーの発生状況の偏りに基づいて前記攻撃を検知する。
【００２０】
このような構成により、各識別情報間での通信エラーの発生状況の偏りに基づいて、たとえば、車載ネットワークにおける各車載装置において満遍なく通信エラーが発生しているのか、または当該各車載装置のうちの特定の少数の車載装置に通信エラーが発生しているのかを認識することができる。これにより、たとえば、各車載装置において満遍なく通信エラーが発生している場合には電気的ノイズの影響も考慮して攻撃の検知を慎重に判断することができ、また、特定の少数の車載装置に通信エラーが発生している場合には、攻撃の可能性が高いと判断することができる。
【００２１】
（３）好ましくは、前記検知部は、前記通信エラーの発生回数の前記識別情報ごとの合計、および前記通信エラーの発生した前記識別情報の数であるエラーＩＤ数に基づいて前記攻撃を検知する。
【００２２】
このような構成により、たとえば、通信エラーの発生回数の多い車載装置に対して攻撃を受けたと判断しようとする場合において、通信エラーの発生した車載装置数を考慮することができるので、攻撃の有無をより正しく判断することができる。
【００２３】
（４）より好ましくは、前記検知部は、第１の監視間隔における前記合計と第１のしきい値との第１の比較結果および前記エラーＩＤ数と第２のしきい値との第２の比較結果、ならびに複数の前記第１の監視間隔からなる第２の監視間隔における前記合計と第３のしきい値との第３の比較結果および前記エラーＩＤ数の平均と第４のしきい値との第４の比較結果の少なくともいずれか一方に基づいて前記攻撃を検知する。
【００２４】

このような構成により、たとえば、第１の監視間隔における合計が第１のしきい値より大きい場合においても、エラーＩＤ数が第２のしきい値以上であるときには、電気的ノイズによって通信エラーが広範に発生していることが考えられるので、攻撃を誤って検知してしまうことを防ぐことができる。また、たとえば、第１の監視間隔における合計が第１のしきい値より大きく、かつエラーＩＤ数が第２のしきい値より小さいときには、特定の少数の車載装置において通信エラーが発生していることから、当該特定の少数の車載装置に対する攻撃をより正しく検知することができる。また、第２の監視間隔における合計が第３のしきい値より大きい場合においても、エラーＩＤ数の平均が第４のしきい値以上であるときには、電気的ノイズによって通信エラーが広範に発生していることが考えられるので、攻撃を誤って検知してしまうことを防ぐことができる。また、たとえば、第２の監視間隔における合計が第３のしきい値より大きく、かつエラーＩＤ数の平均が第４のしきい値より小さいときには、特定の少数の車載装置において通信エラーが発生していることから、当該特定の少数の車載装置に対する攻撃をより正しく検知することができる。

【００２５】

（５）より好ましくは、前記検知部は、前記第１の比較結果、前記第２の比較結果および前記エラーＩＤ数と前記第２のしきい値より大きい第５のしきい値との比較結果、ならびに前記第３の比較結果、前記第４の比較結果および前記平均と前記第４のしきい値より大きい第６のしきい値との比較結果の少なくともいずれか一方に基づいて前記攻撃を検知する。

【００２６】

たとえば、第１の監視間隔におけるエラーＩＤ数、および第２の監視間隔におけるエラーＩＤ数の平均の少なくともいずれか一方が極端に大きい場合、車載ネットワークにおける多数の車載装置に対して攻撃が行われていると考えられる。上記の構成により、車載ネットワークにおける各車載装置に対する一斉攻撃をより精度よく検知することができる。

【００２７】

（６）本発明の実施の形態に係る検知方法は、差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置における検知方法であって、前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、前記バスにおける通信エラーを監視するステップと、監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計するステップと、集計結果に基づいて前記攻撃を検知するステップとを含む。

【００２８】

このような構成により、識別情報ごとの通信エラーの発生状況の集計結果に基づいて、フレームの差出元または宛先の車載装置ごとの通信エラーの発生状況を認識することができるので、たとえば、バスにおいて伝送される信号を電気的に操作するようなサイバー攻撃を受けて通信エラーの発生した車載装置を、特定することができる。したがって、車載ネットワークにおける攻撃を精度よく検知することができる。

【００２９】

（７）本発明の実施の形態に係る検知プログラムは、差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置において用いられる検知プログラムであって、前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、コンピュータを、前記バスにおける通信エラーを監視する監視部と、前記監視部の監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計する集計部と、前記集計部の集計結果に基づいて前記攻撃を検知する検知部、として機能させるためのプログラムである。

【００３０】

このような構成により、識別情報ごとの通信エラーの発生状況の集計結果に基づいて、フレームの差出元または宛先の車載装置ごとの通信エラーの発生状況を認識することができるので、たとえば、バスにおいて伝送される信号を電気的に操作するようなサイバー攻撃を受けて通信エラーの発生した車載装置を、特定することができる。したがって、車載

ネットワークにおける攻撃を精度よく検知することができる。

【００３１】

以下、本発明の実施の形態について図面を用いて説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰り返さない。また、以下に記載する実施の形態の少なくとも一部を任意に組み合わせてもよい。

【００３２】

［構成および基本動作］

図１は、本発明の実施の形態に係る車載通信システムの構成を示す図である。

【００３３】

図１を参照して、車載通信システム３０１は、ゲートウェイ装置（検知装置）１０１と、複数の車載ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ）１２１とを備える。

【００３４】

車載通信システム３０１は、車両１に搭載される。車載ネットワーク１２は、車両１の内部における車載装置の一例である、複数の車載ＥＣＵ１２１およびゲートウェイ装置１０１を含む。

【００３５】

ゲートウェイ装置１０１には、バス１３Ａ，１３Ｂ，１３Ｃ，１３Ｄが接続される。以下、バス１３Ａ，１３Ｂ，１３Ｃ，１３Ｄの各々を、バス１３とも称する。

【００３６】

なお、ゲートウェイ装置１０１には、４つのバス１３が接続される構成に限らず、３つ以下または５つ以上のバス１３が接続されてもよい。

【００３７】

バス１３には、たとえば複数の車載ＥＣＵ１２１が接続される。バス１３は、たとえば、非特許文献１（ルネサス エレクトロニクス株式会社、”ＣＡＮ入門書 Ｒｅｖ．１．００”、［ｏｎｌｉｎｅ］、［平成２９年６月１７日検索］、インターネット〈ＵＲＬ：ｈｔｔｐｓ：／／ｗｗｗ．ｒｅｎｅｓａｓ．ｃｏｍ／ｊａ－ｊｐ／ｄｏｃ／ｐｒｏｄｕｃｔｓ／ｍｐｕｍｃｕ／ａｐｎ／００３／ｒｊｊ０５ｂ０９３７＿ｃａｎａｐ．ｐｄｆ〉）に記載のＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ Ａｒｅａ Ｎｅｔｗｏｒｋ）（登録商標）の規格に従うバスである。

【００３８】

なお、バス１３には、複数の車載ＥＣＵ１２１が接続される構成に限らず、１つの車載ＥＣＵ１２１が接続される構成であってもよい。また、バス１３は、ＦｌｅｘＲａｙ（登録商標）、ＭＯＳＴ（Ｍｅｄｉａ Ｏｒｉｅｎｔｅｄ Ｓｙｓｔｅｍｓ Ｔｒａｎｓｐｏｒｔ）（登録商標）、イーサネット（登録商標）、およびＬＩＮ（Ｌｏｃａｌ Ｉｎｔｅｒｃｏｎｎｅｃｔ Ｎｅｔｗｏｒｋ）等の規格に従うバスであってもよい。

【００３９】

車載ＥＣＵ１２１は、たとえば、ＴＣＵ（Ｔｅｌｅｍａｔｉｃｓ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｕｎｉｔ）、自動運転ＥＣＵ、エンジンＥＣＵ、センサ、ナビゲーション装置、ヒューマンマシンインタフェース、およびカメラ等である。

【００４０】

ゲートウェイ装置１０１は、バス１３を介して車載ＥＣＵ１２１と通信を行うことが可能である。ゲートウェイ装置１０１は、車両１において、異なるバス１３に接続された車載ＥＣＵ１２１間でやり取りされる情報を中継する中継処理を行う。

【００４１】

図２は、本発明の実施の形態に係る車載通信システムにおける車載ネットワークにおいて伝送されるデータフレームの一例を示す図である。図２には、標準フォーマットのデータフレームが示される。

【００４２】

図２を参照して、バス１３において、データフレームは、インターフレームスペースＩ

ＦＳ間において伝送される。
【００４３】
データフレームは、先頭から、ＳＯＦ（Ｓｔａｒｔ　Ｏｆ　Ｆｒａｍｅ）、ＩＤ（Ｉｄｅｎｔｉｆｉｅｒ）、ＲＴＲ（Ｒｅｍｏｔｅ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｒｅｑｕｅｓｔ）、ＣＯＮＴＲＯＬ、ＤＡＴＡ、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）、ＣＲＣ　ＤＥＬＩＭＩＴＥＲ、ＡＣＫ　ＳＬＯＴ、ＡＣＫ　ＤＥＬＩＭＩＴＥＲおよびＥＯＦ（Ｅｎｄ　Ｏｆ　Ｆｒａｍｅ）の領域を有する。
【００４４】
領域は、対応のビット数の長さを有する。また、各領域におけるビットのレベルは、レセシブ固定、ドミナント固定、ならびにレセシブおよびドミナントの可変のうちのいずれか１つである。
【００４５】
具体的には、ＳＯＦ領域は、１ビットの長さを有する。ＳＯＦ領域における１ビットのレベルは、ドミナント固定である。
【００４６】
ＩＤ領域は、１１ビットの長さを有する。ＩＤ領域における１１個のビットは、レセシブおよびドミナントの可変である。
【００４７】
ＩＤ領域における１１個のビットの示す値（以下、ＣＡＮ－ＩＤとも称する。）は、識別情報の一例であり、データフレームの差出元および宛先を認識可能である。
【００４８】
また、ＣＡＮ－ＩＤは、たとえば、データフレームに含まれるデータの種類を示す。
【００４９】
車載ネットワーク１２におけるバス１３において、互いに異なるＣＡＮ－ＩＤを含む複数のデータフレームが伝送される。
【００５０】
車載ネットワーク１２では、データフレームの送信は、たとえばブロードキャストにより行われる。たとえば、バス１３に接続されたある車載装置が、送信ノードとして、予め設定されたＣＡＮ－ＩＤを含むデータフレームをブロードキャストした場合、当該バス１３に接続された他の車載装置は受信ノードとして動作し、ブロードキャストされたデータフレームを受信する。
【００５１】
この際、受信ノードは、受信したデータフレームに含まれるＣＡＮ－ＩＤに基づいて、受信したデータフレームが自己にとって必要であるか否かを判断する。
【００５２】
車載ネットワーク１２では、１つの受信ノードが、受信したデータフレームを自己にとって必要であると判断することもあるし、複数の受信ノードが、受信したデータフレームを自己にとって必要であると判断することもある。
【００５３】
上記のように、車載ネットワーク１２では、データフレームに含まれるＣＡＮ－ＩＤに基づいて、当該データフレームの差出元および宛先を特定することが可能である。
【００５４】
また、ＣＡＮ－ＩＤは、たとえば、通信調停の優先順位に用いられる。
【００５５】
バス１３では、ＣＡＭＡ／ＣＡ（Ｃａｒｒｉｅｒ　Ｓｅｎｓｅ　Ｍｕｌｔｉｐｌｅ　Ａｃｃｅｓｓ　ｗｉｔｈ　Ｃｏｌｌｉｓｉｏｎ　Ａｖｏｉｄａｎｃｅ）方式に従って、最初にデータフレームを送信した車載ＥＣＵ１２１が送信権を獲得する。
【００５６】
たとえば、２つ以上の車載ＥＣＵ１２１がほぼ同時にデータフレームの送信を開始した場合、ＩＤ領域の１ビット目から調停を行い、ドミナントレベルを最も長く連続して送信

した車載ＥＣＵ１２１がデータフレームの送信を行うことができる。調停の敗者となった車載ＥＣＵ１２１は、データフレームの送信を停止し、受信動作を開始する。

【００５７】

車載ネットワーク１２では、レセシブレベルおよびドミナントレベルは、それぞれ論理値１および論理値ゼロに対応するので、より小さいＣＡＮ－ＩＤを含むデータフレームが優先的に伝送される。

【００５８】

図３は、本発明の実施の形態に係る車載通信システムにおける車載ネットワークにおいて伝送されるデータフレームの一例を示す図である。図３には、拡張フォーマットのデータフレームが示される。

【００５９】

図３を参照して、拡張フォーマットのデータフレームでは、図２に示す標準フォーマットのデータフレームと比べて、ＩＤ領域とＲＴＲ領域との間において、ＳＲＲ（Ｓｕｂｓｔｉｔｕｔｅ　Ｒｅｍｏｔｅ　Ｒｅｑｕｅｓｔ）、ＩＤＥ（Ｉｄｅｎｔｉｆｉｅｒ　Ｅｘｔｅｎｓｉｏｎ）およびＥＸＴＥＮＤＥＤ　ＩＤの領域がさらに設けられる。

【００６０】

［バスオフ攻撃］

図４は、本発明の実施の形態に係る車載通信システムにおけるトランシーバの状態遷移の一例を示す図である。

【００６１】

図４を参照して、バス１３を介して通信するゲートウェイ装置１０１および車載ＥＣＵ１２１には、トランシーバが設けられる。トランシーバは、送信エラーカウンタＴＥＣおよび受信エラーカウンタＲＥＣを有する。

【００６２】

トランシーバは、ＣＡＮの通信規格に従って動作し、エラーアクティブ状態、エラーパッシブ状態およびバスオフ状態のいずれか１つの状態をとる。

【００６３】

エラーアクティブ状態は、バス１３上の通信に正常に参加することができる状態である。エラーパッシブ状態は、エラーを起こしやすい状態である。バスオフ状態は、バス１３上の通信に参加できない状態であり、すべての通信が禁止される。

【００６４】

エラーアクティブ状態またはエラーパッシブ状態にあるトランシーバは、エラーを検出した場合、エラーを検出したことを示すエラーフレームをバス１３へ送信する。また、当該トランシーバは、たとえば、ＩＤ毎プロトコルエラー監視区間（図２および図３参照）におけるデータの送信中にエラーを検出した場合、データフレームの送信を中断することもある。

【００６５】

また、トランシーバは、自己が送信ユニットとして動作するときにエラーを検出した場合、送信エラーカウンタＴＥＣのカウント値を、検出したエラーの内容に応じて増加させる。

【００６６】

また、トランシーバは、自己が受信ユニットとして動作するときにエラーを検出した場合、受信エラーカウンタＲＥＣのカウント値を、検出したエラーの内容に応じて増加させる。

【００６７】

また、トランシーバは、自己が送信ユニットとして動作するときにエラーを検出せずにメッセージを送信できた場合、送信エラーカウンタＴＥＣのカウント値をデクリメントする。

【００６８】

また、トランシーバは、自己が受信ユニットとして動作するときにエラーを検出せずに

メッセージを受信できた場合、受信エラーカウンタＲＥＣのカウント値をデクリメントする。

【００６９】

トランシーバは、たとえば、起動されると初期状態を経てエラーアクティブ状態になる。

【００７０】

エラーアクティブ状態にあるトランシーバは、送信エラーカウンタＴＥＣのカウント値または受信エラーカウンタＲＥＣのカウント値が１２７より大きい値になると、エラーパッシブ状態へ遷移する。

【００７１】

エラーパッシブ状態にあるトランシーバは、送信エラーカウンタＴＥＣのカウント値および受信エラーカウンタＲＥＣのカウント値の両方が１２８より小さい値になると、エラーアクティブ状態へ遷移する。

【００７２】

また、エラーパッシブ状態にあるトランシーバは、送信エラーカウンタＴＥＣのカウント値が２５５より大きい値になると、バスオフ状態へ遷移する。

【００７３】

バスオフ状態にあるトランシーバは、連続する１１ビットのレセシブビットを１２８回バス１３上において検出した場合、送信エラーカウンタＴＥＣのカウント値および受信エラーカウンタＲＥＣのカウント値の両方をゼロにリセットするとともに、エラーアクティブ状態へ遷移する。

【００７４】

図５は、本発明の実施の形態に係る車載ネットワークにおける攻撃を説明するための図である。

【００７５】

図５を参照して、バス１３には、車載ＥＣＵ１２１である車載ＥＣＵ１２１Ａ，１２１Ｂと、攻撃デバイス１２３とが接続されている。車載ＥＣＵ１２１Ａ，１２１Ｂは、トランシーバ１２２を含む。

【００７６】

バスオフ攻撃は、たとえば、非特許文献２（Ｋ．　Ｃｈｏ、外１名、「Ｅｒｒｏｒ　Ｈａｎｄｌｉｎｇ　ｏｆ　Ｉｎ－ｖｅｈｉｃｌｅ　Ｎｅｔｗｏｒｋｓ　Ｍａｋｅｓ　Ｔｈｅｍ　Ｖｕｌｎｅｒａｂｌｅ」、ＣＣＳ　’１６　Ｐｒｏｃｅｅｄｉｎｇｓ　ｏｆ　ｔｈｅ　２０１６　ＡＣＭ　ＳＩＧＳＡＣ　Ｃｏｎｆｅｒｅｎｃｅ　ｏｎ　Ｃｏｍｐｕｔｅｒ　ａｎｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｓｅｃｕｒｉｔｙ、Ｐ．１０４４－１０５５）および非特許文献３（亀岡　良太、外５名、「ラズベリーパイからのスタッフエラー注入によるＣＡＮ　ＥＣＵへのバスオフ攻撃」、２０１７　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｃｒｙｐｔｏｇｒａｐｈｙ　ａｎｄ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ、１Ｅ２－２）に記載されている。

【００７７】

バスオフ攻撃では、攻撃デバイス１２３は、攻撃対象の車載ＥＣＵ１２１におけるトランシーバ１２２の自己検査機能を攻撃することにより当該トランシーバ１２２の送信品質が低下したと誤認識させ、攻撃対象の車載ＥＣＵ１２１をバス１３から離脱させる。この結果、攻撃を受けた車載ＥＣＵ１２１は、通信不能に追い込まれる。

【００７８】

より詳細には、トランシーバ１２２は、たとえば、データフレームを送信する際に受信も同時に行うことにより、バス１３へ送信したデータと同じデータがバス１３から受信されたか否かを確認する。

【００７９】

トランシーバ１２２は、バス１３へ送信したデータと同じデータがバス１３から受信された場合、送信が正常に行われたと判断する。一方、トランシーバ１２２は、バス１３へ

送信したデータと異なるデータがバス１３から受信された場合、送信においてエラーが発生したと判断する。

【００８０】

より詳細には、攻撃デバイス１２３は、たとえば、車載ＥＣＵ１２１Ｂを攻撃する場合、ＩＤ毎プロトコルエラー監視区間（図２および図３参照）において、車載ＥＣＵ１２１Ｂが送信するレセシブビットをドミナントビットで上書きする。

【００８１】

これにより、車載ＥＣＵ１２１Ｂにおけるトランシーバ１２２は、レセシブビットを送信したにも関わらずドミナントビットを受信したため送信においてエラーが発生したと判断し、送信エラーカウンタＴＥＣのカウント値を増加させる。

【００８２】

攻撃デバイス１２３がこの攻撃を繰り返すことにより、車載ＥＣＵ１２１Ｂのトランシーバ１２２における送信エラーカウンタＴＥＣのカウント値はさらに増加する。当該送信エラーカウンタＴＥＣのカウント値が２５５より大きくなると、車載ＥＣＵ１２１Ｂにおけるトランシーバ１２２はバスオフ状態に遷移し、トランシーバ１２２は、バス１３上の通信に参加できなくなってしまう。

【００８３】

［電気的データ改ざん攻撃］

図６は、本発明の実施の形態に係る車載ネットワークにおける電気的データ改ざん攻撃を説明するための図である。

【００８４】

図６を参照して、図２および図３に示すデータフレームにおける１ビットの期間には、シンクロナイゼーションセグメントＳＳ、プロパゲーションタイムセグメントＰＴＳ、フェーズバッファセグメントＰＢＳ１およびフェーズバッファセグメントＰＢＳ２が含まれる。

【００８５】

各セグメントは、Ｔｑ（Ｔｉｍｅ　ｑｕａｎｔｕｍ）という最小時間単位で構成される。ＳＳのＴｑ数は、１に固定である。ＰＴＳ、ＰＢＳ１およびＰＢＳ２のＴｑ数は、所定の範囲内で任意の値に設定可能である。

【００８６】

また、サンプルタイミングＳＰは、ＰＢＳ１とＰＢＳ２との間に設けられる。車載ネットワーク１２において、ＰＴＳ、ＰＢＳ１およびＰＢＳ２のＴｑ数は車載ＥＣＵ１２１ごとに様々な値に設定されるので、車載ネットワーク１２における各車載ＥＣＵ１２１のサンプルタイミングＳＰは、一般にばらついている。

【００８７】

電気的データ改ざん攻撃は、たとえば、非特許文献４（中山　淑文、外３名、「車載ＣＡＮバスにおける電気的データ改竄の効果」、２０１７　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｃｒｙｐｔｏｇｒａｐｈｙ　ａｎｄ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ、１Ｅ２－３）に記載されている。

【００８８】

電気的データ改ざん攻撃では、送信ユニットのサンプリングポイントＳＰより遅いサンプリングポイントＳＰを有する受信ユニットに対して攻撃が行われる。

【００８９】

たとえば、図５において、車載ＥＣＵ１２１Ｂにおけるトランシーバ１２２および車載ＥＣＵ１２１Ａにおけるトランシーバ１２２がそれぞれ送信ユニットおよび受信ユニットとして動作する状況を想定する。

【００９０】

この例では、送信ユニットにおけるサンプルタイミングＳＰがビットの先頭から４Ｔｑ目であり、また受信ユニットにおけるサンプルタイミングＳＰがビットの先頭から６Ｔｑ目である。

【００９１】
攻撃デバイス１２３は、送信ユニットのサンプリングポイントＳＰでは改ざんせずに、受信ユニットのサンプリングポイントＳＰにおいてデータ改ざん用の電気信号をバス１３へ送信することで、送信ユニットからのデータを改ざんする。これにより、送信ユニットにおけるビットエラー検出を回避しつつ受信ユニットが受信するデータを改ざんすることが可能となる。
【００９２】
より詳細には、攻撃デバイス１２３は、送信ユニットがデータビットを送信する場合において、ビットの先頭から４Ｔｑ目が経過してから６Ｔｑ目に至るまでに、当該データビットを改ざんするための電気信号をバス１３へ送信する。
【００９３】
送信ユニットは、自己が送信したデータビットを４Ｔｑ目のサンプルタイミングで取得するので、正常に送信したと判断する。
【００９４】
一方、受信ユニットは、攻撃デバイス１２３によって改ざんされた不正なデータビットを６Ｔｑ目に取得してしまう。
【００９５】
このような電気的データ改ざん攻撃では、送信ユニットおよび受信ユニットの両方においてエラーが検出されない。
【００９６】
しかしながら、上述したように、各車載ＥＣＵ１２１のサンプルタイミングＳＰがばらついているので、車載ネットワーク１２におけるすべての車載ＥＣＵ１２１においてエラーを検出させずに電気的データ改ざん攻撃を行うことは困難であると考えられる。
【００９７】
したがって、一般に、車載ネットワーク１２における一部の車載ＥＣＵ１２１が、電気的データ改ざん攻撃を検出してエラーフレームをバス１３へ送信する状況となる。
【００９８】
このような、バスオフ攻撃および電気的データ改ざん攻撃等の車載ネットワーク１２における攻撃をより精度よく検知するための技術が求められる。
【００９９】
そこで、本発明の実施の形態に係るゲートウェイ装置では、以下のような構成および動作により、このような課題を解決する。
【０１００】
［ゲートウェイ装置１０１の構成］
図７は、本発明の実施の形態に係る車載通信システムにおけるゲートウェイ装置の構成を示す図である。
【０１０１】
図７を参照して、ゲートウェイ装置１０１は、送受信部（監視部）５１Ａ，５１Ｂ，５１Ｃ，５１Ｄと、中継部５２と、集計部５４と、検知部５５と、記憶部５６とを備える。以下、送受信部５１Ａ，５１Ｂ，５１Ｃ，５１Ｄの各々を、送受信部５１とも称する。
【０１０２】
なお、ゲートウェイ装置１０１は、４つの送受信部５１を備える構成に限らず、３つ以下、または５つ以上の送受信部５１を備える構成であってもよい。
【０１０３】
ゲートウェイ装置１０１は、検知装置として機能し、識別情報を含むデータフレームが伝送されるバス１３を含む車載ネットワーク１２における攻撃を検知する。
【０１０４】
より詳細には、ゲートウェイ装置１０１における送受信部５１は、たとえば、トランシーバであり、バス１３に接続される。具体的には、送受信部５１Ａ，５１Ｂ，５１Ｃ，５１Ｄは、それぞれバス１３Ａ，１３Ｂ，１３Ｃ，１３Ｄに接続される。

【０１０５】
送受信部５１は、自己の接続されたバス１３からデータフレームを受信すると、ＩＤ監視区間において受信した各ビットのレベルからＣＡＮ－ＩＤを取得する（図２および図３参照）。
【０１０６】
送受信部５１は、取得したＣＡＮ－ＩＤに基づいて、受信したデータフレームが中継を要するフレームであるか否かを判断する。
【０１０７】
送受信部５１は、受信したデータフレームが中継を要するフレームであると判断した場合、当該データフレームを中継部５２へ出力する。
【０１０８】
中継部５２は、データフレームの中継処理を行う。具体的には、中継部５２は、たとえば、送受信部５１Ａからデータフレームを受けると、受けたデータフレームに含まれるＣＡＮ－ＩＤに基づいて、当該データフレームを出力すべき送受信部５１を特定する。
【０１０９】
より詳細には、中継部５２は、たとえば、ＣＡＮ－ＩＤと送受信部５１との対応関係を示すテーブルを有している。この例では、中継部５２は、当該対応関係に基づいて、当該ＣＡＮ－ＩＤに対応する送受信部５１として送受信部５１Ｂを特定する。そして、中継部５２は、上記データフレームを送受信部５１Ｂへ出力する。
【０１１０】
送受信部５１Ｂは、中継部５２からデータフレームを受けると、受けたデータフレームをバス１３Ｂへ送信する。
【０１１１】
また、送受信部５１は、バス１３における通信エラーを監視する。より詳細には、送受信部５１は、ＩＤ監視区間においてＣＡＮ－ＩＤを取得した後、ＩＤ毎プロトコルエラー監視区間におけるビット列を監視する。
【０１１２】
送受信部５１は、たとえば、差出元の車載ＥＣＵ１２１によるデータフレームの送信の中断を検出した場合、およびエラーフレームを受信した場合、通信エラーが発生したと判断する。
【０１１３】
そして、送受信部５１は、通信エラーが発生したと判断したデータフレームのＣＡＮ－ＩＤを集計部５４へ通知する。
【０１１４】
図８は、本発明の実施の形態に係るゲートウェイ装置において用いられる長監視間隔期間および短監視間隔期間の一例を示す図である。なお、図８において、横軸は時間を示す。
【０１１５】
図８を参照して、集計部５４は、送受信部５１の監視結果に基づいて、識別情報ごとの通信エラーの発生状況を集計する。
【０１１６】
より詳細には、集計部５４は、たとえば、短監視間隔期間ＳＴ１，ＳＴ２，ＳＴ３，ＳＴ４，ＳＴ５を含む長監視間隔期間ＬＴを設定する。短監視間隔期間ＳＴ１～ＳＴ５は、連続している。以下、短監視間隔期間ＳＴ１，ＳＴ２，ＳＴ３，ＳＴ４，ＳＴ５の各々を、短監視間隔期間ＳＴとも称する。
【０１１７】
なお、集計部５４は、５つの短監視間隔期間ＳＴを含む長監視間隔期間ＬＴを設定する構成に限らず、２つ、３つ、４つまたは６つ以上の短監視間隔期間ＳＴを含む長監視間隔期間ＬＴを設定してもよい。
【０１１８】

図９は、本発明の実施の形態に係るゲートウェイ装置における集計部が作成する集計表の一例を示す図である。

【０１１９】

図９を参照して、集計部５４は、たとえば、短監視間隔期間ＳＴの各々における通信エラーの発生回数の合計値、および長監視間隔期間ＬＴにおける通信エラーの発生回数の合計値を含む集計表Ｔｂｌ１を送受信部５１ごとに作成して保持する。図９に示す集計表Ｔｂｌ１は、たとえば、送受信部５１Ａ用の集計表である。

【０１２０】

集計表Ｔｂｌ１では、車載ネットワーク１２において用いられるＣＡＮ－ＩＤ数分の行が設けられ、各行には、短監視間隔期間ＳＴ１～ＳＴ５および長監視間隔期間ＬＴにそれぞれ対応するフィールドが設けられる。

【０１２１】

集計部５４は、送受信部５１ＡからＣＡＮ－ＩＤの通知を受けるごとに、以下の処理を行う。

【０１２２】

すなわち、集計部５４は、集計表Ｔｂｌ１において、通知されたＣＡＮ－ＩＤに対応する行において、通知を受けたタイミングを含む短監視間隔期間ＳＴに対応するフィールドにおけるプロトコルエラー発生回数をインクリメントする。

【０１２３】

具体的には、集計部５４は、たとえば、短監視間隔期間ＳＴ１において、送受信部５１ＡからＣＡＮ－ＩＤとして「１」の通知を受けると、ＣＡＮ－ＩＤが「１」の行において、短監視間隔期間ＳＴ１に対応するフィールドにおけるプロトコルエラー発生回数をインクリメントする。

【０１２４】

集計部５４がこのような処理を行うことにより、短監視間隔期間ＳＴ１が満了すると、ＣＡＮ－ＩＤが「１」、「２」および「Ｎ」の行において、短監視間隔期間ＳＴ１に対応するフィールドにおけるプロトコルエラー発生回数としてそれぞれ５回、５回およびゼロ回が集計表Ｔｂｌ１に記録される。

【０１２５】

集計部５４は、短監視間隔期間ＳＴ２～短監視間隔期間ＳＴ５においても、同様の処理を行う。

【０１２６】

そして、集計部５４は、長監視間隔期間ＬＴが満了すると、長監視間隔期間ＬＴにおけるＣＡＮ－ＩＤごとのプロトコルエラー発生回数を集計表Ｔｂｌ１に書き込む。

【０１２７】

より詳細には、集計部５４は、短監視間隔期間ＳＴ１～ＳＴ５におけるプロトコルエラー発生回数の合計値をＣＡＮ－ＩＤごとに算出する。

【０１２８】

集計部５４は、ＣＡＮ－ＩＤごとに、算出した合計値を、当該ＣＡＮ－ＩＤの行において長監視間隔期間ＬＴに対応するフィールドに書き込む。

【０１２９】

具体的には、集計部５４は、たとえば、ＣＡＮ－ＩＤが「１」の行において、短監視間隔期間ＳＴ１～ＳＴ５におけるプロトコルエラー発生回数の合計値として５０回を算出する。

【０１３０】

集計部５４は、算出した５０回を、ＣＡＮ－ＩＤが「１」の行において長監視間隔期間ＬＴに対応するフィールドに書き込む。

【０１３１】

図１０は、本発明の実施の形態に係るゲートウェイ装置における集計部が作成する集計表の一例を示す図である。

【０１３２】
図１０を参照して、集計部５４は、たとえば、各短監視間隔期間ＳＴにおけるバス内プロトコルエラー分布、および長監視間隔期間ＬＴにおけるバス内プロトコルエラー分布の平均を含む集計表Ｔｂｌ２を送受信部５１ごとに作成して保持する。図１０に示す集計表Ｔｂｌ２は、たとえば、送受信部５１Ａ用の集計表である。
【０１３３】
集計表Ｔｂｌ２では、短監視間隔期間ＳＴ１～ＳＴ５および長監視間隔期間ＬＴにそれぞれ対応するフィールドが設けられる。
【０１３４】
集計部５４は、短監視間隔期間ＳＴが満了すると、当該短監視間隔期間ＳＴにおけるバス内プロトコルエラー分布を算出し、算出したバス内プロトコルエラー分布を当該短監視間隔期間ＳＴに対応するフィールドに書き込む。
【０１３５】
ここで、バス内プロトコルエラー分布は、通信エラーの発生した識別情報の数であるエラーＩＤ数の一例である。具体的には、バス内プロトコルエラー分布は、短監視間隔期間ＳＴにおいて、プロトコルエラー発生回数が１回以上となったＣＡＮ－ＩＤの個数である。
【０１３６】
具体的には、集計部５４は、たとえば、短監視間隔期間ＳＴ１が満了すると、短監視間隔期間ＳＴ１において、プロトコルエラー発生回数が１回以上のＣＡＮ－ＩＤが「１」および「２」であることから、バス内プロトコルエラー分布として２を算出する。
【０１３７】
そして、集計部５４は、算出した２を当該短監視間隔期間ＳＴ１に対応するフィールドに書き込む。
【０１３８】
集計部５４は、短監視間隔期間ＳＴ２～短監視間隔期間ＳＴ５の各々が満了した場合においても、同様の処理を行う。
【０１３９】
そして、集計部５４は、長監視間隔期間ＬＴが満了すると、長監視間隔期間ＬＴにおけるバス内プロトコルエラー分布の平均を長監視間隔期間ＬＴに対応するフィールドに書き込む。
【０１４０】
具体的には、集計部５４は、短監視間隔期間ＳＴ１～ＳＴ５における各バス内プロトコルエラー分布の平均として、（２＋２＋１＋１＋１）を５で除した値である１．４を算出する。
【０１４１】
集計部５４は、算出した１．４を長監視間隔期間ＬＴに対応するフィールドに書き込む。
【０１４２】
再び図７を参照して、検知部５５は、集計部５４の集計結果に基づいて車載ネットワーク１２における攻撃を検知する。
【０１４３】
詳細には、検知部５５は、たとえば、集計結果における各ＣＡＮ－ＩＤ間での通信エラーの発生状況の偏りに基づいて車載ネットワーク１２における攻撃を検知する。
【０１４４】
より詳細には、検知部５５は、たとえば、通信エラーの発生回数のＣＡＮ－ＩＤごとの合計、およびバス内プロトコルエラー分布に基づいて車載ネットワーク１２における攻撃を検知する。
【０１４５】
検知部５５は、たとえば、短監視間隔ごとに短間隔検知処理を行う。具体的には、検知

部５５は、たとえば、短監視間隔期間ＳＴにおける通信エラーの発生回数のＣＡＮ－ＩＤごとの合計としきい値Ｔｈ１との比較結果Ｒｓｔ１、バス内プロトコルエラー分布としきい値Ｔｈ２との比較結果Ｒｓｔ２、およびバス内プロトコルエラー分布としきい値Ｔｈ２より大きいしきい値Ｔｈ５との比較結果Ｒｓｔ５に基づいて車載ネットワーク１２における攻撃を検知する。

【０１４６】

より具体的には、検知部５５は、たとえば、集計部５４によって設定された短監視間隔期間ＳＴ１，ＳＴ２，ＳＴ３，ＳＴ４，ＳＴ５および長監視間隔期間ＬＴに従って動作し、短監視間隔期間ＳＴ１が満了すると、以下の処理を行う。

【０１４７】

すなわち、検知部５５は、短監視間隔期間ＳＴ１におけるプロトコルエラー発生回数のＣＡＮ－ＩＤごとの合計値を、集計部５４が保持する集計表Ｔｂｌ１（図９参照）から取得する。

【０１４８】

また、検知部５５は、短監視間隔期間ＳＴ１におけるバス内プロトコルエラー分布を、集計部５４が保持する集計表Ｔｂｌ２（図１０参照）から取得する。

【０１４９】

検知部５５は、たとえば、「１」～「Ｎ」のＣＡＮ－ＩＤの中から昇順にＣＡＮ－ＩＤを１つずつ選択し、選択したＣＡＮ－ＩＤに対応するプロトコルエラー発生回数を用いた評価を行う。

【０１５０】

具体的には、検知部５５は、たとえば、選択したＣＡＮ－ＩＤ（以下、対象ＣＡＮ－ＩＤとも称する。）に対応するプロトコルエラー発生回数の合計がしきい値Ｔｈ１より大きく、かつバス内プロトコルエラー分布がしきい値Ｔｈ２より小さい場合、少数の車載ＥＣＵ１２１に対するサイバー攻撃である少数攻撃が発生したと判断する。検知部５５は、判断結果をログとして記憶部５６に記録する。

【０１５１】

たとえば、１～２個の車載ＥＣＵ１２１に対してサイバー攻撃があった場合、サイバー攻撃された車載ＥＣＵ１２１が差出元または宛先となるデータフレームに含まれるＣＡＮ－ＩＤについてのプロトコルエラー発生回数は大きくなる。一方、サイバー攻撃された車載ＥＣＵ１２１を差出元または宛先として示すＣＡＮ－ＩＤの個数は少数であるため、バス内プロトコルエラー分布は大きくならない。上記の構成により、検知部５５は、少数攻撃が発生したことをより正しく判断することができる。

【０１５２】

また、検知部５５は、たとえば、対象ＣＡＮ－ＩＤに対応するプロトコルエラー発生回数の合計がしきい値Ｔｈ１より大きく、かつバス内プロトコルエラー分布がしきい値Ｔｈ５より大きい場合、多数の車載ＥＣＵ１２１に対するサイバー攻撃である多数攻撃が発生したと判断する。検知部５５は、判断結果をログとして記憶部５６に記録する。

【０１５３】

たとえば、多数の車載ＥＣＵ１２１に対してサイバー攻撃があった場合、サイバー攻撃された車載ＥＣＵ１２１が差出元または宛先となるデータフレームに含まれるＣＡＮ－ＩＤについてのプロトコルエラー発生回数は大きくなる。また、サイバー攻撃された車載ＥＣＵ１２１を差出元または宛先として示すＣＡＮ－ＩＤの個数も多数であるため、バス内プロトコルエラー分布が極めて大きくなる。上記の構成により、検知部５５は、多数攻撃が発生したことをより正しく判断することができる。

【０１５４】

また、検知部５５は、たとえば、対象ＣＡＮ－ＩＤに対応するプロトコルエラー発生回数の合計がしきい値Ｔｈ１以下であるか、またはバス内プロトコルエラー分布がしきい値Ｔｈ２以上でありかつしきい値Ｔｈ５以下である場合、ノイズまたは車載ＥＣＵ１２１の故障等による通信エラーが発生したと判断する。この場合、検知部５５は、判断結果を記

憶部５６に記録しない。

【０１５５】

たとえば、ノイズはランダムに発生することが多いので、通信エラーの発生するデータフレームもランダムとなる。このため、バス内プロトコルエラー分布は大きくなる。また、車載ＥＣＵ１２１が経年劣化する場合、車載ＥＣＵ１２１が差出元または宛先となるデータフレームの通信エラーが散発的に発生すると考えられる。このため、バス内プロトコルエラー分布が小さくても、車載ＥＣＵ１２１が差出元または宛先となるデータフレームに含まれるＣＡＮ－ＩＤについてのプロトコルエラー発生回数も小さくなる。上記の構成により、検知部５５は、少数攻撃または多数攻撃の発生を誤って判断してしまうことを防ぐことができる。

【０１５６】

検知部５５は、たとえば、集計部５４によって設定された短監視間隔期間ＳＴ２，ＳＴ３，ＳＴ４，ＳＴ５が満了した場合の各々においても、短監視間隔期間ＳＴ１が満了した場合と同様に、短間隔検知処理を行う。

【０１５７】

また、検知部５５は、たとえば、長監視間隔ごとに長間隔検知処理を行う。具体的には、検知部５５は、たとえば、長監視間隔期間ＬＴにおける通信エラーの発生回数のＣＡＮ－ＩＤごとの合計としきい値Ｔｈ３との比較結果Ｒｓｔ３、バス内プロトコルエラー分布の平均としきい値Ｔｈ４との比較結果Ｒｓｔ４、および当該平均としきい値Ｔｈ４より大きいしきい値Ｔｈ６との比較結果Ｒｓｔ６に基づいて車載ネットワーク１２における攻撃を検知する。

【０１５８】

より具体的には、検知部５５は、長監視間隔期間ＬＴが満了すると、長監視間隔期間ＬＴにおけるプロトコルエラー発生回数のＣＡＮ－ＩＤごとの合計値を、集計部５４が保持する集計表Ｔｂｌ１（図９参照）から取得する。

【０１５９】

また、検知部５５は、長監視間隔期間ＬＴにおけるバス内プロトコルエラー分布の平均を、集計部５４が保持する集計表Ｔｂｌ２（図１０参照）から取得する。

【０１６０】

検知部５５は、たとえば、「１」～「Ｎ」のＣＡＮ－ＩＤの中から昇順にＣＡＮ－ＩＤを１つずつ選択し、選択したＣＡＮ－ＩＤに対応するプロトコルエラー発生回数を用いた評価を行う。

【０１６１】

具体的には、検知部５５は、たとえば、選択したＣＡＮ－ＩＤすなわち対象ＣＡＮ－ＩＤに対応するプロトコルエラー発生回数の合計がしきい値Ｔｈ３より大きく、かつバス内プロトコルエラー分布の平均がしきい値Ｔｈ４より小さい場合、少数攻撃が発生したと判断する。検知部５５は、判断結果をログとして記憶部５６に記録する。

【０１６２】

たとえば、１～２個の車載ＥＣＵ１２１に対してサイバー攻撃があった場合、サイバー攻撃された車載ＥＣＵ１２１が差出元または宛先となるデータフレームに含まれるＣＡＮ－ＩＤについてのプロトコルエラー発生回数は大きくなる。一方、サイバー攻撃された車載ＥＣＵ１２１を差出元または宛先として示すＣＡＮ－ＩＤの個数は少数であるため、バス内プロトコルエラー分布の平均は大きくならない。上記の構成により、検知部５５は、少数攻撃が発生したことをより正しく判断することができる。

【０１６３】

また、検知部５５は、たとえば、対象ＣＡＮ－ＩＤに対応するプロトコルエラー発生回数の合計がしきい値Ｔｈ３より大きく、かつバス内プロトコルエラー分布の平均がしきい値Ｔｈ６より大きい場合、多数攻撃が発生したと判断する。検知部５５は、判断結果をログとして記憶部５６に記録する。

【０１６４】

たとえば、多数の車載ＥＣＵ１２１に対してサイバー攻撃があった場合、サイバー攻撃された車載ＥＣＵ１２１が差出元または宛先となるデータフレームに含まれるＣＡＮ－ＩＤについてのプロトコルエラー発生回数は大きくなる。また、サイバー攻撃された車載ＥＣＵ１２１を差出元または宛先として示すＣＡＮ－ＩＤの個数も多数であるため、バス内プロトコルエラー分布の平均が極めて大きくなる。上記の構成により、検知部５５は、多数攻撃が発生したことをより正しく判断することができる。

【０１６５】

また、検知部５５は、たとえば、対象ＣＡＮ－ＩＤに対応するプロトコルエラー発生回数の合計がしきい値Ｔｈ３以下であるか、またはバス内プロトコルエラー分布の平均がしきい値Ｔｈ４以上でありかつしきい値Ｔｈ６以下である場合、ノイズまたは車載ＥＣＵ１２１の故障等による通信エラーが発生したと判断する。この場合、検知部５５は、判断結果を記憶部５６に記録しない。

【０１６６】

たとえば、ノイズはランダムに発生することが多いので、通信エラーの発生するデータフレームもランダムとなる。このため、バス内プロトコルエラー分布の平均は大きくなる。また、車載ＥＣＵ１２１が経年劣化する場合、車載ＥＣＵ１２１が差出元または宛先となるデータフレームの通信エラーが散発的に発生すると考えられる。このため、バス内プロトコルエラー分布の平均が小さくても、車載ＥＣＵ１２１が差出元または宛先となるデータフレームに含まれるＣＡＮ－ＩＤについてのプロトコルエラー発生回数も小さくなる。上記の構成により、検知部５５は、少数攻撃または多数攻撃の発生を誤って判断してしまうことを防ぐことができる。

【０１６７】

［動作の流れ］

ゲートウェイ装置１０１は、コンピュータを備え、当該コンピュータにおけるＣＰＵ等の演算処理部は、以下に示すフローチャートの各ステップの一部または全部を含むプログラムを図示しないメモリから読み出して実行する。この装置のプログラムは、外部からインストールすることができる。この装置のプログラムは、記録媒体に格納された状態で流通する。

【０１６８】

図１１は、本発明の実施の形態に係るゲートウェイ装置がサイバー攻撃を検知する際の動作手順を定めたフローチャートである。

【０１６９】

図１１を参照して、まず、ゲートウェイ装置１０１は、短監視間隔期間ＳＴが満了するまで、データフレームの中継処理を行いながら、発生した通信エラーを記録する（ステップＳ１０２でＮＯ）。

【０１７０】

そして、ゲートウェイ装置１０１は、短監視間隔期間ＳＴが満了すると（ステップＳ１０２でＹＥＳ）、当該短監視間隔期間ＳＴにおいて発生した通信エラーを集計する（ステップＳ１０４）。

【０１７１】

次に、ゲートウェイ装置１０１は、車載ネットワーク１２において用いられる複数のＣＡＮ－ＩＤのうちの１つを選択する（ステップＳ１０６）。

【０１７２】

次に、ゲートウェイ装置１０１は、選択したＣＡＮ－ＩＤすなわち対象ＣＡＮ－ＩＤに対応するプロトコルエラー発生回数の短監視間隔期間ＳＴにおける合計ＥＮｓがしきい値Ｔｈ１より大きく、かつ当該短監視間隔期間ＳＴにおけるバス内プロトコルエラー分布ＥＤｓがしきい値Ｔｈ２より小さい場合（ステップＳ１０８でＹＥＳ）、少数攻撃を検知する（ステップＳ１１８）。

【０１７３】

また、ゲートウェイ装置１０１は、合計ＥＮｓがしきい値Ｔｈ１より大きく、かつバス

内プロトコルエラー分布ＥＤｓがしきい値Ｔｈ５より大きい場合（ステップＳ１０８でＮＯおよびステップＳ１１０でＹＥＳ）、多数攻撃を検知する（ステップＳ１１２）。

【０１７４】

次に、ゲートウェイ装置１０１は、少数攻撃を検知するか（ステップＳ１１８）、または多数攻撃を検知すると（ステップＳ１１２）、検知結果をログに記録する（ステップＳ１１４）。

【０１７５】

また、ゲートウェイ装置１０１は、合計ＥＮｓがしきい値Ｔｈ１以下であるか、もしくはバス内プロトコルエラー分布ＥＤｓがしきい値Ｔｈ２以上かつしきい値Ｔｈ５以下である場合（ステップＳ１０８でＮＯおよびステップＳ１１０でＮＯ）、または検知結果をログに記録すると（ステップＳ１１４）、車載ネットワーク１２において用いられる複数のＣＡＮ－ＩＤをすべて選択したか否かを確認する（ステップＳ１１６）。

【０１７６】

ゲートウェイ装置１０１は、上記複数のＣＡＮ－ＩＤの中で未選択のＣＡＮ－ＩＤが存在する場合（ステップＳ１１６でＮＯ）、上記複数のＣＡＮ－ＩＤにおいて未選択のＣＡＮ－ＩＤを１つ選択する（ステップＳ１０６）。

【０１７７】

一方、ゲートウェイ装置１０１は、上記複数のＣＡＮ－ＩＤをすべて選択した場合（ステップＳ１１６でＹＥＳ）、新たな短監視間隔期間ＳＴが満了するまで、データフレームの中継処理を行いながら、発生した通信エラーを記録する（ステップＳ１０２でＮＯ）。

【０１７８】

図１２は、本発明の実施の形態に係るゲートウェイ装置がサイバー攻撃を検知する際の動作手順を定めたフローチャートである。

【０１７９】

図１２を参照して、まず、ゲートウェイ装置１０１は、長監視間隔期間ＬＴが満了するまで、データフレームの中継処理を行いながら、長監視間隔期間ＬＴに含まれる各短監視間隔期間ＳＴにおいて発生した通信エラーを記録する（ステップＳ２０２でＮＯ）。

【０１８０】

そして、ゲートウェイ装置１０１は、長監視間隔期間ＬＴが満了すると（ステップＳ２０２でＹＥＳ）、当該各短監視間隔期間ＳＴにおいて発生した通信エラーを集計する（ステップＳ２０４）。

【０１８１】

次に、ゲートウェイ装置１０１は、車載ネットワーク１２において用いられる複数のＣＡＮ－ＩＤのうちの１つを選択する（ステップＳ２０６）。

【０１８２】

次に、ゲートウェイ装置１０１は、選択したＣＡＮ－ＩＤすなわち対象ＣＡＮ－ＩＤに対応するプロトコルエラー発生回数の長監視間隔期間ＬＴにおける合計ＥＮｐがしきい値Ｔｈ３より大きく、かつ当該長監視間隔期間ＬＴにおけるバス内プロトコルエラー分布ＥＤｐがしきい値Ｔｈ４より小さい場合（ステップＳ２０８でＹＥＳ）、少数攻撃を検知する（ステップＳ２１８）。

【０１８３】

また、ゲートウェイ装置１０１は、合計ＥＮｐがしきい値Ｔｈ３より大きく、かつバス内プロトコルエラー分布ＥＤｐがしきい値Ｔｈ６より大きい場合（ステップＳ２０８でＮＯおよびステップＳ２１０でＹＥＳ）、多数攻撃を検知する（ステップＳ２１２）。

【０１８４】

次に、ゲートウェイ装置１０１は、少数攻撃を検知するか（ステップＳ２１８）、または多数攻撃を検知すると（ステップＳ２１２）、検知結果をログに記録する（ステップＳ２１４）。

【０１８５】

また、ゲートウェイ装置１０１は、合計ＥＮｐがしきい値Ｔｈ３以下であるか、もしく

はバス内プロトコルエラー分布ＥＤｐがしきい値Ｔｈ４以上かつしきい値Ｔｈ６以下である場合（ステップＳ２０８でＮＯおよびステップＳ２１０でＮＯ）、または検知結果をログに記録すると（ステップＳ２１４）、車載ネットワーク１２において用いられる複数のＣＡＮ－ＩＤをすべて選択したか否かを確認する（ステップＳ２１６）。

【０１８６】

ゲートウェイ装置１０１は、上記複数のＣＡＮ－ＩＤの中で未選択のＣＡＮ－ＩＤが存在する場合（ステップＳ２１６でＮＯ）、上記複数のＣＡＮ－ＩＤにおいて未選択のＣＡＮ－ＩＤを１つ選択する（ステップＳ２０６）。

【０１８７】

一方、ゲートウェイ装置１０１は、上記複数のＣＡＮ－ＩＤをすべて選択した場合（ステップＳ２１６でＹＥＳ）、新たな長監視間隔期間ＬＴが満了するまで、データフレームの中継処理を行いながら、新たな長監視間隔期間ＬＴにおいて発生した通信エラーを記録する（ステップＳ２０２でＮＯ）。

【０１８８】

なお、本発明の実施の形態に係るゲートウェイ装置は、バス１３Ａ～１３Ｄのすべてを攻撃の検知対象とする構成であるとしたが、これに限定するものではない。ゲートウェイ装置１０１は、バス１３Ａ～１３Ｄの一部を攻撃の検知対象とする構成であってもよい。

【０１８９】

また、本発明の実施の形態に係る車載ネットワークでは、ゲートウェイ装置１０１が、車載ネットワーク１２における攻撃を検知する構成であるとしたが、これに限定するものではない。バス１３に接続された各車載ＥＣＵ１２１のうちの少なくともいずれか１つが、ゲートウェイ装置１０１と同様に、検知装置として動作し、対応のバス１３における攻撃を検知する構成であってもよい。

【０１９０】

また、本発明の実施の形態に係る車載ネットワークでは、差出元および宛先の両方を認識可能な識別情報を含むデータフレームが伝送される構成であるとしたが、これに限定するものではない。差出元および宛先のいずれか一方を認識可能な識別情報を含むデータフレームが伝送される構成であってもよい。

【０１９１】

また、本発明の実施の形態に係る車載ネットワークでは、差出元および宛先の両方を認識可能なＣＡＮ－ＩＤを含むデータフレームが伝送される構成であるとしたが、これに限定するものではない。差出元および宛先の少なくともいずれか一方を直接示す識別情報、たとえばアドレスを含むデータフレームが伝送される構成であってもよい。

【０１９２】

また、本発明の実施の形態に係るゲートウェイ装置では、検知部５５は、集計部５４における集計結果における各ＣＡＮ－ＩＤ間での通信エラーの発生状況の偏りに基づいて車載ネットワーク１２における攻撃を検知する構成であるとしたが、これに限定するものではない。検知部５５は、上記偏りに基づかずに車載ネットワーク１２における攻撃を検知する構成であってもよい。具体的には、検知部５５は、たとえば、図１０に示す集計表Ｔｂｌ２を用いずに、車載ネットワーク１２における攻撃を検知する。

【０１９３】

また、本発明の実施の形態に係るゲートウェイ装置では、検知部５５は、短間隔検知処理および長間隔検知処理の両方を行う構成であるとしたが、これに限定するものではない。検知部５５は、短間隔検知処理および長間隔検知処理のいずれか一方を行う構成であってもよい。

【０１９４】

また、本発明の実施の形態に係るゲートウェイ装置では、検知部５５は、比較結果Ｒｓｔ１、比較結果Ｒｓｔ２および比較結果Ｒｓｔ５に基づいて車載ネットワーク１２における攻撃を検知する構成であるとしたが、これに限定するものではない。検知部５５は、比較結果Ｒｓｔ１および比較結果Ｒｓｔ２に基づいて車載ネットワーク１２における攻撃を

検知する構成であってもよい。

【０１９５】

また、本発明の実施の形態に係るゲートウェイ装置では、検知部５５は、比較結果Ｒｓｔ３、比較結果Ｒｓｔ４および比較結果Ｒｓｔ６に基づいて車載ネットワーク１２における攻撃を検知する構成であるとしたが、これに限定するものではない。検知部５５は、比較結果Ｒｓｔ３および比較結果Ｒｓｔ４に基づいて車載ネットワーク１２における攻撃を検知する構成であってもよい。

【０１９６】

ところで、特許文献１に記載の車載通信システムでは、車載ネットワークに限定して接続される第１のＥＣＵおよび第２のＥＣＵがメッセージ認証に用いる第１の暗号鍵と、車載ネットワークおよび車外ネットワークの両方に接続される第３のＥＣＵが用いる第２の暗号鍵とが異なることにより、車外ネットワークに接続されない第１のＥＣＵおよび第２のＥＣＵに対する車外ネットワークからのサイバー攻撃を防いでいる。

【０１９７】

しかしながら、たとえば、各ＥＣＵ間を接続するバスにおいて伝送される信号を電気的に操作するようなサイバー攻撃に対しては、上記のようなセキュリティ対策が無効化されることがある。

【０１９８】

このような攻撃を受けた場合において、車載ネットワークにおける攻撃を精度よく検知するための技術が求められる。

【０１９９】

これに対して、本発明の実施の形態に係るゲートウェイ装置は、差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むデータフレームが伝送されるバス１３を含む車載ネットワーク１２における攻撃を検知する。バス１３において、互いに異なる識別情報を含む複数のデータフレームが伝送される。送受信部５１は、バス１３における通信エラーを監視する。集計部５４は、送受信部５１の監視結果に基づいて、識別情報ごとの通信エラーの発生状況を集計する。そして、検知部５５は、集計部５４の集計結果に基づいて車載ネットワーク１２における攻撃を検知する。

【０２００】

このような構成により、識別情報ごとの通信エラーの発生状況の集計結果に基づいて、データフレームの差出元または宛先の車載装置ごとの通信エラーの発生状況を認識することができるので、たとえば、バス１３において伝送される信号を電気的に操作するようなサイバー攻撃を受けて通信エラーの発生した車載装置を、特定することができる。したがって、車載ネットワークにおける攻撃を精度よく検知することができる。

【０２０１】

また、本発明の実施の形態に係るゲートウェイ装置では、検知部５５は、集計結果における各識別情報間での通信エラーの発生状況の偏りに基づいて車載ネットワーク１２における攻撃を検知する。

【０２０２】

このような構成により、各識別情報間での通信エラーの発生状況の偏りに基づいて、たとえば、車載ネットワーク１２における各車載装置において満遍なく通信エラーが発生しているのか、または当該各車載装置のうちの特定の少数の車載装置に通信エラーが発生しているのかを認識することができる。これにより、たとえば、各車載装置において満遍なく通信エラーが発生している場合には電気的ノイズの影響も考慮して攻撃の検知を慎重に判断することができ、また、特定の少数の車載装置に通信エラーが発生している場合には、攻撃の可能性が高いと判断することができる。

【０２０３】

また、本発明の実施の形態に係るゲートウェイ装置では、検知部５５は、通信エラーの発生回数の識別情報ごとの合計、および通信エラーの発生した識別情報の数であるエラーＩＤ数に基づいて車載ネットワーク１２における攻撃を検知する。

【０２０４】
このような構成により、たとえば、通信エラーの発生回数の多い車載装置に対して攻撃を受けたと判断しようとする場合において、通信エラーの発生した車載装置数を考慮することができるので、攻撃の有無をより正しく判断することができる。
【０２０５】
また、本発明の実施の形態に係るゲートウェイ装置では、検知部５５は、短監視間隔期間ＳＴにおける合計としきい値Ｔｈ１との比較結果Ｒｓｔ１およびエラーＩＤ数としきい値Ｔｈ２との比較結果Ｒｓｔ２、ならびに複数の短監視間隔期間ＳＴからなる長監視間隔期間ＬＴにおける合計としきい値Ｔｈ３との比較結果Ｒｓｔ３およびエラーＩＤ数の平均としきい値Ｔｈ４との比較結果Ｒｓｔ４の少なくともいずれか一方に基づいて車載ネットワーク１２における攻撃を検知する。
【０２０６】
このような構成により、たとえば、短監視間隔期間ＳＴにおける合計がしきい値Ｔｈ１より大きい場合においても、エラーＩＤ数がしきい値Ｔｈ２以上であるときには、電気的ノイズによって通信エラーが広範に発生していることが考えられるので、攻撃を誤って検知してしまうことを防ぐことができる。また、たとえば、短監視間隔期間ＳＴにおける合計がしきい値Ｔｈ１より大きく、かつエラーＩＤ数がしきい値Ｔｈ２より小さいときには、特定の少数の車載装置において通信エラーが発生していることから、当該特定の少数の車載装置に対する攻撃をより正しく検知することができる。また、長監視間隔期間ＬＴにおける合計がしきい値Ｔｈ３より大きい場合においても、エラーＩＤ数の平均がしきい値Ｔｈ４以上であるときには、電気的ノイズによって通信エラーが広範に発生していることが考えられるので、攻撃を誤って検知してしまうことを防ぐことができる。また、たとえば、長監視間隔期間ＬＴにおける合計がしきい値Ｔｈ３より大きく、かつエラーＩＤ数の平均がしきい値Ｔｈ４より小さいときには、特定の少数の車載装置において通信エラーが発生していることから、当該特定の少数の車載装置に対する攻撃をより正しく検知することができる。
【０２０７】
また、本発明の実施の形態に係るゲートウェイ装置では、検知部５５は、比較結果Ｒｓｔ１、比較結果Ｒｓｔ２およびエラーＩＤ数としきい値Ｔｈ２より大きいしきい値Ｔｈ５との比較結果、ならびに比較結果Ｒｓｔ３、比較結果Ｒｓｔ４およびエラーＩＤ数の平均としきい値Ｔｈ４より大きいしきい値Ｔｈ６との比較結果の少なくともいずれか一方に基づいて車載ネットワーク１２における攻撃を検知する。
【０２０８】
たとえば、短監視間隔期間ＳＴにおけるエラーＩＤ数、および長監視間隔期間ＬＴにおけるエラーＩＤ数の平均の少なくともいずれか一方が極端に大きい場合、車載ネットワーク１２における多数の車載装置に対して攻撃が行われていると考えられる。上記の構成により、車載ネットワーク１２における各車載装置に対する一斉攻撃をより精度よく検知することができる。
【０２０９】
上記実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記説明ではなく特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。
【０２１０】
以上の説明は、以下に付記する特徴を含む。
【０２１１】
［付記１］
差出元および宛先の少なくともいずれか一方を認識可能な識別情報を含むフレームが伝送されるバスを含む車載ネットワークにおける攻撃を検知する検知装置であって、
前記バスにおいて、互いに異なる前記識別情報を含む複数の前記フレームが伝送され、
前記バスにおける通信エラーを監視する監視部と、

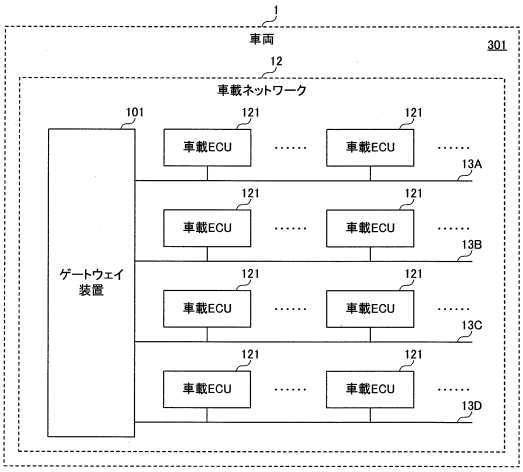
前記監視部の監視結果に基づいて、前記識別情報ごとの通信エラーの発生状況を集計する集計部と、
前記集計部の集計結果に基づいて前記攻撃を検知する検知部とを備え、
前記検知装置は車両に搭載され、前記フレームを中継するゲートウェイ装置、または車載ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ）であり、
前記識別情報は、ＣＡＮ－ＩＤ（Ｃｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ－Ｉｄｅｎｔｉｆｉｅｒ）であり、
前記車載ネットワークは、前記車両に搭載されるＴＣＵ（Ｔｅｌｅｍａｔｉｃｓ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｕｎｉｔ）、自動運転ＥＣＵ、エンジンＥＣＵ、センサ、ナビゲーション装置、ヒューマンマシンインタフェースまたはカメラを含み、
前記フレームは、ＣＡＮ、ＦｌｅｘＲａｙ、ＭＯＳＴ（Ｍｅｄｉａ　Ｏｒｉｅｎｔｅｄ　Ｓｙｓｔｅｍｓ　Ｔｒａｎｓｐｏｒｔ）、イーサネットまたはＬＩＮ（Ｌｏｃａｌ　Ｉｎｔｅｒｃｏｎｎｅｃｔ　Ｎｅｔｗｏｒｋ）の通信規格に従って前記車載ネットワークにおいて伝送され、
前記集計部は、前記監視部の監視結果に基づいて、前記ＣＡＮ－ＩＤごとのプロトコルエラー発生回数を集計する、検知装置。

【符号の説明】

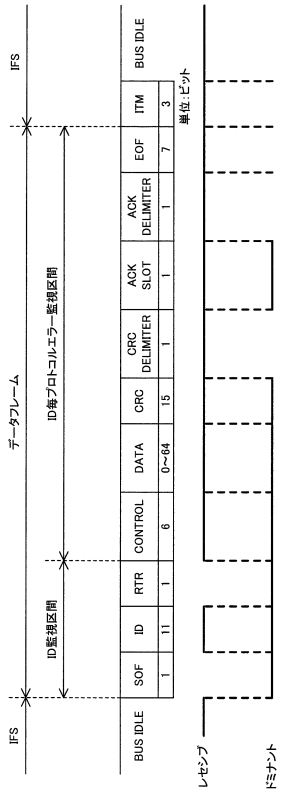
【０２１２】

１　車両
１２　車載ネットワーク
１３　バス
５１　送受信部（監視部）
５２　中継部
５４　集計部
５５　検知部
５６　記憶部
１０１　ゲートウェイ装置
１２１　車載ＥＣＵ
１２２　トランシーバ
１２３　攻撃デバイス
３０１　車載通信システム

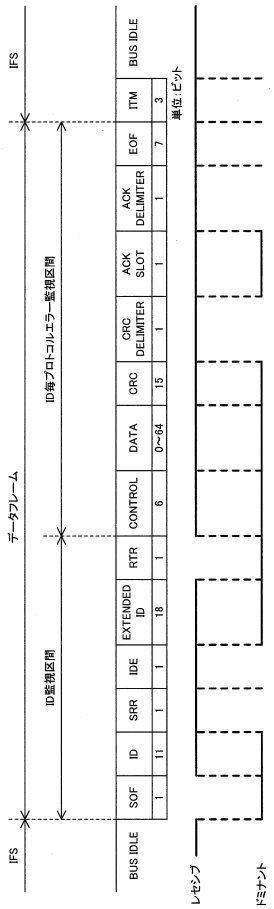
【図１】


1
車両
301
12
車載ネットワーク
101
121
車載ECU
13A
13B
13C
13D
ゲートウェイ装置

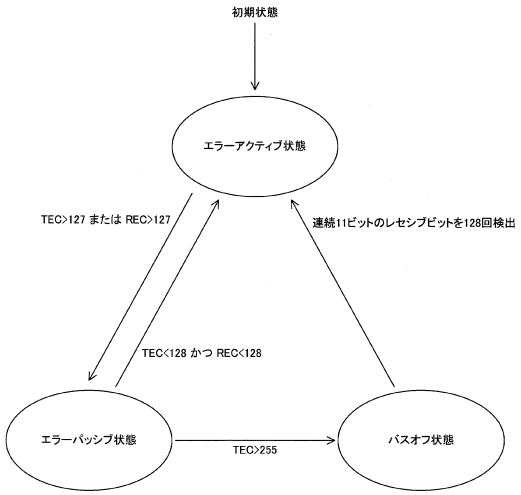
【図２】


IFS
BUS IDLE
ITM
EOF
ACK DELIMITER
ACK SLOT
CRC DELIMITER
CRC
DATA
CONTROL
RTR
ID
SOF
データフレーム
ID毎プロトコルエラー監視区間
ID監視区間
単位：ビット
レセシブ
ドミナント

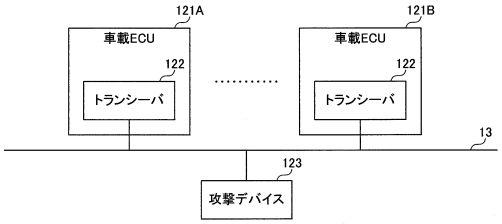
【図３】


IFS
BUS IDLE
ITM
EOF
ACK DELIMITER
ACK SLOT
CRC DELIMITER
CRC
DATA
CONTROL
RTR
EXTENDED ID
IDE
SRR
ID
SOF
データフレーム
ID毎プロトコルエラー監視区間
ID監視区間
単位：ビット
レセシブ
ドミナント

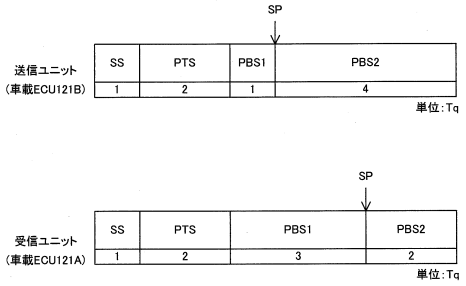
【図４】


初期状態
エラーアクティブ状態
TEC>127 または REC>127
連続11ビットのレセシブビットを128回検出
TEC<128 かつ REC<128
エラーパッシブ状態
TEC>255
バスオフ状態

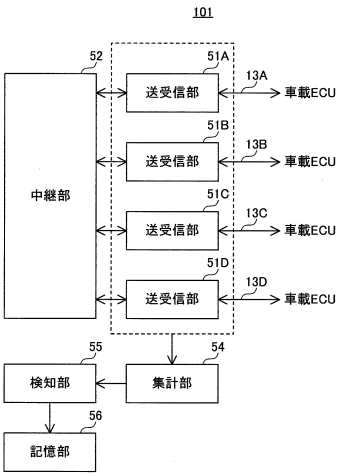
【図５】


121A
車載ECU
122
トランシーバ
121B
車載ECU
122
トランシーバ
13
123
攻撃デバイス

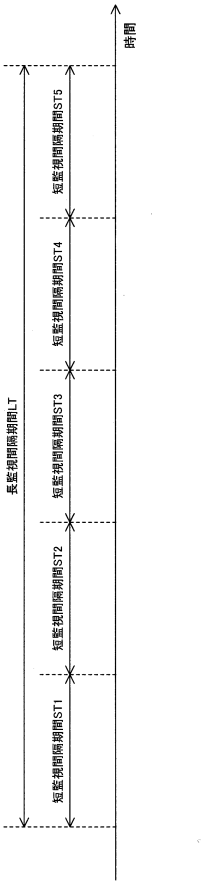
【図６】



【図７】



【図８】



【図９】

Tbl1

CAN-ID	ST1	ST2	ST3	ST4	ST5	LT
1	5回	10回	5回	10回	20回	50回
2	5回	5回	0回	0回	0回	10回
.....	.....	.....	.....	.....	.....	.....
N	0回	0回	0回	0回	0回	0回

プロトコルエラー発生回数

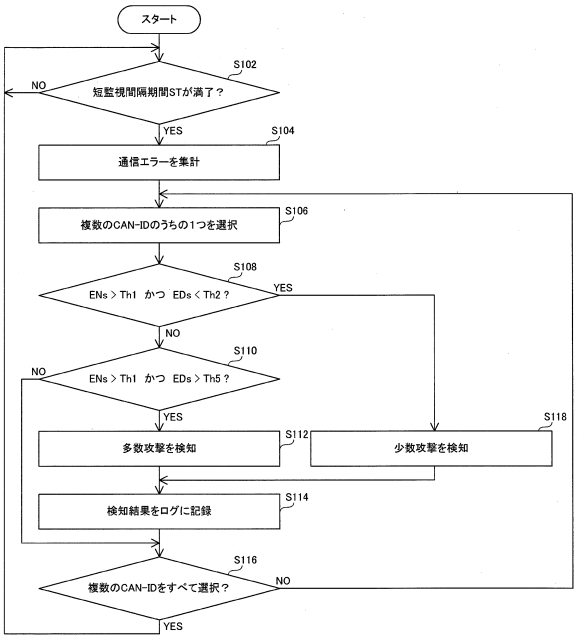
【図１０】

Tbl2

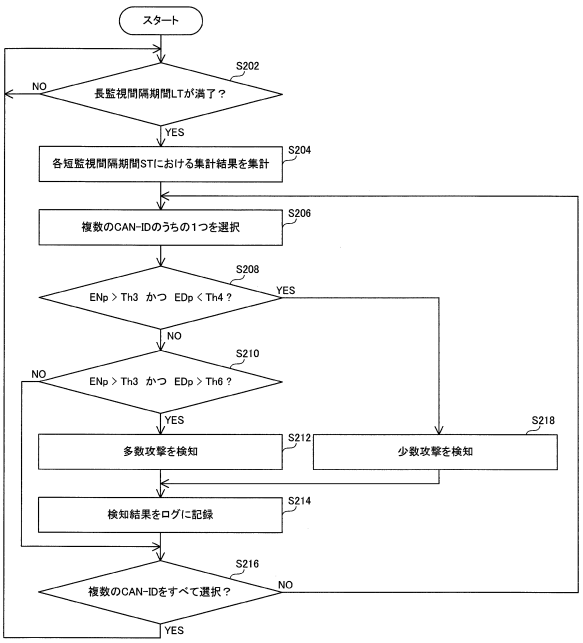
ST1	ST2	ST3	ST4	ST5	LT
2	2	1	1	1	平均
					1.4

バス内プロトコルエラー分布

【図１１】


スタート
S102
短監視間隔期間STが満了？
NO
YES
S104
通信エラーを集計
S106
複数のCAN-IDのうちの１つを選択
S108
ENs＞Th1 かつ EDs＜Th2？
YES
NO
S110
ENs＞Th1 かつ EDs＞Th5？
NO
YES
S112
多数攻撃を検知
S118
少数攻撃を検知
S114
検知結果をログに記録
S116
複数のCAN-IDをすべて選択？
NO
YES

【図１２】


スタート
S202
長監視間隔期間LTが満了？
NO
YES
S204
各短監視間隔期間STにおける集計結果を集計
S206
複数のCAN-IDのうちの１つを選択
S208
ENp＞Th3 かつ EDp＜Th4？
YES
NO
S210
ENp＞Th3 かつ EDp＞Th6？
NO
YES
S212
多数攻撃を検知
S218
少数攻撃を検知
S214
検知結果をログに記録
S216
複数のCAN-IDをすべて選択？
NO
YES

フロントページの続き

審査官　鈴木　肇

(56)参考文献　特開２０１３－１３１９０７（ＪＰ，Ａ）
国際公開第２０１５／１５１４１８（WO，Ａ1）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／００－１２／９５５
Ｈ０４Ｌ　９／００－　９／０４
Ｂ６０Ｒ　１６／００－１７／０２