International Journal of Engineering, Management and Humanities (IJEMH)
Volume 4, Issue 5, Sep.-Oct., 2023 pp: 219-224 www.ijemh.com

An Intrusion Detection process base on Machine Learning Spectator Communication Systems

S.Naveen
Dr.M.Sathyabalaji
Department of Computer Science and Engineering, JKK Munirajah College of Technology, Erode, Tamilnadu 638 506, India

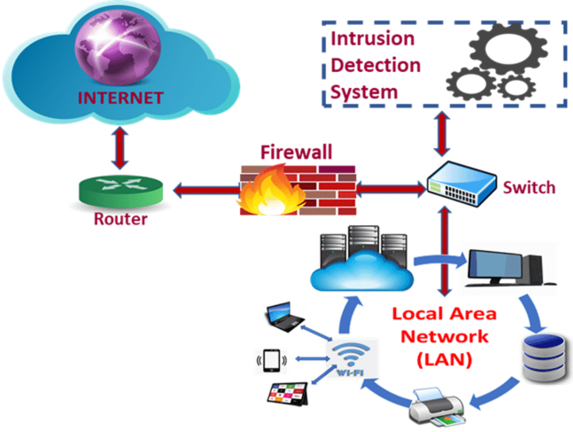
Date of Submission: 23-09-2023 Date of Acceptance: 06-10-2023

Abstract:
Communication-based train control (CBTC) systems are typical cyber-physical systems in urban rail transport. The vehicle-ground communication system is a very important subsystem in the CBTC system, which uses wireless communication protocols to transmit control commands. However, it also faces some potential information security risks. The detection system can not only detect the abnormality of the wireless network data, but also detect the abnormality of the physical condition of the train. The method consists of two layers. The first layer is used to detect and identify wireless network attacks based on machine learning algorithms such as Random Forest Algorithm and Gradient Boosting Decision Tree Algorithm. The second layer is used to detect abnormal physical conditions of train movement based on state observers. By combining the results of the above two layers, a comprehensive intrusion detection result is presented. Simulation results show that the proposed method is effective and practical. In order to ensure the information security of vehicle-ground communication system, this paper proposes an intrusion detection method based on machine learning and state observers to detect and identify various attacks.

Index: Intrusion Detection, Machine Learning, wireless communication

I. Introduction:

AT PRESENT, with the development of economy and the expansion of city scale, urban rail transit has been a primary passenger transportation method. The communication-based train control (CBTC) system, as a popular train operation control system, is widely used in urban rail transit. In the CBTC system, the train-ground communication subsystem is a critical security-related subsystem. It adopts wireless protocols to transmit control commands and train state information. Because of openness and vulnerability of wireless communication, the train-ground communication system can be a potential target for an attacker. Once the train-ground communication system suffers from an attack, the train operation will become less efficient. In serious cases, train operation security accidents can happen. Therefore, in the CBTC system, it is vital to ensure the security of the train-ground communication system [3]. For traditional information technology (IT) networks, various schemes are proposed to defense attacks. Especially, the intrusion detection method is a primary information security defense method, which can be divided into anomaly detection and misuse detection.



The anomaly detection method needs to model normal behaviors accurately. Based on the normal behavior model, this method determines whether a newly received data is abnormal. The anomaly detection method can detect zero-day attacks. However, this method usually has a higher false positive rate, because any tiny change different from the normal model can cause an attack alarm. Besides, this method can only detect an abnormal behavior, but cannot identify its attack type. The misuse detection method needs to model a specific attack behavior in advance, which causes this method not to detect unknown attacks, for example zero-day attacks. This method also needs to manually update the attack model database when a new attack is identified. In addition, there are some intrusion detection methods that combine anomaly detection and misuse detection methods, called hybrid intrusion detection methods, which can avoid the disadvantages of each method.

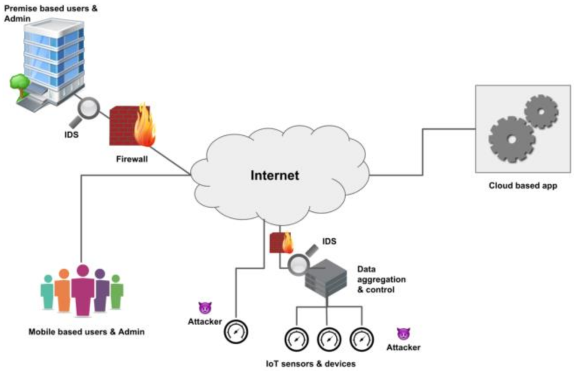
Intrusion detection methods, many results have been published. An intrusion detection method is proposed to detect black-hole and gray-hole attacks by using the continuous time Markov chain and stochastic reward net in wireless ad hoc networks. Present a hybrid intrusion detection method based on the theory of evidence to detect virtual jamming attacks in an network. This method combines the advantages of the signature-based and the anomaly-based intrusion detection method. Proposes two architectures to develop an anomaly detection system for the single access point and the distributed wireless fidelity (WIFI) networks, which can classify the attacks and track the location of the attackers, when the attacks have been detected. In this system, a sequence of n-grams in a given time period is introduced to model wireless network traffic. Agarwal et al. [8] introduce a novel intrusion detection system based on machine learning algorithms, which not only detects flood attacks, but also helps the victim station recover

At present, the research on information security is still in a preliminary stage in the CBTC system. Although the information security research on the industrial control system and the traditional IT network has achieved some results, the existing results cannot be directly used for the CBTC system.

For the information security research on the CBTC system, it is necessary to analyze the information security characteristics of the CBTC systems by referring to the research results of traditional IT networks and industrial control systems.

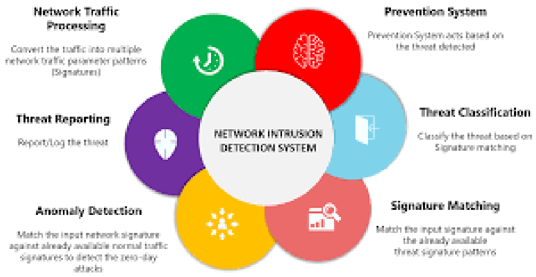
Communication system has some specific features, such as underground tunnel environment, high mobility speed, and fixed moving direction, strict requirement for accurate train-location information and using wireless communication protocols to transmit control commands. Therefore, the existing intrusion detection equipment's cannot be directly used in the train-ground communication system.

Focus on coexistence between intrusion detection systems and privacy mechanisms, because there exists a conflict between the privacy mechanisms and the intrusion detection systems. For example, an intrusion detection system could monitor packet dropping by checking whether an incoming packet is resent in a reasonable time frame, but a privacy mechanism that uses anonymity mixing mechanism will interfere with the detection.


Premise based users & Admin
IDS
Firewall
Internet
Cloud based app
IDS
Data aggregation & control
Mobile based users & Admin
Attacker
IoT sensors & devices
Attacker

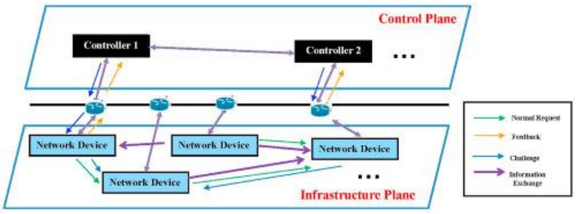
The existing methods are used to detect the attacks coming from the traditional IT network. In urban rail transit systems, the current works mainly focus on the functional safety, such as two-out of three safety computers, double two out of two safety computers and a redundant network design. The related research on information security has not received enough attention. Except the firewalls, there are no effective information security-related products which have been applied to the train-ground communication system, for example effective intrusion detection equipment. Different from the traditional IT network, the train-ground communication system has some specific features, such as underground tunnel environment, high mobility speed, fixed moving direction, strict requirement for accurate train-location information and using wireless communication protocols to transmit control commands.

Therefore, the existing intrusion detection equipments can not be directly used in the train-ground communication system. For solving this problem, this paper proposes a two-layer intrusion detection method to ensure the security of the train-ground communication system. The main contributions of the proposed method are summarized as follows:


NETWORK INTRUSION DETECTION SYSTEM
Network Traffic Processing
Convert the traffic into multiple network traffic parameter patterns (Signatures)
Prevention System
Prevention System acts based on the threat detected
Threat Reporting
Report/Log the threat
Threat Classification
Classify the threat based on Signature matching
Anomaly Detection
Match the input network signature against already available normal traffic signatures to detect the zero-day attacks
Signature Matching
Match the input signature against the already available threat signature patterns

• In the first layer, machine learning algorithms, such as the random forest algorithm and gradient boosted decision tree algorithm, are introduced to detect attacks on the wireless network. It can not only detect attacks, but also identify the types of attacks.

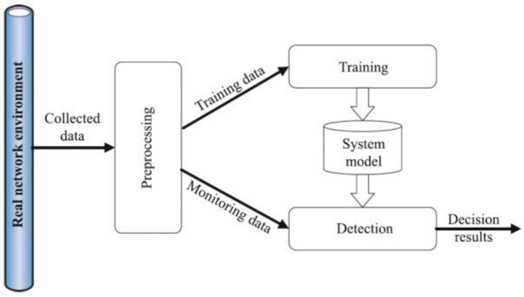
• In the second layer, an intrusion detection method based on the state observer is proposed. In each communication period, the observer calculates the deviation between the real value and the estimated value to detect abnormal behaviors.



• Based on the results of the two layers, a comprehensive conclusion is given, which divides the detection results into three categories, according to the impact on the train state. Furthermore, different alarm modes are adopted, which improves the detection effect of the train-ground communication system.

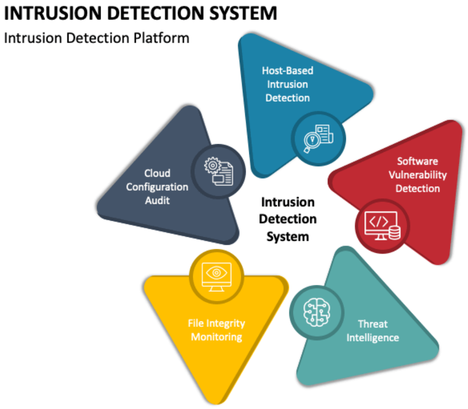
As a typical information physical system, the CBTC system transmits control commands through a communication network. Different from other industrial control systems, a large number of mechanisms are designed in the CBTC system, which makes the failure of communication does not always cause the anomaly of train states. Therefore, in the CBTC system, it is necessary to specifically consider whether the attack of communication link can affect the train states.

A comparison between the proposed method and other methods. Traditional IT network, there are no involved physical devices, so there is no need to study this problem. In other industrial control systems, the network attack is studied, or the fault detection of the physical devices is studied, there is no connection between them.



In the CBTC system, because the control commands of physical device are transmitted by the communication network and the mechanisms are designed, it is important to study the following contents. When the communication link is attacked, whether the train state is affected and the degree of the influence need to be studied, which makes a comprehensive understanding for the specific impact of communication link attacks on the physical devices.

The main contributions of the proposed method are summarized as follows:

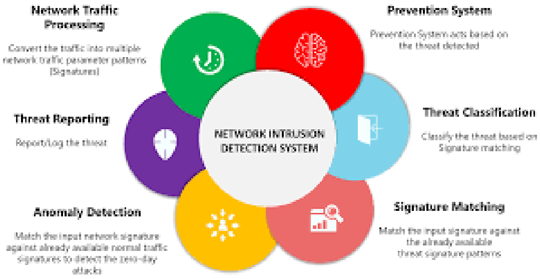

INTRUSION DETECTION SYSTEM
Intrusion Detection Platform
Host-Based Intrusion Detection
Cloud Configuration Audit
Intrusion Detection System
Software Vulnerability Detection
File Integrity Monitoring
Threat Intelligence

• In the first layer, machine learning algorithms, such as the random forest algorithm and gradient boosted decision tree algorithm, are introduced to detect attacks on the wireless network. It cannot only detect attacks, but also identify the types of attacks.

• In the second layer, an intrusion detection method based on the state observer is proposed. In each communication period, the observer calculates the deviation between the real value and the estimated value to detect abnormal behaviors.

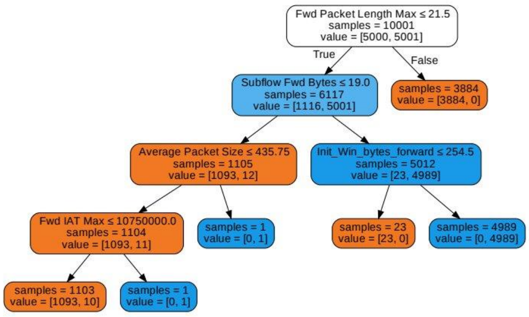
• Based on the results of the two layers, a comprehensive conclusion is given, which divides the detection results into three categories, according to the impact on the train state. Furthermore, different alarm modes are adopted, which improves the detection effect of the train-ground communication system.

This method combines the advantages of the signature-based and the anomaly-based intrusion detection method. Satam proposes two architectures to develop an anomaly detection system for the single access point and the distributed wireless fidelity (WIFI) networks, which can classify the attacks and track the location of the attackers, when the attacks have been detected. In this system, a sequence of n-grams in a given time period is introduced to model wireless network traffic.


Network Traffic Processing
Convert the traffic into multiple network traffic parameter patterns (Signatures)
Prevention System
Prevention System acts based on the threat detected
Threat Reporting
Report/Log the threat
NETWORK INTRUSION DETECTION SYSTEM
Threat Classification
Classify the threat based on Signature matching
Anomaly Detection
Match the input network signature against already available normal traffic signatures to detect the zero-day attacks
Signature Matching
Match the input signature against the already available threat signature patterns

As a typical information physical system, the CBTC system transmits control commands through a communication network. Different from other industrial control systems, a large number of "fail-safe" mechanisms are designed in the CBTC system, which makes the failure of communication does not always cause the anomaly of train states.

Besides, this method can only detect an abnormal behavior, but cannot identify its attack type.

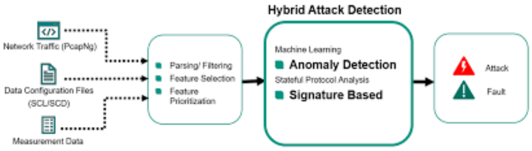


The misuse detection method needs to model a specific attack behavior in advance, which causes this method not to detect unknown attacks, for example zero-day attacks. This method also needs to manually update the attack model database when a new attack is identified. In addition, there are some intrusion detection methods that combine anomaly detection and misuse detection methods, called hybrid intrusion detection methods, which can avoid the disadvantages of each method.

Intrusion detection

To ensure information security of the train-ground communication system, an intrusion detection method based on machine learning and state observer is proposed to detect and recognize various attacks in this paper. The detection system not only detects the anomalies of the wireless network data, but also detects the anomalies of the train physical states. This method includes two layers.

For traditional information technology (IT) networks, various schemes are proposed to defense attacks. Especially, the intrusion detection method is a primary information security defense method, which can be divided into anomaly detection and misuse detection.



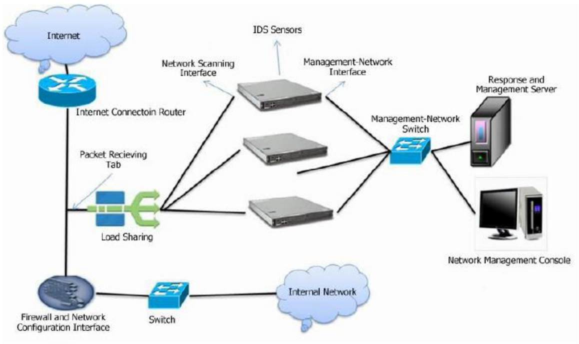
Train-ground communication system

The related research on information security has not received enough attention. Except the firewalls, there are no effective information security-related products which have been applied to the train-ground communication system, for example an effective intrusion detection equipment. Different from the traditional IT network, the train-ground communication system has some specific features, such as underground tunnel environment, high mobility speed, and fixed moving direction, strict requirement for accurate train-location information and using wireless communication protocols to transmit control commands.

Machine learning

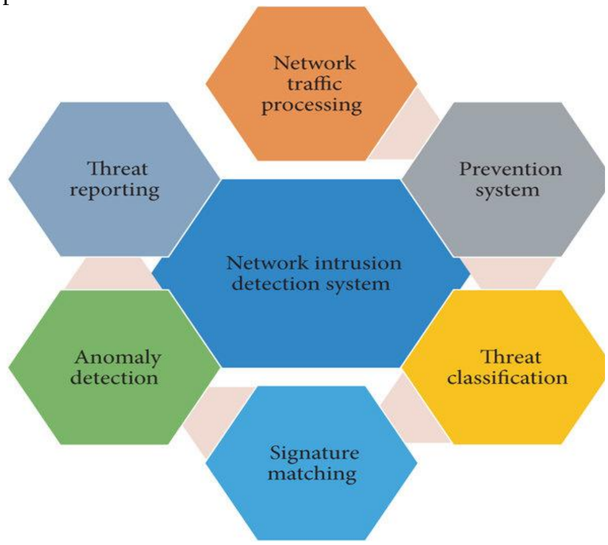
In the model training module, a multi-classification detection model is derived based on the training sample set and machine learning algorithms. The training sample set consists of the normal behaviors and abnormal behaviors. Machine learning algorithms can be the random forest (RF) algorithm, the support vector machine (SVM) algorithm, the AdaBoost algorithm or the gradient boosting decision tree (GBDT) algorithm.

In the first layer of the proposed intrusion detection algorithm, four machine learning algorithms are selected to construct their respective multi-classification detection models and validate their respective performance.


Internet
IDS Sensors
Network Scanning Interface
Management-Network Interface
Response and Management Server
Internet Connectoin Router
Management-Network Switch
Packet Recieving Tab
Load Sharing
Network Management Console
Internal Network
Firewall and Network Configuration Interface
Switch

State observer

If the detection results based on wireless data indicate that an attack occurs, meanwhile the detection results based on the state observer data indicate that an attack occurs, it will be defined as a first-level alarm in train-ground communication system. For the first-level alarm, an alarm is continually given and the prevention measures are performed.



If the detection results of only one layer reveal that there exists an attack, it will be defined as a secondary-level alarm which only has an alarm. Specifically, if the detection result of wireless data shows that there is an attack and the detection result of physical state data shows that it is normal, an alarm is given.

Algorithm: This method includes two layers. The first layer is used to detect and identify wireless network attacks based on machine learning algorithms, such as the random forest algorithm and the gradient boosted decision tree algorithm.

The second layer is used to detect the abnormal physical state of train operation based on a state observer. By combining the results of the above two layers, a comprehensive intrusion detection result is given. The simulation results show that the proposed method is effective and practical.

In the first layer, machine learning algorithms, such as the random forest algorithm and gradient boosted decision tree algorithm, are introduced to detect attacks on the wireless network. It can not only detect attacks, but also identify the types of attacks.

II. Conclusion:

An intrusion detection method based on machine learning and state observer is proposed in the train-ground communication system. The method includes two layers. In the first layer, machine learning algorithms areused to detect and identify the intrusion behavior on wireless network data. The machine learning algorithms include the random forest algorithm, the gradient boosted decision tree algorithm, the AdaBoost algorithm and the support vector machine algorithm. Further, in the second layer, an intrusion detection method based on state observer is proposed to recognize the abnormal train physical states. Finally, based on the detection results of wireless network data and train physical states, a reliable intrusion detection result is given, which is important for CBTC systems. Both theoretical analysis and simulation results show that only long-term continuous attacks can affect the train’s operation, while short-term continuous or random attacks do not affect the train’s operation

Future work:

Based on these experiments, some conclusions can be drawn. If the intrusion detection only focuses on the network layer, invalid alarms and defenses will increase, which aggravates the system overhead. If the intrusion detection only focuses on physical layer, the detection result has serious hysteresis, which means that the attack cannot be reported in time. When the attack is recognized, the system has been greatly affected and an emergency braking or collision will be inevitable. In the proposed method, the attack is simultaneously detected in the network layer and the physical layer. And the results are comprehensively analyzed.

Reference:

[1]. X. Wang, L. Liu, L. Zhu, and T. Tang, "Train-centric CBTC meets age of information in train-to-train communications," IEEE Trans. Intell. Transp. Syst., vol. 21, no. 10, pp. 4072–4085, Oct. 2020.

[2]. X. Wang, L. Liu, T. Tang, and W. Sun, "Enhancing communicationbased train control systems through train-to-train communications," IEEE Trans. Intell. Transp. Syst., vol. 20, no. 4, pp. 1544–1561, Apr. 2019.

[3]. X. Wang, L. Liu, L. Zhu, and T. Tang, "Joint security and QoS provisioning in train-centric CBTC systems under Sybil attacks," IEEE Access, vol. 7, pp. 91169–91182, 2019.

[4]. H. Alipour, Y. B. Al-Nashif, P. Satam, and S. Hariri, "Wireless anomaly detection based on IEEE 802.11 behavior analysis," IEEE Trans. Inf. Forensics Security, vol. 10, no. 10, pp. 2158–2170, Oct. 2015.

[5]. R. Entezari-Maleki, M. Gharib, M. Khosravi, and A. Movaghar, "IDS modelling and evaluation in WANETs against black/grey-hole attacks using stochastic models," Int. J. Ad Hoc Ubiquitous Comput., vol. 27, no. 3, pp. 171–186, 2018.

[6]. D. Santoro, G. Escudero-Andreu, K. G. Kyriakopoulos, F. J. Aparicio-Navarro, D. J. Parish, and M. Vadursi, "A hybrid intrusion detection system for virtual jamming attacks on wireless networks," Measurement, vol. 109, pp. 79–87, Oct. 2017.

[7]. P. Satam, "Anomaly based Wi-Fi intrusion detection system," in Proc. IEEE 2nd Int. Workshops Found. Appl. Self∗ Syst. (FAS∗W), Sep. 2017, pp. 377–378.

[8]. M. Agarwal, D. Pasumarthi, S. Biswas, and S. Nandi, "Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization," Int. J. Mach. Learn. Cybern., vol. 7, no. 6, pp. 1035–1051, Dec. 2016.

[9]. N. K. Mittal, "A survey on wireless sensor network for community intrusion detection systems," in Proc. 3rd Int. Conf. Recent Adv. Inf. Technol. (RAIT), Mar. 2016, pp. 107–111.

[10]. M. Usha and P. Kavitha, "Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier," Wireless Netw., vol. 23, no. 8, pp. 2431–2446, Nov. 2017.