

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7588587号
(P7588587)

(45)発行日 令和6年11月22日(2024.11.22)

(24)登録日 令和6年11月14日(2024.11.14)

(51)国際特許分類

F I

H O 4 L 43/022 (2022.01)

H O 4 L 12/22 (2006.01)

H O 4 L 12/28 (2006.01)

H O 4 L 43/022

H O 4 L 12/22

H O 4 L 12/28 1 0 0 A

請求項の数 13 (全40頁)

(21)出願番号	特願2021-539055(P2021-539055)	(73)特許権者	514136668
(86)(22)出願日	令和3年1月18日(2021.1.18)		パナソニック インテレクチュアル プロ
(86)国際出願番号	PCT/JP2021/001545		パティ コーポレーション オブ アメリカ
(87)国際公開番号	WO2021/149651		Panasonic Intellec
(87)国際公開日	令和3年7月29日(2021.7.29)		tual Property Corpo
審査請求日	令和5年10月30日(2023.10.30)		ration of America
(31)優先権主張番号	特願2020-7070(P2020-7070)		アメリカ合衆国 9 0 5 0 4 カリフォル
(32)優先日	令和2年1月20日(2020.1.20)		ニア州, トーランス, スイート 4 5 0
(33)優先権主張国・地域又は機関	日本国(JP)	(74)代理人	100109210
			弁理士 新居 広守
		(74)代理人	100137235
			弁理士 寺谷 英作
		(74)代理人	100131417
			弁理士 道坂 伸一

最終頁に続く

(54)【発明の名称】 攻撃検知方法、攻撃検知システム、及びプログラム

(57)【特許請求の範囲】
【請求項1】

モビリティ内部でモビリティの制御のために送受信されるセンサデータに対する攻撃を検知する攻撃検知方法であって、

前記センサデータに含まれるセンサ値の識別子ごとに、前記センサデータの前記センサ値のばらつきを示す統計値、及び、前記センサ値の変化のタイミングを示す前記モビリティのイベント情報の少なくとも一方に基づいて、前記センサデータから前記攻撃を検知するための前記センサ値を抽出する、サンプリング間隔と当該サンプリング間隔ごとのサンプリング時間とを含むサンプリング方針を決定するサンプリング方針決定ステップと、

前記サンプリング間隔と前記サンプリング時間とに基づいて前記センサデータから抽出された2以上のセンサ値と、前記サンプリング時間中の前記2以上のセンサ値の時間的な順序を示す第一の順序情報と、前記サンプリング間隔ごとの前記2以上のセンサ値の時間的な順序を示す第二の順序情報とを含むサンプリングデータを生成するサンプリングデータ生成ステップと、

前記サンプリングデータに含まれる評価対象データのセンサ値と、前記第一の順序情報と、前記評価対象データが取得された前記サンプリング時間における前記評価対象データより過去のセンサ値の時系列データを示す短期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第一の異常スコアを算出し、前記評価対象データのセンサ値と、前記第二の順序情報と、前記評価対象データが取得された前記サンプリング間隔より過去の前記サンプリング間隔で取得されたセンサ値の変化を示す長期センサフローとに基

づいて、前記評価対象データの異常の度合いを示す第二の異常スコアを算出し、算出された前記第一の異常スコアと前記第二の異常スコアとに基づいて、前記評価対象データが前記攻撃によるものであるか否かを判定し、判定結果を出力する攻撃判定ステップと、を含む、

攻撃検知方法。

【請求項 2】

前記統計値は、前記識別子ごとのセンサ値のばらつきを示す分散値を含み、

前記イベント情報は、前記センサ値の変化が生じたか否かを示すフラグ情報を含み、

前記サンプリング方針決定ステップでは、前記分散値と前記フラグ情報とに基づいて、前記サンプリング間隔と前記サンプリング時間とを決定する、

請求項 1 に記載の攻撃検知方法。

【請求項 3】

前記サンプリング方針決定ステップでは、前記分散値が第一の閾値以上であるか否かの判定結果と、前記フラグ情報が前記センサ値の変化が生じていないことを示すか否かとの組み合わせに応じて、前記サンプリング時間と前記サンプリング間隔とを決定する、

請求項 2 に記載の攻撃検知方法。

【請求項 4】

前記フラグ情報は、前記モビリティの駆動部の ON 及び OFF の切り替え、シフトレバーの切り替え、自動運転モードの ON 及び OFF の切り替えの少なくとも 1 つが生じたか否かを示す情報を含む、

請求項 2 又は 3 に記載の攻撃検知方法。

【請求項 5】

前記サンプリングデータ生成ステップでは、前記サンプリング時間中に観測されるべき正常受信データ数に基づいて、前記サンプリング時間内において抽出するセンサデータの抽出数を決定し、決定された前記抽出数のセンサデータを抽出する、

請求項 1 ～ 4 のいずれか 1 項に記載の攻撃検知方法。

【請求項 6】

前記サンプリングデータ生成ステップでは、前記サンプリング時間中に観測された前記センサ値の数が前記正常受信データ数以上であるか否かを判定し、前記正常受信データ数以上である場合、所定数の前記センサ値を抽出し、前記正常受信データ数以上でない場合、前記センサデータに含まれる前記センサ値を全数抽出する、

請求項 5 に記載の攻撃検知方法。

【請求項 7】

前記第一の順序情報は、前記サンプリング時間中において前記 2 以上のセンサ値が取得された順序を示す第一のインデックスであり、

前記第二の順序情報は、前記 2 以上のセンサ値が取得された前記サンプリング間隔の順序を示す第二のインデックスであり、

前記攻撃判定ステップでは、前記評価対象データに対応づく前記第一のインデックスが第三の閾値未満であり、かつ、前記評価対象データに対応づく前記第二のインデックスが第四の閾値未満である場合、前記評価対象データが前記攻撃によるものであるか否かが不明であると判定し、前記第一の異常スコア及び前記第二の異常スコアに基づく第三の異常スコアが第五の閾値以上の場合、前記評価対象データが前記攻撃によるものであると判定し、前記第三の異常スコアが前記第五の閾値未満の場合、前記評価対象データが正常であると判定し、判定した結果を示す前記評価対象データに対応づく前記判定結果を出力する、

請求項 1 ～ 6 のいずれか 1 項に記載の攻撃検知方法。

【請求項 8】

さらに、前記評価対象データに対応づく前記判定結果と、前記第一の順序情報と、前記第二の順序情報とに基づいて、前記短期センサフローと前記長期センサフローとを更新する更新ステップを含む、

請求項 1 ～ 7 のいずれか 1 項に記載の攻撃検知方法。

10

20

30

40

50

【請求項 9】

前記更新ステップでは、前記評価対象データに対応づく前記判定結果が攻撃である場合、前記評価対象データが取りうるべきセンサ値を前記短期センサフロー及び前記長期センサフローの少なくとも1つを用いて推定し、推定された推定センサ値と、前記第一の順序情報と、前記第二の順序情報とに基づいて、前記短期センサフローと前記長期センサフローとを更新し、前記評価対象データに対応づく前記判定結果が正常もしくは不明である場合、前記評価対象データのセンサ値と、前記第一の順序情報と、前記第二の順序情報とに基づいて、前記短期センサフローと前記長期センサフローとを更新する、

請求項 8 に記載の攻撃検知方法。

【請求項 10】

前記センサデータは、前記モビリティに搭載される機器に記憶され、CAN (Controller Area Network: 登録商標)、CAN FD (CAN with Flexible Data-rate)、FlexRay (登録商標)、及びEthernet (登録商標) の少なくとも1つのプロトコルに従って、任意の走行時間間隔で送受信されるバイト表現のネットワークデータをデコードした結果である、

請求項 1 ～ 9 のいずれか 1 項に記載の攻撃検知方法。

【請求項 11】

前記モビリティは、車両である、

請求項 1 ～ 10 のいずれか 1 項に記載の攻撃検知方法。

【請求項 12】

モビリティ内部でモビリティの制御のために送受信されるセンサデータに対する攻撃を検知する攻撃検知システムであって、

前記センサデータに含まれるセンサ値の識別子ごとに、前記センサデータの前記センサ値のばらつきを示す統計値、及び、前記センサ値の変化のタイミングを示す前記モビリティのイベント情報の少なくとも一方に基づいて、前記センサデータから前記攻撃を検知するための前記センサ値を抽出する、サンプリング間隔と当該サンプリング間隔ごとのサンプリング時間とを含むサンプリング方針を決定するサンプリング方針決定部と、

前記サンプリング間隔と前記サンプリング時間とに基づいて、前記センサデータから抽出された 2 以上のセンサ値と、前記サンプリング時間中の前記 2 以上のセンサ値の時間的な順序を示す第一の順序情報と、前記サンプリング間隔ごとの前記 2 以上のセンサ値の時間的な順序を示す第二の順序情報とを含むサンプリングデータを生成するサンプリングデータ生成部と、

前記サンプリングデータに含まれる評価対象データのセンサ値と、前記第一の順序情報と、前記評価対象データが取得された前記サンプリング時間における前記評価対象データより過去のセンサ値の時系列データを示す短期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第一の異常スコアを算出し、前記評価対象データのセンサ値と、前記第二の順序情報と、前記評価対象データが取得された前記サンプリング間隔より過去の前記サンプリング間隔で取得されたセンサ値の変化を示す長期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第二の異常スコアを算出し、算出された前記第一の異常スコアと前記第二の異常スコアとに基づいて、前記評価対象データが前記攻撃によるものであるか否かを判定し、判定結果を出力する攻撃判定部と、を備える、攻撃検知システム。

【請求項 13】

請求項 1 ～ 11 のいずれか 1 項に記載の攻撃検知方法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】

本開示は、センサデータに対する攻撃を検知する攻撃検知方法、攻撃検知システム、及びプログラムに関する。

10

20

30

40

50

【背景技術】

【0002】

自動車を監視するシステム（監視システム）は、車両制御を目的として送受信される車両センサデータに対する攻撃を検知すること（攻撃検知）が求められる。監視システムは、監視対象が大規模であることも特徴である。その為、自動車とシステムとの間の通信コスト又は攻撃検知の演算コストといった監視コストを抑える必要がある。演算コストを抑えた監視システムとして、監視対象であるセンサデータに対して周波数解析の結果からピーク値などの特徴量を抽出することで、データ量を削減したサンプリングログを監視システムへ送信する技術が開示されている（例えば、特許文献1参照）。

【先行技術文献】

【特許文献】

【0003】

【文献】特開2018-164159号公報

【文献】国際公開第2019/187350号

【非特許文献】

【0004】

【文献】P. Malhotra, “Long Short Term Memory Networks for Anomaly Detection in Time Series”, 23rd European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, ESANN 2015.

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、特許文献1に記載の技術において、サンプリングするデータは、データ量削減のため、監視システムが定める一意の時間間隔のデータである。その為、サンプリングされたデータの中に攻撃メッセージが含まれず、攻撃を見逃してしまう可能性がある。

【0006】

また、センサデータの正常な周期からの乖離を用いて、サンプリングされたメッセージから攻撃（攻撃メッセージ）を検知する技術が知られている（例えば、特許文献2参照）。しかしながら、このような技術においても、攻撃メッセージの取得間隔によっては、攻撃を正確に検知することが困難である。

【0007】

そのため、データ量削減と攻撃検知性能とを両立することが望まれているが、上記のように従来技術では、データ量削減と攻撃検知性能とを両立することが困難である。

【0008】

そこで、本開示は、データ量削減と攻撃検知性能とを両立することができる攻撃検知方法、攻撃検知システム、及びプログラムを提供する。

【課題を解決するための手段】

【0009】

本開示の一態様に係る攻撃検知方法は、モビリティ内部でモビリティの制御のために送受信されるセンサデータに対する攻撃を検知する攻撃検知方法であって、前記センサデータに含まれるセンサ値の識別子ごとに、前記センサデータの前記センサ値のばらつきを示す統計値、及び、前記センサ値の変化のタイミングを示す前記モビリティのイベント情報の少なくとも一方に基づいて、前記センサデータから前記攻撃を検知するための前記センサ値を抽出する、サンプリング間隔と当該サンプリング間隔ごとのサンプリング時間とを含むサンプリング方針を決定するサンプリング方針決定ステップと、前記サンプリング間隔と前記サンプリング時間とに基づいて前記センサデータから抽出された2以上のセンサ値と、前記サンプリング時間中の前記2以上のセンサ値の時間的な順序を示す第一の順序情報と、前記サンプリング間隔ごとの前記2以上のセンサ値の時間的な順序を示す第二の

10

20

30

40

50

順序情報とを含むサンプリングデータを生成するサンプリングデータ生成ステップと、前記サンプリングデータに含まれる評価対象データのセンサ値と、前記第一の順序情報と、前記評価対象データが取得された前記サンプリング時間における前記評価対象データより過去のセンサ値の時系列データを示す短期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第一の異常スコアを算出し、前記評価対象データのセンサ値と、前記第二の順序情報と、前記評価対象データが取得された前記サンプリング間隔より過去の前記サンプリング間隔で取得されたセンサ値の変化を示す長期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第二の異常スコアを算出し、算出された前記第一の異常スコアと前記第二の異常スコアとに基づいて、前記評価対象データが前記攻撃によるものであるか否かを判定し、判定結果を出力する攻撃判定ステップと、を含む。

10

【0010】

また、本開示の一態様に係る攻撃検知システムは、モビリティ内部でモビリティの制御のために送受信されるセンサデータに対する攻撃を検知する攻撃検知システムであって、前記センサデータに含まれるセンサ値の識別子ごとに、前記センサデータの前記センサ値のばらつきを示す統計値、及び、前記センサ値の変化のタイミングを示す前記モビリティのイベント情報の少なくとも一方に基づいて、前記センサデータから前記攻撃を検知するための前記センサ値を抽出する、サンプリング間隔と当該サンプリング間隔ごとのサンプリング時間とを含むサンプリング方針を決定するサンプリング方針決定部と、前記サンプリング間隔と前記サンプリング時間とに基づいて、前記センサデータから抽出された2以上のセンサ値と、前記サンプリング時間中の前記2以上のセンサ値の時間的な順序を示す第一の順序情報と、前記サンプリング間隔ごとの前記2以上のセンサ値の時間的な順序を示す第二の順序情報とを含むサンプリングデータを生成するサンプリングデータ生成部と、前記サンプリングデータに含まれる評価対象データのセンサ値と、前記第一の順序情報と、前記評価対象データが取得された前記サンプリング時間における前記評価対象データより過去のセンサ値の時系列データを示す短期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第一の異常スコアを算出し、前記評価対象データのセンサ値と、前記第二の順序情報と、前記評価対象データが取得された前記サンプリング間隔より過去の前記サンプリング間隔で取得されたセンサ値の変化を示す長期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第二の異常スコアを算出し、算出された前記第一の異常スコアと前記第二の異常スコアとに基づいて、前記評価対象データが前記攻撃によるものであるか否かを判定し、判定結果を出力する攻撃判定部と、を備える。

20

30

【0011】

また、本開示の一態様に係るプログラムは、上記の攻撃検知方法をコンピュータに実行させるためのプログラムである。

【発明の効果】

【0012】

本開示の一態様によれば、データ量削減と攻撃検知性能とを両立することができる攻撃検知方法、攻撃検知システム、及びプログラムを提供することができる。

【図面の簡単な説明】

【0013】

40

【図1】図1は、実施の形態に係る監視システムの構成を示すブロック図である。

【図2】図2は、実施の形態に係る監視システムの動作の概要を示すフローチャートである。

【図3】図3は、実施の形態に係るサンプリング方針生成部の構成を示すブロック図である。

【図4】図4は、実施の形態に係るサンプリング方針生成処理を示すフローチャートである。

【図5】図5は、実施の形態に係る車両センサデータの一例を示す図である。

【図6】図6は、実施の形態に係るサンプリングを説明する図である。

【図7】図7は、実施の形態に係るサンプリング方針データの一例を示す図である。

50

【図 8】図 8 は、実施の形態に係るサンプリングデータ生成部の構成を示すブロック図である。

【図 9】図 9 は、実施の形態に係るサンプリングデータ生成処理を示すフローチャートである。

【図 10】図 10 は、実施の形態に係るサンプリングデータの一例を示す図である。

【図 11】図 11 は、実施の形態に係る攻撃検知部の構成を示すブロック図である。

【図 12】図 12 は、実施の形態に係る攻撃検知処理を示すフローチャートである。

【図 13】図 13 は、実施の形態に係る基点データの一例を示す図である。

【図 14】図 14 は、実施の形態に係る検知結果の一例を示す図である。

【図 15】図 15 は、実施の形態に係る基点データ更新部の構成を示すブロック図である。

10

【図 16】図 16 は、実施の形態に係る基点データ更新処理を示すフローチャートである。

【図 17】図 17 は、実施の形態に係る監視システムの構成を示す概略図である。

【図 18】図 18 は、実施の形態に係る車載装置の構成を示す概略図である。

【発明を実施するための形態】

【0014】

(本開示の基礎となった知見)

低監視コストで実現できる監視システムを実現するためには、適切なサンプリング手法と攻撃検知手法との双方を構築する必要がある。

【0015】

特許文献 1 では、監視システムにおける監視コストを抑えるために、周期的なセンサデータの周波数解析の結果に基づき、サンプリング間隔でピーク値などの代表値を抽出することで、低密度のデータを生成する。したがって、センサ値が周期的に取得できること又は規則的な値を有することを前提としている。

20

【0016】

しかしながら、攻撃者により、取得周期又はセンサ値の規則性が大きく崩される場合がある。特許文献 1 では、単純に代表値を抽出するので、周期的なセンサデータのサンプリング時に攻撃者により注入された攻撃値を欠損してしまい、攻撃の検知が困難な場合がある。つまり、サンプリング時に攻撃者により注入された攻撃値がサンプリングされない場合がある。そのため、攻撃検知に適した、更なるサンプリング手法を構築することが求められる。

30

【0017】

特許文献 2 では、攻撃検知手法として、センサデータの正常な周期を事前に算出し、実際に観測された周期が正常な周期にマージンを加えた範囲にない場合に、攻撃メッセージと判定する。マージンは、正常メッセージと攻撃メッセージとの衝突により生じる遅れを許容する範囲である。本手法は、追加された攻撃メッセージなどを検知できる手法としてロバストである。

【0018】

しかしながら、特許文献 2 では、メッセージの取得時間に基づいて、攻撃の有無の判定をするため、センサデータのサンプリングにより、1つのセンサ値の取得間隔がサンプリング間隔となったデータには適用することが困難である。

40

【0019】

また、非特許文献 1 では、攻撃検知手法として、センサ値の正常な振る舞いを事前に学習し、実際に観測されたセンサ値のリストに基づいて次のセンサ値を予測した結果が、正常な振る舞いから乖離している場合には、攻撃メッセージと判定する技術が開示されている。本手法は、サンプリング間隔など周期と比較して長い時間間隔の時系列データへも適用できる。

【0020】

しかしながら、次のセンサ値を予測するための実際に観測されたセンサ値のリストは、攻撃メッセージが混入しないように充足しなければならない。

【0021】

50

したがって、上記の課題を解決するために、サンプリング手法の構築に合わせて、攻撃検知手法も更なる改良が必要である。つまり、データ量削減と攻撃検知性能とを両立することが望まれる。そこで、本願発明者らは、データ量削減と攻撃検知性能とを両立することができる攻撃検知方法等について鋭意検討を行い、以下に説明する攻撃検知方法等を創案した。

【0022】

本開示の一態様に係る攻撃検知方法は、モビリティ内部でモビリティの制御のために送信されるセンサデータに対する攻撃を検知する攻撃検知方法であって、前記センサデータに含まれるセンサ値の識別子ごとに、前記センサデータの前記センサ値のばらつきを示す統計値、及び、前記センサ値の変化のタイミングを示す前記モビリティのイベント情報の少なくとも一方に基づいて、前記センサデータから前記攻撃を検知するための前記センサ値を抽出する、サンプリング間隔と当該サンプリング間隔ごとのサンプリング時間とを含むサンプリング方針を決定するサンプリング方針決定ステップと、前記サンプリング間隔と前記サンプリング時間とに基づいて前記センサデータから抽出された2以上のセンサ値と、前記サンプリング時間中の前記2以上のセンサ値の時間的な順序を示す第一の順序情報と、前記サンプリング間隔ごとの前記2以上のセンサ値の時間的な順序を示す第二の順序情報とを含むサンプリングデータを生成するサンプリングデータ生成ステップと、前記サンプリングデータに含まれる評価対象データのセンサ値と、前記第一の順序情報と、前記評価対象データが取得された前記サンプリング時間における前記評価対象データより過去のセンサ値の時系列データを示す短期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第一の異常スコアを算出し、前記評価対象データのセンサ値と、前記第二の順序情報と、前記評価対象データが取得された前記サンプリング間隔より過去の前記サンプリング間隔で取得されたセンサ値の変化を示す長期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第二の異常スコアを算出し、算出された前記第一の異常スコアと前記第二の異常スコアとに基づいて、前記評価対象データが前記攻撃によるものであるか否かを判定し、判定結果を出力する攻撃判定ステップと、を含む。

【0023】

これによれば、攻撃検知処理の対象となるセンサデータの特徴に合わせて、サンプリング間隔とサンプリング時間とを調整して、サンプリングデータの生成が行われる。さらに、サンプリング時間（短期）とサンプリング間隔（長期）とにおけるセンサ値の時間的な順序を示す2種の順序情報（例えば、インデックス）を含むサンプリングデータに基づいて、2種の異常スコアを算出することで、攻撃の判定が行われる。例えば、サンプリング間隔及びサンプリング時間の少なくとも一方が長く設定されることで、データ量を削減することができる。また、2種の異常スコアを算出することで、1種の異常スコアのみを算出する場合に比べて、精度よく攻撃を検知することができる。これにより、監視コストを抑えつつ精度良く攻撃検知ができる。よって、データ量削減と攻撃検知性能とを両立することができる。

【0024】

また、例えば、前記統計値は、前記識別子ごとのセンサ値のばらつきを示す分散値を含み、前記イベント情報は、前記センサ値の変化が生じたか否かを示すフラグ情報を含み、前記サンプリング方針決定ステップでは、前記分散値と前記フラグ情報とに基づいて、前記サンプリング間隔と前記サンプリング時間とを決定してもよい。

【0025】

これによれば、センサ値の分散値及びフラグ情報の両方を用いるので、サンプリング間隔とサンプリング時間とをより正確に決定することができる。

【0026】

また、例えば、前記サンプリング方針決定ステップでは、前記分散値が第一の閾値以上であるか否かの判定結果と、前記フラグ情報が前記センサ値の変化が生じていないことを示すか否かとの組み合わせに応じて、前記サンプリング時間と前記サンプリング間隔とを決定してもよい。

【0027】

これによれば、センサデータの分散値の判定結果とイベント情報の内容との組み合わせにより、サンプリング間隔とサンプリング時間とを決定することができる。よって、判定結果により適切なサンプリング間隔とサンプリング時間とを決定することができる。例えば、分散値が第一の閾値以上ではない場合、センサ値が安定しているので、サンプリング間隔及びサンプリング時間の少なくとも一方を、長い時間に決定することができる。これにより、抽出されるセンサデータのデータ量を適切に削減することが可能となる。

【0028】

また、例えば、前記フラグ情報は、前記モビリティの駆動部のON及びOFFの切り替え、シフトレバーの切り替え、自動運転モードのON及びOFFの切り替えの少なくとも1つが生じたか否かを示す情報を含んでいてもよい。

10

【0029】

これによれば、モビリティの駆動部、シフトレバー、及び自動運転モードの切り替えに応じたサンプリング間隔とサンプリング時間とを決定することができる。例えば、切り替えが生じてから所定時間経過後のサンプリング間隔及びサンプリング時間の少なくとも一方を、長い時間に決定することができる。これにより、センサデータのデータ量をより適切に削減することが可能となる。

【0030】

また、例えば、前記サンプリングデータ生成ステップでは、前記サンプリング時間中に観測されるべき正常受信データ数に基づいて、前記サンプリング時間内において抽出するセンサデータの抽出数を決定し、決定された前記抽出数のセンサデータを抽出してもよい。

20

【0031】

これによれば、観測されたセンサデータの数に基づいて、センサデータのデータ量をより適切に削減することが可能となる。

【0032】

また、例えば、前記サンプリングデータ生成ステップでは、前記サンプリング時間中に観測された前記センサ値の数が前記正常受信データ数以上であるか否かを判定し、前記正常受信データ数以上である場合、所定数の前記センサ値を抽出し、前記正常受信データ数以上でない場合、前記センサデータに含まれる前記センサ値を全数抽出してもよい。

【0033】

これによれば、センサデータが攻撃データを含む場合、攻撃データの欠損を抑えつつサンプリングを行うことができる。よって、サンプリングデータに対して精度良く攻撃検知ができる。

30

【0034】

また、例えば、前記第一の順序情報は、前記サンプリング時間中において前記2以上のセンサ値が取得された順序を示す第一のインデックスであり、前記第二の順序情報は、前記2以上のセンサ値が取得された前記サンプリング間隔の順序を示す第二のインデックスであり、前記攻撃判定ステップでは、前記評価対象データに対応づく前記第一のインデックスが第三の閾値未満であり、かつ、前記評価対象データに対応づく前記第二のインデックスが第四の閾値未満である場合、前記評価対象データが前記攻撃によるものであるか否かが不明であると判定し、前記第一の異常スコア及び前記第二の異常スコアに基づく第三の異常スコアが第五の閾値以上の場合、前記評価対象データが前記攻撃によるものであると判定し、前記第三の異常スコアが前記第五の閾値未満の場合、前記評価対象データが正常であると判定し、判定した結果を示す前記評価対象データに対応づく前記判定結果を出力してもよい。

40

【0035】

これによれば、サンプリングデータにおける攻撃検知が困難である評価対象データを削減しつつ、短期的及び長期的なセンサ値の変化に基づいた統合的な判定を行うことができる。よって、サンプリングデータに対して精度良く攻撃検知ができる。

【0036】

50

また、例えば、さらに、前記評価対象データに対応づく前記判定結果と、前記第一の順序情報と、前記第二の順序情報とに基づいて、前記短期センサフローと前記長期センサフローとを更新する更新ステップを含んでいてもよい。

【0037】

これによれば、攻撃検知の判定に用いる短期センサフローと長期センサフローとを更新することができる。更新された短期センサフローと長期センサフローとを用いることで、攻撃検知性能を向上させることができる。

【0038】

また、例えば、前記更新ステップでは、前記評価対象データに対応づく前記判定結果が攻撃である場合、前記評価対象データが取りうるべきセンサ値を前記短期センサフロー及び前記長期センサフローの少なくとも1つを用いて推定し、推定された推定センサ値と、前記第一の順序情報と、前記第二の順序情報とに基づいて、前記短期センサフローと前記長期センサフローとを更新し、前記評価対象データに対応づく前記判定結果が正常もしくは不明である場合、前記評価対象データのセンサ値と、前記第一の順序情報と、前記第二の順序情報とに基づいて、前記短期センサフローと前記長期センサフローとを更新してもよい。

【0039】

これによれば、サンプリングデータに攻撃データが含まれる場合でも、攻撃データを除去して、適切な短期センサフロー及び長期センサフローに更新することができる。つまり、短期センサフロー及び長期センサフローに攻撃データが含まれることを抑制することができる。よって、サンプリングデータに対してさらに精度良く攻撃検知ができる。

【0040】

また、例えば、前記センサデータは、前記モビリティに搭載される機器に記憶され、CAN (Controller Area Network: 登録商標)、CAN FD (CAN with Flexible Data-rate)、FlexRay (登録商標)、及びEthernet (登録商標) の少なくとも1つのプロトコルに従って、任意の走行時間間隔で送受信されるバイト表現のネットワークデータをデコードした結果であってもよい。

【0041】

これによれば、CAN、CAN FD、FlexRay、及びEthernetの少なくとも1つのプロトコルに従って通信するネットワークにおいて、データ量削減と攻撃検知性能とを両立することができる。

【0042】

また、例えば、前記モビリティは、車両であってもよい。

【0043】

これによれば、計算リソースが限られる車両におけるデータ量を削減しつつ、当該車両に対する攻撃の攻撃検知性能の低下を抑制することができる。

【0044】

また、本開示の一態様に係る攻撃検知システムは、モビリティ内部でモビリティの制御のために送受信されるセンサデータに対する攻撃を検知する攻撃検知システムであって、前記センサデータに含まれるセンサ値の識別子ごとに、前記センサデータの前記センサ値のばらつきを示す統計値、及び、前記センサ値の変化のタイミングを示す前記モビリティのイベント情報の少なくとも一方に基づいて、前記センサデータから前記攻撃を検知するための前記センサ値を抽出する、サンプリング間隔と当該サンプリング間隔ごとのサンプリング時間とを含むサンプリング方針を決定するサンプリング方針決定部と、前記サンプリング間隔と前記サンプリング時間とに基づいて、前記センサデータから抽出された2以上のセンサ値と、前記サンプリング時間中の前記2以上のセンサ値の時間的な順序を示す第一の順序情報と、前記サンプリング間隔ごとの前記2以上のセンサ値の時間的な順序を示す第二の順序情報とを含むサンプリングデータを生成するサンプリングデータ生成部と、前記サンプリングデータに含まれる評価対象データのセンサ値と、前記第一の順序情報

10

20

30

40

50

と、前記評価対象データが取得された前記サンプリング時間における前記評価対象データより過去のセンサ値の時系列データを示す短期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第一の異常スコアを算出し、前記評価対象データのセンサ値と、前記第二の順序情報と、前記評価対象データが取得された前記サンプリング間隔より過去の前記サンプリング間隔で取得されたセンサ値の変化を示す長期センサフローとに基づいて、前記評価対象データの異常の度合いを示す第二の異常スコアを算出し、算出された前記第一の異常スコアと前記第二の異常スコアとに基づいて、前記評価対象データが前記攻撃によるものであるか否かを判定し、判定結果を出力する攻撃判定部と、を備える。また、本開示の一態様に係るプログラムは、上記の攻撃検知方法をコンピュータに実行させるためのプログラムである。

10

【0045】

これによれば、上記の攻撃検知方法と同様の効果を奏する。

【0046】

なお、これらの全般的又は具体的な態様は、システム、方法、集積回路、コンピュータプログラム又はコンピュータで読み取り可能なCD-ROM等の記録媒体で実現されても良く、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意な組み合わせで実現されてもよい。

【0047】

以下、実施の形態に係る監視方法（攻撃検知方法の一例）等について、図面を参照しながら説明する。ここで示す実施の形態は、いずれも包括的又は具体的な例を示すものである。したがって、以下の実施の形態で示される数値、構成要素、構成要素の配置及び接続形態、並びに、ステップ及びステップの順序等は一例であって、本開示に係る発明を限定するものではない。また、以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意に付加可能な構成要素である。また、各図は模式図であり、必ずしも厳密に図示されたものではない。

20

【0048】

（実施の形態）

まず、本実施の形態に係る監視システムの構成を説明する。本実施の形態では、監視システム100が車両内部で車両制御のために送受信されるセンサデータ（車両センサデータ）に対する攻撃を検知するための情報処理システムである例について説明する。車両は、監視システム100が攻撃を検知する対象であるモビリティの一例である。また、監視システム100は、攻撃検知システムの一例である。

30

【0049】

[1-1. 監視システムの構成]

図1は、本実施の形態に係る監視システム100の構成を示すブロック図である。

【0050】

監視システム100は、車両センサデータ（図5を参照）中の評価対象データごとに攻撃か否かを判定するためのシステムである。監視システム100は、当該評価対象データが攻撃によるものか否かを判定する。なお、当該評価対象データが攻撃によるものか否かを判定することを、攻撃データであるか否かを判定するとともに記載する。評価対象データは、攻撃データであるか否かを判定する対象のセンサ値であるとも言える。

40

【0051】

また、車両センサデータは、車両に搭載される機器に記憶され、例えば、CAN（Controller Area Network：登録商標）、CAN FD（CAN with Flexible Data-rate）、FlexRay（登録商標）、及びEthernet（登録商標）の少なくとも1つのプロトコルに従って、任意の走行時間間隔（移動時間間隔の一例）で送受信されるバイト表現のネットワークデータをデコードした結果である。

【0052】

監視システム100は、サンプリング部101と、サンプリングデータ監視部102と

50

を備える。サンプリング部 101 は、例えば、車両に搭載され、サンプリングデータ監視部 102 は、例えば、車両とは異なる場所（例えば、遠隔地にある監視センター）に配置される。サンプリング部 101 及びサンプリングデータ監視部 102 は、互いに通信可能（例えば、無線通信可能）に接続される。

【0053】

サンプリング部 101 は、車両の車両制御のために送受信される車両センサデータを蓄積し、蓄積されている複数のセンサ値（車両センサデータ）からサンプリングデータ監視部 102 での監視に用いられるセンサ値をサンプリング方針に基づいて抽出し、抽出したセンサ値を含むサンプリングデータをサンプリングデータ監視部 102 に送信する。サンプリング方針は、サンプリング部 101 により動的に決定される。サンプリング部 101 は、例えば、車両センサデータに含まれるセンサ値の識別子（以降において、センサ識別子とも記載する）ごとに、車両センサデータのセンサ値のばらつきを示す統計値、及び、センサ値の特徴の変化（例えば、センサ値の変化）のタイミングを示す車両イベント情報の少なくとも一方に基づいて、サンプリング方針を決定する。サンプリングデータは、例えば、2 以上のセンサ値を含む。なお、センサ識別子については後述するが、「車速」、「シフト」などの車両センサデータを一意に特定するための情報である。

【0054】

車両センサデータには、車両に搭載される各種センサのセンサ値（例えば、車速、加速度、操舵角などセンシング結果）が含まれる。なお、サンプリング方針については後述する（図 6 参照）が、サンプリング方針にはサンプリング間隔、及び当該サンプリング間隔ごとのサンプリング時間を含む。

【0055】

車両イベント情報には、周期的ではない車両イベントに関する情報が含まれ、例えば、センサ値の変化が生じたか否かを示すフラグ情報が含まれる。フラグ情報は、例えば、車両のエンジン（モビリティの駆動部の一例）の ON 及び OFF の切り替え、シフトレバーの切り替え、自動運転モードの ON 及び OFF の切り替えの少なくとも 1 つが生じたか否かを示す情報を含む。例えば、フラグ情報は、車両イベントが発生した場合、「有」を示す「1」を含み、車両イベントが発生していない場合、「無」を示す「0」を含んでいてもよい。また、監視には、車両へのサイバー攻撃の検知処理が含まれる。なお、車両のエンジンの ON 及び OFF の切り替えとは、例えば、エンジンが再起動したことであってもよい。

【0056】

サンプリング部 101 は、サンプリング方針生成部 110 と、サンプリングデータ生成部 111 と、車両センサデータ記憶部 112 と、サンプリング方針記憶部 113 と、車両情報記憶部 114 と、通信部 115 とを備える。

【0057】

サンプリング方針生成部 110 は、車両センサデータ及び車両イベントの少なくとも一方に基づいて、サンプリングデータを生成するためのサンプリング方針を決定する処理部である。本実施の形態では、サンプリング方針生成部 110 は、車両センサデータ及び車両イベントの両方に基づいてサンプリング方針を決定する。サンプリング方針生成部 110 は、例えば、車両センサデータのセンサ値のばらつきを示す統計値と、車両イベントの発生のタイミングとに基づいて、サンプリング方針を決定する。サンプリング方針生成部 110 は、サンプリング方針決定部の一例である。

【0058】

なお、センサ値の統計値は、センサ値のばらつきを示すいかなる指標が用いられてもよい。本実施の形態では、センサ値の統計値は、識別子ごとのセンサ値のばらつきを示す分散値（データ分散）が用いられる。分散値は、センサ値の散らばり度合いを示す値であり、偏差（それぞれのセンサ値と平均値との差）を二乗し、平均を取ることで算出される。分散値は、例えば、標準偏差であってもよい。

【0059】

車両イベントの発生のタイミングは、車両イベントが発生したときのタイミングを示しており、例えば、センサ値の特徴の変化のタイミングを示すとも言える。また、車両イベントの発生のタイミングは、車両イベントの発生の有無を示すとも言える。

【0060】

サンプリング方針生成部110は、例えば、車両センサデータに含まれるセンサ値のセンサ識別子ごとにサンプリング方針を決定する処理部である。サンプリング方針生成部110は、例えば、一のセンサ識別子に対応する複数のセンサ値に基づいて、当該一のセンサ識別子におけるサンプリング方針を決定する。当該サンプリング方針は、当該一のセンサ識別子に対応する複数のセンサ値からサンプリングデータを生成するためのサンプリング方針である。

【0061】

サンプリングデータ生成部111は、サンプリング方針生成部110が決定したサンプリング方針に基づいて、サンプリングデータ監視部102に送信するためのサンプリングデータを生成する処理部である。サンプリングデータ生成部111は、例えば、車両センサデータ記憶部112に記憶されている複数のセンサ値から、決定されたサンプリング方針に基づいて2以上のセンサ値を抽出することで、抽出された2以上のセンサ値を含むサンプリングデータを生成する。

【0062】

サンプリングデータ生成部111は、例えば、サンプリング間隔とサンプリング時間とに基づいて、複数のセンサ値（車両センサデータ）から抽出された2以上のセンサ値と、サンプリング時間中の2以上のセンサ値の時間的な順序を示す第一のインデックスと、サンプリング間隔ごとの2以上のセンサ値の時間的な順序を示す第二のインデックスとを含むサンプリングデータを生成する。センサ値ごとに、第一のインデックス及び第二のインデックスが付与される。

【0063】

第一のインデックスは、サンプリング時間中において2以上のセンサ値が取得された（観測された）順序を示しており、サンプリング時間中の短期的なセンサ値の動き（変化）の順序を示すとも言える。第二のインデックスは、2以上のセンサ値が取得された（観測された）サンプリング間隔の順序を示しており、サンプリング間隔での長期的なセンサ値の動き（変化）の順序を示すとも言える。第一のインデックスは、第一の順序情報の一例であり、第二のインデックスは、第二の順序情報の一例である。

【0064】

車両センサデータ記憶部112は、車両の車両制御のために送受信される複数のセンサ値（車両センサデータ）を記憶する記憶装置である。車両センサデータ記憶部112は、複数のセンサ値を蓄積する。

【0065】

サンプリング方針記憶部113は、サンプリング方針生成部110が決定したサンプリング方針を記憶する記憶装置である。

【0066】

車両情報記憶部114は、車両イベントを記憶する記憶装置である。車両情報記憶部114は、例えば、車両イベントの内容と、車両イベントが発生した時刻とが対応づけられた車両イベント情報を記憶する。

【0067】

通信部115は、インターネット等の公衆通信ネットワークを介してサンプリングデータ監視部102と通信する機能を有する処理部である。通信部115は、例えば、通信回路（通信モジュール）を含んで構成される。

【0068】

次に、サンプリングデータ監視部102は、サンプリング部101から取得したサンプリングデータに基づいて車両を監視する。具体的には、サンプリングデータ監視部102は、サンプリングデータに基づいて、短期的な異常を示す第一の異常スコア、及び長期的

10

20

30

40

50

な異常を示す第二の異常スコアのそれぞれを算出し、算出した2つの異常スコアに基づいて評価対象となるセンサ値（以降において、評価対象データとも記載する）が攻撃によるものであるか否かを判定する。つまり、サンプリングデータ監視部102は、評価対象データが攻撃データであるか否かを判定する。サンプリングデータ監視部102は、車両がサイバー攻撃を受けているか否かを判定するとも言える。サンプリングデータ監視部102が2つの異常スコアに基づいて攻撃検知を行う点に特徴を有する。

【0069】

なお、短期的な異常とは、短期間に取得された車両センサデータに基づいて検知される異常を示しており、例えば、1つのサンプリング時間内に取得された車両センサデータに基づいて検知される異常を示している。また、長期的な異常とは、短期間より長い長期間に取得された車両センサデータに基づいて検知される異常を示しており、例えば、複数のサンプリング間隔ごとに取得された車両センサデータに基づいて検知される異常を示している。

10

【0070】

サンプリングデータ監視部102は、攻撃検知部120と、基点データ更新部121と、検知器記憶部122と、検知結果記憶部123と、基点データ記憶部124と、サンプリングデータ記憶部125とを備える。

【0071】

攻撃検知部120は、サンプリング部101から取得したサンプリングデータに基づいて、評価対象データが攻撃データであるか否かの判定を行う処理部である。攻撃検知部120は、第一の異常スコアと第二の異常スコアとを算出し、算出された第一の異常スコアと第二の異常スコアとに基づいて、評価対象データが攻撃によるものであるか否かを判定し、判定結果を出力する。第一の異常スコア及び第二の異常スコアの算出については、後述する。

20

【0072】

基点データ更新部121は、評価対象データに対応づく攻撃検知部120の検知結果を示す検知結果情報と、抽出された車両センサデータにおける、第一のインデックス及び第二のインデックスとに基づいて、短期センサフローと長期センサフローとを更新する処理部である。

【0073】

短期センサフローは、短期的な異常を検知するために用いられるセンサ値の時系列データであり、例えば、1つのサンプリング時間内に取得されたセンサ値に基づいて生成される。短期センサフローは、例えば、評価対象データが取得されたサンプリング時間内のセンサ値に基づいて生成される。短期センサフローは、正常であると判定された又は正常だと推定される、短期的なセンサ値の動きを示すとも言える。

30

【0074】

長期センサフローは、短期センサフローより長い長期的な異常を検知するために用いられるセンサ値の時系列データであり、例えば、複数のサンプリング間隔ごとのセンサ値に基づいて生成される。長期センサフローは、正常であると判定された又は正常だと推定される、長期的なセンサ値の動きを示すとも言える。

40

【0075】

なお、短期センサフロー及び長期センサフローを含むデータを、基点データとも記載する。基点データには、攻撃検知部120が異常である（攻撃である）と判定したセンサ値は含まれない。基点データは、正常と判定された又は正常だと推定されるセンサ値の時系列データを示すとも言える。

【0076】

検知器記憶部122は、短期センサフローと評価対象データとの乖離の度合いを示す第一の異常スコアを算出するための第一の検知器、及び長期センサフローと当該評価対象データとの乖離の度合いを示す第二の異常スコアを算出する第二の検知器とを記憶する記憶装置である。第一の検知器は、例えば、短期センサフローと評価対象データとを入力とし

50

、第一の異常スコアを算出するように機械学習された学習済みモデルにより実現される。また、第二の検知器は、例えば、長期センサフローと評価対象データとを入力とし、第二の異常スコアを算出するように機械学習された学習済みモデルにより実現される。なお、学習済みモデルを記憶するとは、機械学習モデルにおけるネットワークパラメータ、演算のアルゴリズム（機械学習アルゴリズム）等の情報を記憶することを意味する。

【0077】

検知結果記憶部123は、攻撃検知部120の検知結果を記憶する記憶装置である。

【0078】

基点データ記憶部124は、攻撃検知部120が攻撃の有無の判定に用いる短期センサフロー及び長期センサフロー（基点データ）を記憶する記憶装置である。

【0079】

サンプリングデータ記憶部125は、サンプリング部101から取得したサンプリングデータを記憶する記憶装置である。

【0080】

通信部126は、インターネット等の公衆通信ネットワークを介してサンプリング部101と通信する機能を有する処理部である。通信部126は、例えば、通信回路（通信モジュール）を含んで構成される。

【0081】

車両センサデータ記憶部112、サンプリング方針記憶部113、車両情報記憶部114、検知器記憶部122、検知結果記憶部123、基点データ記憶部124、及びサンプリングデータ記憶部125は、例えば、ハードディスクドライブ又はソリッドステートドライブ等の書き換え可能な不揮発性のメモリで構成される。

【0082】

サンプリング方針生成部110、サンプリングデータ生成部111、通信部115、攻撃検知部120、基点データ更新部121、及び通信部126は、例えば、CPU、ASIC、又はFPGA（Field Programmable Gate Array）等のプロセッサで構成される。なお、監視システム100が備える各機能ブロックは、CPU等のプロセッサが、コンピュータに保持されている、コンピュータ読み取り可能なプログラムを実行することで実現される。

【0083】

なお、サンプリング部101及びサンプリングデータ監視部102の通信方法は特に限定されない。通信方法が無線通信である場合、サンプリング部101及びサンプリングデータ監視部102の通信は、赤外線通信又は電波通信により行われてもよい。電波通信とは、Wi-Fi（登録商標）（Wireless Fidelity）、又は、Bluetooth（登録商標）による通信であってもよい。また、例えば、サンプリング部101及びサンプリングデータ監視部102の通信は、有線通信により行われてもよい。

【0084】

なお、サンプリング部101とサンプリングデータ監視部102とを一体で構成する場合、サンプリング部101とサンプリングデータ監視部102との間の通信は、それぞれ、通信部115と通信部126とを介さなくてもよい。この場合、通信部115及び通信部126の構成は不要である。

【0085】

〔1-2. 監視システムの動作の概略〕

次に、上記のように構成された監視システム100の動作を説明する。図2は、本実施の形態に係る監視システム100の動作（攻撃検知方法）の概要を示すフローチャートである。図2に示すステップS101及びS102は、例えば、サンプリング部101において実行される処理であり、ステップS103及びS104は、例えば、サンプリングデータ監視部102において実行される処理である。

【0086】

まず、監視システム100は、車両センサデータ記憶部112に記憶されている、車両

10

20

30

40

50

における所定の走行時間の車両センサデータを用いて、サンプリング間隔及びサンプリング時間を示すサンプリング方針を生成するサンプリング方針生成処理を行う（S101）。ステップS101の処理は、サンプリング方針生成部110により実施される。所定の走行時間は、例えば、予め設定されていてもよいし、監視システム100により車両を監視する監視者により設定されてもよい。なお、ステップS101は、サンプリング方針決定ステップの一例である。

【0087】

次に、監視システム100は、決定されたサンプリング方針に基づいて、車両センサデータからサンプリングデータを生成するサンプリングデータ生成処理を行う（S102）。ステップS102の処理は、サンプリングデータ生成部111により実施される。なお、ステップS102は、サンプリングデータ生成ステップの一例である。

10

【0088】

サンプリングデータ生成部111は、サンプリング方針に基づいて、車両センサデータから一部の車両センサデータ（センサ値）を抽出し、抽出した車両センサデータ（センサ値）それぞれに対して、第一のインデックスと、第二のインデックスとを付加してサンプリングデータを生成する。つまり、サンプリングデータは、抽出された車両センサデータ、第一のインデックス及び第二のインデックスを含む。

【0089】

そして、サンプリングデータ生成部111は、生成したサンプリングデータを、通信部115により通信部126に送信する。つまり、サンプリングデータ生成部111は、生成したサンプリングデータをサンプリングデータ監視部102に送信する。

20

【0090】

次に、監視システム100は、サンプリングデータの車両センサデータ（評価対象データ）に対して異常スコアを算出する攻撃検知処理を行う（S103）。ステップS103の処理は、攻撃検知部120により実施される。ステップS103は、攻撃判定ステップの一例である。

【0091】

攻撃検知部120は、基点データ記憶部124に記憶されている基点データを用いて、評価対象データのセンサ値の異常の度合いを示す異常スコアを2種類の算出方法で算出し、算出した2種の異常スコアを用いて、評価対象データのセンサ値が攻撃であるか否かを判定する攻撃判定処理を実施する。

30

【0092】

次に、監視システム100は、評価対象データの第一のインデックスと第二のインデックスと攻撃検知処理の結果（判定結果）とを用いて、次の評価対象データにおける攻撃検知処理のために、基点データを更新する基点データ更新処理を実施する（S104）。ステップS104の処理は、基点データ更新部121により実施される。ステップS104は、更新ステップの一例である。

【0093】

以降において、各処理部の詳細な構成及びフローチャートの各ステップの詳細な動作について説明する。

40

【0094】

[2-1. サンプリング方針生成部の構成]

図3は、本実施の形態に係るサンプリング方針生成部110の構成を示すブロック図である。図3に示すように、サンプリング方針生成部110は、車両センサデータ取得部130と、センサデータ安定度算出部131と、サンプリング方針判定部132とを備える。

【0095】

車両センサデータ取得部130は、車両センサデータ記憶部112から車両サンプリングデータを取得する処理部である。車両センサデータ取得部130は、車両センサデータ記憶部112に記憶されている車両センサデータを読み出す。

【0096】

50

センサデータ安定度算出部 131 は、サンプリング方針判定部 132 におけるサンプリング方針の判定に用いるための情報を車両センサデータに基づいて算出する処理部である。例えば、センサデータ安定度算出部 131 は、センサ識別子ごとに、センサ値の統計値を算出する。本実施の形態では、センサデータ安定度算出部 131 は、センサ識別子ごとに、センサ値の分散値を算出する。

【0097】

なお、センサ識別子には、車速等の周期的に送受信される周期型の識別子、及びシフトの切り替え等の運転者による操作等に応じて発生するイベント型の識別子が含まれる。

【0098】

サンプリング方針判定部 132 は、車両センサデータに含まれるセンサ識別子ごとに、統計値及び車両イベント情報の少なくとも一方を用いてサンプリング方針を決定する。本実施の形態では、サンプリング方針判定部 132 は、統計値及び車両イベント情報の両方を用いてサンプリング方針を決定する。

【0099】

[2-2. サンプリング方針生成部の動作]

図4は、本実施の形態に係るサンプリング方針生成処理(S101)を示すフローチャートである。

【0100】

まず、サンプリング方針生成部 110 は、車両センサデータ記憶部 112 に記憶されている車両における所定の走行時間の車両センサデータを取得する(S111)。ステップ S111 の処理は、車両センサデータ取得部 130 により実施される。車両センサデータ取得部 130 は、例えば、車両センサデータを車両センサデータ記憶部 112 から取得する。

【0101】

ここで、車両センサデータについて説明する。図5は、本実施の形態に係る車両センサデータの一例を示す図である。車両センサデータは、バイナリ表現された車両ネットワークデータから攻撃検知処理の入力となりうる情報を抽出したデータである。図5に示すように、車両センサデータは、センサ識別子 142 と、データ ID 143 と、取得時刻 144 と、センサ値 145 とを含む。

【0102】

センサ識別子 142 は、車両センサデータに含まれる1つのセンサデータの車両制御対象を一意に特定するための識別子である。例えば、センサ識別子 142 として、「車速」、「シフト」等を含む。

【0103】

データ ID 143 は、車両センサデータに含まれる上記のセンサ識別子ごとに1つの車両センサデータ 141 を一意に特定するための識別子である。例えば、データ ID 143 として、1から順番に割り当てられた数値を含む。データ ID 143 は、例えば、センサ識別子ごとに、1から順番に割り当てられる。また、データ ID 143 は、例えば、取得時刻の順番に割り当てられる。

【0104】

取得時刻 144 は、車両センサデータを車両ネットワークから受信した時刻を示す時刻データである。取得時刻 144 は、例えば、センサ識別子 142 が「車速」の場合、周期的な時刻を示し、センサ識別子 142 が「シフト」などのイベント発生を有しうる識別子である場合、非周期的な時刻も取りうる。取得時刻 144 は、例えば、車両センサデータを送信するメッセージのタイムスタンプに応じて取得可能である。

【0105】

なお、取得時刻 144 は、サンプリング部 101 が車両ネットワークから車両センサデータを受信した時刻であってもよい。また、取得時刻 144 は、基準となる時刻からの経過時間(相対時刻)である例を示しているが、これに限定されず、絶対時刻であってもよい。

10

20

30

40

50

【0106】

センサ値145は、センサ識別子142に対応づく車両制御内容を示す数値データである。センサ値は、車両センサデータに複数含まれる。

【0107】

図5において、例えばセンサ識別子142が「車速」の場合、取得時刻144が「25.00ms」の時にセンサ値145が「22.11km/h」であり、次の取得時刻144が「50.01ms」の時にセンサ値145が「22.50km/h」であり、車速の受信周期が、約25msであることがわかる。以下では、車速の受信周期は、約25msである例について説明するが、受信周期はこれに限定されない。

【0108】

図4を再び参照して、サンプリング方針生成処理の説明に戻る。サンプリング方針生成部110は、車両センサデータに含まれるセンサ識別子142ごとに、センサ値145のばらつきを示すデータ分散（例えば、分散値）、及び車両センサデータに含まれる、イベント型のセンサ識別子142を示す車両イベントが発生したか否かを示す車両イベント情報（例えば、フラグ情報）を算出する（S112）。イベント型のセンサ識別子142は、例えば、エンジンONとOFFの切り替え及びシフトの切り替えなどを含む。ステップS112の処理は、センサデータ安定度算出部131により実施される。

【0109】

次に、サンプリング方針生成部110は、車両イベント情報（フラグ情報）が「有」であるか否か、もしくはデータ分散が第一の閾値以上であるか否かを判定する（S113）。ステップS113の処理は、サンプリング方針判定部132により実施される。

【0110】

サンプリング方針判定部132は、データ分散が第一の閾値以上である場合、もしくは車両イベントフラグ情報が「有」、すなわち、車両イベントが発生している場合（S113でYes）、サンプリング方針を高密度なサンプリング（高密度サンプリング）に設定する（S114）。例えば、データ分散が第一の閾値以上である場合、車両センサデータの安定度が小さい（例えば、ばらつきが大きい）ので、高密度サンプリングが行われる。これは、データ分散が第一の閾値以上である場合、サンプリング後の攻撃の有無の判定結果の再現率が低いためである。また、例えば、車両イベントの発生直後から一定時間は、車両センサデータの安定度が小さいことが想定されるので、高密度サンプリングが行われる。これは、車両イベントが発生することで長期センサフローが初期化（リセット）される場合、長期センサフローにおけるセンサ値が十分ではないためである。

【0111】

また、サンプリング方針判定部132は、それ以外の場合（S113でNo）、すなわち、データ分散が第一の閾値未満であり、かつ車両イベント情報が「無」である場合、サンプリング方針を低密度なサンプリング（低密度サンプリング）に設定する（S115）。例えば、データ分散が第一の閾値未満である場合、車両センサデータの安定度が大きい（例えば、ばらつきが小さい）ので、低密度サンプリングが行われる。これは、それ以外の場合、サンプリング後の攻撃の有無の判定結果の再現率が高いためである。また、例えば、車両イベントの発生直後から一定時間以外は、車両センサデータの安定度が大きいことが想定されるので、低密度サンプリングが行われる。これは、当該一定時間以外であれば、長期センサフローにおけるセンサ値が十分にあるためである。

【0112】

なお、ここでの低密度及び高密度とは、相対的な意味であり、高密度サンプリングとは、低密度サンプリングよりサンプリング密度が高いことを意味する。また、サンプリング密度は、サンプリング時間及びサンプリング間隔の少なくとも1つの増減により実現される。高密度サンプリングは、例えば、低密度サンプリングに比べて、サンプリング時間が長い、及び、サンプリング間隔が短い、の少なくとも1つを満たす。例えば、高密度サンプリングは、低密度サンプリングに比べて、サンプリング時間が長く、かつ、サンプリング間隔が短くてもよい。

10

20

30

40

50

【0113】

次に、サンプリング方針判定部132は、設定されたサンプリング方針をサンプリング方針記憶部113に記憶する(S116)。

【0114】

上記のように、サンプリング方針生成部110は、例えば、分散値とフラグ情報とに基づいて、サンプリング間隔と前記サンプリング時間とを決定する。例えば、サンプリング方針生成部110は、分散値が第一の閾値以上であるか否かの判定結果と、フラグ情報がセンサ値の変化が生じていないことを示すか否かとの組み合わせに応じて、サンプリング時間とサンプリング間隔とを決定してもよい。

【0115】

ここで、サンプリングの詳細について説明する。図6は、本実施の形態に係るサンプリングを説明する図である。図6に示す「○」は、車両センサデータが取得されたことを示しており、図6の横軸は時間を示す。図6では、サンプリング間隔T秒において、10個の車両センサデータ(センサ値)が取得された例を示している。

【0116】

図6に示すように、サンプリング間隔は、車両センサデータのサンプリングを行う間隔であり、サンプリング時間は、当該サンプリング間隔においてサンプリングを継続する時間である。サンプリング時間は、時間的に連続する時間であり、例えば、離散的な時間は含まれない。つまり、サンプリング時間にサンプリングされた車両センサデータは、時間的に連続したデータとなる。サンプリング開始時刻は、車両センサデータのサンプリングを開始する時刻であり、例えば、サンプリング時間の開示時刻であってもよい。なお、サンプリング開始時刻は、サンプリング間隔の開始時刻(例えば、サンプリング間隔の時間の計測を開始する時刻)であることに限定されず、サンプリング間隔の開始時刻から(T-S)秒経過する前であればよい。つまり、サンプリング開始時刻をNとすると、Nは以下の式を満たすように決定されるとよい。

【0117】

$$0 \leq N < T - S \quad (\text{式1})$$

【0118】

車両センサデータのサンプリングは、サンプリング間隔T秒のうち、サンプリング開始時刻N秒目からサンプリング時間S秒の間にわたって行われる。

【0119】

サンプリング間隔T秒のうち、サンプリング開始時刻N秒目からサンプリング時間S秒の間の車両センサデータを、サンプリングデータとする。つまり、図6では、サンプリング間隔T秒において10個の車両センサデータが取得されているが、そのうち3個の車両センサデータがサンプリングデータとして抽出される例を示している。言い換えると、サンプリング間隔T秒において取得された10個の車両センサデータのうち、7個の車両センサデータは、サンプリングデータ監視部102には送信されない。ここで、サンプリング間隔及びサンプリング時間を調整することで、高密度なサンプリングと低密度なサンプリングとを実現する。サンプリングの具体例は後述する。

【0120】

図7は、本実施の形態に係るサンプリング方針データの一例を示す図である。図7の例では、高密度サンプリングにおけるサンプリング間隔が200.00msであり、サンプリング時間が75.00msであり、低密度サンプリングにおけるサンプリング間隔が1000.00msであり、サンプリング時間が55.00msである。このように、例えば、高密度サンプリングにおけるサンプリング間隔は、低密度サンプリングにおけるサンプリング間隔より短く、例えば、低密度サンプリングにおけるサンプリング間隔の1/5程度である。また、例えば、高密度サンプリングにおけるサンプリング時間は、低密度サンプリングにおけるサンプリング時間より長く、例えば、低密度サンプリングにおけるサンプリング間隔の1.35倍程度である。なお、高密度サンプリングにおけるサンプリング間隔及びサンプリング時間と、低密度サンプリングにおけるサンプリング間隔及びサン

10

20

30

40

50

プリング時間とは、上記に限定されない。

【0121】

図7に示すように、サンプリング方針データは、センサ識別子152と、ファイル番号153と、データ分散154と、車両イベントフラグ155と、サンプリング間隔156と、サンプリング時間157とを含む。サンプリング方針データは、サンプリング方針記憶部113に記憶されており、センサ識別子152と、サンプリング方針判定部132の判定に用いられた情報（データ分散154及び車両イベントフラグ155）と、サンプリング方針（サンプリング間隔156及びサンプリング時間157）とが対応づけられた履歴である。

【0122】

センサ識別子152は、車両センサデータのセンサ識別子142と対応づいており、車両制御対象を一意に特定するための識別子である。

【0123】

ファイル番号153は、通信部115により送信される1ファイル単位を識別するためのファイル識別子である。例えば、所定の走行時間ごとに取得される車両センサデータに従って、ファイル番号がインクリメントされ、異なるサンプリング方針が算出される。

【0124】

データ分散154は、ファイル単位で、センサ識別子152ごとに算出する所定走行時間内のセンサ値のばらつきを示す数値データである。

【0125】

車両イベントフラグ155は、センサ識別子152とは別にエンジンONとOFFとの切替及びシフトの切替等のイベント型のセンサ識別子142を示す車両イベントが発生したか否かを示すフラグ情報である。

【0126】

サンプリング間隔156は、ファイル単位で、センサ識別子152ごとに算出する、サンプリングの密度を示す。

【0127】

サンプリング時間157は、ファイル内で、センサ識別子152ごとに算出する、サンプリングの密度を示す。

【0128】

また、サンプリング方針生成部110は、ステップS111～S115の処理を、処理対象となる車両センサデータが更新される度に、繰り返し実行する。

【0129】

例えば、図7のファイル番号が「2」であり、センサ識別子152が「車速」の場合、データ分散が0.22であり、車両イベントフラグが「無」である。データ分散の閾値を10と定めると、0.22は閾値以下である。そのため、上記の場合、低密度なサンプリングをする方針となり、例えば、上記の周期「約25ms」に対して長くするように、サンプリング間隔を「1000ms」とし、上記の周期の約2倍となるように、サンプリング時間を「55ms」とすることで、送信するデータ量を大幅に削減することができる。

【0130】

なお、サンプリング方針判定部132は、データ分散が第一の閾値以上である場合と、車両イベントフラグ情報が「有」である場合とで、互いに異なるサンプリング密度を設定してもよい。つまり、高密度サンプリングにおいて、複数のサンプル密度が設定されていてもよい。

【0131】

[3-1. サンプリングデータ生成部の構成]

図8は、本実施の形態に係るサンプリングデータ生成部111の構成を示すブロック図である。図8に示すように、サンプリングデータ生成部111は、車両センサデータ取得部130と、サンプリング情報取得部160と、データ抽出部161と、インデックス付与部162とを備える。

10

20

30

40

50

【0132】

車両センサデータ取得部130は、車両センサデータ記憶部112から車両サンプリングデータを取得する処理部である。車両センサデータ取得部130は、車両センサデータ記憶部112に記憶されている車両サンプリングデータを読み出す。なお、車両センサデータ取得部130は、サンプリング方針生成部110が有する車両センサデータ取得部130と共通の構成要素であってもよいし、互いに異なる構成要素であってもよい。

【0133】

サンプリング情報取得部160は、サンプリング方針生成部110が決定したサンプリング方針をサンプリング方針記憶部113から取得する処理部である。

【0134】

データ抽出部161は、車両センサデータ取得部130が取得した車両センサデータから、サンプリング方針記憶部113が取得したサンプリング方針に基づいた車両センサデータを抽出する処理部である。

【0135】

インデックス付与部162は、データ抽出部161が抽出した車両センサデータに時間的な順序を示すインデックスをセンサ値に対応付けて付与する処理部である。インデックス付与部162は、車両センサデータ（センサ値）ごとに、第一のインデックス及び第二のインデックスの両方を付与する。

【0136】

[3-2. サンプリングデータ生成部の動作]

図9は、本実施の形態に係るサンプリングデータ生成処理（S102）を示すフローチャートである。

【0137】

まず、サンプリングデータ生成部111は、センサ識別子ごとに、サンプリング間隔とサンプリング時間とを含むサンプリング方針データ151及び車両情報を取得する（S121）。ステップS121の処理は、サンプリング情報取得部160により実施される。サンプリング情報取得部160は、例えば、サンプリング方針データ151をサンプリング方針記憶部113から取得し、車両情報を車両情報記憶部114から取得する。

【0138】

サンプリング方針データ151は、車両のアーキテクチャを一意に示す車両番号（図示しない）と、車両センサデータに含まれるセンサ識別子ごとの取得周期を示す周期（サンプリング間隔及びサンプリング時間）とを含む。また、車両情報は、例えば、車両イベント情報を含む。

【0139】

次に、サンプリングデータ生成部111は、車両センサデータ記憶部112に含まれる所定の走行時間の車両センサデータを取得する（S122）。ステップS122の処理は、車両センサデータ取得部130により実施される。車両センサデータ取得部130は、例えば、図5に示す車両センサデータを取得する。

【0140】

次に、サンプリングデータ生成部111は、車両センサデータと、サンプリング方針データに含まれるサンプリング時間とに基づいて、1サンプリング間隔ごとにサンプリング時間中の受信データ数を計算する（S123）。ステップS123の処理は、データ抽出部161により実施される。ステップS123以降は、サンプリング時間ごとに実行される。

【0141】

次に、サンプリングデータ生成部111は、受信データ数が第二の閾値より多いか否かを判定する（S124）。ステップS124の処理は、データ抽出部161により実施される。データ抽出部161は、上記の受信データ数が、サンプリング時間における正常受信データ数に所定のマージンを加えた値（第二の閾値の一例）より大きい場合（S124でYes）、サンプリング時間内の所定データ数の、時間的に連続する車両センサデータ

10

20

30

40

50

を抽出する。ステップ S 1 2 4 で Y e s である場合、受信データ（センサ値）には攻撃によるデータが多数含まれている可能性がある。このような場合に、全てのデータを抽出するとデータ数が多くなりデータ量の増加につながる。そこで、データ抽出部 1 6 1 は、ステップ S 1 2 4 で Y e s である場合、所定データ数の受信データのみを抽出する（S 1 2 5）。これにより、攻撃によるデータを含む所定データ数の受信データを抽出することができるので、データ量を削減しつつ、攻撃検知を行えるサンプリングデータを生成することが可能となる。

【0 1 4 2】

なお、所定データ数は、例えば、正常受信データ数より大きい数である。また、第二の閾値は、正常受信データ数に所定のマージンを加えた値であることに限定されず、正常受信データ数であってもよいし、センサ識別子ごとに予め設定された固定値であってもよい。また、所定のマージンは、例えば、正常受信データ数に応じて設定されていてもよいし、固定値であってもよい。

【0 1 4 3】

また、データ抽出部 1 6 1 は、上記の受信データ数が、サンプリング時間における正常受信データ数に所定のマージンを加えた値以下である場合（S 1 2 4 で N o）、正常受信データ数を抽出する（S 1 2 6）。データ抽出部 1 6 1 は、例えば、サンプリング時間中における受信データ（センサ値）の全てを抽出する。

【0 1 4 4】

このように、ステップ S 1 2 4 ～ S 1 2 6 では、サンプリング時間中に観測されるべき正常受信データ数に基づいて、サンプリング時間内において抽出する車両センサデータの抽出数を決定し、決定された抽出数のセンサデータが抽出される。例えば、サンプリング時間中に観測されたセンサ値の数が正常受信データ数以上であるか否かを判定し、正常受信データ数以上である場合、所定数のセンサ値が抽出され、正常受信データ数以上でない場合、車両センサデータに含まれるセンサ値が全数抽出されてもよい。

【0 1 4 5】

ここで、正常受信データ数は、上記のサンプリング時間内の正常な受信データ数を示し、センサ識別子ごとの上記周期に基づいて事前に算出される。例えば、図 7 で示した通り、センサ識別子が「車速」の場合のサンプリング時間を「5 5 m s」とすると、周期は「約 2 5 m s」であるため、正常受信データ数は「2」となる。

【0 1 4 6】

次に、サンプリングデータ生成部 1 1 1 は、上記の抽出データに対して、サンプリング時間中の短期的なセンサ値の動きのデータ順序を示す第一のインデックスと、サンプリング間隔での長期的なセンサ値の動きの順序を示す第二のインデックスとを付与する。つまり、サンプリングデータ生成部 1 1 1 は、抽出データに含まれるセンサ値のそれぞれに対して、2 種のインデックスを付与する（S 1 2 7）。ステップ S 1 2 7 の処理は、インデックス付与部 1 6 2 により実施される。

【0 1 4 7】

インデックス付与部 1 6 2 は、例えば、サンプリング時間を「5 5 m s」とした場合、サンプリング時間「5 5 m s」中に抽出した複数のデータを先頭から順に、第一のインデックスを 1、2、3・・・と付与する。例えば、インデックス付与部 1 6 2 は、抽出した複数のデータを取得時刻が古いデータから順に第一のインデックスを付与する。

【0 1 4 8】

インデックス付与部 1 6 2 は、例えば、さらに、上記ステップ S 1 2 5 もしくは S 1 2 6 が実行されるごとに一意に定まる第二のインデックスを付与する。例えば、インデックス付与部 1 6 2 は、抽出した複数のデータをサンプリング時間が古いデータから順に第二のインデックスを付与する。ここで、サンプリング間隔を「1 0 0 0 m s」とした場合、第二のインデックスが変化するのは、約「1 0 0 0 m s」後のデータに対して処理する際である。

【0 1 4 9】

次に、サンプリングデータ生成部 111 は、抽出されたセンサ値のそれぞれに対してインデックスを付与したか否かを判定する（S128）。ステップ S128 の処理は、インデックス付与部 162 により実施される。インデックス付与部 162 は、例えば、所定の走行時間に含まれる 2 以上のサンプリング間隔それぞれのサンプリング時間の全てにおいて、ステップ S123～S127 の処理を行ったか否かを判定する。

【0150】

インデックス付与部 162 は、抽出されたセンサ値のそれぞれに対してインデックスを付与していない場合（S128 で No）、ステップ S123 に戻り、次のサンプリング時間に対してステップ S123 以降の処理を実行する。つまり、ステップ S123～S127 の処理を、処理対象となる車両センサデータに対して、サンプリング間隔ごとに、繰り返し実行する。

【0151】

サンプリングデータ生成部 111 は、インデックス付与部 162 が抽出されたセンサ値のそれぞれに対してインデックスを付与した場合（S128 で Yes）、抽出データをサンプリングデータとして、通信部 115 により通信部 126 に送信する。つまり、サンプリングデータ生成部 111 は、サンプリングデータ監視部 102 へインデックスが付与された抽出データ（サンプリングデータ）を送信する（S129）。

【0152】

ここで、サンプリングデータ生成部 111 が送信するサンプリングデータ（抽出データ）について、図 10 を参照しながら説明する。図 10 は、本実施の形態に係るサンプリングデータの一例を示す図である。

【0153】

図 10 に示すように、サンプリングデータは、センサ識別子 172 と、評価 ID 173 と、センサ値 174 と、第一のインデックス 175 と、第二のインデックス 176 とを含む。

【0154】

センサ識別子 172 及びセンサ値 174 は、車両センサデータにおけるセンサ識別子 142 及びセンサ値 145（図 5 を参照）と同様である。評価 ID 173 は、サンプリングデータに含まれるセンサ識別子 172 ごとに 1 つのセンサデータ 171 を一意に特定するための識別子である。

【0155】

上述した通り、第一のインデックス 175 は、短期的なセンサ値の動きの順序を示し、第二のインデックス 176 は、長期的なセンサ値の動きの順序を示す。

【0156】

例えば、評価 ID「1」及び「2」が示すセンサ値は、第二のインデックスがともに「1」であるので、同じサンプリング時間に取得されたセンサ値である。また、評価 ID「1」が示すセンサ値は、第一のインデックスが「1」であり、評価 ID「2」が示すセンサ値は、第一のインデックスが「2」であるので、評価 ID「1」が示すセンサ値が取得された後に続けて、評価 ID「2」が示すセンサ値が取得されたことを示す。

【0157】

また、第二のインデックスが「1」及び「2」のときのセンサ値の数は 2 つであるが、第二のインデックスが「3」のときのセンサ値の数は 3 以上である。サンプリング時間ごとにサンプリング方針が決定されるので、サンプリング時間ごと、つまり第二のインデックスごとにセンサ値の数は変化し得る。

【0158】

例えば、図 10 に示すサンプリングデータがサンプリングデータ監視部 102 へ送信される。

【0159】

[4-1. 攻撃検知部の構成]

図 11 は、本実施の形態に係る攻撃検知部 120 の構成を示すブロック図である。図 1

10

20

30

40

50

1に示すように、攻撃検知部120は、サンプリングデータ取得部181と、基点データ取得部182と、第一の異常スコア算出部183と、第二の異常スコア算出部184と、攻撃判定部185とを備える。

【0160】

サンプリングデータ取得部181は、サンプリングデータ記憶部125からサンプリングデータを取得する処理部である。サンプリングデータ取得部181は、例えば、図10に示すサンプリングデータを取得する。

【0161】

基点データ取得部182は、基点データ記憶部124から攻撃判定部185による判定に用いる基点データを取得する処理部である。基点データ取得部182は、基点データとして、短期センサフロー及び長期センサフローを取得する。

【0162】

第一の異常スコア算出部183は、評価対象データ191及び短期センサフローに基づいて、評価対象データ191と短期センサフローとの乖離の度合いを示す第一の異常スコアを算出する処理部である。つまり、第一の異常スコア算出部183は、評価対象データ191が取得されたサンプリング時間に取得された他のデータを用いて、当該評価対象データ191に対する第一の異常スコアを算出する。第一の異常スコア算出部183は、1つのサンプリング時間内といった短期間でのセンサ値の変化に対する異常スコアを算出する。短期間とは、例えば、1つのサンプリング間隔以下の時間（例えば、1つのサンプリング時間）であることを意味する。

【0163】

第一の異常スコア算出部183は、例えば、サンプリングデータに含まれる評価対象データのセンサ値と、第一のインデックスと、評価対象データが取得されたサンプリング時間における当該評価対象データより過去のセンサ値の時系列データを示す短期センサフローとに基づいて、評価対象データの異常の度合いを示す第一の異常スコアを算出するとも言える。

【0164】

第二の異常スコア算出部184は、評価対象データ191及び長期センサフローに基づいて、評価対象データ191と長期センサフローとの乖離の度合いを示す第二の異常スコアを算出する処理部である。つまり、第二の異常スコア算出部184は、評価対象データ191が取得されたサンプリング間隔を含む複数のサンプリング間隔のデータを用いて、当該評価対象データ191に対する第二の異常スコアを算出する。第二の異常スコア算出部184は、複数のサンプリング間隔といった長期間でのセンサ値の変化に対する異常スコアを算出する。長期間とは、短期間より長い時間であり、例えば、1つのサンプリング間隔より長いことを意味する。

【0165】

第二の異常スコア算出部184は、例えば、評価対象データのセンサ値と、第二のインデックスと、評価対象データが取得されたサンプリング間隔より過去のサンプリング間隔で取得されたセンサ値の変化を示す長期センサフローとに基づいて、評価対象データの異常の度合いを示す第二の異常スコアを算出するとも言える。

【0166】

攻撃判定部185は、算出された第一の異常スコア及び第二の異常スコアに基づいて、評価対象データ191が攻撃によるものであるか否か、つまり車両がサイバー攻撃を受けているか否かを判定し、判定結果を出力する処理部である。本実施の形態では、攻撃判定部185は、第一の異常スコア及び第二の異常スコアに基づいて第三の異常スコアを算出し、算出した第三の異常スコアと所定の閾値（第五の閾値）とを比較し、比較結果に基づいて評価対象データ191が攻撃によるものであるか否かを判定する。なお、攻撃判定部185は、第三の異常スコアを算出することに限定されず、第一の異常スコア及び第二の異常スコアのそれぞれについて対応する閾値との比較を行い、比較結果に基づいて評価対象データ191が攻撃によるものであるか否かを判定してもよい。

【0167】

〔4-2. 攻撃検知部の動作〕

図12は、本実施の形態に係る攻撃検知処理（S103）を示すフローチャートである。なお、図12に示す攻撃検知処理は、例えば、サンプリングデータに含まれる任意のセンサ値に対して行われてもよいし、サンプリングデータに含まれるセンサ値の全てに対して行われてもよい。センサ値の全てに対しての攻撃検知処理が行われる場合、例えば、取得時刻が古いセンサ値から順に図12に示す処理が行われてもよい。

【0168】

まず、攻撃検知部120は、サンプリングデータを取得し、サンプリングデータ中の1つのデータである評価対象データ（図13に示す評価対象データ191を参照）を取り出す（S131）。ステップS131の処理は、サンプリングデータ取得部181により実施される。

【0169】

次に、攻撃検知部120は、評価対象データ191に対応づく基点データを取得する（S132）。ステップS132の処理は、基点データ取得部182により実施される。

【0170】

図13は、本実施の形態に係る基点データの一例を示す図である。

【0171】

図13に示すように、基点データは、センサ識別子192と、評価ID193と、センサ値194と、第一のインデックス195と、第二のインデックス196と、短期センサフロー197と、長期センサフロー198とを含む。

【0172】

センサ識別子192と、評価ID193と、センサ値194と、第一のインデックス195と、第二のインデックス196とは、サンプリングデータにおける、センサ識別子172と、評価ID173と、センサ値174と、第一のインデックス175と、第二のインデックス176（図10を参照）と同様である。

【0173】

短期センサフロー197は、評価対象データ191と同一の第二のインデックスを有し、評価対象データ191の第一のインデックスより前のインデックスを参照キーとして、一意のセンサ値が定まる過去のセンサ値のリストである。

【0174】

例えば、図13において、評価IDが「82」の評価対象データの場合、第二のインデックスが「3」を有し、第一のインデックスが「2」より前である「1」を参照キーとして、評価IDが81の評価対象データのセンサ値の代表値が、短期センサフローとして格納されている。また、上述した代表値の算出方法に関しては、後述する。

【0175】

一方、長期センサフロー198は、評価対象データ191の第二のインデックスより前のインデックスを参照キーとして、一意の値を有する過去のセンサ値の代表値リストである。

【0176】

例えば、図13において、評価IDが「82」の評価対象データの場合、第二のインデックスが「3」より前である「1」と「2」を参照キーとして、評価対象データのセンサ値の代表値が、長期センサフローとして格納されている。また、上述した代表値の算出方法に関しては、後述する。

【0177】

図14は、本実施の形態に係る検知結果情報の一例を示す図である。

【0178】

図14に示すように、検知結果情報は、センサ識別子202と、評価ID203と、センサ値204と、第一の異常スコア205と、第二の異常スコア206と、第三の異常スコア207と、検知結果208とを含む。検知結果208は、評価対象データに対応づく

10

20

30

40

50

判定結果の一例である。

【0179】

センサ識別子202と、評価ID203と、センサ値204とは、サンプリングデータにおける、センサ識別子172と、評価ID173と、センサ値174（図10を参照）と同様である。

【0180】

第一の異常スコア205と、第二の異常スコア206と、第三の異常スコア207と、検知結果208とは後述する。

【0181】

図12を再び参照して、次に、攻撃検知部120は、第一のインデックス及び第二のインデックスの少なくとも一方が所定値以上であるか否かを判定する（S133）。所定値は、予め設定されており、記憶部に記憶されている。第一のインデックスにおける所定値と第二のインデックスにおける所定値とは、同じ値であってもよいし、互いに異なる値であってもよい。

【0182】

攻撃検知部120は、評価対象データに対する第一のインデックス及び第二のインデックスの少なくとも一方が所定値以上である場合（S133でYes）、後述する異常スコア（第一の異常スコア及び第二の異常スコアの少なくとも一方）を算出し、第一のインデックス及び第二のインデックスのそれぞれが所定値未満の場合（S133でNo）、検知結果を「不明」とする（S134）。攻撃検知部120は、ステップS133でYesの場合、第一のインデックスが所定値以上であるか否かを判定する（S135）。所定値は、予め設定されており、記憶部に記憶されている。ステップS135で用いられる所定値は、第三の閾値の一例である。第三の閾値は、例えば、第一の異常スコアが正確に算出可能な値に設定される。

【0183】

例えば、図13において、評価ID「1」のデータが評価対象データである場合、第一のインデックスは「1」であり、第二のインデックスは「1」である。そのため、例えば、所定値が2である場合、図14に示すように、上記該当データの検知結果は「不明」となる。なお、「不明」と判定された場合、第一の異常スコア、第二の異常スコア及び第三の異常スコアは、「0」であってもよい。

【0184】

次に、攻撃検知部120は、評価対象データに対する第一のインデックス及び第二のインデックスの少なくとも一方が所定値以上であり（S133でYes）、かつ、第一のインデックスが所定値以上である場合（S135でYes）、評価対象データと短期的なセンサ値の正常なフロー（短期センサフロー）との乖離の度合いを示す第一の異常スコアを算出する第一の検知器を読み出し、上記の評価対象データ191と、短期センサフローとに基づいて、第一の異常スコアを算出する（S136）。ステップS136の処理は、第一の異常スコア算出部183により実施される。

【0185】

第一の異常スコア算出部183は、ステップS133及びS135でYesの場合、第一の検知器を検知器記憶部122から読み出す。第一の検知器は、評価対象データ191と、短期センサフローとを入力とし、評価対象データ191と短期センサフローとの乖離の度合いを示す第一の異常スコアを出力するように学習された学習済みモデルにより実現されてもよい。第一の検知器は、乖離の度合いが大きいほど、大きな値の第一の異常スコアを出力するように学習されるが、これに限定されない。また、第一の異常スコアは、例えば、0～100までの値（例えば、正規化された値）であるが、レベル（「高」、「中」、「低」等）であってもよい。

【0186】

例えば、図13において、評価IDが「82」の評価対象データの場合、第一のインデックスが「2」であり、短期センサフローに「35.11」が含まれ、センサ値が「10

10

20

30

40

50

0.50」である。この場合、図14に示すように、第一の検知器が出力する第一の異常スコアは、例えば「95」である。第一の異常スコアが95であることが第一の異常スコア算出部183により算出される。

【0187】

なお、第一の検知器は、評価対象データのセンサ値と、短期センサフローとの間のセンサ値の差分に基づく、OC-SVM (One Class-Support Vector Machine) などの機械学習モデルによる外れ値検知器を用いても良い。また、第一の検知器は、センサ値の代わりに取得時間を用いて、短期センサフローと評価対象データとの間の取得時間の差分が周期に基づいているか否かで判定する検知器を用いても良い。なお、前述の検知器を統合して用いても良い。

10

【0188】

なお、第一の異常スコア算出部183は、機械学習モデルを用いて第一の異常スコアを算出することに限定されない。第一の異常スコア算出部183は、例えば、評価対象データ191及び短期センサフローと、第一の異常スコアとが対応付けられたテーブル（ルックアップテーブル）を用いて第一の異常スコアを算出してもよいし、評価対象データ191及び短期センサフローを用いて所定の演算を行うことにより第一の異常スコアを算出してもよい。

【0189】

また、攻撃検知部120は、評価対象データに対する第一のインデックス及び第二のインデックスの少なくとも一方が所定値以上であり（S133でYes）、かつ、第一のインデックスが所定値未満である場合（S135でNo）、ステップS137に進む。ステップS135がNoである場合、評価対象データが取得されたサンプリング時間内における、当該評価対象データより以前に取得された車両センサデータの数少なく、当該評価対象データが異常であるか否かを正確に判定することが困難である。よって、攻撃検知部120は、ステップS135でNoの場合、第一の異常スコアを算出しなくてもよい。なお、攻撃検知部120は、ステップS135でNoの場合、第一の異常スコアを「0」としてもよい。

20

【0190】

次に、攻撃検知部120は、第二のインデックスが所定値以上であるか否かを判定する（S137）。所定値は、予め設定されており、記憶部に記憶されている。ステップS137で用いられる所定値は、ステップS133で用いられる所定値と同じ値であってもよいし、異なってもよい。ステップS137で用いられる所定値は、第四の閾値の一例である。第四の閾値は、例えば、第二の異常スコアが正確に算出可能な値に設定される。

30

【0191】

次に、攻撃検知部120は、第二のインデックスが所定値以上の場合（S137でYes）、評価対象データと長期的なセンサ値の正常なフロー（長期センサフロー）との乖離の度合いを示す第二の異常スコアを算出する第二の検知器を読み出し、上記の評価対象データ191と、長期センサフローとに基づいて、第二の異常スコアを算出する（S138）。ステップS138の処理は、第二の異常スコア算出部184により実施される。

【0192】

第二の異常スコア算出部184は、ステップS137でYesの場合、第二の検知器を検知器記憶部122から読み出す。第二の検知器は、評価対象データ191と、長期センサフローとを入力とし、評価対象データ191と長期センサフローとの乖離の度合いを示す第二の異常スコアを出力するように学習された学習済みモデルにより実現されてもよい。第二の検知器は、乖離の度合いが大きいほど、大きな値の第二の異常スコアを出力するように学習されるが、これに限定されない。また、第二の異常スコアは、例えば、0～100までの値（例えば、正規化された値）であるが、レベル（「高」、「中」、「低」等）であってもよい。

40

【0193】

例えば、図13において、評価ID「82」のデータが評価対象データである場合、第

50

二のインデックスが「3」であり、長期センサフローに「22.50」及び「33.50」が含まれ、センサ値が「100.50」である。この場合、図14に示すように、第二の検知器が出力する第二の異常スコアは「80」である。第二の異常スコアが80であることが第二の異常スコア算出部184により算出される。

【0194】

なお、第二の検知器は、再帰型ニューラルネットワークモデル（RNN：Recurrent Neural Network）または自己回帰移動平均モデル（ARIMA：Auto Regressive Integrated Moving Average）を用いて、正常なセンサ値の振る舞いを予測し、実測値との誤差に基づいて異常と判定する変化点検知器を用いても良い。

10

【0195】

また、攻撃検知部120は、評価対象データに対する第二のインデックスが所定値未満である場合（S137でNo）、ステップS139に進む。ステップS137がNoである場合、評価対象データが取得されたサンプリング間隔における、当該評価対象データより以前に取得された車両センサデータが少なく、当該評価対象データが異常であるか否かを正確に判定することが困難である。よって、攻撃検知部120は、ステップS137でNoの場合、第二の異常スコアを算出しなくてもよい。なお、攻撃検知部120は、ステップS137でNoの場合、第二の異常スコアを「0」としてもよい。

【0196】

なお、第一の検知器及び第二の検知器は、互いに異なる検知器であってもよいし、1つの検知器であってもよい。

20

【0197】

次に、攻撃検知部120は、第一の異常スコアと第二の異常スコアとから、第三の異常スコアを算出する（S139）。ステップS139の処理は、攻撃判定部185により実施される。

【0198】

なお、第三の異常スコアは、第一の異常スコア及び第二の異常スコアに基づく異常スコアである。第三の異常スコアは、例えば、第一の異常スコアであってもよいし、第二の異常スコアであってもよいし、第一の異常スコアと第二の異常スコアとに基づく統計値であってもよい。統計値は、例えば、平均値（例えば、重みづけ平均）であるが、中央値、最頻値、最大値、最小値のいずれかであってもよい。

30

【0199】

なお、第三の異常スコアを算出することは、必須ではない。

【0200】

次に、攻撃検知部120は、第三の異常スコアを用いて、攻撃の有無を判定する（S140）。ステップS139の処理は、攻撃判定部185により実施される。攻撃判定部185は、評価対象データが攻撃によるデータであるか否かを判定するとも言える。攻撃判定部185は、例えば、第三の異常スコアが第五の閾値以上である場合、“攻撃”（攻撃有り）と判定し、第五の閾値未満である場合、“正常”（攻撃なし）と判定する。

【0201】

例えば、図14において、評価IDが「82」の場合、該当データの第一の異常スコアの「95」、及び第二の異常スコアの「80」はどちらも算出され（S135がYesであり、かつS137がYesの場合）、第三の異常スコアとして平均値である「87」が算出されている。この場合、攻撃判定部185は、第五の閾値を「60」とすると、評価IDが「82」のセンサ値を“攻撃”と判定する。つまり、攻撃判定部185は、センサ値「100.50」を攻撃によるものであると判定する。

40

【0202】

また、図14において、評価IDが「81」の場合、該当データの第二の異常スコアの「6」のみが算出され（S135がNoであり、S137がYesの場合）、第三の異常スコアとして「6」が算出されている。この場合、攻撃判定部185は、第五の閾値を「

50

60」とすると、“正常”と判定する。つまり、攻撃判定部185は、センサ値「35.1」を攻撃によるものではないと判定する。

【0203】

ステップS135がNoであり、かつ、ステップS137がYesである場合とは、例えば、第二のインデックスが所定値以上であるときのサンプリング間隔の開始時刻の直後等である場合が想定される。この場合、当該サンプリング間隔におけるサンプリング時間内の車両センサデータの全てが取得されていない状態（例えば、サンプリング時間の先頭のタイミングである状態）であるが、サンプリング間隔ごとの車両センサデータは攻撃の有無を判定可能な数だけある状態である。言い換えると、ステップS135がNoであり、かつ、ステップS137がYesである場合とは、第一の検知器を用いた攻撃の検知が不可であり、かつ、第二の検知器を用いた攻撃の検知が可能である場合である。

10

【0204】

このとき、攻撃検知部120は、第二の検知器による第二の異常スコアを用いて評価対象データが攻撃によるものであるか否かを判定することができる。

【0205】

また、ステップS135がYesであり、かつ、ステップS137がNoである場合とは、例えば、経過したサンプリング間隔は少ないが、経過したサンプリング間隔におけるサンプリング時間内の車両センサデータは全て取得済みである場合が想定される。この場合、サンプリング間隔ごとの車両センサデータの数は少ないが、サンプリング時間内の車両センサデータは攻撃の有無を判定可能な数だけある状態である。言い換えると、ステップS135がYesであり、かつ、ステップS137がNoである場合とは、第一の検知器を用いた攻撃の検知が可能であり、かつ、第二の検知器を用いた攻撃の検知が不可である場合である。

20

【0206】

このとき、攻撃検知部120は、第一の検知器による第一の異常スコアを用いて評価対象データが攻撃によるものであるか否かを判定することができる。

【0207】

このように、第一の検知器及び第二の検知器は、互いの検知不可の時間における攻撃検知を補完し合うことができる。つまり、攻撃検知部120は、攻撃の検知が不可となる時間を減らすことができる。よって、攻撃検知部120における攻撃の検知性能を向上させることができる。

30

【0208】

次に、攻撃検知部120は、ステップS134又はS140の判定結果を検知結果記憶部123に記憶する（S141）。攻撃検知部120は、判定結果を検知結果記憶部123に出力するとも言える。

【0209】

このように、攻撃検知部120は、評価対象データに対応づく第一のインデックスが第三の閾値未満であり、かつ、当該評価対象データに対応づく第二のインデックスが第四の閾値未満である場合、当該評価対象データが攻撃によるものであるか否かが不明であると判定する（S134）。また、攻撃検知部120は、第一の異常スコア及び第二異常スコアに基づく第三の異常スコアが第五の閾値以上の場合、評価対象データが攻撃によるものと判定し、第三の異常スコアが第五の閾値未満の場合、評価対象データが正常であると判定し（S140）、判定した結果を示す検知結果を出力する。

40

【0210】

なお、図12において、攻撃検知部120は、さらに車両イベント情報を用いて、異常スコアを算出してもよい。攻撃検知部120は、例えば、車両イベント情報が、車両のエンジンのON及びOFFの切り替え、シフトレバーの切り替え、自動運転モードのON及びOFFの切り替えの少なくとも1つが生じたことを示す場合、長期センサフローに含まれるセンサ値を初期化（リセット）してもよい。つまり、攻撃検知部120は、当該少なくとも1つが生じた場合、当該時刻より後に取得されたセンサ値に基づいて第二の異常ス

50

コアを算出してもよい。この場合、長期センサフローに含まれるセンサ値を蓄積する必要があるため、蓄積する期間（例えば、2以上のサンプリング間隔に相当する期間）は、第二の異常スコアを算出することができないが、第一のインデックスが所定値以上である場合、第一の異常スコアは算出可能である。

【0211】

このように、攻撃検知部120は、当該少なくとも1つが生じた場合には、第一の異常スコアに基づいて攻撃の検知を行うことで、攻撃の検知が不可となる時間を減らすことができる。よって、攻撃検知部120における攻撃の検知性能をさらに向上させることができる。

【0212】

〔5-1. 基点データ更新部の構成〕

図15は、本実施の形態に係る基点データ更新部121の構成を示すブロック図である。図15に示すように、基点データ更新部121は、基点データ取得部182と、検知結果取得部201と、基点データ追加部302とを備える。

【0213】

基点データ取得部182は、基点データ記憶部124から基点データを取得する処理部である。

【0214】

検知結果取得部201は、検知結果記憶部123から攻撃検知部120の検知結果を取得する処理部である。

【0215】

基点データ追加部302は、基点データ取得部182が取得した基点データに検知結果取得部201が取得した検知結果に応じたデータを追加する処理部である。基点データ追加部302は、基点データを更新するとも言える。

【0216】

〔5-2. 基点データ更新部の動作〕

図16は、本実施の形態に係る基点データ更新処理（S104）を示すフローチャートである。基点データ更新処理は、基点データ更新部121により実施される。

【0217】

まず、基点データ更新部121は、基点データ取得部182により取得された評価対象データに応じて、基点データを初期化する（S151）。基点データ更新部121は、評価対象データ191に対応づく基点データを取得し、評価対象データ191の第一のインデックスが1である場合、基点データにおける短期センサフローを初期化し、評価対象データ191の第二のインデックスが1の場合、基点データにおける長期センサフローを初期化する。なお、ここでの初期化は、短期センサフロー又は長期センサフローにセンサ値が含まれていない状態にすることを意味する。例えば、図13の評価IDが「1」のときの短期センサフロー197及び長期センサフロー、並びに、評価IDが「81」のときの短期センサフロー197（図13に示す[]）は、初期化がされていることを示す。

【0218】

次に、基点データ更新部121は、評価対象データに対応づく検知結果を取得する（S152）。ステップS152の処理は、検知結果取得部201により実施される。検知結果取得部201は、評価対象データ191に対応づく検知結果を検知結果記憶部123から読み出す。検知結果取得部201は、例えば、図14に示す検知結果を読み出す。

【0219】

次に、基点データ更新部121は、取得した検知結果が“攻撃”であるか否かを判定する（S153）。ステップS153～S157までの処理は、基点データ追加部302により実施される。基点データ追加部302は、例えば、評価対象データの評価ID203に対応する検知結果208に基づいて、ステップS153の判定を行う。

【0220】

次に、基点データ追加部302は、検知結果が“攻撃”である場合（S153でYes）

10

20

30

40

50

、センサ値を補完するための値として、推定センサ値を追加データに設定し（S 1 5 4）、検知結果が“正常”もしくは“不明”である場合（S 1 5 3でNo）、評価対象データのセンサ値（実測値）を追加データに設定する（S 1 5 5）。

【0 2 2 1】

なお、推定センサ値は、評価対象データに対応づく短期センサフローの最後に追加された値でも、短期センサフローの平均値でも良い。また、推定センサ値は、上記の長期センサフローに基づいて、第二の検知器が算出する評価対象データのセンサ値の予測値でも良い。

【0 2 2 2】

基点データ追加部302は、例えば、図13において、評価IDが「82」の場合、検知結果が「“攻撃”」であるため、推定センサ値を評価対象データに対応づく短期センサフローの最後に追加された値として、「35.11」を設定する。

【0 2 2 3】

次に、基点データ追加部302は、下記（数2）に従って、次の評価対象データの判定に用いる短期センサフロー（数1）を更新する（S 1 5 6）。

【0 2 2 4】

【数1】

$$S = \{s_1, s_2, s_3, s_i, \dots \dots \dots\} \quad (\text{式2})$$

【数2】

$$s_i = \begin{cases} p_i^j, & (\text{label}_i^j = \text{"Attack"}) \\ x_i^j, & (\text{otherwise}) \end{cases} \quad (\text{式3})$$

【0 2 2 5】

ここで、 s_i は、短期センサフローに含まれる1つのセンサ値を示しており、 i は評価対象データの第一のインデックスを示し、 j は評価対象データの第二のインデックスを示す。基点データ追加部302は、上記の検知結果 label_{i-j} が「“攻撃”（“Attack”）」である場合、上記の推定センサ値 p_{i-j} で s_i を更新する。また、基点データ追加部302は、 label_{i-j} が「“正常”（“Normal”）」もしくは「“不明”（“Unknown”）」である場合、上記の評価対象データのセンサ値 x_{i-j} で s_i を更新する。なお、 s_i は、代表値の一例である。

【0 2 2 6】

次に、基点データ追加部302は、下記（数4）に従って、長期センサフロー（数3）を更新する（S 1 5 7）。

【0 2 2 7】

【数3】

$$H = \{h_1, h_2, h_3, h_j, \dots \dots \dots\} \quad (\text{式4})$$

【数4】

10

20

30

40

50

$$h_j = \begin{cases} p_i^j, & (\text{label}_i^j = \text{"Attack"}) \\ x_i^j, & (\text{otherwise}) \end{cases} \quad (\text{式 } 5)$$

【0228】

ここで、 h_j は、長期センサフローに含まれる1つのセンサ値を示す。基点データ追加部302は、上記の検知結果 label_{i-j} が「攻撃」(“Attack”)であった場合、上記の推定センサ値 p_{i-j} で h_j を更新する。また、基点データ追加部302は、 label_{i-j} が「正常」もしくは「不明」であった場合、上記の評価対象データのセンサ値 x_{i-j} で h_j を更新する。なお、 h_j は、代表値の一例である。

【0229】

このように、基点データ追加部302は、攻撃か否かの判定の度に、2種類の基点データを更新し、次の判定に用いる。

【0230】

なお、上記説明では、監視システム100において、サンプリング処理と、攻撃検知処理とが互いに異なる装置で行われる例を示したが、同一の装置(例えば、1つの装置)で行われても良い。

【0231】

以上のように、監視処理(例えば、攻撃検知処理)の対象となる車両センサデータの特徴に合わせて、サンプリング間隔とサンプリング時間とを調整して、サンプリングデータの生成が行われる。さらに、短期及び長期のセンサ値の動きを示す2種のインデックスを含むサンプリングデータに基づいて、2種の異常スコアを算出することで、攻撃の判定が行われる。これにより、監視コストを抑えつつ精度良く攻撃検知ができる。

【0232】

また、基点データ更新部121は、評価対象データに対応づく検知結果が攻撃である場合、評価対象データが取りうるべきセンサ値を、短期センサフロー及び長期センサフローの少なくとも1つを用いて推定し、推定された推定センサ値と、第一のインデックスと、第二のインデックスとに基づいて、短期センサフローと長期センサフローとを更新する。また、基点データ更新部121は、評価対象データに対応づく検知結果が正常もしくは不明である場合、評価対象データのセンサ値(実測値)と、第一のインデックス報と、第二のインデックスとに基づいて、短期センサフローと長期センサフローとを更新する。

【0233】

これにより、攻撃などの外れ値が基点リストに混在することを抑制することができる。よって、そのような基点リストを用いることで、監視コストを抑えつつ精度良く攻撃検知ができる。

【0234】

以下、上述した監視システム100の利用形態について説明する。

【0235】

図17は、本実施の形態に係る監視システム100の構成を示す概略図である。図17は、サンプリング部401及びサンプリングデータ監視部501を備える監視システム100の構成を示すブロック図である。監視システム100は、クラウド上に存在するサーバ500と、車載装置400とを備える。監視システム100は、車載装置400を介して、抽出された車両センサデータ(サンプリングデータ)を取得し、取得された車両センサデータに基づいて攻撃を検知することができる。

【0236】

車載装置400及びサーバ500は、例えば、インターネット等の公衆通信ネットワークを介して通信可能に接続されている。車載装置400は、セキュリティECU(Ele

10

20

30

40

50

ctronic Control Unit) 又はカーナビなどである。

【0237】

車載装置400は、サンプリング部401と、攻撃通知装置402とを備える。

【0238】

サンプリング部401は、車両ネットワークデータをサンプリングした結果（サンプリングデータ）を、サンプリングデータ監視部501へ送信する装置である。サンプリング部401は、例えば、所定の走行時間ごとに、バイナリ表現されたCANデータをセンサ値に変換し、さらにサンプリングデータに変換する。そして、サンプリング部401は、サンプリングデータをサンプリングデータ監視部501に送信する。

【0239】

攻撃通知装置402は、サーバ500から受信した車両ネットワークに対する攻撃の発生を、運転者に通知するための装置である。攻撃通知装置402は、例えば、攻撃の発生を知らせ、ネットワークから遮断されたセーフティモードで運転することを指示する音声もしくは画面により出力する。攻撃通知装置402は、ディスプレイ装置、スピーカ装置等により実現される。

【0240】

サンプリングデータ監視部501は、車載装置400から受信した車両ネットワークデータ（例えば、サンプリングデータ）に対する攻撃の有無を判定し、攻撃がある場合に攻撃通知装置402に攻撃検知の結果を送信する。

【0241】

なお、サンプリング部401の構成は、サンプリング部101と同様であってもよい。また、サンプリングデータ監視部501の構成は、サンプリングデータ監視部102と同様であってもよい。

【0242】

図18は、本実施の形態に係る車載装置600の構成を示す概略図である。図18は、監視装置601を備える車載装置600の構成を示すブロック図である。車載装置600は、監視装置601と、攻撃通知装置602とを備える。

【0243】

監視装置601は、車両内部のみで、車両ネットワークデータをサンプリングした結果に対して、攻撃の有無を判定し、攻撃がある場合に攻撃通知装置602に攻撃検知の結果を送信する。なお、監視装置601は、例えば、サンプリング部101及びサンプリングデータ監視部102が有する機能を有するように構成される。このように、サンプリング部101及びサンプリングデータ監視部102が有する機能は、1つの装置（例えば、車両に搭載される装置）により実現されてもよい。監視装置601は、攻撃検知システムの一例である。

【0244】

攻撃通知装置602は、監視装置601から受信した車両ネットワークに対する攻撃の発生を、運転者に通知するための装置である。攻撃通知装置602は、ディスプレイ装置、スピーカ装置等により実現される。

【0245】

このように、図17の監視システム100及び図18の監視装置601では、車両ネットワークをサンプリングした結果に対して、攻撃があるか否かを適切に判定することで、低監視コストで攻撃検知が実現できる。また、監視システム100及び監視装置601では、さらに、検知結果の通知により、攻撃が検知されたことを運転者に通知することができるため、攻撃による事故発生を軽減することが可能である。

【0246】

（その他の実施の形態）

以上、実施の形態に係る監視装置について説明したが、本開示は、この実施の形態に限定されるものではない。

【0247】

例えば、上記実施の形態では、自動車等の車両に搭載される車載ネットワークにおけるセキュリティ対策として説明したが、適用範囲はこれに限定されない。例えば、自動車等の車両以外に、移動体としての建機、農機、船舶、鉄道及び飛行機等のモビリティにも適用してもよい。すなわち、モビリティネットワークおよびモビリティネットワークシステムにおけるサイバーセキュリティ対策として適用可能である。

【0248】

また、上記実施の形態に係る監視装置に含まれる各処理部は典型的には集積回路であるLSIとして実現される。これらは個別に1チップ化されてもよいし、一部又は全てを含むように1チップ化されてもよい。

【0249】

また、集積回路化はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製造後にプログラムすることが可能なFPGA、又はLSI内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。

【0250】

また、本開示は、監視システムにより実行される監視方法（例えば、攻撃検知方法）として実現されてもよい。例えば、本開示の一態様は、監視方法に含まれる特徴的な各ステップをコンピュータに実行させるコンピュータプログラムであってもよい。また、本開示の一態様は、そのようなプログラムが記録された、DVD等のコンピュータ読み取り可能な非一時的な記録媒体であってもよい。例えば、そのようなプログラムを記録媒体に記録して頒布又は流通させてもよい。例えば、そのようなプログラム及び当該プログラムからなるデジタル信号は、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものであってもよい。例えば、頒布されたプログラムを、他のプロセッサを有する装置にインストールして、そのプログラムをそのプロセッサに実行させることで、その装置に、上記各処理を行わせることが可能となる。

【0251】

また、上記実施の形態では、第一の順序情報は、第一のインデックスである例について説明したが、これに限定されない、第一の順序情報は、例えば、絶対時刻であってもよい。また、上記実施の形態では、第二の順序情報は、第二のインデックスである例について説明したが、これに限定されない、第二の順序情報は、例えば、サンプリング間隔が開始される絶対時刻であってもよい。

【0252】

また、上記実施の形態において、各構成要素は、専用のハードウェアで構成されるか、各構成要素に適したソフトウェアプログラムを実行することによって実現されてもよい。各構成要素は、CPUまたはプロセッサなどのプログラム実行部が、ハードディスクまたは半導体メモリなどの記録媒体に記録されたソフトウェアプログラムを読み出して実行することによって実現されてもよい。

【0253】

また、ブロック図における機能ブロックの分割は一例であり、複数の機能ブロックを一つの機能ブロックとして実現したり、一つの機能ブロックを複数の分割したり、一部の機能を他の機能ブロックに移してもよい。また、類似する機能を有する複数の機能ブロックの機能を単一のハードウェア又はソフトウェアが並列又は時分割に処理してもよい。

【0254】

また、監視システムが複数の装置により実現される場合、サンプリング部が有する機能及びサンプリングデータ監視部が有する機能は、複数の装置にどのように振り分けられてもよい。

【0255】

また、フローチャートにおける各ステップが実行される順序は、本開示を具体的に説明するために例示するためのものであり、上記以外の順序であってもよい。また、上記ステップの一部が、他のステップと同時（並列）に実行されてもよい。

【0256】

以上、一つまたは複数の態様に係る監視システムについて、実施の形態に基づいて説明したが、本開示は、この実施の形態に限定されるものではない。本開示の趣旨を逸脱しない限り、当業者が思いつく各種変形を本実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、一つまたは複数の態様の範囲内に含まれてもよい。

【産業上の利用可能性】

【0257】

本開示は、車両センサデータに対する監視装置に適用でき、例えば、車両センサデータに含まれる車両制御用のデータが攻撃か否かを適切に判定できる。例えば、本開示は、セキュリティ用ECUなどの車載装置もしくは、遠隔監視サーバにおけるSIEM (Security Information and Event Management) など、監視装置又は監視システムに利用可能である。

【符号の説明】

【0258】

100 監視システム

101、401 サンプリング部

102、501 サンプリングデータ監視部

110 サンプリング方針生成部

111 サンプリングデータ生成部

112 車両センサデータ記憶部

113 サンプリング方針記憶部

114 車両情報記憶部

115、126 通信部

120 攻撃検知部

121 基点データ更新部

122 検知器記憶部

123 検知結果記憶部

124 基点データ記憶部

125 サンプリングデータ記憶部

130 車両センサデータ取得部

131 センサデータ安定度算出部

132 サンプリング方針判定部

141 車両センサデータ

142、152、172、192、202 センサ識別子

143 データID

144 取得時刻

145、174、194、204 センサ値

151 サンプリング方針データ

153 ファイル番号

154 データ分散

155 車両イベントフラグ

156 サンプリング間隔

157 サンプリング時間

160 サンプリング情報取得部

161 データ抽出部

162 インデックス付与部

173、193、203 評価ID

175、195 第一のインデックス

176、196 第二のインデックス

10

20

30

40

50

- 1 8 1 サンプルングデータ取得部
- 1 8 2 基点データ取得部
- 1 8 3 第一の異常スコア算出部
- 1 8 4 第二の異常スコア算出部
- 1 8 5 攻撃判定部
- 1 9 1 評価対象データ
- 1 9 7 短期センサフロー
- 1 9 8 長期センサフロー
- 2 0 1 検知結果取得部
- 2 0 5 第一の異常スコア
- 2 0 6 第二の異常スコア
- 2 0 7 第三の異常スコア
- 2 0 8 検知結果
- 3 0 2 基点データ追加部
- 4 0 0、6 0 0 車載装置
- 4 0 2、6 0 2 攻撃通知装置
- 5 0 0 サーバ
- 6 0 1 監視装置

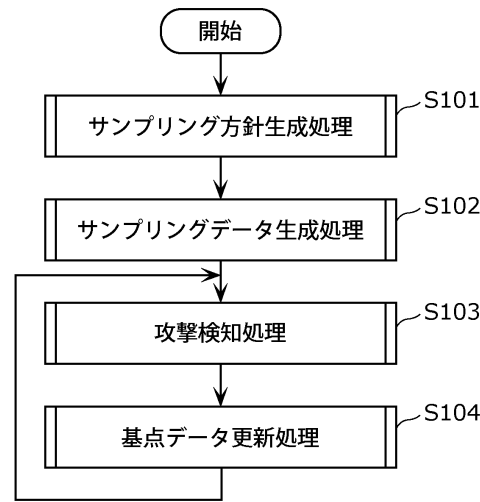
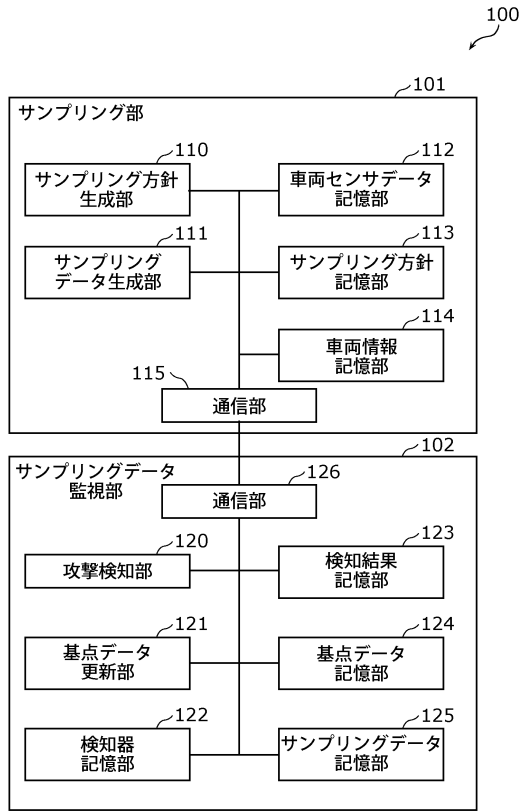
10

【図面】

【図 1】

【図 2】

20

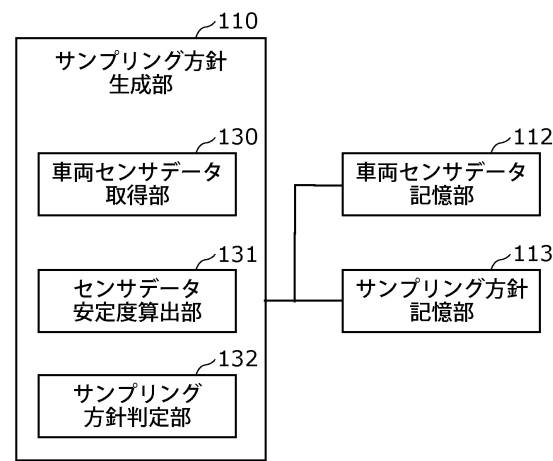


30

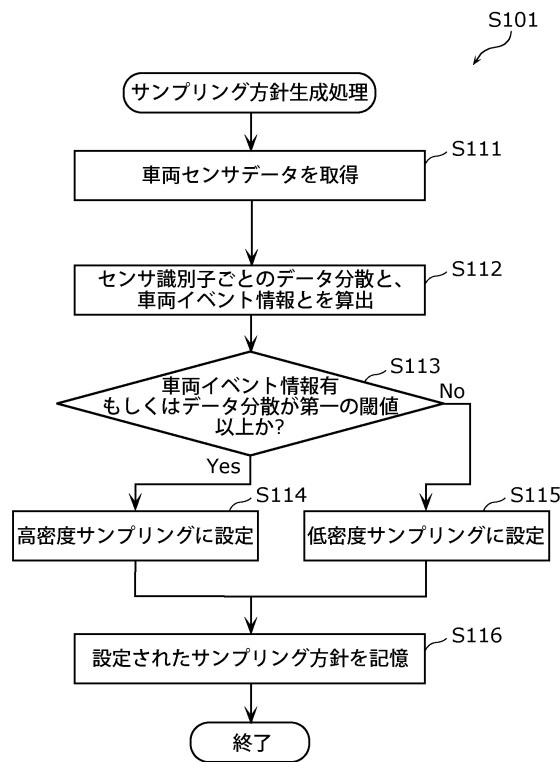
40

50

【図 3】



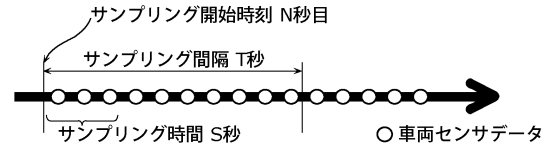
【図 4】



【図 5】

センサ識別子	データID	取得時刻[ms]		センサ値
		142	143	
車速	1	25.00	22.11	22.11
車速	2	50.01	22.50	22.50
車速	3	75.15	23.11	23.11
...	...	...	...	...
車速	41	1025.00	30.11	30.11
車速	42	1050.00	33.50	33.50
車速	43	1075.00	33.50	33.50
...	...	...	...	...
車速	81	2025.00	35.11	35.11
車速	82	2048.00	100.50	100.50
車速	83	2050.00	35.50	35.50
...	...	...	...	...
車速	2401	60025.00	40.11	40.11
シフト	1	30.00	3.00(Drive)	3.00(Drive)
...	...	...	...	...
シフト	2000	60010.00	0.00(Drive)	0.00(Drive)
...	...	...	...	...

【図 6】



10

20

30

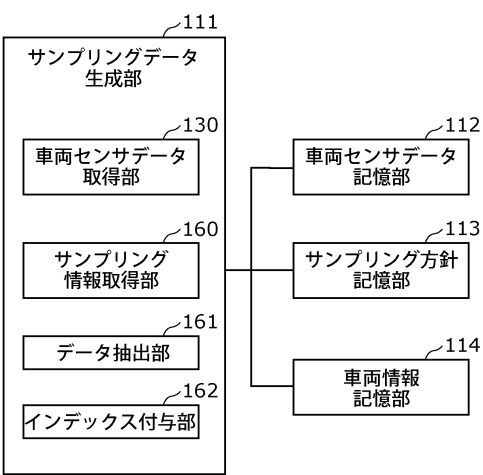
40

50

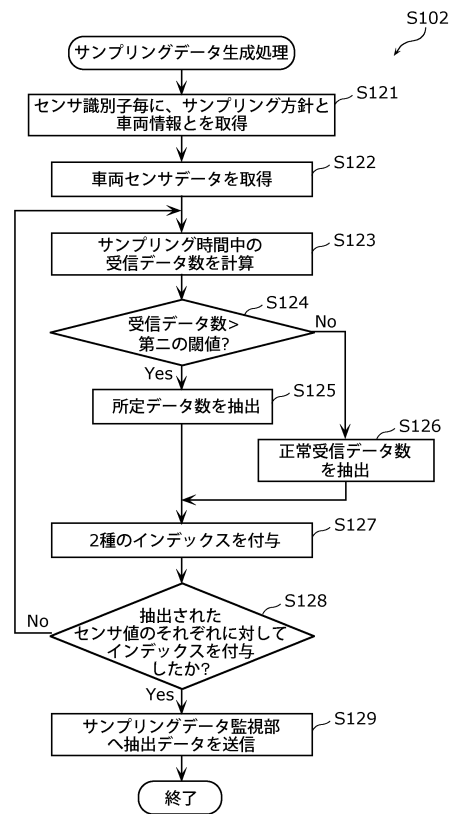
【図 7】

152 センサ識別子	153 ファイル番号	154 データ分散	155 車両イベントフラグ	156 サンプリング間隔[ms]	157 サンプリング時間[ms]
車速	1	0.22	有	200.00	75.00
...	1	...		...	...
車速	2	0.22	無	1000.00	55.00
...	2	...		...	...
車速	3	10.22	無	200.00	75.00
...	3	...		...	...

【図 8】



【図 9】



【図 10】

172 センサ識別子	173 評価ID	174 センサ値	175 第一のインデックス	176 第二のインデックス
車速	1	22.11	1	1
車速	2	22.50	2	1
車速	41	30.11	1	2
車速	42	33.50	2	2
車速	81	35.11	1	3
車速	82	100.50	2	3
車速	83	35.50	3	3
...	...	...	...	...
車速	2401	40.11	1	60
...	...	...	...	...

10

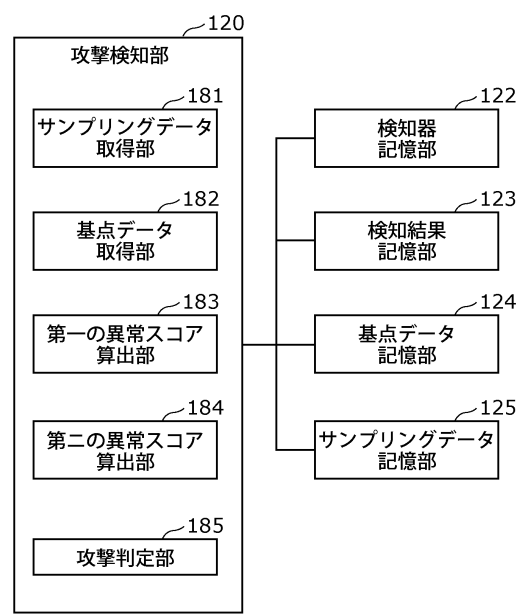
20

30

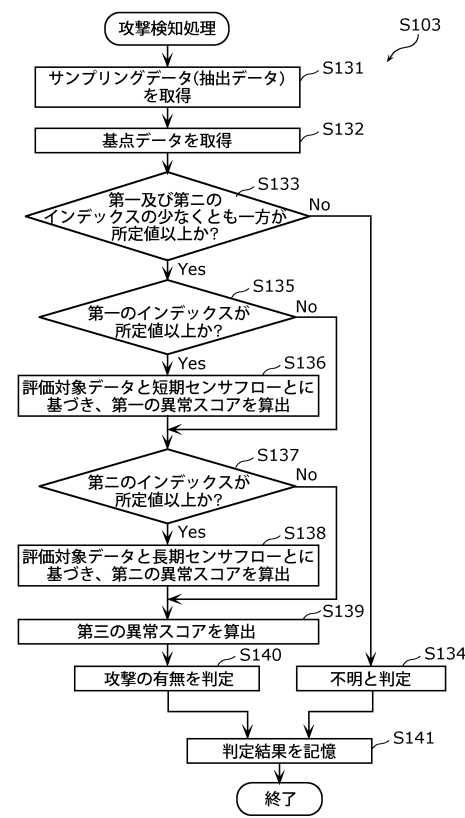
40

50

【図 1 1】



【図 1 2】



【図 1 3】

	192	193	194	195	196	197
センサ識別子	評価ID	センサ値	第一のインデックス	第二のインデックス	短期センサフロー	長期センサフロー
車速	1	22.11	1	1	[]	[]
...	...	...	...	...	...	...
車速	81	35.11	1	3	[]	[22.50, 33.50]
車速	82	100.50	2	3	[35.11]	[22.50, 33.50]
車速	83	35.50	3	3	[35.11, 35.11]	[22.50, 33.50, 35.11]
...	...	...	...	...	...	...

【図 1 4】

	202	203	204	205	206	207
センサ識別子	評価ID	センサ値	第一の異常スコア	第二の異常スコア	第三の異常スコア	検知結果
車速	1	22.11	0	0	0	"不明"
...	...	...	...	...	...	...
車速	81	35.11	0	6	6	"正常"
車速	82	100.50	95	80	87	"攻撃"
車速	83	35.50	2	0	1	"正常"
...	...	...	...	...	...	...

10

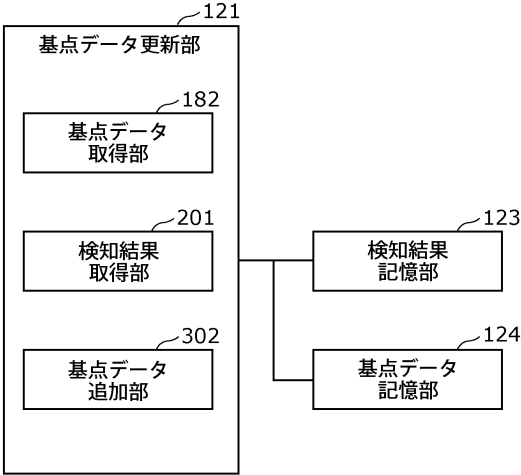
20

30

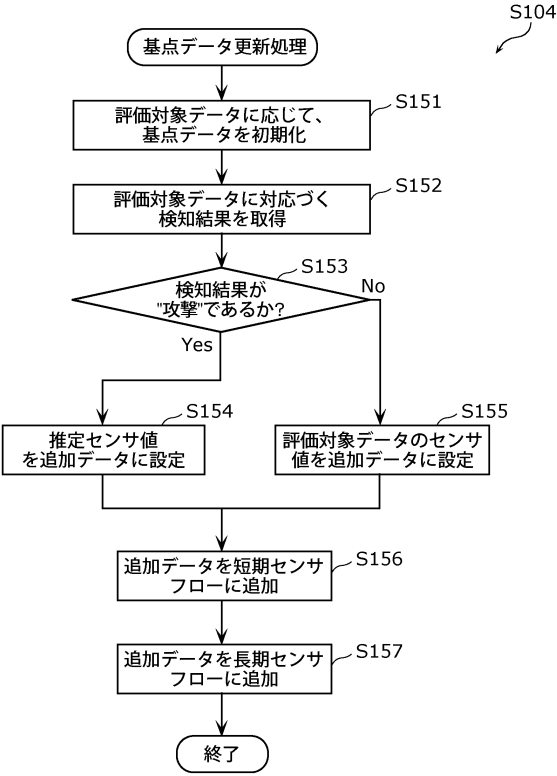
40

50

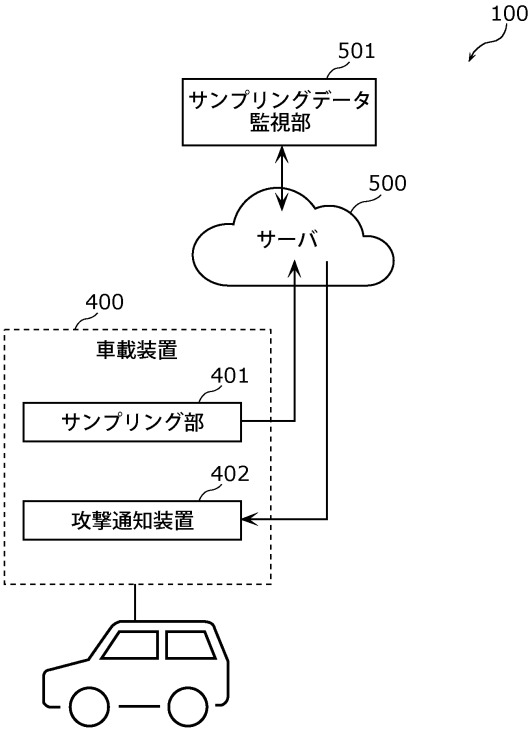
【図 1 5】



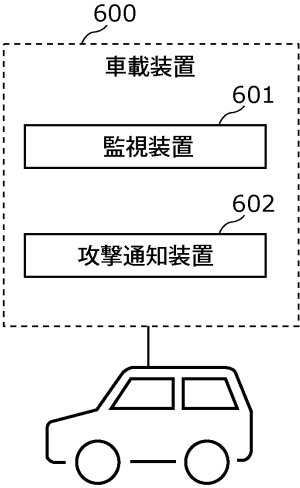
【図 1 6】



【図 1 7】



【図 1 8】



10

20

30

40

50

フロントページの続き

(72)発明者 牛尾 貴志

日本国大阪府門真市大字門真１００６番地 パナソニック株式会社内

(72)発明者 佐々木 崇光

日本国大阪府門真市大字門真１００６番地 パナソニック株式会社内

審査官 羽岡 さやか

(56)参考文献 国際公開第２０１８／１０５３１９（WO，A１）

特開２０１９－１４６１４５（JP，A）

米国特許出願公開第２０１９／０１３８４２３（US，A１）

牛尾 貴志, 佐々木 崇光, 芳賀 智之, 松島 秀樹, 大規模な車両遠隔監視を実現するための攻撃
検知に適したCANサンプリング手法の提案, ２０２０年 暗号と情報セキュリティシンポ
ジウム予稿集 [online] , 2020年01月21日, P.1-7

(58)調査した分野 (Int.Cl., DB名)

H04L 12/00-12/66

H04L 41/00-69/40