Multi-Feature Transmission Behavior Analysis-Based Intrusion Detection in IoT Networks

Dr. Kumar Shwetabh[1], Pawan Kumar[2]

[1]Assistant Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India, ku.kumarshwetabh@kalingauniversity.ac.in
[2]Assistant Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India, ku.pawankumar@kalingauniversity.ac.in

Intrusion attack in Internet of Things (IoT) has been well studied. There exist number of approaches which detect the intrusion attack like payload and signature based approaches. However, they suffer to achieve higher performance in detecting intrusion attack in IoT networks. To handle this issue, an efficient Multi Feature Transmission Behavior based Intrusion Detection model (MFTBIDM) is presented in this paper. The method considers payload, frequency, signature, behavior of IoT nodes in the network to perform intrusion detection. To perform this, the Edge server monitors the frequency of data transmission, the signature of data packets towards any service, payload of data being sent, and behavior of IoT nodes. Accordingly, the method computes different trust score like Payload Trust Score (PTS), Frequency Trust Score (FTS), Signature Trust Score (STS), and Behavior Trust Score (BTS). Using all these trust scores, the method computes the value of Legitimate Transmission Score (LTS) to perform intrusion detection. The proposed method improves the performance of intrusion detection.

Keywords: IoT Networks, Intrusion Attack, Behavior Analysis, MFTBIDM, LTS..

1. Introduction

The growing use of communication technology has been adapted to different domain of educational world. Use of sensors and sensor networks are greatly adapted to different scenario to support different processes. The IoT network is the one which uses the development to perform variety of activities. It has been designed and integrated with various other networks to support the requirement. The use of IoT devices is getting increased day by day. It comes with sensor devices which support them to communicate with remote cloud networks or edge servers. It has been used to perform variety of monitoring and regulation on day to day life. For example, it has been used to monitor the patient health and submit the data to the remote server. Based on the reply, it would perform variety of activities. For example, when the IoT devices are integrated with the vehicle, it would get the

navigation data about the traffic and support to perform different diversion on the road traffic. Similarly, it has been used to monitor the remote activity and control variety of other devices.

The IoT network involve in data transmission through number of IoT devices and sensors. They involve in transmitting limited size of data which support the analysis of various information to perform different decision making. In general, the cooperative transmission introduces different security threat. The presence of malicious IoT node would perform intrusion attack towards the service being accessed over the cloud or edge server. If the adversary is managed to learn the pattern of data transmission, then it would capture the service data to perform different other threats. Presence of intrusion attack, degrades the performance of entire environment.

The presence of intrusion attack can be identified based on different metrics. For example, payload can be used to detect the intrusion attack. When the payload size crosses a limit, then you can conclude that there is intrusion attack. Similarly, the signature based approach would identify the presence of intrusion attack by mapping the signature of the data being received. In this way, number of approaches can be named to detect the intrusion attack. But, they introduce poor performance in intrusion attack detection. By considering all these, an efficient multi feature transmission behavior analysis model is presented in this article.

The MFTBAIDM model consider number of features like payload, signature, behavior and frequency features in detecting the presence of intrusion attack. The method analyzes the behavior of IoT nodes in sending payload data, signature, frequency of sending data packet and previous activity. By analyzing all these behaviors, the method estimates different trust scores on each behavior metric to perform intrusion detection. Complete working of the model is detailed in the next section.

2. Related Works:

Number of approaches can be named and described in literature to detect intrusion attack in IoT networks. Such methods are described in detail in this part.

An adaptive bi-recommendation and self-improving network (ABRSI) is presented in [1], which works based on unsupervised heterogeneous domain adaptation (HDA). The method performs recommendation matching in two ways to achieve higher performance. A Flow Topology based Graph Convolutional Network (FT-GCN) is presented in [2], which uses traffic flow patterns in detecting intrusion attack.

A Deep Convolutional Generative Adversarial Network based model is presented in [3], which uses fuzzy rough set scheme for feature selection and trained with CNN to perform classification.

MAC Protocol orient approach is presented in [4], which preprocess the data with reformed histogram equalization method, and feature selection is done with modified honey badger algorithm (MHBA). At last intrusion detection is performed with IEsBCCA-Net scheme.

A Graph Neural Network scheme is given in [5]. An explainable deep learning-based intrusion detection framework [6], uses SHapley Additive exPlanations (SHAP) to make decision on IDS.

A geometric graph alignment (GGA) scheme is presented in [7]. A machine learning model is presented towards intrusion detection in IoT communication [8]. A deep blockchain framework is given in [9], which uses bidirectional long short-term memory (BiLSTM) to perform intrusion detection.

A deep learning-based intrusion detection with generative adversarial network (GAN) is presented in [10], which perform feature selection and classification with deep learning architecture based on GAN.

A joint semantic transfer network (JSTN) model is presented in [11], to perform intrusion detection. The model uses multisource heterogeneous domain adaptation (MS-HDA) method, to perform knowledge-rich network intrusion. A conditional GAN is given in [12], which works according to the distribution features.

A semi supervised deep learning based IDS (SS-Deep-ID) is presented in [13]. A Regularized Cross Layer Ladder Network is presented in [14], to perform intrusion detection in industrial networks. A contrastive learning over random fourier feature based intrusion detection scheme is presented in [15].

3. Multi Feature Transmission Behavior Based Intrusion Detection Model (MFTBIDM):

The Multi Feature Transmission Behavior based Intrusion Detection model (MFTBIDM) monitors the network services and access at all the time. It considers payload, frequency, signature, behavior of IoT nodes in the network to perform intrusion detection. To perform this, the Edge server monitors the frequency of data transmission, the signature of data packets towards any service, payload of data being sent, and behavior of IoT nodes. Accordingly, the method computes different trust score like Payload Trust Score (PTS), Frequency Trust Score (FTS), Signature Trust Score (STS), and Behavior Trust Score (BTS). With the trust score computed, Legitimate Transmission Score (LTS) is measured to perform intrusion detection.

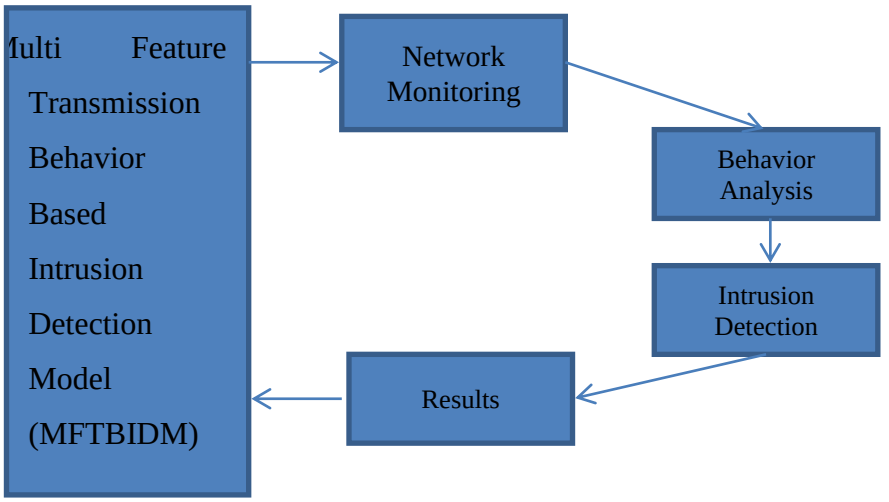

Figure 1: Architecture of Proposed MFTBIDM Model

The working diagram of proposed MFTBIDM model is presented in Figure 1, and the functions are described in detail in this section.

Network Monitoring:

The proposed method monitors the network behavior all the time. By receiving each service packet from the devices, it performs behavior analysis. Based on the behavior analysis, the method generates a trace about the devices and data transmission. Such trace has been used in further behavior analysis to support intrusion detection.

Given: Service Packet Sp, Trace T

Obtain : Trace T

Start

Read service packet sp and trace T.

While true

Feature set Fs = {sp.payload, sp.deviceId}

{PTS, STS, FTS, BTS} = Behavior Analysis (Fs, T)

Perform intrusion detection (PTS, STS, FTS,BTS}

Update Trace T.

Wait for another packet sp.

End

Stop

The network monitoring scheme monitor the incoming packets and applies behavior analysis and perform intrusion detection to improve the system performance.

Behavior Analysis:

The behavior analysis algorithm reads the feature vector given and the traces belongs to the IoT device given. Using them, the value of payload trust score (PTS) is measured with average payload for the service and current payload. Similarly, Signature Trust Score (STS) is measured as per the schema of the service and the schema given. Further, the method computes Frequency Trust score (FTS) based on the average access made by another IoT device and the current one. Finally, the Behavior Trust Score (BTS) is measured as per number of correct service access produced by the IoT device and number of malformed service access performed by the device. Such measured values are given to the intrusion detection function to perform intrusion detection.

Algorithm:

Given: Feature set Fs, Trace T

Obtain: {PTS, STS, FTS, BTS}

Start

Read Fs and T.

$$\text{Identify service trace ST} = \sum_{i=1}^{size(T)} T(i).\,ServiceId == Fs(ServiceId)$$

$$\text{Compute PTS} = \frac{Fs(payload).size}{\frac{size(ST)}{\frac{size(\sum_{i=1} ST(i).payload)}{Size(ST)}}}$$

$$\text{Compute STS} = \frac{\sum_{i=1}^{size(FS)} Count(Fs(payload).signature == Serviceid.signature)}{size(Fs(Payload).SignnatureCount)}$$

$$\text{Compute FTS} = \frac{\sum_{i=1}^{size(ST)} Count(ST(i).DeviceId != Fs.DeviceId) \Big/ DutyCycle}{\sum_{i=1}^{size(ST)} Count(ST(i).DeviceId == Fs.DeviceId) \Big/ DutyCycle}$$

$$\text{Compute BTS} = \frac{\sum_{i=1}^{size(STS)} Count(STS(i).DeviceId == FS.DeviceID \;\&\&\; STS(i).state == malicious)}{\sum_{i=1}^{size(STS)} Count(STS(i).DeviceId == FS.DeviceID)}$$

Stop

The behavior analysis scheme measures various trust score for the device

given and estimated values are used to perform intrusion detection.

Intrusion Detection:

The intrusion detection scheme reads the set of trust scores measured. Using them the method computes Legitimate Transmission Score (LTS), which represent the genuine of the device in transmitting exact data to the cloud server or Edge server. Based on the value of LTS, the method decide the legitimacy of the device and perform intrusion detection.

Algorithm:

Given: {PTS, STS, FTS, BTS, T}

Obtain: T

Start

Read PTS, STS, FTS, BTS, T.

Compute LTS = $\frac{\text{PTS}}{\text{STS}} \times \frac{\text{FTS}}{\text{BTS}}$

If LTS> Th then

Genuine

Generate a trace on the T.

Else

Malicious

Generate a trace on T.

End

Stop

The intrusion detection scheme computes the LTS value and based on the threshold, the method perform intrusion detection.

4. Results and Discussion:

The proposed MFTBIDM model has been implemented using advanced java. The performance of the model is evaluated using kaggle data set which contains number of features and tuples. Obtained results are compared with the performance of other approaches.

Parameter	Value
Tool used	Advanced Java
Data set	Kaggle
Number of features	15

Number of records	50000

Table 1: Evaluation Details

The details of evaluation have been presented in Table 1, and obtained results are compared in this section.

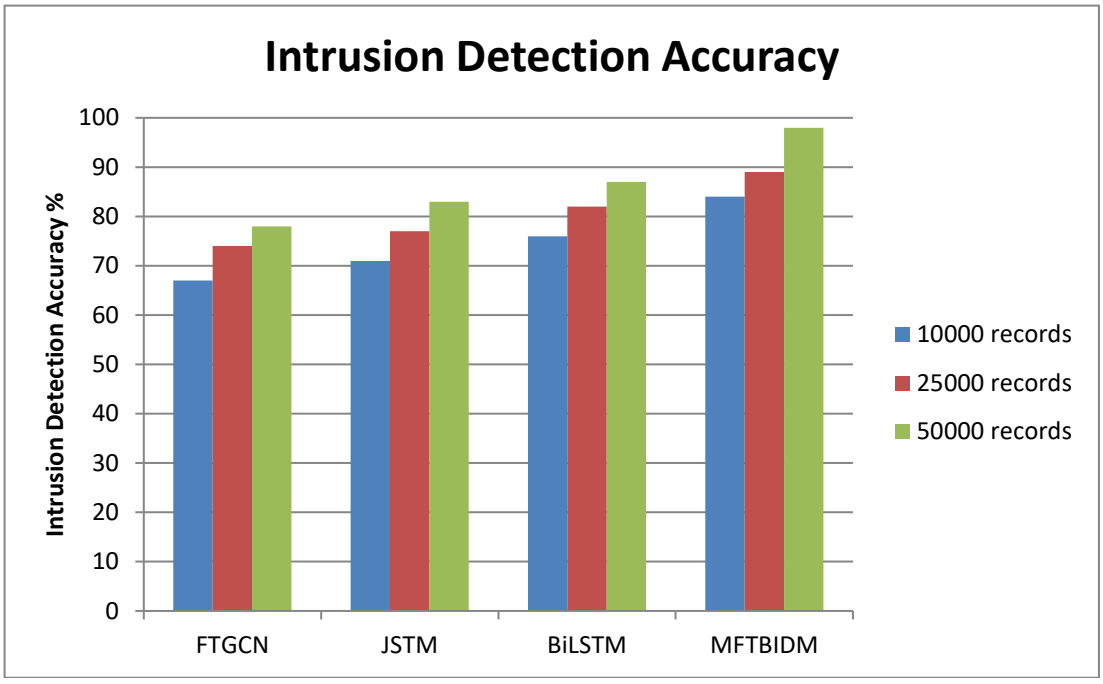

Figure 2: Analysis on Intrusion Detection Accuracy

The accuracy of methods in detecting intrusion attacks are measured and presented in Figure 2. The proposed MFTBIDM is produced higher accuracy than others.

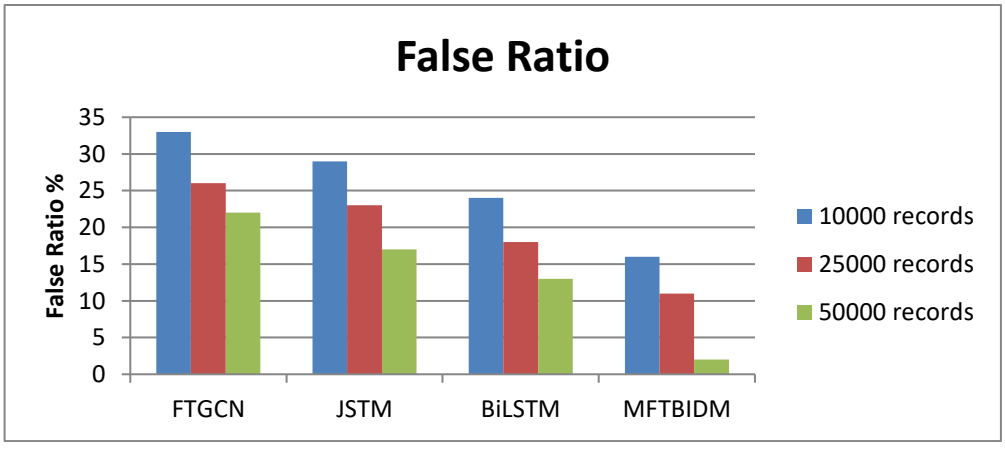

Figure 3: False ratio in intrusion detection

The false rate in detecting intrusion attack is gauged and displayed in Figure 3. The MFTBIDM introduces less false classification ratio than others.

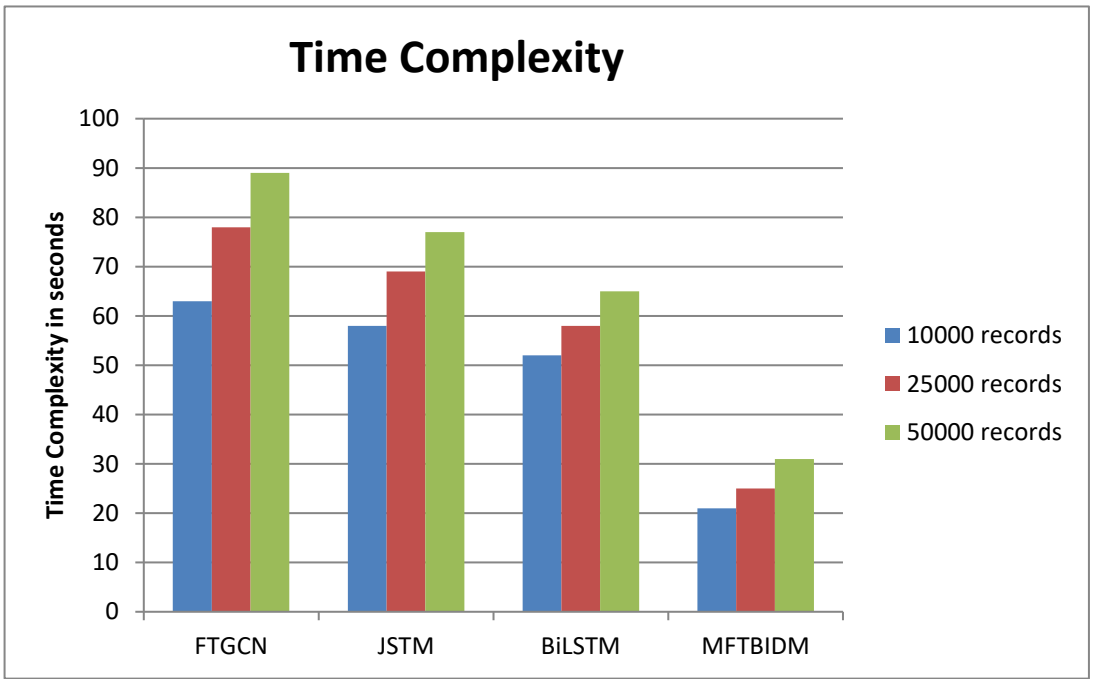

Figure 4: Time complexity

The value of time taken for classification is evaluated for all the methods and given in Figure 4, where MFTBIDM introduces less time complexity than others.

5. Conclusion:

This article detailed a novel Multi Feature Transmission Behavior based intrusion detection model (MFTBIDM). The model estimates Payload Trust Score (PTS), Frequency Trust Score (FTS), Signature Trust Score (STS), and Behavior Trust Score (BTS). Using all these trust scores, the method computes the value of Legitimate Transmission Score (LTS) to perform intrusion detection. The proposed method introduces higher intrusion detection accuracy with less time complexity.

References

1. J. Wu, Y. Wang, H. Dai, C. Xu and K. B. Kent, "Adaptive Bi-Recommendation and Self-Improving Network for Heterogeneous Domain Adaptation-Assisted IoT Intrusion Detection," IEEE (ITJ), Volume. 10, Number 15, pp. 13205-13220, 2023.
2. X. Deng, J. Zhu, X. Pei, L. Zhang, Z. Ling and K. Xue, "Flow Topology-Based Graph Convolutional Network for Intrusion Detection in Label-Limited IoT Networks," IEEE (TN&SM), Volume. 20, Number 1, pp. 684-696, 2023.

3. Y. Wu, L. Nie, S. Wang, Z. Ning and S. Li, "Intelligent Intrusion Detection for Internet of Things Security: A Deep Convolutional Generative Adversarial Network-Enabled Approach," IEEE (ITJ), Volume.10, Number 4, pp. 3094-3106, 2023.
4. N. K. S. Nayak and B. Bhattacharyya, "MAC Protocol Based IoT Network Intrusion Detection Using Improved Efficient Shuffle Bidirectional COOT Channel Attention Network," in IEEE Access, Volume. 11, pp. 77385-77402, 2023.
5. X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu and K. I. -K. Wang, "Hierarchical Adversarial Attacks Against Graph-Neural-Network-Based IoT Network Intrusion Detection System," IEEE (ITJ), Volume. 9, Number 12, pp. 9310-9319, 2022.
6. A. Oseni et al., "An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks," IEEE (TITS), Volume. 24, Number 1, pp. 1000-1014, 2023.
7. J. Wu, H. Dai, Y. Wang, K. Ye and C. Xu, "Heterogeneous Domain Adaptation for IoT Intrusion Detection: A Geometric Graph Alignment Approach," IEEE (ITJ), Volume. 10, Number 12, pp. 10764-10777, 2023.
8. G. -P. Fernando, A. -A. H. Brayan, A. M. Florina, C. -B. Liliana, A. -M. Héctor-Gabriel and T. -S. Reinel, "Enhancing Intrusion Detection in IoT Communications Through ML Model Generalization With a New Dataset (IDSAI)," in IEEE Access, Volume. 11, pp. 70542-70559, 2023.
9. O. Alkadi, N. Moustafa, B. Turnbull and K. -K. R. Choo, "A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," IEEE (ITJ), Volume. 8, Number 12, pp. 9463-9472, 15 June15, 2021.
10. L. Nie et al., "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," IEEE (TCSS), Volume. 9, Number 1, pp. 134-145, 2022.
11. J. Wu et al., "Joint Semantic Transfer Network for IoT Intrusion Detection," IEEE (ITJ), Volume. 10, Number 4, pp. 3368-3383, 2023.
12. I. Ullah and Q. H. Mahmoud, "A Framework for Anomaly Detection in IoT Networks Using Conditional Generative Adversarial Networks," in IEEE Access, Volume. 9, pp. 165907-165931, 2021.
13. M. Abdel-Basset, H. Hawash, R. K. Chakrabortty and M. J. Ryan, "Semi-Supervised Spatiotemporal Deep Learning for Intrusions Detection in IoT Networks," IEEE (ITJ), Volume. 8, Number 15, pp. 12251-12265, 2021.
14. J. Long, W. Liang, K. -C. Li, Y. Wei and M. D. Marino, "A Regularized Cross-Layer Ladder Network for Intrusion Detection in Industrial Internet of Things," IEEE (TII), Volume. 19, Number 2, pp. 1747-1755, 2023.
15. M. Lopez-Martin, A. Sanchez-Esguevillas, J. I. Arribas and B. Carro, "Contrastive Learning Over Random Fourier Features for IoT Network Intrusion Detection," IEEE (ITJ), Volume 10, Number 10, pp. 8505-8513, 2023.