Intelligent electronic monitoring supervision system based on multi-label classification

Suwan Park
Cyber Security Research Division
Electronics and Telecommunications Research Institute
Daejeon, Republic of Korea
parksw10@etri.re.kr

Geonwoo Kim
Cyber Security Research Division
Electronics and Telecommunications Research Institute
Daejeon, Republic of Korea
kimgw@etri.re.kr

***Abstract*— As the current electronic monitoring supervision system faces the problem of increasing work fatigue of probation officers and decreasing the efficiency of supervision work due to the rapid increase in the number of probationers, the Ministry of Justice is trying to solve the problem through an artificial intelligence-based electronic supervision service. To solve this problem, we propose an intelligent electronic monitoring supervision system that builds a daily life model using the location information of each probationer and applies it to real-time location information to detect individual deviations (abnormal situations) and provide the cause of deviation. Furthermore, we demonstrate the feasibility and efficiency of the proposed method through simulations that detect deviations from daily routines based on collected location information.**

Keywords*— *Intelligent electronic monitoring system, Anomaly detection, electronic monitoring supervision system, GPS tracking

I. Introduction

The electronic monitoring supervision system[1] is a system that prevents recidivism by attaching a location-tracking electronic device (electronic anklet) to criminals with a high risk of recidivism and providing close guidance and supervision by probation officers. Electronic supervision subjects (probationer) are categorized into 1:1 supervision, intensive supervision, and general supervision according to their risk level, which takes into account criminal methods, criminal history, and living conditions. According to data from the Ministry of Justice, the appropriate number of supervisors per person for each type is 1 for 1:1 supervision, 10 for intensive supervision, and 40 for general supervision. However, in practice, the staff managing general electronic supervision also serves as probation for general criminals, meaning that one staff member actually manages 108 people, more than double the recommended number. In addition, it is expected that the number of management targets per electronic monitoring officer will increase as the ‘Electronic Device Attachment Act’ has been introduced to allow people who have been sentenced to prison for stalking to be managed as electronic monitoring targets[2].

The existing electronic monitoring supervision system has the problem that frequent daily alarms, such as visiting a specific area (school zone) or going out at a certain time, increase the work fatigue of probation officers and reduce the efficiency of supervision work. Thus, the Ministry of Justice is currently exploring various AI-based electronic monitoring supervision services such as real-time risk analysis, automatic classification of alarms, and assessment of the risk of sexual offense recidivism through the intelligence project for electronic monitoring supervision system. However, there is still no AI-based automatic electronic monitoring system based on high efficiency.

Therefore, in order to maximize the efficiency of supervision beyond the limitations of simple alarm processing, this paper proposes an Intelligent Electronic Monitoring Supervision System(IEMSS) that builds an AI model of the individual's daily life by analyzing the past location information of each probationer in-depth and applies it to real-time location information to not only detect individual deviations but also provide the cause and degree of deviation.

II. The proposed System

This paper describes an anomaly detection method[5] for active electronic supervision that monitors the daily movement patterns of individuals by analyzing the past location information of probationers based on AI in-depth and multifacetedly, with the aim of supporting the efficient operation of electronic supervision tasks. In particular, we propose an explainable IEMSS that enables more efficient electronic supervision by providing the cause of anomaly detection and the weight of the cause, beyond the limitations of electronic monitoring tasks that only provide anomaly detection.

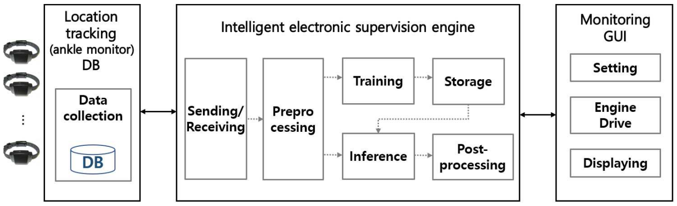

Fig. 1. Intelligent electronic monitoring supervision system diagram

The IEMSS can be composed of a location tracking (electronic anklet) DB, an intelligent electronic supervision engine, and a monitoring GUI. First, data collected from the location tracking electronic devices of probationers are stored and managed through the location tracking DB, and the intelligent electronic supervision engine performs abnormal situation detection or anomaly detection for each probationer based on real-time location data collected from the location tracking electronic devices. The monitoring GUI provides an interface for requesting the setting and operation of the

979-8-3503-1327-7/23/$31.00 ©2023 IEEE

intelligent electronic supervision engine, and is responsible for displaying the result of the request, whether an abnormality is detected for each probationer, and the cause(attribute) of the abnormality and the weight of the cause, to the user.

The intelligent electronic supervision engine consists of the following units:

- Sending/receiving: Responsible for sending and receiving to and from the monitoring GUI and location tracking DB.
- Preprocessing: Preprocesses location tracking raw data so that it can be used in the training or the inference.
- Training: Creates a neural network model of a probationer's daily movement patterns using training data over a period of time.
- Storage: Manage the network models generated by training using information such as probationer ID, date, training period, etc.
- Inference: Perform anomaly detection for probationers in the system background using the latest network model of each probationer managed by the storage.
- Post-processing: Receives anomaly detection results from the inference, analyses the causes, and calculates the weight of the anomaly causes.

III. THE PROPOSED METHOD

This section describes in more detail the role of each unit that constitutes the intelligent electronic supervision engine.

A. *Features in Preprocessing*

The preprocessing unit of the engine, which receives location tracking raw data containing latitude, longitude, date, and time, etc. from the location tracking DB, processes the data to generate feature values for use in training and inference. In this paper, we only use latitude, longitude, date, and time information, while location tracking raw data can be used to generate more diverse features. Latitude and longitude are represented by four values (x, y, z, velocity) from which position and velocity information can be inferred, date can be represented by seven values to represent the day of the week using one-hot encoding, and time is represented by two values using sine and cosine functions to consider time continuity. In Table I, row 1 shows the location tracking raw data, row 2 shows the features converted by preprocessing, and row 3 shows the sample values of the features with data scaling applied. Lastly, row 4 shows the attributes indicating the cause of the anomaly that will be utilized in post-processing.

TABLE I. Features in preprocessing

Location tracking DB	latitude, longitude		date	time
Features	*x, y, z*	*vel*	*mon, tue, wed, thu, tri, sat, sun*	*sinhour, coshour*
Data expression sample	(0.3909, 0.4035, 0.4166)	0.4569	(1.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0)	(0.5116, 0.5116)
Attributes	location	velocity	day	time

B. *Network in Training/ Inference*

The network of training and inference can apply unsupervised learning. The proposed method uses Autoencoder (AE)[3] for single data input(m=1) and LSTM Autoencoder (LSTMAE)[4] for multiple data inputs, and detects an anomaly when the reconstruction loss between the input X and the output $\hat{\boldsymbol{X}}$ exceeds the set threshold. Depending on the network model, various loss functions such as MSE, BCE, and CEE, etc. can be optionally used, and MSE is used in the proposed method as shown in Equation 1.

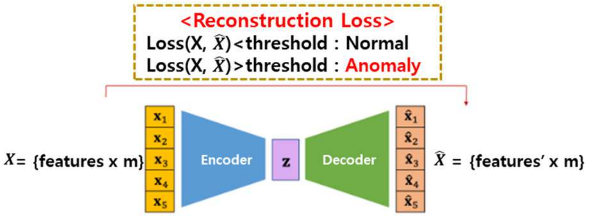

Fig. 2. Anomaly detection network for electronic monitoring engine

$$Loss = \frac{1}{nm}\sum_{i=1,\, j=1}^{n,m}(x_{ij} - x_{ij}')^2, \qquad (1)$$

$$n = \textit{Number of features},\ \ m = \textit{Number of input data}$$

C. *Attributes in Post-processing*

In general, anomaly detection is a problem of classifying whether a life path or daily movement pattern is normal or abnormal. However, the reconstruction loss (integrated loss of features) values provided by inference cannot provide the cause of anomaly detection, resulting in the ambiguity of results. Therefore, post-processing analyzes the results obtained through inference to determine the cause of the anomaly. As shown in Equation 2, we can reclassify the input features into attributes and use the loss per attribute to determine the cause of the anomaly. In addition, each attribute can be given weight(α) for its influence.

$$Location = \alpha_1 \frac{1}{3}\{(\,x - x')^2 + (\,y - y')^2 + (\,z - z')^2\}$$
$$Velocity\ = \alpha_2\ (\,vel - vel')^2$$
$$Day = \alpha_3 \frac{1}{7}\sum_{i=1}^{n}(day_i - day_i')^2,\ \mathrm{n} = \{mon,\ tue,\ \ldots,\ sun\}$$
$$Time\ = \alpha_4 \frac{1}{2}\{(sinhour - sinhour')^2 + (coshour - coshour')^2\}\ (2)$$

As a result, each attribute can have a range of minimum and maximum values, and attribute-specific thresholds allow for more precise anomaly detection.

IV. EXPERMENTS

In this section, we evaluate our proposed method through experiments. For the simulation, we collected location tracking data from an electronic anklet, which includes electronic location value (latitude, longitude), location tracking method (cell, GPS, home, WiFi, etc.), date, and time, etc. In the preprocessing, features(x, y, z, vel, mon, tue, wed, thu, tri, sat, sun, sinhour, coshour) were generated and min-max scaling was used. The neural network used LSTMAE, and the reconstruction loss function uses MSE. We first trained an individual's life pattern with 7 days of data, and then performed anomaly detection using 2 days of untrained test data. Table II shows the results of four experiments that depend on the number of input data and threshold.

1) Good performance with multiple inputs: LSTMAE is a model for detecting anomalies in sequence or time series data. In our experiments, we tested the number of input data(m) up to 3, because the data interval of data collected from electronic anklets is wide and varies from 40 seconds to 4 minutes. The results showed that the best performance was achieved with F1=0.97 on 3 input data when the threshold of reconstruction loss was set to 0.02.

TABLE II. ANOMALY DETECTION RESULTS

	1)	**2)**	**3)**	**4)**
Num. of input data(m)	1	1	2	3
Threshold(Th)	0.03	0.02	0.02	0.02
Accuracy	0.78	0.60	0.96	**0.97**
Precision	0.69	0.60	0.96	**0.98**
Recall	1.00	1.00	0.96	**0.96**
F1	0.82	0.75	0.96	**0.97**

2) Importance of threshold settings: Since IEMSS runs multiple engines for multiple probationers, setting thresholds for reconstruction loss becomes an important issue. We can consider setting individual thresholds or using a common low threshold to filter major anomalies. The difference in threshold settings can be seen in 1) and 2) in Table II and in Figure 3, and this is still an open issue for us.

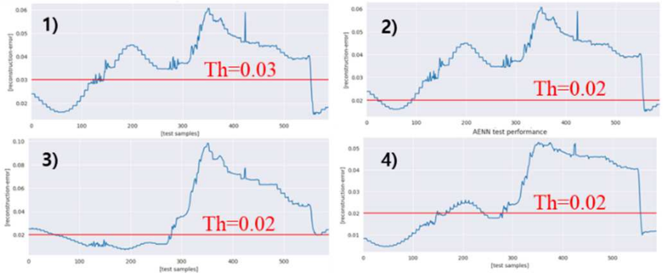

Fig. 3. Differences in results based on thresholds

3) Clarity of anomaly cause: As shown in Figure 3, simply determining whether an anomaly occurred leads to ambiguity in the results. Therefore, we identified the attributes and provided anomaly causes through the weight of each attribute. Figure 4 shows the attributes of the anomalies that occur when the thresholds in Figure 3 are exceeded, and we can infer that large time and location values mean places that have never been visited before.

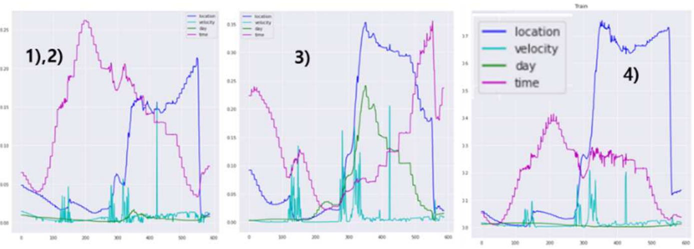

Fig. 4. Attribute-specific weights in anomaly detection

4) Efficiency of electronic supervisory systems: Anomaly detection results can be described through the monitoring GUI of IEMSS as shown in Figure 5. The left side of Figure 5 shows the coordinates of the training data (blue dotted line) and the coordinates of the test data (yellow dotted line), and the detected points (red dots) are plotted over the actual anomaly coordinates (Ground Truth, green dots). The right side of Figure 5 shows the result of plotting the largest attributes in Figure 4 over the test data coordinates. We believe that IEMSS will help probation officers do their jobs more efficiently.

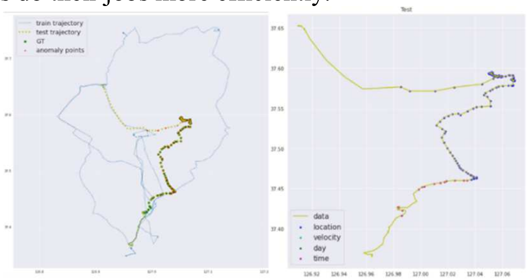

Fig. 5. Map of anomaly detection results by experiment 4)

V. Conclusion

This paper proposes an intelligent electronic surveillance system to solve the inefficiency of simple alarm processing in existing location-based electronic surveillance systems. It is characterized by generating daily movement patterns of each electronic surveillance target with an AI model, detecting anomalies based on real-time location information, and providing the causes(attributes) of the anomalies and the weight of each cause. The simulation results confirm the feasibility and efficiency of the proposed method, but more test data are still needed for performance verification. In addition, in future research, we plan to study the utilization of various attribute information such as direction and the setting of global and attribute-specific thresholds.

Acknowledgment

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2019-0-00203, Development of 5G-based Predictive Visual Security Technology for Preemptive Threat Response).

References

[1] "Electronic Monitoring". Electronic Frontier Foundation. Retrieved 2020.05.

[2] "Use of Electronic Offender-Tracking Devices Expands Sharply". pew.org. Retrieved 2020.05

[3] Z. Chen, C. K. Yeo, B. S. Lee and C. T. Lau, "Autoencoder-based network anomaly detection," 2018 Wireless Telecommunications Symposium (WTS), pp. 1-5, 2018.

[4] A. Zhang, X. Zhao and L. Wang, "CNN and LSTM based Encoder-Decoder for Anomaly Detection in Multivariate Time Series," 2021 IEEE 5th Information Technology, Networking,Electronic and Automation Control Conference (ITNEC), pp. 571-575, 2021.

[5] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, ″Deep Learning for Anomaly Detection: A Review,″ ACM Comput. Surv. 54, 2, Article 38, Mar. 2022.