

# An Immunological Approach to Raising Alarms in Video Surveillance

Lukman Sasmita, Wanquan Liu, and Svetha Venkatesh

Curtin University of Technology, Perth Western Australia 6845  
{sasmita, wanquan, svetha}@cs.curtin.edu.au,  
WWW home page: <http://www.computing.edu.au>

**Abstract.** Inspired by the human immune system, and in particular the negative selection algorithm, we propose a learning mechanism that enables the detection of abnormal activities. Three detectors for detecting abnormal activity are generated using negative selection. Tracks gathered by people's movements in a room are used for experimentation and results have shown that the classifier is able to discriminate abnormal from normal activities in terms of both trajectory and time spent at a location.

## 1 Introduction

Most current systems [1–3] that detect abnormal behaviours work by building models of normal behaviour or activities and detecting deviation from these models as a signature of abnormality. In this paper, we explore an alternative method for abnormal activity detection based on biological immune systems, which take an alternative approach to intrusion detection. Instead of building models for *normal* behaviours, the immune system develops a set of *abnormal* detectors, by sampling the entire space and choosing detectors that do not conform to normal. Thus, the abnormal detectors are modelled explicitly, even though the cases may be rare or unobserved. To explore this alternate formulation, we formulate abnormal detectors to find abnormal behaviours for tracking people in spaces. Such abnormalities could include people walking in areas not normally traversed in or spending too much time in a given space. We propose three detectors generated by negative selection and demonstrate their utility in abnormal track detection.

The novelty of this paper lies in an alternate model for abnormal activity detection based on the immune system. Unlike current activity classification systems, the model in this system explicitly models the abnormalities instead of the normalities of the activities to be recognised.

The rest of the paper is organised as follows: First, a short review on the human immune system is presented in Section 2. An overview of the architecture and the design of the system is explained in Section 3. Section 4 analyses the results of the experiments. Section 5 concludes the discussion.

## 2 Preliminary Background

The immune system (IS) is an adaptive, robust and distributed system that continuously maintain stable functions of our body (homeostasis) [4]. The system is capable of identifying and eliminating our own cancerous cells (*infectious self*) as well as external microorganisms harmful to the body (*infectious non-self*). The system maintain constant surveillance for an almost unlimited variety of infectious cells, known as *non-self* elements, distinguishing them from native cells of the host (*self* elements). These non-self elements include a plethora of viruses, bacteria and other foreign objects which are collectively known as *pathogens*. In addition, the IS is also capable of memorising past infections to mount a more efficient response to further encounters. The immune cells which are involved are collectively known as *lymphocytes*. These lymphocytes become activated in the presence of external entities such as viruses or bacteria. Specifically, the entities that interact with lymphocytes are termed *antigens*.

Lymphocyte cells are designed to match external entities not belonging to our bodies. The immune system achieves this discrimination by using *negative selection* [5]. In this process, certain lymphocyte-antigen interactions cause the death of the lymphocyte instead of activation.

During maturation, immature lymphocyte cells are exposed to self-antigens. If a lymphocyte binds to one of the self-antigens, they are programmed to perform self-destruction [6]. This process is called negative selection. For these cells to survive the maturation period, they must not bind to a self-antigens. Mature lymphocytes are therefore tolerant to our body and will bind only to nonself-antigens. In the context of learning, this is how our body learns about pathogens. The collection of lymphocytes as a whole represents the complementary set of our self cells. For a more detailed explanation of the immune system, see [7].

[8, 9] and [10] have investigated the use of immunological concepts in computer security, specifically in intrusion detection systems (IDS). IDS is a system put in place over a network to detect *misuse* or *anomalies* [10] in the network. The misuse of the system constitutes abnormal behaviours which the IDS should detect. In contrast, normal behaviours are defined as normal usage of the system.

## 3 Proposed Approach

### 3.1 System Architecture

Data was acquired by using a top-view camera overlooking a room 7 metres long by 7 metres wide. Background subtraction [2] is first performed to extract the object and a Kalman filter [11] is then used to track the object. Examples of isolated objects are shown in Figure 2. The center of the bounding rectangle is used as the *observed* position of the object in the real world.

The use of the centre of the bounding box to represent the position of the object results in a noisy observation. Since the object width and height determine the centre of the box, an object such as a person standing still but moving his/her limbs may change the *observed* positions as the box changes its size.

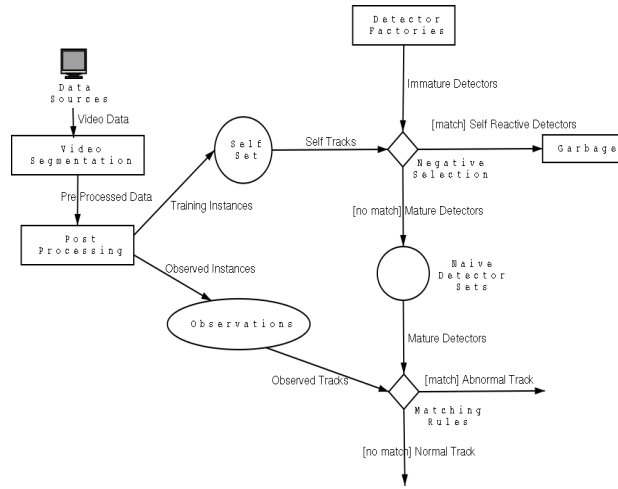


Fig. 1. System Architecture

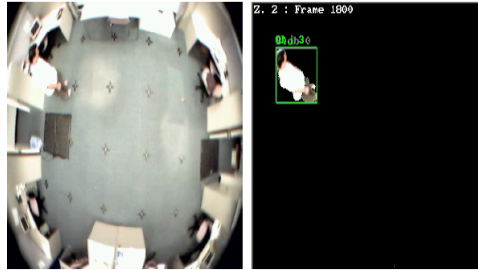


Fig. 2. Raw frame and its isolated foreground

To remedy this problem, an averaging method is used to smooth the data. The number of observations used to calculate the average is termed the *window size*. This method results in a reduced amount of detail of the observed object but smoothes the overall observed position data.

The overall architecture of the system is shown in Figure 1. The system is divided into two phases, the *training* phase and the *deployed* phase. The training phase (the top half of Figure 1) involves recording the movements of the objects (or people) in the room over a period of time. These movements form the self set which defines the normal behaviours in that room. This self set is then used in the detector generation process.

The detectors are generated randomly by generators called *factories*. These random detectors are then exposed to the self set. If a detector is deemed to match a behaviour in the self set, then it is discarded. Randomly generated detectors that do not match the self set are then admitted into the system as

*naive* detectors. This process follows closely the negative selection algorithm in the immune system.

After training, the system is deployed where it will continually survey moving objects in a room. The behaviours of the objects are exposed to the detectors. If a detector matches a behaviour of an object, then that object is said to be abnormal.

### 3.2 Point Detector

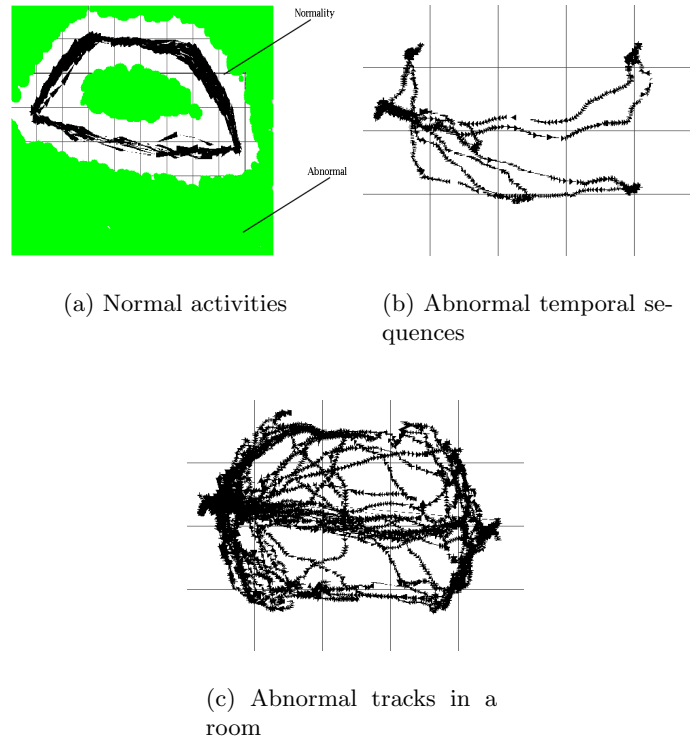
We introduce three types of detectors to detect abnormality. An object that is spatially normal will share the same spatial locality as other normal objects. For example, people traversing through a room will share one or more multiple paths, thus these paths define what is normal in that room. If a path is found to be deviating away from the normal space, then the path is behaving abnormally. A *point detector* is a circle on the observed space. The detector triggers if the object's observed position falls inside the detector's circle. Since a point detector is generated by negative selection, the area bounded by the detector models an abnormal space. Therefore, an object that has entered abnormal space, will trigger multiple point detectors and raise an alarm for being spatially abnormal.

A visual representation of the naive point detectors after training can be seen in Figure 3(a). The black arrows represent the tracks of a normal person as it moves in the room. In this case, abnormal space is the area that is not traversed by the people and has already been covered by the detectors after training. There is an envelope surrounding each normal track to account for variability in the behaviours.

### 3.3 Time Detector

Aside from spatial abnormality, a temporal abnormality occurs when a person is stationary in one position for a long time. Point detectors cannot raise an alarm from such behaviours because they do not encode a notion of time. The second type of detector is able to do so and we termed it a *time detector*. The conception and structure of a time detector is similar to a point detector. The main difference is in the matching rule. A time detector has an additional variable *time limit* which maintains a bound as to how long a person can stay inside the circle bounded by that time detector. If the length of time in which a person is stationary exceeds the threshold, then the person is considered to have a temporal abnormality. The length of time that a person has been stationary is given by how many observed positions share the same spatial locality.

Figure 3(b) shows a track where people spend a long period of time being stationary in the room. These tracks are normal spatially because they traverse the normal areas shown in Figure 3(a). Although normal in spatial dimension, they are abnormal temporally because of the long duration of stationary period. Figure 3(c) shows a collection of tracks which are abnormal when compared to Figure 3(a).



**Fig. 3.** Observed tracks in a room

### 3.4 Trajectory Detector

The third type of detector attempts to detect an abnormal behaviour that can only be detected by observing the direction of the moving object. We term this detector a *trajectory* detector and its working is similar to the chain coding approach. A vector can be drawn from the object's previous position to the object's current position. The major angle that this vector makes to the *north* vector, is the direction of the object at that particular time.

The structure of a trajectory detector is a list of angles. The detector is deemed to have found a match if this list of angles matches with a sequence of angles acquired from the object's trajectories.

This detector is heavily affected by the smoothing process described above. Without smoothing, the noisy data cause very small but many trajectory changes. By having many trajectory changes, the system becomes sensitive and we expect to have many false alarms. With the addition of smoothing, small changes in trajectories will be removed and therefore we expect to have the rate of false

alarms reduced. However, at larger smoothing levels we will expect a drop in the rate of the positive alarms due to the reduced details of the track.

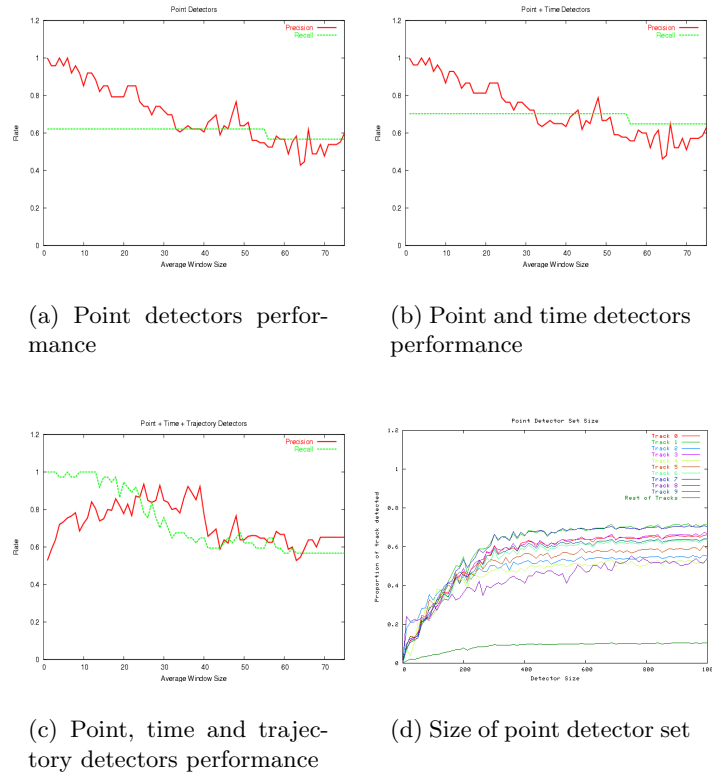
## 4 Experiments

### 4.1 Discrimination Capability

A series of recordings were taken which consists of people moving in the room over a certain period of time. The system is first trained with the notion of self, which are the normal activities in the room. Naive detector sets for the three types of detectors are generated. Next, the system is deployed and exposed to people in the room. In this exposure, 34 sequences or tracks which are abnormal are presented along with 40 normal tracks for which the system should not raise suspicion. The experimentation is done first with the point detectors, and then with time and trajectory detectors. This is to determine the discriminating performance of the system as more complex detectors are added. The experiments were also done with varying window sizes, to test our hypothesis that a small window size will produce many alarms due to trajectory detectors being too sensitive. Figures 4(a), 4(b), 4(c) shows the precision and recall values plotted against the window size. The horizontal axis of the graph indicates increased levels of smoothing. The recall of all detectors declined when the window size is increased due to the decreased detail available.

The recall of the system (the green line) increases as more complex detectors are added. In Figure 4(b), the recall of the system increased with the added discrimination power of the time detectors. In Figure 4(c), without any smoothing of data the three detectors successfully raised an alarm for every abnormal behaviour (100% recall rate). There is a decrease in the overall recall rates as the level of smoothing is increased. In the worst case, a large smoothing will cause all tracks to become straight. Therefore, what is previously an abnormal track is now normal to the system.

The precision trend among the three graphs also decrease as the smoothing level increases. The system becomes less precise in raising alarms because of the reduction in detail of the track. This reduction may add an element of abnormality to a normal track and vice versa. In Figure 4(c), the precision first increases and then decreases. The initial low precision rate in Figure 4(c) is due to trajectory detectors raising false alarms because of the noisy data. As smoothing reduces the noise, the rate of false alarms decreases, increasing the precision rate. At some point, the precision rate starts to decrease due to the lost detail as the averaged values no longer reflect the original values. This is inline with our hypothesis that the trajectory detectors are heavily affected by the smoothing process. However, an optimal smoothing window size can be determined from Figure 4(c) and is in the range of 20 to 25. The introduction of trajectory detectors comes with the expense of a smoothing process being used. However, the tradeoff of losing the resolution of the observation by smoothing is justified by the increase in the system’s discriminating power.



**Fig. 4.** Experimental Results

## 4.2 Size of detector set

In human immune systems, trillions of lymphocyte cells roam around our body [6]. The large number is needed so that the system can model all non-self elements completely. The size of the detector sets thus provide a measure of completeness, as small sets cannot represent a complete abnormality model but on the other hand, limited resources enforce a limit on how large the set should be.

An experiment was performed to investigate what is the minimum point detector set size that can be used without reducing the system performance. In this experiment, the total area of the space is  $250000 \text{ units}^2$  and the average area of a point detector is  $706 \text{ units}^2$  (detector radius of 5 to 25 units), which is only 0.20% of the whole space. In each experiment set, the detector size is increased by 5 detectors. The system is then exposed to 10 abnormal tracks and 40 other normal tracks to test its capability to raise an alarm. Figure 4(d) shows the experimental results. The horizontal axis shows an increasing number of detectors in the set, while the vertical axis represents the proportion of each

track that is detected by the detector set, which is the proportion of the track considered by the set to be abnormal. The system detects a large proportion of track 0 to 9 to be abnormal. The proportion of abnormality detected increases as the detector size becomes larger. However, after a size of 600 the proportion detected stays constant. Therefore, we can safely set the minimum point detector size to be 600, since larger sets do not add to the discrimination power in this data set. This is a very small size considering that a single detector only covers 0.20% of the total space. This stems from the fact that cross reactivity and the multi reactivity of the detectors can provide sufficient detection [7].

## 5 Conclusions

The paper has shown that applying immune system concepts especially negative selection provides a useful solution for abnormal activity detection. Although only three types of abnormal behaviours are examined, more complex detectors which takes into consideration the context of the room warrant further investigation and may reduce the rate of false alarms.

## References

1. Makris, D., Ellis, T.: Path detection in video surveillance. *Image and Vision Computing* **20** (2002) 895–903
2. Stauffer, C., Grimson, W.E.L.: Learning patterns of activity using real-time tracking. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **22** (2000) 747–757
3. Johnsom, N., Hogg, D.: Learning the distribution of object trajectories for event recognition. *Image and Vision Computing* **14** (1996) 609–615
4. Janeway, A. C., Travers, P.: *Immunobiology: The Immune system in Health and Disease*. 2nd edn. Garland Publishing, Inc., New York (1996)
5. Forrest, S., Perelson, A.S., Allen, L., Cherukuri, R.: Self-nonsel self discrimination in a computer. In: *Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy*, Los Alamitos, CA, IEEE Computer Society Press (1994) 202–212
6. Hofmeyr, S.A.: An interpretative introduction to the immune system. In Cohen, I., Segel, L., eds.: *Design Principles for the Immune System and other Distributed Autonomous Systems*. Oxford University Press (2000)
7. de Castro, L.N., Von Zuben, F.J.: *Artificial immune systems: Part I: Basic theory and applications*. Technical Report 01/99, DCA (1999)
8. Hofmeyr, S.A., Forrest, S.: Architecture for an artificial immune system. *Evolutionary Computation* **7** (2000) 45–68
9. Forrest, S., Perelson, A., Allen, L., Cherukuri, R.: A change-detection algorithm inspired by the immune system. [Online] <http://citeseer.nj.nec.com/51699.html> (1995)
10. Puglisi, S.: *An immunological approach to network intrusion detection* (2002) Honours Thesis, Department of Computer Science, Curtin University of Technology.
11. Kalman, R.: A new approach to linear filtering and prediction problems. In: *Transaction of the ASME – Journal of Basic Engineering*. (1960) 33–45