

【公報種別】特許法第 17 条の 2 の規定による補正の掲載

【部門区分】第 7 部門第 3 区分

【発行日】令和 2 年 11 月 5 日 (2020.11.5)

【公開番号】特開 2019-83534 (P2019-83534A)

【公開日】令和 1 年 5 月 30 日 (2019.5.30)

【年通号数】公開・登録公報 2019-020

【出願番号】特願 2018-241048 (P2018-241048)

【国際特許分類】

H 0 4 L 12/28 (2006.01)

H 0 4 L 12/66 (2006.01)

G 0 6 F 21/55 (2013.01)

B 6 0 R 16/023 (2006.01)

【F I】

H 0 4 L 12/28 2 0 0 Z

H 0 4 L 12/66 B

G 0 6 F 21/55

B 6 0 R 16/023 P

【手続補正書】

【提出日】令和 2 年 9 月 17 日 (2020.9.17)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

記憶部を含む情報処理システムで実行される、ネットワーク及び前記ネットワークに接続される 1 以上の電子制御ユニットを含む車載ネットワークシステムにおける不正通信の検知方法であって、

前記ネットワークに送出されたメッセージが攻撃メッセージであるか否かを判定する不正検知ステップと、

前記メッセージが攻撃メッセージである場合、前記攻撃メッセージに関する情報を前記記憶部に保存する情報保存ステップと、

前記攻撃メッセージに関する情報から、前記ネットワークにおいて発生する通信パターンを識別する通信パターン識別ステップと、

前記メッセージが、前記通信パターン識別ステップで識別された通信パターンに適合するか否かを判定する通信パターン判定ステップとを含み、

少なくとも前記不正検知ステップ及び前記通信パターン判定ステップは、前記ネットワークに順次送出されて受信された複数のメッセージのそれぞれに対して実行され、

前記通信パターン判定ステップの実行後に受信されたメッセージに対して実行される前記不正検知ステップでは、当該メッセージが攻撃メッセージであるか否かの判定に、実行済みの当該通信パターン判定ステップにおける判定結果を用い、

前記通信パターン識別ステップにおいて、前記攻撃メッセージに関する情報に統計学的処理を実行して得られるモデルを前記通信パターンとして取得することで前記通信パターンを識別し、

さらに、前記通信パターンを用いて、次に受信されるメッセージに含まれるデータ値の予測値を算出するデータ値予測ステップを含み、

前記通信パターン判定ステップにおいて、前記予測値と、前記受信されたメッセージが

含むデータ値との比較の結果に基づいて当該受信されたメッセージが前記通信パターンに適合するか否かを判定し、

前記通信パターン識別ステップにおいて、前記モデルとして、AR (Auto Regressive) モデル、ARMA (Auto Regressive Moving Average) モデル、HMM (Hidden Markov Model)、又はベイジアン (Bayesian) モデルを取得し、

前記情報保存ステップでは、前記不正検知ステップにおいて攻撃メッセージであるか否かの判定が不可能であったグレーメッセージに関する情報をさらに前記記憶部に保存し、

前記通信パターン識別ステップでは、さらに前記グレーメッセージに関する情報を前記統計学的処理の実行の対象として前記通信パターンを取得する、

不正通信検知方法。

【請求項 2】

前記通信パターン識別ステップでは、前記通信パターンとして、前記複数のメッセージに含まれるデータ値の変化に関するパターンが識別される、

請求項 1 に記載の不正通信検知方法。

【請求項 3】

前記データ値の変化に関するパターンは、前記複数のメッセージに含まれる同じ種類のデータ量を表す複数のメッセージそれぞれに含まれる前記データ値の変化の有無に関するパターン、前記同じ種類のデータ量を表す複数のメッセージに含まれるデータ量の増加若しくは減少に関するパターン、又は前記同じ種類のデータ量を表すメッセージに含まれるデータ値と、他の種類のデータ量を表すメッセージに含まれるデータ値との差分若しくは比に関するパターンである、

請求項 2 に記載の不正通信検知方法。

【請求項 4】

前記通信パターン識別ステップでは、前記通信パターンとして、前記複数のメッセージの通信タイミングに関するパターンが識別される、

請求項 1 に記載の不正通信検知方法。

【請求項 5】

前記複数のメッセージの通信タイミングに関する通信パターンは、前記複数のメッセージに含まれる同じ種類のデータ量を表す複数のメッセージの送信時刻の間隔に関するパターン、又は前記同じ種類のデータ量を表す複数のメッセージ同士又は異なる種類のデータ量を表すメッセージ間の送信時刻の差分に関するパターンである、

請求項 4 に記載の不正通信検知方法。

【請求項 6】

前記車載ネットワークシステムを搭載する車両は、運転者による当該車両の運転行動の少なくとも一部を支援又は代行するための自動運転機能を備え、

さらに、前記自動運転機能が実行中であるか否かを認識する車両状態認識ステップを含み、

前記情報保存ステップは、前記車両状態認識ステップにおいて前記自動運転機能が実行中でないと認識されているときに実行され、

前記通信パターン判定ステップは、前記車両状態認識ステップにおいて前記自動運転機能が実行中であると認識されているときに実行される、

請求項 1 から 5 のいずれか一項に記載の不正通信検知方法。

【請求項 7】

前記攻撃メッセージは、前記車載ネットワークシステムに含まれる前記 1 以上の電子制御ユニットのいずれかによって前記ネットワークに送出され、

前記不正検知ステップ、前記情報保存ステップ、前記通信パターン識別ステップ、及び前記通信パターン判定ステップの少なくとも一部は、前記攻撃メッセージを送出する電子制御ユニットとは別の前記車載ネットワークシステムに含まれる電子制御ユニット、又は前記車載ネットワークシステムがさらに含むゲートウェイによって実行される

請求項 1 から 6 のいずれか一項に記載の不正通信検知方法。

【請求項 8】

前記車載ネットワークシステムに含まれる前記 1 以上の電子制御ユニットの少なくとも 1 つは、前記車載ネットワークシステムの外部から送信されたデータを取得する送信データ取得部を備え、

前記送信データ取得部を備える前記電子制御ユニットは、前記車載ネットワークシステムの外部から送信されたデータに含まれるメッセージに対して少なくとも前記不正検知ステップを実行する

請求項 1 から 7 のいずれか一項に記載の不正通信検知方法。

【請求項 9】

ネットワーク及び前記ネットワークに接続される 1 以上の電子制御ユニットを含む車載ネットワークシステムにおける不正制御を検知するための不正通信検知システムであって、

1 個以上のプロセッサと、

記憶部とを含み、

前記 1 個以上のプロセッサは、前記ネットワークに送出されたメッセージが攻撃メッセージであるか否かを判定する不正検知を実行し、

前記メッセージが攻撃メッセージである場合、前記攻撃メッセージに関する情報を前記記憶部に保存し、

前記攻撃メッセージに関する情報から、前記ネットワークにおいて発生する通信パターンを識別し、

前記メッセージが、識別された前記通信パターンに適合するか否かを判定する通信パターン判定を実行し、

少なくとも前記不正検知及び前記通信パターン判定は、前記ネットワークに順次送出された複数のメッセージのそれぞれに対して実行し、

前記通信パターン判定の実行後に送出されたメッセージに対する前記不正検知において、当該メッセージが攻撃メッセージであるか否かの判定に、実行済みの当該通信パターン判定における判定結果を用い、

前記通信パターンの識別において、前記攻撃メッセージに関する情報に統計学的処理を実行して得られるモデルを前記通信パターンとして取得することで前記通信パターンを識別し、

さらに、前記通信パターンを用いて、次に受信されるメッセージに含まれるデータ値の予測値を算出し、

前記通信パターンの判定において、前記予測値と、前記受信されたメッセージが含むデータ値との比較の結果に基づいて当該受信されたメッセージが前記通信パターンに適合するか否かを判定し、

前記通信パターンの識別において、前記モデルとして、AR (AutoRegressive) モデル、ARMA (AutoRegressive Moving Average) モデル、HMM (Hidden Markov Model)、又はベイジアン (Bayesian) モデルを取得し、

前記記憶部への保存では、前記不正検知において攻撃メッセージであるか否かの判定が不可能であったグレーメッセージに関する情報をさらに前記記憶部に保存し、

前記通信パターンの識別では、さらに前記グレーメッセージに関する情報を前記統計学的処理の実行の対象として前記通信パターンを取得する、

不正通信検知システム。

【請求項 10】

ネットワーク及び前記ネットワークに接続される 1 以上の電子制御ユニットを含む車載ネットワークシステムにおける不正通信を検知するためのシステムであって、1 個以上のプロセッサと記憶部とを含む不正通信検知システムにおいて、前記 1 個以上のプロセッサに請求項 1 に記載の不正通信検知方法を実施させるためのプログラム。