Technical Scientific Report: Network Security Inventions

Abstract

This report analyzes a collection of patent documents related to network security, focusing on inventions that address intrusion detection and prevention, vulnerability detection, and overall network protection. The inventions span various technical fields, including application layer firewalls, vehicle network security, industrial control systems, cloud computing, and mobile device security. The primary objective of these inventions is to enhance network security by providing improved mechanisms for detecting intrusions, preventing cyberattacks, and mitigating vulnerabilities in diverse network environments.

Background and Context

The increasing connectivity and complexity of modern networks have led to significant challenges in maintaining network security. Traditional layered security solutions often fail to provide early detection of intrusion incidents, leaving key network elements exposed (WO 2011115856). The rise of cyberattacks targeting various sectors, including vehicles (EP 4384992, EP 4149051, EP 4105801), industrial systems (EP 3671509, EP 3839782), cloud environments (WO 2016140198, EP 4380108, WO 2023180169, EP 4380107, WO 2025015187), and mobile devices (EP 2975818), necessitates advanced security measures. Existing security assessment tools often lack the capability to model complex relationships between assets, limiting the accuracy of asset/vulnerability associations (EP 1768046). Furthermore, dynamic network changes can invalidate security points, rendering countermeasures ineffective (WO 2016140198). The inventions discussed in this report address these challenges by providing innovative solutions for intrusion detection, vulnerability management, and overall network protection.

Technical Fields of Invention

The inventions covered in the provided patent texts relate to the following technological areas and fields:

- **Intrusion Detection and Prevention Systems (IDPS):** (WO 2011115856, EP 4384992, EP 3671509, WO 2021034441, WO 2017160913, EP 4149051).

- **Firewall Technology:** (WO 2011115856, EP 4380108, EP 3682325, WO 2023180169, EP 3888323).
- **Vulnerability Detection and Management:** (WO 2022068742, EP 4416625, EP 1768046).
- **Network Security in Specific Environments:** (EP 4384992, EP 4149051, EP 4105801) (Vehicle Networks), (EP 3671509, EP 3839782) (Industrial Systems), (WO 2016140198, EP 4380108, WO 2023180169, EP 4380107, WO 2025015187) (Cloud Computing), (EP 2975818) (Mobile Devices).
- **Anomaly Detection:** (WO 2020127027, EP 3523944, EP 3839782, EP 4380107, EP 1682990, EP 2618538, EP 3913882, WO 2024028114).
- **Cybersecurity for AI/ML Systems:** (EP 4483303, WO 2023215720, WO 2024035629, WO 2024091915).
- **API Security:** (WO 2024155835).
- **Software Container Security:** (WO 2019110512).
- **Privilege Assurance:** (WO 2022046366, WO 2024258881).
- **Cyber Threat Defense Systems:** (EP 4539423).
- **Data Exfiltration Prevention:** (WO 2024091915).
- **System Recovery:** (WO 2024023527).
- **Automated Forensics:** (EP 2946332).
- **Encrypted Traffic Analysis:** (EP 3306890).
- **Peripheral Device Security:** (WO 2019070456).
- **Network Intrusion Detection:** (WO 2003051018).
- **Suspicious Traffic Detection:** (WO 2023178479).

Inventions Related to Network Security

The following are some of the most related inventions with novelty and objectives:

- **Application Layer Firewall with Deep Packet Inspection (WO 2011115856):** This invention introduces an application layer firewall function with integrated deep packet inspection for early intrusion detection and prevention. It solves the problem of conventional layered network security solutions not providing early detection of intrusion incidents. The novelty lies in its ability to analyze application layer data for malicious content, enabling proactive security measures. (Relevant)

- **Intrusion Prevention in Industrial Systems (EP 3671509):** This invention focuses on reducing the time required for inspecting packets and detecting unauthorized commands in OT networks. It utilizes an intrusion prevention device with an analysis table storage, a parse part, and an analysis part to analyze commands and their time information in slots. The objective is to minimize packet transmission delays while ensuring security in industrial systems. (Relevant)

- **Cyber-Attack Response Methods for a Fleet of Vehicles (EP 4149051):** This invention addresses the problem of ineffective cyber-attack protection in areas where attacked vehicles lack internet access. The technical solution involves attacked vehicles directly informing nearby vehicles via a short-range communication protocol. The novelty is the use of short-range communication for rapid dissemination of cyber-attack information within a vehicle fleet. (Relevant)

- **Intrusion Detection in Operational Control Systems (WO 2017160913):** This invention aims to detect subtly malicious sequences of operationally valid control messages that can harm or disrupt devices. It monitors control messages, determines system-level correlations, generates potentially harmful message sequences, and reports threats. The novelty lies in its ability to identify complex attack patterns that are difficult to detect using traditional methods. (Relevant)

- **Intelligent Firewall Policy Processing in Cloud Data Centers (EP 4380108):** This invention addresses the technical problem of inefficient firewall policy processing due to the large number of policies and the dynamic nature of cloud applications. The technical solution involves using telemetry data and machine learning to determine a subset of relevant firewall policies for each host, reducing the processing load. (Relevant)

- **Dynamic Intent-Based Firewall (EP 3888323):** This invention solves the problem of inflexibility and complexity in configuring conventional Zone-Based Firewalls (ZFWs) by decoupling zone definitions from network interfaces and enabling centralized management. This is achieved by using a network controller to generate a master route table, receive zone definitions and ZFW policies, evaluate these policies to determine edge network devices and routing information, and then transmit this information to the edge network devices. (Relevant)

- **API Security Service with Data Obfuscation (WO 2024155835):** This invention addresses the problem of inspecting API traffic for malicious activity while avoiding the processing of sensitive information. The objective is achieved by applying a data obfuscation process to structured data in API requests and responses, retaining the structural aspects while obfuscating the content. (Relevant)
- **AI Security Platform (EP 4483303):** This invention addresses the problem of securing AI/ML models, simplifying AI security for enterprise applications, and providing visibility across an entire organization. The invention can be used by CISOs, AI security teams, and AI engineering teams to protect against AI-specific risks, monitor AI implementations, and ensure data integrity and model behavior. (Relevant)

Applicability and Uses

The inventions related to network security have a wide range of practical applications and uses:

- **Service Provider Networks (WO 2011115856):** The application layer firewall can be used in service provider networks to protect devices such as session border controllers, class 4 or class 5 network switches, and media gateways. (Relevant)
- **Vehicle Networks (EP 4384992, EP 4149051, EP 4105801, WO 2023178479, EP 3523944):** The intrusion detection and prevention systems can be used to protect vehicle networks from malware, ransomware, and unauthorized access, ensuring the safe and reliable operation of the vehicle. The cyber-attack response methods can be used to protect fleets of vehicles, such as police cars, buses, and mining trucks, against cyber-attacks, especially in areas with limited network signals. (Relevant)
- **Industrial Systems (EP 3671509, EP 3839782):** The intrusion prevention device can be used to protect industrial systems, such as those controlling electric power, gas, water supply, chemical, and oil infrastructures, from cyber attacks. (Relevant)

- **Cloud Computing (WO 2016140198, EP 4380108, WO 2023180169, EP 4380107, WO 2025015187):** The security invalidation prevention device can be used in cloud computing or software-defined networking (SDN) environments. The intelligent firewall policy processing can be used in cloud data centers and other network environments to improve firewall performance, enhance security, and optimize resource utilization. The smart SDN method can be used in software-defined networks with micro segmentation to prevent malicious traffic from moving freely inside a cloud environment. (Relevant)

- **Mobile Devices (EP 2975818):** The security server can be used to enhance the security of communication systems involving mobile devices. (Relevant)

- **Financial Technology (Fintech) (WO 2022068742):** The vulnerability detection method can be used for vulnerability detection in various security frameworks. (not Relevant)

- **AI/ML Systems (EP 4483303, WO 2023215720, WO 2024035629, WO 2024091915):** The AI security platform can be used by CISOs, AI security teams, and AI engineering teams to protect against AI-specific risks, monitor AI implementations, and ensure data integrity and model behavior. The secure access mechanisms can be used in 5G core networks to secure the sharing and distribution of ML models among network functions, enhancing the overall security of AI/ML-driven network analytics. (Relevant)

- **Zero-Trust Computing Environments (WO 2024091915):** The data exfiltration analysis can be used in scenarios where algorithm developers need to train algorithms on sensitive data held by data stewards, such as in healthcare, finance, or other industries dealing with proprietary or regulated data. (Relevant)

- **General Network Security (WO 2020127027, EP 1682990, EP 2618538, EP 3306890, WO 2003051018):** The anomaly detection methods can be used to improve network security by monitoring network traffic for abnormal patterns, protecting computer systems from malware and unauthorized network communications. The automated forensics can be used to enhance network security and increase the efficiency of detection and inhibition of security threats. (Relevant)

Conclusion

The patents analyzed in this report showcase a diverse range of inventions aimed at enhancing network security across various domains. These inventions address critical challenges such as early intrusion detection, vulnerability management, protection of industrial systems and vehicle networks, securing cloud environments, and mitigating advanced cyber threats. By leveraging technologies like deep packet inspection, machine learning, and dynamic policy management, these inventions provide innovative solutions for protecting networks and systems from evolving security risks. The collective impact of these inventions is a significant advancement in the field of network security, enabling organizations to better defend against cyberattacks and maintain the integrity and availability of their critical assets.

Citations

- WO 2011115856 (Relevant)
- EP 4384992 (Relevant)
- EP 3671509 (Relevant)
- WO 2021034441 (Relevant)
- EP 4149051 (Relevant)
- WO 2017160913 (Relevant)
- WO 2019070456 (Relevant)
- WO 2003051018 (Relevant)
- WO 2016140198 (Relevant)
- WO 2022046366 (Relevant)
- EP 4380108 (Relevant)
- EP 1768046 (Relevant)
- WO 2023180169 (Relevant)
- WO 2024258881 (Relevant)
- EP 3682325 (Relevant)
- WO 2022068742 (not Relevant)
- EP 4416625 (Relevant)

- EP 3888323 (Relevant)
- WO 2025015187 (Relevant)
- WO 2024091915 (Relevant)
- WO 2024023527 (Relevant)
- WO 2020127027 (Relevant)
- EP 2975818 (Relevant)
- EP 4483303 (Relevant)
- WO 2019110512 (Relevant)
- WO 2024155835 (Relevant)
- WO 2024035629 (Relevant)
- WO 2024028114 (Relevant)
- WO 2023215720 (Relevant)
- EP 3523944 (Relevant)
- EP 3839782 (Relevant)
- EP 4380107 (Relevant)
- EP 1682990 (Relevant)
- EP 4539423 (Relevant)
- EP 4105801 (Relevant)
- EP 2618538 (Relevant)
- EP 3913882 (Relevant)
- WO 2023178479 (Relevant)
- EP 2946332 (Relevant)
- EP 3306890 (Relevant)

Contexts: WO 2011115856 :: METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR PROVIDING APPLICATION LAYER FIREWALL AND INTEGRATED DEEP PACKET INSPECTION FUNCTIONS FOR PROVIDING EARLY INTRUSION DETECTION AND INTRUSION PREVENTION AT AN EDGE NETWORKING DEVICE\n EP 4384992 :: UNIVERSAL INTRUSION DETECTION AND PREVENTION FOR VEHICLE NETWORKS\n EP 3671509 :: INTRUSION PREVENTION DEVICE, INTRUSION PREVENTION METHOD, AND PROGRAM\n WO 2021034441 :: INTRUDER DETECTION FOR A NETWORK\n EP 4149051 :: A TRACKING AND MANAGEMENT METHOD FOR RESPONDING TO A CYBER-ATTACK\n WO 2017160913 :: INTRUSION DETECTION VIA SEMANTIC FUZZING AND MESSAGE PROVENANCE\n WO 2019070456 :: PERIPHERAL CYBER-SECURITY DEVICE\n

WO 2003051018 :: DETECTING INTRUSIONS IN A NETWORK\n
WO 2016140198 :: SECURITY MEASURE INVALIDATION PREVENTION DEVICE, SECURITY MEASURE INVALIDATION PREVENTION METHOD, AND SECURITY MEASURE INVALIDATION PREVENTION PROGRAM\n
WO 2022046366 :: PRIVILEGE ASSURANCE OF ENTERPRISE COMPUTER NETWORK ENVIRONMENTS\n
EP 4380108 :: INTELLIGENT FIREWALL POLICY PROCESSOR\n
EP 1768046 :: Systems and methods of associating security vulnerabilities and assets\n
WO 2023180169 :: SMART SDN FOR INTRUSION PREVENTION\n
WO 2024258881 :: DYNAMIC AUTHENTICATION REVOCATION UTILIZING PRIVILEGE ASSURANCE\n
EP 3682325 :: FINE-GRAINED FIREWALL POLICY ENFORCEMENT USING SESSION APP ID AND ENDPOINT PROCESS ID CORRELATION\n
WO 2022068742 :: VULNERABILITY DETECTION METHOD AND APPARATUS, ELECTRONIC DEVICE, AND COMPUTER-READABLE STORAGE MEDIUM\n
EP 4416625 :: SECURITY VULNERABILITY COMMUNICATION AND REMEDIATION WITH MACHINE LEARNING\n
EP 3888323 :: DYNAMIC INTENT-BASED FIREWALL\n
WO 2025015187 :: SYSTEMS AND METHODOLOGIES FOR AUTO LABELING VULNERABILITIES\n
WO 2024091915 :: SYSTEMS AND METHODS FOR DATA EXFILTRATION PREVENTION IN A ZERO-TRUST ENVIRONMENT\n
, WO 2024023527 :: DETECTION OF ANOMALOUS BACK-UP COPIES\n
WO 2020127027 :: MALWARE DETECTION IN NETWORK TRAFFIC TIME SERIES\n
EP 2975818 :: Method and system for enhancing the security of mobile devices\n
EP 4483303 :: SYSTEM AND METHOD FOR IMPLEMENTING AN ARTIFICIAL INTELLIGENCE SECURITY PLATFORM\n
WO 2019110512 :: SOFTWARE CONTAINER APPLICATION SECURITY\n
WO 2024155835 :: API SECURITY BASED ON INSPECTION OF OBFUSCATED REQUEST AND RESPONSE BODIES\n
WO 2024035629 :: AUTHORIZATION OF APPLICATION FUNCTION FOR POLICY MANAGEMENT\n
WO 2024028114 :: DETERMINING ANOMALOUS STATE OF WIRELESS COMMUNICATION DEVICES\n
WO 2023215720 :: AUTHORIZATION AND AUTHENTICATION OF MACHINE LEARNING MODEL TRANSFER\n
EP 3523944 :: SYSTEM FOR ANOMALY DETECTION ON CAN BUS DATA WITH SPARSE AND LOW RANK DECOMPOSITION OF TRANSFER ENTROPY MATRIX\n
EP 3839782 :: DYNAMIC MONITORING AND SECURING OF FACTORY PROCESSES, EQUIPMENT AND AUTOMATED SYSTEMS\n
EP 4380107 :: SELF-LEARNING EGRESS TRAFFIC CONTROLLER\n
EP 1682990 :: APPARATUS METHOD AND MEDIUM FOR DETECTING PAYLOAD ANOMALY USING N-GRAM DISTRIBUTION OF NORMAL DATA\n
EP 4539423 :: A CYBER THREAT DEFENSE SYSTEM, COMPONENTS, AND A METHOD FOR USING ARTIFICIAL INTELLIGENCE MODELS TRAINED ON A NORMAL PATTERN OF LIFE FOR SYSTEMS WITH UNUSUAL DATA SOURCES\n
EP 4105801 :: USING STAGED MACHINE LEARNING TO ENHANCE VEHICLES CYBERSECURITY\n
EP 2618538 :: Apparatus Method and Medium for Detecting Payload Anomoly using N-Gram Distribution of Normal Data\n
EP 3913882 :: METHOD AND INFORMATION PROCESSING APPARATUS FOR FLAGGING ANOMALIES IN TEXT DATA\n

WO 2023178479 :: METHOD FOR DETECTING SUSPICIOUS TRAFFIC FOR A VEHICLE AND RELATED DEVICE\n
EP 2946332 :: AUTOMATED FORENSICS OF COMPUTER SYSTEMS USING BEHAVIORAL INTELLIGENCE\n
EP 3306890 :: ANALYZING ENCRYPTED TRAFFIC BEHAVIOR USING CONTEXTUAL TRAFFIC DATA\n