Title of the Invention: MULTI-TIERED HYBRID INTRUSION DETECTION SYSTEM FOR INTERNET OF VEHICLES

Background of the Invention:

Field of the Invention:

The present invention relates to the field of cybersecurity and specifically to intrusion detection systems (IDS) designed for the Internet of Vehicles (IoV). More particularly, the invention relates to a multi-tiered hybrid intrusion detection system that enhances the security of IoV by efficiently detecting and mitigating cyber-attacks targeting connected vehicles.

Description of the Related Art:

The IoV has emerged as a revolutionary concept that interconnects vehicles, infrastructure, and other entities to provide a wide range of applications and services. However, the connectivity of vehicles in the IoV also introduces significant security risks. Cyber-attacks targeting vehicles can compromise safety, privacy, and the overall integrity of the IoV system. Conventional intrusion detection systems have limitations when it comes to detecting sophisticated attacks and ensuring the security of the IoV environment.

Hence, there is a need for an improved intrusion detection system specifically designed for the IoV that can effectively identify and mitigate various types of attacks, ensuring the security and reliability of the IoV system.

Summary of the Invention:

The present invention discloses a multi-tiered hybrid intrusion detection system for the Internet of Vehicles. The system incorporates a combination of signature-based and anomaly-based intrusion detection techniques, along with a hierarchical structure to efficiently detect and respond to cyber-attacks targeting connected vehicles in the IoV environment.

The multi-tiered hybrid intrusion detection system comprises multiple tiers, each responsible for a specific function in the detection and mitigation process. The tiers include:

Data Collection Tier: This tier collects and aggregates network traffic data from various sensors, communication devices, and control units deployed in the IoV environment. The collected data is securely transmitted to the next tier for further analysis.

Preprocessing Tier: In this tier, the collected data undergoes preprocessing tasks such as data cleaning, filtering, and normalization. These tasks ensure the data's consistency and reliability for accurate intrusion detection.

Signature-Based Detection Tier: This tier employs signature-based detection techniques to compare the collected data against a comprehensive database of known attack signatures. If a match is found, the system raises an alarm indicating a potential intrusion.

Anomaly-Based Detection Tier: The anomaly-based detection tier utilizes machine learning algorithms and statistical models to establish a baseline behavior profile of the IoV system. Deviations from the established baseline are flagged as anomalies and investigated further to identify potential attacks.

Decision-Making Tier: This tier analyzes the outputs of the previous tiers and combines them to make informed decisions regarding the presence or absence of an intrusion. Advanced decision-making algorithms and rule-based engines are used to evaluate the severity of detected anomalies and initiate appropriate responses.

Response Tier: The response tier is responsible for executing actions to mitigate and neutralize detected intrusions. These actions may include isolating affected vehicles, alerting the authorities, or triggering countermeasures to prevent further damage.

The multi-tiered hybrid intrusion detection system for the Internet of Vehicles provides an advanced and comprehensive approach to detect and mitigate cyber-attacks effectively. By combining signature-based and anomaly-based techniques in a hierarchical structure, the system can enhance the security of connected vehicles, safeguard the privacy of passengers, and ensure the integrity of the IoV system.

Description of the Drawings:

The multi-tiered hybrid intrusion detection system for the Internet of Vehicles (IoV) consists of several interconnected tiers, each with specific functions in the intrusion detection and response process. These tiers work together to enhance the security of the IoV environment.

Data Collection Tier:

The Data Collection Tier is responsible for collecting network traffic data from various sources within the IoV environment, including sensors, communication devices, and control units. It gathers relevant data such as network packets, telemetry information, and communication logs.

Preprocessing Tier:

The Preprocessing Tier receives the collected data from the Data Collection Tier. Its primary role is to perform necessary preprocessing tasks on the data to ensure its quality and reliability. These tasks may include data cleaning, filtering, and normalization. The data is cleaned to remove noise, irrelevant information, and inconsistencies. Filtering techniques are applied to focus on specific types of traffic or data relevant to intrusion detection. Normalization techniques standardize the data format and range, enabling accurate analysis and comparison.

Signature-Based Detection Tier:

The Signature-Based Detection Tier receives the preprocessed data from the Preprocessing Tier. It utilizes signature-based detection techniques to compare the data against a comprehensive database of known attack signatures. The database contains patterns, signatures, or behavioral characteristics associated with known cyber-attacks. By matching the data against this database, the tier identifies potential intrusions and raises alarms for further investigation.

Anomaly-Based Detection Tier:

The Anomaly-Based Detection Tier receives the preprocessed data and employs machine learning algorithms and statistical models to establish a baseline behavior profile of the IoV system. During the training phase, the system learns the normal behavior patterns of the IoV system using historical data. During operation, the tier compares the incoming data against the established baseline and identifies anomalies or deviations from the normal behavior. These anomalies are flagged for further investigation as they may indicate potential cyber-attacks.

Decision-Making Tier:

The Decision-Making Tier receives the outputs from both the Signature-Based Detection Tier and the Anomaly-Based Detection Tier. It analyzes the results and makes informed decisions regarding the presence or absence of an intrusion. This tier utilizes advanced decision-making algorithms, rule-based engines, or machine learning classifiers to evaluate the severity and credibility of the detected anomalies. Based on these assessments, the tier determines the appropriate response actions.

Response Tier:

The Response Tier is responsible for executing actions to mitigate and neutralize detected intrusions. It takes the decisions made in the Decision-Making Tier and initiates appropriate response mechanisms. These actions may include isolating affected vehicles from the network, altering the behavior of the IoV system, alerting authorities or security teams, and implementing countermeasures to prevent further damage.

The architecture of the multi-tiered hybrid intrusion detection system facilitates the efficient detection and response to cyber-attacks in the IoV environment by combining signature-based and anomaly-based techniques. The data flows sequentially through the tiers, with each tier performing specific tasks and passing the processed data to the next tier, leading to effective intrusion detection and response.

Detailed Description of the Invention:

Data Collection Tier:

The Data Collection Tier is responsible for collecting and aggregating network traffic data from sensors, communication devices, and control units deployed in the IoV environment. This tier utilizes various data collection mechanisms, such as network sniffing or monitoring

interfaces, to capture the relevant traffic data. The collected data includes network packets, vehicle telemetry information, and communication logs.

Preprocessing Tier:

The Preprocessing Tier performs essential tasks to ensure the quality and reliability of the collected data. These tasks include data cleaning, filtering, and normalization. Data cleaning removes noise, irrelevant information, and inconsistencies from the raw data. Filtering techniques are applied to focus on specific types of traffic or data relevant to intrusion detection. Normalization techniques are used to standardize the data format and range, enabling accurate analysis and comparison.

Signature-Based Detection Tier:

The Signature-Based Detection Tier utilizes signature-based detection techniques to compare the preprocessed data against a comprehensive database of known attack signatures. This database contains patterns, signatures, or behavioral characteristics associated with known cyber-attacks. The tier uses matching algorithms, such as pattern matching or string comparison, to identify potential intrusions. If a match is found, the system raises an alarm, indicating a potential intrusion that requires further investigation.

Anomaly-Based Detection Tier:

The Anomaly-Based Detection Tier employs machine learning algorithms and statistical models to establish a baseline behavior profile of the IoV system. Initially, the system is trained using historical data to learn the normal behavior patterns of the IoV system. This training includes extracting relevant features from the data and building statistical models, such as clustering algorithms, anomaly detection algorithms (e.g., Isolation Forest, One-Class SVM), or time series analysis methods. During operation, the tier compares the incoming data against the established baseline and identifies deviations or anomalies from the normal behavior. These anomalies are then flagged for further investigation, as they may indicate potential cyber-attacks.

Decision-Making Tier:

The Decision-Making Tier analyzes the outputs from the Signature-Based Detection Tier and the Anomaly-Based Detection Tier to make informed decisions regarding the presence or absence of an intrusion. This tier utilizes advanced decision-making algorithms, such as rule-based engines, fuzzy logic systems, or machine learning classifiers, to evaluate the severity and credibility of detected anomalies. It combines the results from both detection techniques and assigns a confidence level or risk score to each potential intrusion. Based on these assessments, the tier makes decisions regarding further actions to be taken.

Response Tier:

The Response Tier is responsible for executing actions to mitigate and neutralize detected intrusions. Upon identifying a potential intrusion, this tier triggers appropriate response mechanisms to minimize the impact and prevent further damage. The responses can include isolating affected vehicles from the network, altering the behavior of the IoV system, alerting relevant authorities or security teams, or implementing countermeasures (e.g., firewall rules, access controls, encryption) to thwart the attack. The specific response actions depend on the severity and nature of the intrusion, as determined by the Decision-Making Tier.

Interactions within the Multi-Tiered Hybrid Intrusion Detection System:

The data flows sequentially through the different tiers of the system, with each tier performing specific tasks and passing the processed data to the next tier. The Data Collection Tier collects raw data from sensors and devices and forwards it to the Preprocessing Tier. The Preprocessing Tier cleans, filters, and normalizes the data and passes it to both the Signature-Based Detection Tier and the Anomaly-Based Detection Tier. The Signature-Based Detection Tier compares the data against known attack signatures, while the Anomaly-Based Detection Tier builds behavior profiles and identifies anomalies. The outputs from these detection tiers are then analyzed by the Decision-Making Tier, which assesses the severity of detected anomalies and makes informed decisions. Finally, the Response Tier executes appropriate actions to mitigate and neutralize the detected intrusions.

The interactions between the tiers allow for the comprehensive detection and response to cyber-attacks in the IoV environment, leveraging both signature-based and anomaly-based detection techniques to enhance the system's accuracy and effectiveness.

Claims:

A multi-tiered hybrid intrusion detection system for the Internet of Vehicles (IoV), comprising:

a. A Data Collection Tier configured to collect and aggregate network traffic data from sensors, communication devices, and control units deployed in the IoV environment.

b. A Preprocessing Tier configured to perform data cleaning, filtering, and normalization on the collected data to ensure its consistency and reliability.

c. A Signature-Based Detection Tier configured to compare the preprocessed data against a comprehensive database of known attack signatures and raise alarms upon detecting a potential intrusion.

d. An Anomaly-Based Detection Tier configured to utilize machine learning algorithms and statistical models to establish a baseline behavior profile of the IoV system and detect anomalies indicative of potential attacks.

e. A Decision-Making Tier configured to analyze outputs from the Signature-Based Detection Tier and the Anomaly-Based Detection Tier to make informed decisions regarding the presence or absence of an intrusion, using advanced decision-making algorithms and rule-based engines.

f. A Response Tier configured to execute actions to mitigate and neutralize detected intrusions, including isolating affected vehicles, alerting authorities, and implementing countermeasures to prevent further damage.

The multi-tiered hybrid intrusion detection system of claim 1, wherein the combination of signature-based and anomaly-based detection techniques enhances the accuracy and effectiveness of intrusion detection in the IoV environment.

The multi-tiered hybrid intrusion detection system of claim 1, further comprising secure communication channels and encryption mechanisms to ensure the confidentiality and integrity of the collected data and system communications.

The multi-tiered hybrid intrusion detection system of claim 1, wherein the hierarchical structure and modular design facilitate scalability, flexibility, and ease of integration with existing IoV infrastructures.

The multi-tiered hybrid intrusion detection system of claim 1, wherein the system incorporates machine learning algorithms and adaptive models that continuously learn and update the behavior profile of the IoV system to adapt to evolving cyber-attack techniques.

A method for detecting and mitigating cyber-attacks in the Internet of Vehicles (IoV) environment, comprising:

a. Collecting and aggregating network traffic data from sensors, communication devices, and control units deployed in the IoV environment.

b. Preprocessing the collected data by performing data cleaning, filtering, and normalization to ensure its consistency and reliability.

c. Comparing the preprocessed data against a comprehensive database of known attack signatures to identify potential intrusions.

d. Utilizing machine learning algorithms and statistical models to establish a baseline behavior profile of the IoV system and detect anomalies indicative of potential attacks.

e. Analyzing outputs from the signature-based and anomaly-based detection processes to make informed decisions regarding the presence or absence of an intrusion.

f. Executing actions to mitigate and neutralize detected intrusions, including isolating affected vehicles, alerting authorities, and implementing countermeasures to prevent further damage.

The method of claim 6, wherein the combination of signature-based and anomaly-based detection techniques enhances the accuracy and effectiveness of intrusion detection in the IoV environment.

The method of claim 6, further comprising securing the communication channels and applying encryption mechanisms to ensure the confidentiality and integrity of the collected data and system communications.

The method of claim 6, wherein the hierarchical structure and modular design of the intrusion detection system facilitate scalability, flexibility, and ease of integration with existing IoV infrastructures.

The method of claim 6, wherein the system incorporates machine learning algorithms and adaptive models that continuously learn and update the behavior profile of the IoV system to adapt to evolving cyber-attack techniques.

Scope of Protection:

The scope of protection sought for the multi-tiered hybrid intrusion detection system for the Internet of Vehicles (IoV) encompasses the novel features and aspects outlined in the claims. These claims cover the specific configuration and arrangement of the data collection, preprocessing, signature-based detection, anomaly-based detection, decision-making, and response tiers within the system. Furthermore, the claims cover the combination of signature-based and anomaly-based detection techniques, secure communication channels, scalability and flexibility features, and the utilization of machine learning algorithms and adaptive models. The protection sought extends to both the system itself and the method for detecting and mitigating cyber-attacks in the IoV environment.

Abstract:

The present invention discloses a multi-tiered hybrid intrusion detection system for the Internet of Vehicles (IoV). The system employs a combination of signature-based and anomaly-based intrusion detection techniques, along with a hierarchical structure, to efficiently detect and mitigate cyber-attacks targeting connected vehicles in the IoV environment. The system comprises multiple tiers, including data collection, preprocessing, signature-based detection, anomaly-based detection, decision-making, and response tiers, each responsible for specific functions in the intrusion detection and response process. The multi-tiered hybrid intrusion detection system enhances the security of the IoV, ensuring the safety, privacy, and integrity of the connected vehicles and the overall IoV system.