Abnormal Events Detection for Infrastructure Security using Key Metrics

Van-Khoa Le, Edith Grall-Maes and Pierre Beauseroy
Institut Charles Delaunay (ICD)/LM2S - CNRS, Troyes University of Technology,
12 rue Marie Curie CS 42060 - 10004 Troyes Cedex, France

Keywords: Anomaly Detection, Statistic Method, Security System, Cyber-physical Attacks, Key Metric.

Abstract: This paper presents a detection process which utilizes various sensors (camera, card readers, movement detector) for detecting automatically abnormal events. The detection process strengthens current security systems to identify attackers in the context of building and office. Key metrics are proposed to describe people's behavior in critical zones of the building. They are built using measures from the sensors, which provide information about the person, the position, and the instant. These metrics are used to classify abnormal behaviors from regular ones, based on a statistical classifier. This technique is tested on both simulated data and real data, in which an attacking scenario was prepared by security experts. Results show that abnormal events from the scenario have been successfully detected. The experiments demonstrate that the proposed key metrics are relevant and the proposed detection scheme is appropriate for infrastructure surveillance.

1 INTRODUCTION

In the last decades, there has been an increasing demand for security protection for citizens due to the increase of crime level. Numbers security guards have been increased in public places to protect the citizen from terrorist attack. In the context of building and office, more CCTV or IP cameras have been installed at critical places to support and reduce the workload of security guards. However, the operation of these camera systems still depends on human, which is a weakness of the security system because the operators cannot keep concentration through an extended period, and they have to observe many screens at a time. So there is a risk that they miss the critical activity on the screen. Therefore, the development of an automatic surveillance system is essential to assist operators to detect abnormal events. An automatic monitoring system is a combination of a set of sensors and a detection process. The system of sensors is used to capture the information in the controlled zone. Sensors can be cameras, movement detectors, iris scanners or card readers. The detection process analyzes the captured information from sensors and compares it with normal situations to give the decision.

According to (Chandola et al., 2009), the detection anomaly techniques can be classified into different categories like classification based and statistic based. In detection anomaly classification based techniques, the authors (Wang et al., 2012) proposed an algorithm to detect abnormal events based on video streams. The algorithm uses optical flow descriptor to extract the video data, and a One-Class SVM classification model to detect the abnormal events. It can work in crowded scenes to detect the abnormal behaviors in public spaces. Activity recognition using deep learning in (Vignesh et al., 2017) is also a popular approach to detect abnormal activities. However, in the context of building and office, the types of activities such as standing or walking are not diversified, so it is not easy to distinct attackers base on their gestures.

In (Morris and Trivedi, 2008b), the authors defined a trajectory as a sequence of Point of Interest (POI) and Activity Path (AP). The POI is the entry/exit of the surveillance zone or the zone where the tracked person stays longer than a threshold. APs are interspersed with POIs, and a classification model is built to detect abnormal sequences of AP. In (Bonhomme et al., 2007), a statistic based method is used for a surveillance system for elderly in a hospital. A detection process is based on movement detector's data and some diagnostic criterions to measure the normality of the patient's behaviors. However, these systems do not combine many types of sensors into the surveillance system. They only use one type of sensors like camera (Wang et al., 2012) or movement

Le, V-K., Grall-Maes, E. and Beauseroy, P.
Abnormal Events Detection for Infrastructure Security using Key Metrics.
DOI: 10.5220/0006552102840290
In *Proceedings of the 7th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2018)*, pages 284-290
ISBN: 978-989-758-276-9

detector (Bonhomme et al., 2007). So the amount and the type of the information used for analysis are limited. Despite many efforts on tracking people in a multi-camera environment, the problem of tracking people inside a building by multi-camera is still challenging. So in a building context, techniques which are built on trajectories classification [(Morris and Trivedi, 2008b), (Morris and Trivedi, 2008a), (Brandle et al., 2006)] need a good tracking capability of the sensor system to perform well. Thus it can be challenging to operate well in a real situation.

In this paper, we concentrate on using data of trajectories of people inside a building and build a detection method based on this data. The data of trajectories come from a system of camera and card reader integrated into a building, and the data collecting steps were done by a company within our project. A combination of these sensors could give us a precise description of people's activities. We propose a detection scheme based on key metrics that uses data from various sensors, and that is adapted for building supervision. These metrics describe the behavior of people in the controlled zone into specific periods of an entire day. The detection process is separated into two parts, offline training, and online detection. Thresholds for key metrics at each period is calculated in the training process, and new observations of the camera are analyzed and compared with thresholds in the online detection process. This model has an advantage that it does not require any prior knowledge about ordinary events in the zone to set threshold. Instead, it learns what constitutes regular activity from its observations in a period, and the confidence intervals automatically describe this knowledge.

The primary contribution of our work is that we have integrated a statistical detection process into an automatic security system in the context of building and office. We define key metrics that can be used to differentiate attackers from regular people and can adapt to different contexts. The detection process can be trained offline and detect abnormal events online.

The rest of the paper is organized as follows. In session 2, we present the general idea of the proposed method. Experimental contents about the detail of the technique and the datasets are presented in section 3. In session 4, experiment results are presented by using simulated data and real data, and we conclude our work in section 5.

2 PROPOSED METHOD

2.1 General Description

The proposed detection process aims to apply for vulnerable local areas in the building. We assume that sensors are installed to capture people's movement in this zone and can provide data in the format [ID, t, Pos], which describe the presence of a person with identity ID at instant t in a position Pos inside the building. Then we define key metrics which are characteristics of the zone and can be used to detect an abnormal behavior. The detection process is a method based on the statistics of the key metrics and is parameterized with thresholds used for decision-making. A training stage uses regular events to determine the threshold values. In the operational stage, the observed metrics are compared with the predefined threshold to raise the alarm if some values exceed the thresholds.

2.2 Key Metrics And Time Windows

In this technique, we are interested in examining the behavior of people in relation to their presence in a critical area. Key metrics describe the duration or the instant of presence at a place. Because a typical duration in the morning may become abnormal in the evening, so we propose to define key metrics depending on the considered moment. For this purpose, the key metrics are attached to a time window. The simplest way is to divide the day into multiple equal parts with a chosen width which we call fixed window. However, some key metrics may be dependent on the position of the window; it may be more suitable to use a sliding window, which is defined by its width and shift, so that a day is a set of overlapped windows. These two types of time window are presented with their parameters in Figure 1.

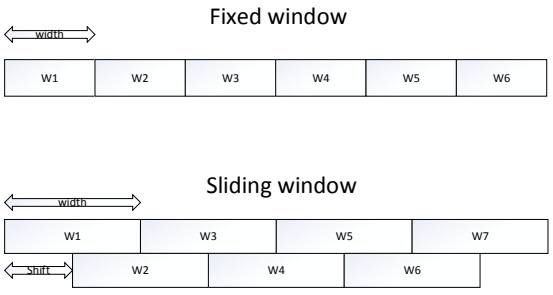

Figure 1: Two types of time window.

For both time windows, there is a trade-off when defining the parameter window's width. If the width is too large, a window may include key metrics with

different statistical properties, and thus the estimated values could be biased. On the contrary, if the width is too short, the number of observed key metrics in the windows may be too small to obtain a reliable estimation of the statistics. Besides, it has to be noted for the sliding window that the computation may be expensive if the shift is too small. The width and the sliding speed are chosen by author's experience.

The primary key metrics that we propose are *duration of stay*, *number of visits* and *occupation rate*, which can be varied in three fields: type of people, time and location. It means we can calculate same primary key metrics for different types of people, time periods or locations according to the input data. For example, the metric *Average duration of each visit of an engineer at the printer zone* is computed by using raw data of engineers at the printer area.

2.3 Training Stage

In the training stage, we use observations of sensors collected during regular days. The aim is to determine the threshold of each predefined key metric in each time window. The following is a summary of this stage:

1. For the predefined key metrics, raw data from the training set is filtered to fit with the appropriate key metrics. This step is called data preprocessing.
2. Next, according to the time window's type, and its parameter (width, shift), the events inside each time window are collected, and the metrics are computed using these events.
3. Finally, thresholds are set for the metrics. The calculations of thresholds are based on the mean and standard deviation of the metric in each time slot.

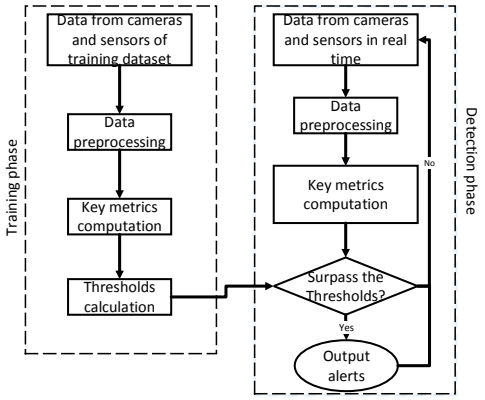

Figure 2: Training and operational stages for detection process.

2.4 Operational Stage

The operational stage is based on the following principle: the events are observed in real time, and when certain activity criteria exceed a reference value (the detection threshold), an alarm is generated. The detection process is as follow:

1. The data from cameras and sensors are collected.
2. A filter allows selecting only events in the predefined zone. It chooses the points of trajectories which are closed to the critical object like printer because the attackers cannot cause much damage if they are distanced from the weak points of the building.
3. The key metrics in each window are computed and compared with the threshold. An event is considered as abnormal if the threshold is exceeded.
4. If the event is normal, we return to the first step and wait for new events, if not, we send an alarm to the system describing the abnormal event and then come back to the first step.

The training and operational stage of the detection process are presented in Figure 2. The alert is sent right at the moment the metric exceeds the threshold.

3 EXPERIMENTAL CONTENT

3.1 Infrastructure

A typical office is presented in Figure 3. Two critical zones in this map are the server room and the area around the printer because there are key elements that can be violated by attackers. We use this building as the applying case for our technique, and simulated data is generated on this cartography. The camera and sensor system is installed in the building so we can observe every movement in the passage, but not inside the office or server room.

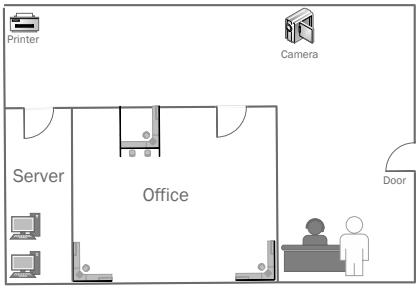

Figure 3: Simulation office.

In the real building, a system of IP cameras and card readers has been installed along passages and

at the main entrance or critical zones such as printer zone or server room to guard the whole building. Employees have to check their card each time they enter or leave the main entrance, or the server room or make a photocopy.

3.2 Key Metrics

In this section, we present the key metrics that were chosen for experiments:

- Number of visits in a time slot in the controlled zone ; the aim is to detect that an abnormal number of persons is visiting the zone. This metric counts the number of visits in a sliding time window, assigning a visit to the time window of the entering moment.
- Occupation rate in a time slot in the controlled zone; the aim is to detect that the percentage of the time window that the place is occupied by at least one person is abnormal. The sliding window is applied for this metric.
- Average duration of a visit of a person in the controlled zone; the aim is to detect the abnormal length of stay. The duration is assigned to the time window which the events begin. This metric utilizes a fixed window. The two previous metrics provide only one value for each time window. On the contrary, for this metric there are many durations in one time window, which correspond to different events. So there are different possibilities to assign a value of duration that can represent the metric. The most common ways are using the average or the maximal duration.

In order to determine the threshold for each metric M_k in time window k, the average μ_{M_k} and the standard deviation σ_{M_k} are estimated using the data in the training set composed of m days, assumed to be without abnormal events, according to:

$$\mu_{M_k} = \frac{\sum_{j=1}^{m} A_{k,j}}{m} \quad (1)$$

$$\sigma_{M_k} = \sqrt{\frac{1}{m}\sum_{j=1}^{m}(A_{k,j} - \mu_{M_k})^2} \quad (2)$$

where $A_{k,j}$ is the value of the metric M_k, in day j. The threshold T_{M_k} is calculated according :

$$T_{M_k} = \mu_{M_k} + \alpha * \sigma_{M_k} \quad (3)$$

where α is a tuning parameter. The bigger the value of α is, the higher the numbers of true positive and false positive are. The value α is chosen as in (Denning, 1987), where the probability of a value falling outside the confidence interval T_{M_k} is at most $1/\alpha^2$. Which is at most 0.0625 for $\alpha = 4$.

3.3 Data description

We use two datasets in this application, a simulated dataset and a real dataset.

3.3.1 Simulated data

The raw simulated data is a vector S with four features: $S = [IDperson, Time, X_{coordinate}, Y_{coordinate}]$. They depict the people's trajectories in the building, as the example given in Table 1. These data allow building events specifying the length of stay in the predefined controlled area. Assuming that the positions of the first three observations in Table 1 are inside the predefined zone *Printer*, and the last observation is out of the area, the event given in Table 2 is created using these data. It defines the ID of the person, the time, the controlled area location, and the duration.

Table 1: Raw data.

ID	Time	X	Y
101	9:20:01	4.5	-5
101	9:20:02	4.6	-4.8
101	9:20:03	4.7	-4.6
101	9:20:04	4.8	-4.3

Table 2: Event description.

ID	Time	Location	Duration (s)
101	9:20:01	Printer	3

To illustrate the estimation of the statistics of the key metrics, a set composed of six events in two days is reported in Table 3.

Table 3: Events in two days.

Day	ID	Time	Location	Duration (s)
1	101	9:05:00	Printer	10
1	103	9:06:01	Printer	35
1	102	9:10:01	Printer	60
2	101	9:20:01	Printer	45
2	102	9:40:01	Printer	20
2	103	10:10:01	Printer	50

Using a window width of 3600 seconds and chosen the metric M as *Average maximal duration of a visit*. This metric is an extension of the metric *Average duration of a visit* which calculates the most atypical duration of an event. $A_{k,j} = \max(D_{i,k,j})$ where $D_{i,k,j}$ is the duration of the i^{th} event in time window k day j. Therefore, $A_{10,1} = 60$ and $A_{10,2} = 45$. M_{10} is the metric in the interval between 9 o'clock and 10 o'clock and M_{11} is the metric in the interval between

10 o'clock and 11 o'clock. Then the estimated values for $\mu_{M_{10}}$ and $\mu_{M_{11}}$ are:

$$\mu_{M_{10}} = \frac{\sum_{j=1}^{2} A_{10,j}}{2} = \frac{60+45}{2} = 52.5 \quad (4)$$

$$\mu_{M_{11}} = \frac{\sum_{j=1}^{2} A_{11,j}}{2} = \frac{0+50}{2} = 25 \quad (5)$$

In the simulated dataset, there were a total of 11 days, including two days with unusual events and nine regular days. Therefore, the typical days were used for training and the abnormal days were used for testing.

3.3.2 Real data

In the real dataset, the tracking process is a combination of face detection and silhouette tracking. The format of the raw data in the real dataset is more complicated than the format for the simulated dataset, but it keeps the same core information. It assigned the UNIX timestamp for each observation in the real dataset. To construct the real dataset, a system of cameras and sensors was installed to capture movements of people in a building for five days. One day contains an abnormal event with the same attacking scenario as the simulated data. Then four days were available for the training phase of the system and one day was used for testing in real-time the detection process.

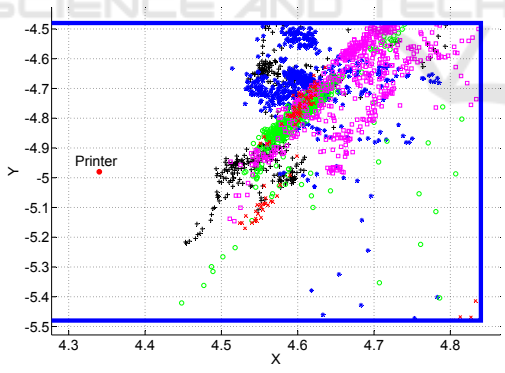

Figure 4: Observations around printer, the blue square is the predefined zone, each color specifies a person's positions.

The visualization of raw data in the real dataset is presented in Figure 4, where the critical zone around the printer is inside the rectangle. Except for the printer point, each point represents position's measurements of people in the zone.

4 EXPERIMENTAL RESULTS

For both datasets, the data of the regular days in the training set were used to determine the thresholds of the chosen key metrics. Then the system was performed using the set containing the day(s) with abnormal data. The critical zone that we used in our experiment is the zone of 0.5 meters around the printer and parameter α was equal to 3. Two metrics chosen for experiments are *Average maximal duration of a visit in a zone* and *Number of visits in a zone* and are symbolized as $A_{location}$ and $N_{location}$ respectively.

4.1 Simulated Data

There are two attack scenarios in the simulated dataset. The first one is an intruder disguised as an employee and who tried to hack into the information system through the printer. The second attack is an intrusion in the server room which happens on a different day.

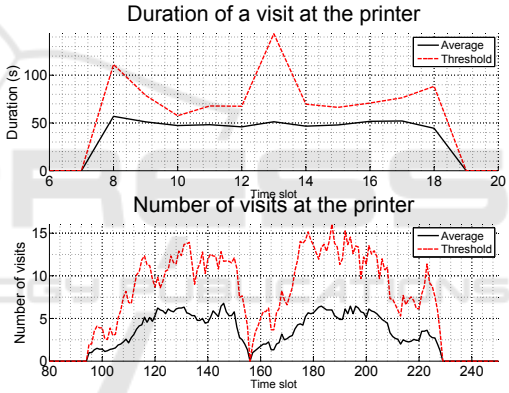

Figure 5: Training results at Printer.

The result of the training stage is a series of thresholds for each key metric, in relation to the time position on the day of the time window. Figure 5 is the curve of means and thresholds of the metrics $A_{printer}$ and $N_{printer}$.

In the metric $A_{printer}$, a fixed window with a width equals to 3600 seconds was applied. So a day is separated into 24-time slots. The time slot i indicates a window from $i-1$ o'clock to i o'clock.

In the metric $N_{printer}$, we used a sliding window with a shift of 300 seconds and a width of 1800 seconds. Therefore, the day contains 288-time slots. For this window, the time slot number i specifies a window in the time interval from $(i*300/3600-1800)$ to $(i*300/3600)$. For example, time slot 160 captures all events between 12:50:00 and 13:20:00. There is no observation before 7 am, and after 19 pm in the dataset, so the figures are scaled for better visualization.

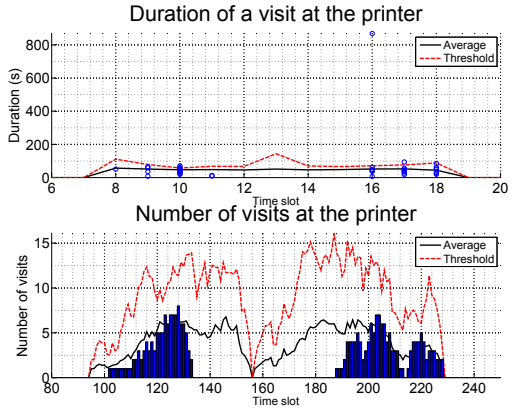

Figure 6: Detection results at printer zone.

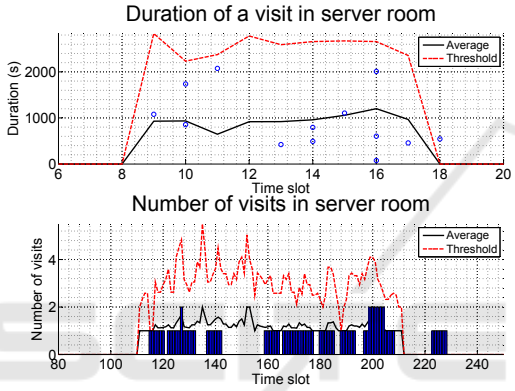

Figure 7: Detection results in server room.

Figure 6 is the detection results of two key metrics mentioned above, and it detects an abnormal duration in the time window 16 (between 15 and 16 o'clock). Figure 7 shows the detection result of the two key metrics A_{server} and N_{server}. Both key metrics detects the abnormal access to the server room between 17 and 18 o'clock.

The different behaviors of people at two different places like the printer zone and server room are explored in Figure 6 and Figure 7. The average duration in the server room is longer than at the printer zone because of the different action's type at each location. The number of visits in the server room is lower and more stable than in the printer area because the printer is placed in an open space like a passage. On the other hand, only administrators have the right to access the server room.

4.2 Real data

The metric $A_{printer}$ was calculated using real data in this experiment. Figure 8 describes the training and detection results of the real dataset. An abnormal event appears in the 15th time slot corresponding to the attack in front of the printer between 14 and 15 o'clock.

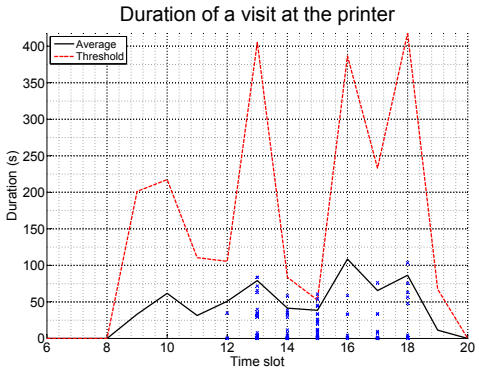

Figure 8: Detection result of real dataset.

5 CONCLUSION

In this article, we have introduced a detection process to detect abnormal events at a zone inside a building. This technique explores different key metrics of critical areas. A training stage allows to determine thresholds, and in the operational stage, the measured metrics are compared with the thresholds to raise possibly an alarm. Cameras and card readers are used to collect daily activities of the people in the building. Key metrics allow describing people's behavior in critical zones of the building. They are built using measures from the sensors, which provide information about the person, the position, and the instant. Sliding time windows or fixed time windows provide key metrics which are time-dependent. We used both simulated dataset and real dataset to train a detection process and detect anomaly given in attacking scenarios. Our experimental evaluation demonstrates that the proposed key metrics are relevant to detect abnormal events in the attacking scenarios for both datasets.

ACKNOWLEDGEMENTS

This work is currently being undertaken as part of the VIRTUALIS project by cooperation between UTT (the University of Technology of Troyes), Thales (https://www.thalesgroup.com/fr) and other companies. Special thanks go to the staff of Thales for their help during the data collection.

REFERENCES

Bonhomme, S., Campo, E., Esteve, D., and Guennec, J. (2007). An extended prosafe platform for elderly monitoring at home. In *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE*, pages 4056–4059. IEEE.

Brandle, N., Bauer, D., and Seer, S. (2006). Track-based finding of stopping pedestrians-a practical approach for analyzing a public infrastructure. In *Intelligent Transportation Systems Conference, 2006. ITSC'06. IEEE*, pages 115–120. IEEE.

Chandola, V., Banerjee, A., and Kumar, V. (2009). Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):15.

Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on software engineering*, (2):222–232.

Morris, B. T. and Trivedi, M. M. (2008a). Learning and classification of trajectories in dynamic scenes: A general framework for live video analysis. In *Advanced Video and Signal Based Surveillance, 2008. AVSS'08. IEEE Fifth International Conference on*, pages 154–161. IEEE.

Morris, B. T. and Trivedi, M. M. (2008b). A survey of vision-based trajectory learning and analysis for surveillance. *IEEE transactions on circuits and systems for video technology*, 18(8):1114–1127.

Vignesh, K., Yadav, G., and Sethi, A. (2017). Abnormal event detection on bmtt-pets 2017 surveillance challenge. In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2017 IEEE Conference on*, pages 2161–2168. IEEE.

Wang, T., Snoussi, H., and Smach, F. (2012). Detection of visual abnormal events via one-class svm. In *Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).