In: 2023 The 23rd International Conference on Control, Automation and Systems (ICCAS 2023),
17-20 October 2023 Yeosu, Korea, pp. 1610-1615
DOI: 10.23919/ICCAS59377.2023.10316828

Perimeter Intrusion Prediction Method Using Trajectory Frequency and Naive Bayes Classifier

Joongsup Yun[1]*, Hyo-Sang Shin[1] and Antonios Tsourdos[1]

[1]School of Aerospace, Transport and Manufacturing, Cranfield University,
MK43 0AL, Cranfield, U.K.

(joongsup.yun@gmail.com * Corresponding author)

Abstract: This paper proposes a novel perimeter intrusion prediction algorithm that can be applied to generic perimeter security systems. The proposed algorithm uses multiple probability mass functions that are computed using trajectory frequency information for different behaviour models: non-intrusive intention and intrusive intention. A Naive Bayes classifier i s u sed t o c ompute t he i ntention p robability f or i ntegrating m ultiple p robabilities f rom d ifferent probability mass functions. The performance of the proposed algorithm is validated by numerical simulations and the classification characteristics are also discussed.

Keywords: perimeter intrusion detection systems, target classification, trajectory frequency, naive Bayes.

1. INTRODUCTION

In areas where access is controlled for safety or security purposes, a surveillance system is used to keep the area and its surroundings under constant surveillance. The purpose of a target surveillance system is to proactively identify and alert to targets attempting to infiltrate a controlled area. If the surveillance system needs to monitor a large number of targets simultaneously, it is essential to introduce automated intrusion identification techniques to reduce the workload of human operators. This paper proposes a novel intrusion prediction method that can be used in perimeter intrusion monitoring and alerting systems.

Research topics related to perimeter intrusion detection include intent inference, anomaly detection, and threat assessment. The concepts of each topic and the problem settings vary across studies. Reference [1] proposes techniques for estimating non-cooperative drones' specific missions, such as image acquisition, smuggling, and kamikaze attack. Meanwhile, [2] defines intent as whether a drone target intends to stay in or leave a particular airspace. In [3], the authors suggested ground target knowledge-based anomaly detection using airborne radar data. Various types of anomalies were modelled using relative geometry information between the target and the road, or between the target and the asset. In [4], a fuzzy inference system using radar data was proposed to estimate the degree of threat of the target. Threat scores are calculated based on relative distance to the defending asset, speed, altitude, and target type.

In this paper, we consider all targets that could be detected by a surveillance system. These targets include cars, humans, birds, drones, and manned aircraft. The measurements considered are kinematic information, such as position, velocity, and acceleration. Radar is the primary instrument that can provide these measurements with precision.

This research is being conducted as part of the Knowledge Transfer Partnerships (KTP) project between Cranfield University and Operational Solutions Ltd (OSL). OSL's advanced Perimeter Intrusion Detection Systems (PIDs) is designed to provide security teams across any site with the situational intelligence needed to rapidly respond to potential perimeter intrusions. The objective of the KTP project is to investigate various threat assessment, target identification, and classification techniques to improve the performance of PIDs.

2. PROBLEM STATEMENT

2.1 Perimeter Surveillance

The schematic plan of the surveillance system considered in this study is shown in Figure 1. A polygonal perimeter is defined around the protected asset, and traffic inside the perimeter is controlled. The surveillance system constantly monitors the area under surveillance, which consists of accessible and controlled access areas. The perimeter we consider in this study is one that does not require significant physical force to penetrate, which we refer to as a virtual perimeter. Examples of virtual perimeter for ground targets include traffic cones, retractable belt barriers, and lanes. On the other hand, for airborne targets, a fence with some height can be included in the virtual perimeter.

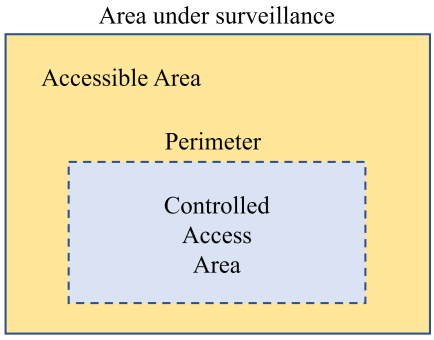

Fig. 1. Schematic plan of area under surveillance

© 2023 IEEE. This is the Author Accepted Manuscript issued with: Creative Commons Attribution License (CC:BY 4.0).
The final published version (version of record) is available online at DOI:10.23919/ICCAS59377.2023.10316828. Please refer to any applicable publisher terms of use.

2.2 Intrusion Prediction and Alarm

Figure 2 illustrates the input/output relationship for an intrusion prediction method within a perimeter surveillance system. The sensor system provides the prediction method with the kinematic information of all targets inside and outside the perimeter, which includes targets' position, velocity, and acceleration. Based on the kinematic information of a given target, the intrusion prediction method determines whether the target has intruded the perimeter or not, and calculates the perimeter intrusion probability (PIB) for targets that have not yet penetrated the perimeter.

Perimeter intrusion can be determined simply based on whether the target's position is inside the perimeter. However, the calculation of the PIB requires a more complex technique that leverages additional information such as the target's velocity and acceleration. The calculated PIB is compared to a threshold, and if the PIB exceeds the threshold, an intrusion alarm is sent to the command and control module. The threshold changes the true positive rate (TPR) and false positive rate (FPR) of the intrusion prediction results, which are discussed in more detail in Section 4.2. The command and control module determines and performs appropriate actions against the target that triggered the alarm.

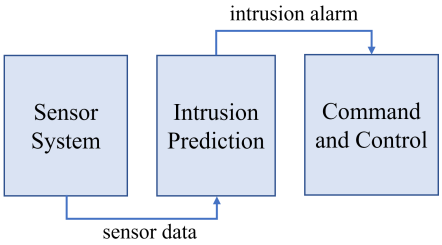

Fig. 2. Intrusion prediction and alarm process

2.3 Challenges of Intrusion Prediction

The introduction of automated intrusion prediction method is essential when the number of targets to be monitored simultaneously is large. Since the information used in intrusion prediction method is supplied by the sensor system, the sensor system is required to have robust detection and tracking performance for multiple targets. Ensuring adequate performance against multiple targets is a major challenge for all types of sensors. Sensors are primarily required to provide accurate kinematic information of multiple targets, but in some cases, they may also need to provide class information for multiple targets such as vehicles, humans, birds, and drones.

Intrusion prediction methods should estimate the probability of an intrusion as promptly as possible based on the target information provided by the sensors. The promptness is a measure of how early the method correctly predicts the intrusion of a target relative to the time of the actual target intrusion. For this reason, the intrusion prediction method needs to be computationally lightweight and predict events as far into the future as possible. The prediction window, or how far into the future an event is predicted, is an important design parameter that affects the performance of intrusion prediction methods. A large prediction window provides more time to react to targets that are expected to breach the perimeter, but can also increase the FPR. Conversely, small prediction window can reduce the FPR, but at the cost of less time to respond to intrusive targets.

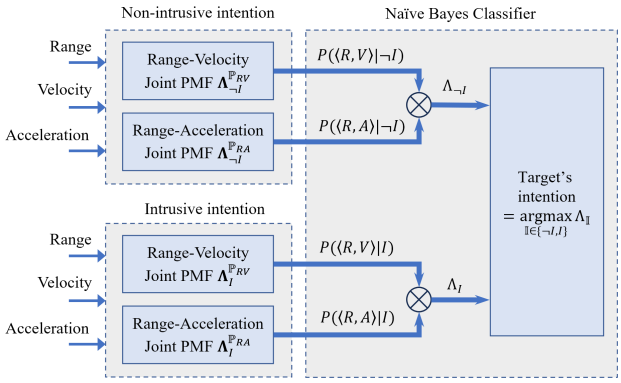

Fig. 3. Process chain of perimeter intrusion prediction using class-conditional probability mass functions and naive Bayes classifier.

To predict the intrusion of a target within the prediction window, it is necessary to estimate the expected behaviour of the target. For this purpose, target behaviour models that can be observed with available sensor information should be established. Reference [2] proposed a method for calculating the probability of drone intrusion into a certain area using the latent destination-following behaviour model. The method is divided into two parts: the first part is to calculate the probability distribution of the drone's latent destination in an area of interest. The probability distribution of the latent destination is then integrated over the area of interest to calculate the probability of entering the area.

In this paper, we define non-intrusive intention and intrusive intention models as behaviour models of targets. The behavioural characteristics of each intention and the intrusion probability estimation method using the behaviour model are described in following sections.

3. INTRUSION PREDICTION

The process chain of the perimeter intrusion prediction method proposed in this paper is shown in Figure 3. The core of the method is to calculate the trajectory likelihood for each of the non-intrusive and intrusive intentions using empirically calculated probability mass functions (PMFs). Trajectory likelihoods are computed using two joint PMFs for each intention, which are used as the basis for identifying the target's intent. To establish the phase planes that best represent the behavioural characteristics of the target, we first consider the characteristics of each behaviour model.

3.1 Behaviour Models

3.1.1 Non-intrusive Intention

Both the waypoints and the final destination of a target with non-intrusive intention are only within the accessible area. If the target approaches a certain level of distance from the perimeter during its movement, a deceleration or turning manoeuvre is triggered to avoid colliding the perimeter.

3.1.2 Intrusive Intention

The final destination of the target with the intrusive intention exists within the perimeter, and waypoints can exist anywhere inside or outside the perimeter. The target will not manoeuvre to avoid colliding with the perimeter.

3.2 Computation of Probability Mass Function

We adopt the trajectory frequency-based target intention estimator proposed in Reference [1] to calculate the perimeter intrusion probability. In the technique proposed by Reference [1], the first thing to do is to set state variables that can properly represent the behavioural characteristics of the target. As discussed in the previous section, the behavioural rules of non-intrusive intention are defined based on the distance information between the target and the perimeter. Based on this, we select the relative range, relative velocity, and relative acceleration of the target as state variables for the construction of the phase planes. Figure 4 shows the geometric definition of these state variables. The velocity and acceleration obtained by differentiating relative range once and twice with respect to time provides more specific behavioural characteristics for each behaviour model. Such characteristics include the expected collision time between the target and the perimeter, and whether the target decelerates and turns.

The first phase plane defined using the selected state variables is the range-velocity phase plane. The trajectory frequency calculated from this phase plane provides a statistical characteristics of the velocity exhibited by the target as it approaches the perimeter. A target with non-intrusive intention will decelerate or turn as its range decreases to avoid colliding with the perimeter, so its velocity towards the perimeter will tend to decrease. On the other hand, a target with intrusive intention may maintain or increase its speed towards the perimeter regardless of the decrease in range.

The second phase plane is the range-acceleration phase plane. Compared with the velocity information, the acceleration information shows more directly the tendency of non-intrusive intention's collision avoidance behaviour, which will help to identify the target's true behaviour model more quickly. The acceleration characteristics of the deceleration and turning generated by the non-intrusive intention are recorded in the corresponding phase plane. For the intrusive intention, the acceleration characteristics for heading towards the destination within the perimeter will be recorded in the range-acceleration phase plane.

The trajectory frequencies for the above two phase

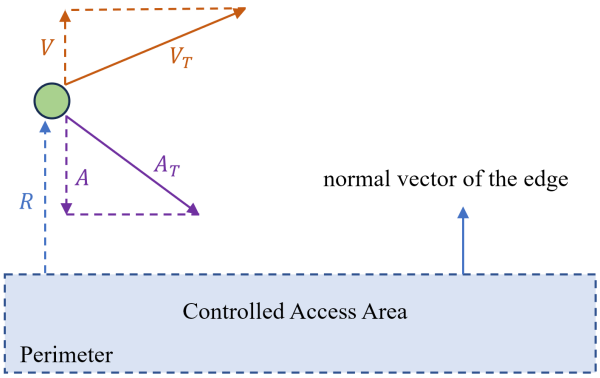

Fig. 4. Definitions of a target's relative range R, velocity V, and acceleration A on the horizontal plane. V_T and A_T denote target's true velocity and acceleration vector, respectively.

planes are calculated offline for each of the intrusive and non-intrusive intentions. Ideally, the trajectory frequencies should be calculated using measurements from actual sensor systems, but this is costly and time consuming. Therefore, this paper uses Monte Carlo simulation to generate four types of trajectory frequency datasets, each of which is defined as a joint PMF. The process of calculating trajectory frequencies through Monte Carlo simulation and converting them into joint PMFs is described in detail in Reference [1].

3.3 Naive Bayes Classifier

The joint PMFs computed offline are used to compute trajectory likelihoods online.

- $\mathbf{\Lambda}_{\neg I}^{\mathbb{P}_{RV}}(\langle R, V\rangle)$ is the joint PMF, or trajectory likelihood, of a measurement coordinate $\langle R, V\rangle$, of the non-intrusive intention ($\neg I$). The function value is an estimate of the class-conditional probability $P(\langle R, V\rangle | \neg I)$.
- Likewise, $\mathbf{\Lambda}_{\neg I}^{\mathbb{P}_{RA}}(\langle R, A\rangle)$ is an estimate of the $P(\langle R, A\rangle | \neg I)$.
- $\mathbf{\Lambda}_{I}^{\mathbb{P}_{RV}}(\langle R, V\rangle)$ is the trajectory likelihood of a measurement coordinate $\langle R, V\rangle$, of the intrusive intention (I). The function value is an estimate of the $P(\langle R, V\rangle | I)$.
- Likewise, $\mathbf{\Lambda}_{I}^{\mathbb{P}_{RA}}(\langle R, A\rangle)$ is an estimate of the $P(\langle R, A\rangle | I)$.

Assuming that the computed trajectory likelihoods are mutually independent, the probability of each intention for a given measurement coordinate can be assumed to be proportional to the multiplication of different trajectory likelihoods [5]. That is,

$$P(C_{\neg I} | \langle R, V, A\rangle) \propto \mathbf{\Lambda}_{\neg I}^{\mathbb{P}_{RV}} \mathbf{\Lambda}_{\neg I}^{\mathbb{P}_{RA}}, \quad (1)$$

$$P(C_I | \langle R, V, A\rangle) \propto \mathbf{\Lambda}_{I}^{\mathbb{P}_{RV}} \mathbf{\Lambda}_{I}^{\mathbb{P}_{RA}}. \quad (2)$$

The right-hand sides of the equations are defined as intention likelihoods

$$\Lambda_{\neg I} = \mathbf{\Lambda}_{\neg I}^{\mathbb{P}_{RV}} \mathbf{\Lambda}_{\neg I}^{\mathbb{P}_{RA}} \quad (3)$$

$$\Lambda_{I} = \mathbf{\Lambda}_{I}^{\mathbb{P}_{RV}} \mathbf{\Lambda}_{I}^{\mathbb{P}_{RA}}, \quad (4)$$

where Λ denotes intention likelihood and the subscripts $\neg I$ and I denote non-intrusive intention and intrusive intention, respectively. By comparing the intention likelihood calculated in (3) and (4), we can estimate the intention of the target. That is,

$$\text{Target's Intention} = \underset{\mathbb{I}\in\{\neg I, I\}}{\operatorname{argmax}} \Lambda_{\mathbb{I}}. \tag{5}$$

The technique of obtaining class likelihood and comparing them to estimate the true class under the assumption of mutual independence, as shown in (3), (4), and (5), is called Naive Bayes classifier.

4. PERFORMANCE ANALYSIS

4.1 Prediction Window

Let t_b be the time when the target with the intrusive intention actually intruded the perimeter. To quantitatively evaluate how quickly a particular intrusion prediction method predicts an intrusion, we introduce a minimum prediction time $\Delta t_{\min}$ and a maximum prediction time $\Delta t_{\max}$. The minimum prediction time is the minimum requirement of prediction time that must be satisfied, and the performance index is calculated only for the time before $t_b - \Delta t_{\min}$. On the other hand, the maximum prediction time sets an upper bound on how fast the intrusion prediction method can predict intrusion, and the performance index is only calculated after $t_b - \Delta t_{\max}$. Then, the prediction window is defined by

$$t - \Delta t_{\max} \leq t \leq t - \Delta t_{\min}. \tag{6}$$

4.2 Performance Metrics

The intrusion prediction problem can be considered as a behaviour model or target intention classification problem as defined in the previous section. Therefore, we use the confusion matrix commonly used in classification problems to define performance metrics for the intrusion prediction problem. Positive in the confusion matrix means that the target has the intrusive intention and has actually breached the perimeter at some point during the surveillance. On the other hand, negative means that the target has a non-intrusive intention and has never intruded the perimeter during the surveillance. Using this definitions, we define the elements of the confusion matrix as follows.

- **True positive (TP)** is the amount of time a target with intrusive intention was classified to have intrusive intention.
- **False negative (FN)** is the amount of time a target with intrusive intention was classified to have non-intrusive intention.
- **False positive (FP)** is the amount of time a target with non-intrusive intention was classified to have intrusive intention.
- **True negative (TN)** is the amount of time a target with non-intrusive intention was classified to have non-intrusive intention.

The TP and FN are calculated for the prediction window (6), and the FP and TN are calculated for the whole duration of the surveillance. True positive rate (TPR) and false positive rate are the two important performance metrics for classification problem and defined as

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \tag{7}$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}}. \tag{8}$$

5. NUMERICAL SIMULATIONS

The probability distributions of joint PMFs obtained by performing 1000 Monte Carlo simulations for each intention are shown in Figure 5. Each trajectory comprising the Monte Carlo simulation results is a random trajectory based on the behaviour model defined in Section 3.1, with no measurement noise applied.

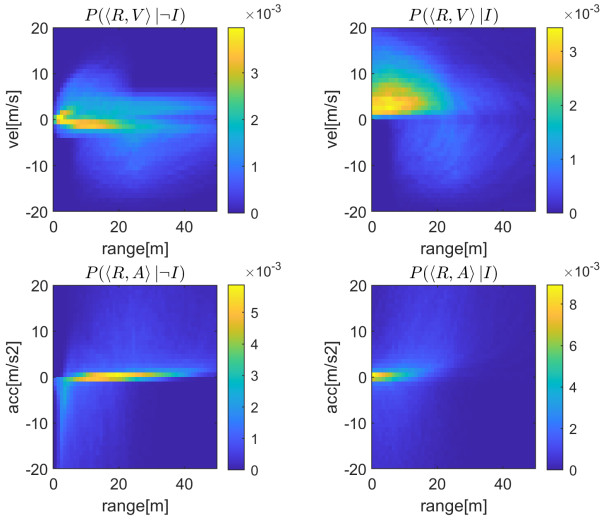

Fig. 5. Joint PMFs calculated by 1000 Monte Carlo simulations.

Figure 6 illustrates a trajectory of the target with non-intrusion intention. The target was initially heading southwest that could cause a collision with the perimeter. The target turned to the right relative to the target's heading just before the collision with the perimeter and locked onto the waypoint while still maintaining its distance from the perimeter. Figure 7 shows the computed trajectory likelihoods and intention likelihoods of non-intrusive and intrusive intention. Initially, the $P(\langle R,V\rangle|I)$ is higher than $P(\langle R,V\rangle|\neg I)$ because the target is moving towards the perimeter at a close distance from it. On the other hand, the initial $P(\langle R,A\rangle|\neg I)$ and $P(\langle R,A\rangle|I)$ are similar, indicating that the target is in a region where the intentions cannot be distinguished by acceleration characteristics. After 2 seconds, the probability of non-intrusive intention likelihood $\Lambda_{\neg I}$ increases sharply, which is due to a clear increase in both $P(\langle R,V\rangle|\neg I)$ and $P(\langle R,A\rangle|\neg I)$.

Figure 8 illustrates a trajectory of the target with intrusion intention. The target was initially heading parallel

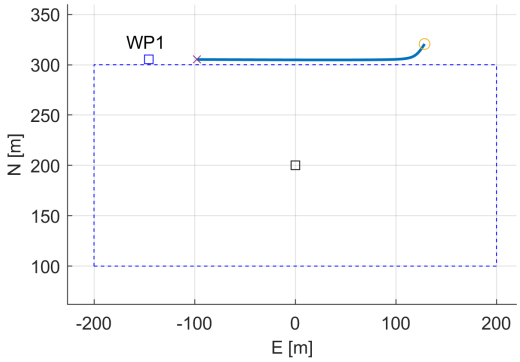

Fig. 6. Trajectory of a target with non-intrusion intention. The circle and cross marker denote initial and final position of the target, respectively.

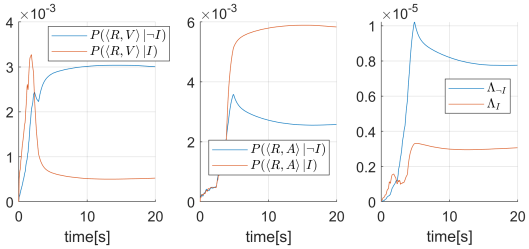

Fig. 7. Trajectory likelihood and intention likelihood of a target with non-intrusion intention.

to the perimeter but began to turn to left and eventually collided with the perimeter. Figure 9 shows the computed trajectory likelihoods and intention likelihoods of non-intrusive and intrusive intention. The $P(\langle R, V\rangle|\neg I)$ shows high probabilities until 4.2 seconds, as the target's heading for the initial phase was not towards the perimeter. On the contrary, the $P(\langle R, V\rangle|\neg I)$ shows distinctly higher magnitudes throughout the entire tracking. This is because the target consistently maintained a manoeuvre of turning towards the perimeter. The probability of intrusive intention likelihood Λ_I shows a dominance over $\Lambda_{\neg I}$ from 3.2 seconds onwards, which is one second earlier than the moment when the $P(\langle R, V\rangle|I)$ becomes greater than $P(\langle R, V\rangle|\neg I)$. This illustrates how the acceleration-based information contributes to the perimeter intrusion prediction.

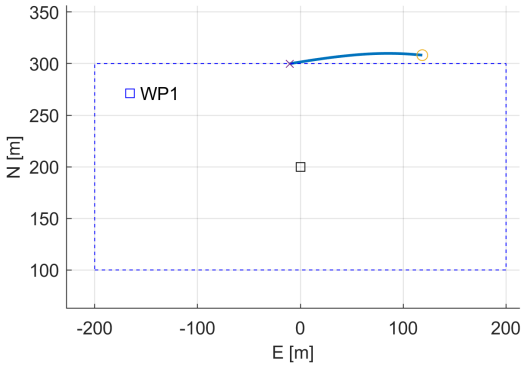

Fig. 8. Trajectory of a target with intrusion intention.

To measure the quantitative performance of the proposed algorithm, a Monte Carlo simulation-based performance metrics calculation technique was used. A total

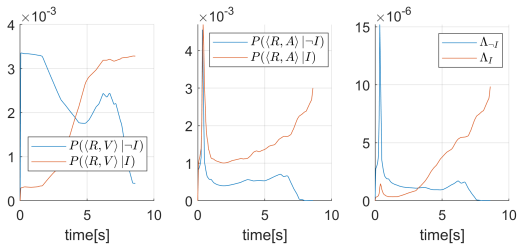

Fig. 9. Trajectory likelihood and intention likelihood of a target with intrusion intention.

of 200 random trajectories were used in the performance tests, half of which were from targets with non-intrusive intention and the remaining half from targets with intrusive intention. The TPR and FPR for each trajectory were first calculated using (7) and (8), and then the final TPR and FPR were calculated by averaging the TPRs and FPRs of each trajectory. Figure 10 shows three receiver operating curves (ROC); each ROC is plotted by varying the threshold for a given prediction window. Table 1 shows the minimum and maximum prediction time of each prediction window applied.

Figure 10 shows a typical form of ROC where TPR and FPR increase simultaneously as the threshold changes. As the prediction window gets larger, the TPR decreases, but the FPR never exceeds 0.1 at most. Table 2 shows the area under curves (AUC) for each prediction window. The closer the AUC is to 1, the better the performance of the classifier. Compared to Prediction Window-1, Prediction Window-3 has four times longer prediction duration and three times earlier start time for AUC calculation. Nevertheless, Prediction Window-3 shows a performance decrease of only 14% in terms of AUC compared to Prediction Window-1.

Table 1. Minimum and maximum prediction time of each prediction window.

	Prediction window-1	Prediction window-2	Prediction window-3
$\Delta t_{min}[s]$	1	1	1
$\Delta t_{max}[s]$	3	6	9

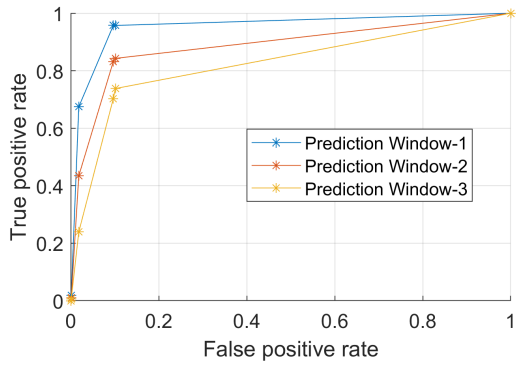

Fig. 10. Receiver operating characteristic of the perimeter intrusion prediction method.

Table 2. Area under the curves

	Prediction window-1	Prediction window-2	Prediction window-3
AUC	0.95	0.89	0.82

6. CONCLUSIONS

This paper proposes a novel perimeter intrusion prediction algorithm that can be applied to generic perimeter intrusion detection systems. The proposed algorithm uses multiple probability mass functions that are computed offline in advance, and the PMFs are based on behavioural models of non-intrusive and intrusive intentions. A Naive Bayes technique is used to compute the intention probability using multiple probabilities from different PMFs. The performance of the algorithm is validated by Monte Carlo simulations. The results show that the proposed method provides robust perimeter intrusion prediction performance even when the prediction window is increased to a certain extent. As future work, we plan to investigate a prediction technique that can consider more complex behavioural characteristics rather than simple intrusion or non-intrusion behaviour.

ACKNOWLEDGEMENT

This work has been co-funded by Innovate UK and Operational Solutions Ltd. [grant number KTP12998].

REFERENCES

[1] J. Yun, D. Anderson and F. Fioranelli, "Estimation of drone intention using trajectory frequency defined in radar's measurement phase planes," in *IET Radar Sonar Navig. 1–16 (2023).* https://doi.org/10.1049/rsn2.12422

[2] J. Liang, B. Ahmad, M. Jahangir and S. Godsill, "Detection of malicious intent in non-cooperative drone surveillance," in *Proc. 2021 Sensor Signal Processing for Defence Conference (SSPD)*, Edinburgh, United Kingdom, 2021. https://doi.org/10.1109/SSPD51364.2021.9541485

[3] F. Katsilieris and A. Charlish, "Knowledge based anomaly detection for ground moving targets," in *Proc. 2018 IEEE Radar Conference (RadarConf18)*, Oklahoma City, OK, USA, Apr. 2018, pp. 786–791.

[4] E. Azimirad and J. Haddadnia, "Target threat assessment using fuzzy sets theory," in *International Journal of Advances in Intelligent Informatics*, vol. 1 no. 2, pp. 57–74, Jul. 2015.

[5] I. Rish, "An empirical study of the naive bayes classifier," in *IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence*, pp. 41–46, Seattle, WA (2001)

Cranfield University

CERES Research Repository **https://dspace.lib.cranfield.ac.uk/**

School of Aerospace, Transport and Manufacturing (SATM) Staff publications (SATM)

Perimeter intrusion prediction method using trajectory frequency and Naive Bayes classifier

Yun, Joongsup

2023-11-20

Attribution 4.0 International

Yun J, Shin HS, Tsourdos A., (2023) Perimeter intrusion prediction method using trajectory frequency and Naive Bayes classifier. In 2023 23rd International Conference on Control, Automation and Systems (ICCAS), 17-20 October 2023, Yeosu, Korea, pp. 1610-1615
https://doi.org/10.23919/ICCAS59377.2023.10316828

Downloaded from CERES Research Repository, Cranfield University