Detecting Separation of Subjects from Their Badge

Shmuel UR, Itzhak POMERANTZ, Vlad DABIJA

***Abstract*—This paper was originally submitted to Xinova as a response to a Request for Invention (RFI) focusing on new Decision and Response Techniques for Security Applications. This paper describes a method to detect the separation of individuals from their entry badges.**

In more detail, this describes how a system can maintain awareness of spectator credentials and issue an alert when an attendee is without a badge, or a badge is without an attendee.

I. Abstract

IN certain crowd gatherings, attendees are expected to wear their badges. The term "badge" means any type of passive or active device or ticket that is given to people in crowds with the expectation that the badge will be on the person throughout the event. The authorities want attendees to be identifiable for security considerations, and the badges are efficient means to identify people.

People with malicious intentions do not want to be easily identified, and have an interest to lose their badges and be anonymous.

People who detach themselves from their badges are a potential security risk. The detection of such people in the crowd is an unsolved problem.

II. Summary of the Invention

The invention is a small set of methods to detect people in a crowd that have ditched their badge. It is based on few assumptions:

1) The security video system can recognize a person in the crowd if that person was captured by the video system upon entrance into the venue.

2) The security system can detect an RFID badge in the venue if an RFID reader is within RFID range from that tag.

3) Upon entering the venue, a person and her/his badge can be paired with each other.

Based on these three assumptions, the system can reliably detect significant security events.

The output of the system can be as shown in the illustration:

Fig. 1. System Output

III. Detailed Explanation

The organizers issue to ticket owners the tickets or badges that have an RFID tag in them.

The visitors enter the venue in a line, so that a camera can take a good quality photo of the attendee and an RFID reader can read the number of the RFID. One may wonder why we need that, rather than associating the ticket with the face upon issuing the ticket in the box office. The reason is that it is typical for a person to buy multiple tickets for a group, and then share the tickets with the group out of the control of the box office. This is a natural behavior and we do not want to change it. So the individual visitor is associated with the ticket upon entry through the gate. In events where the organizer

need to have details of the attendee for the records, this feature is not relevant as then the tag or ticket will necessarily be associated with the individual. An RFID reader is reading the ticket while a camera is taking an image of the attendee. The visual image of the face of the person is associated with the number of the RFID.

The video system is monitoring the crowd throughout the event, and every person with a clear frontal appearance in the video is recognized in reference to his image upon entry. This is mainly done by face recognition but additional visual detail such as clothing, neighbours and gait can be used to increase reliability.

RFID readers are scattered throughout the place on poles, under some tribune seats, in service facilities and carried on personnel such as security forces, cleaners, merchants and service staff. They read RFID's and send the RFID number and the location of the reader to a database of detected tags. The accuracy of location is the range of the RFID reading, typically less than 3 meters. The accuracy of the range can be enhanced by using the strength of the signal received from the RFID as a coarse indication of range. The range can be even more accurate if the RFID is used as a transponder and the time delay of its response is measured.

As there are multiple RFID readers, the system can trace the path of an RFID by tracking its appearance and disappearance in different RFID readers. If the walking path is constrained to a line, by a corridor or by a fence or by a single door into a room – the direction of walking can be detected in a single place without the need to wait until the tracked RFID appears in a far reader. This can be done by placing two readers next to each other. The slight delay between appearance and disappearance of the RFID tag in both readers indicates the direction of walking. This is illustrated in the following drawing. If a certain RFID appears in reader A and keeps showing there for a while, and slightly later it appears in reader B and keeps there for a while as shown in the first two charts below – then the system infers that the person carrying this RFID is walking by the readers and passes A before passing B.

Then if later the same RFID shows up in reader C and after a short while appears in reader D as shown in the two bottom charts. The four charts indicate that the subject walked along the path marked in blue, but the direction of walking can be derived from readers A and B without waiting for the subject to reach readers C and D. The recognized people and the read tags are streaming into a computer that pairs them.

Every pair of person/tag that are reasonably co-located, are screened out as a non-interesting pair, as they indicate an attendee carrying his ticket or tag as required.

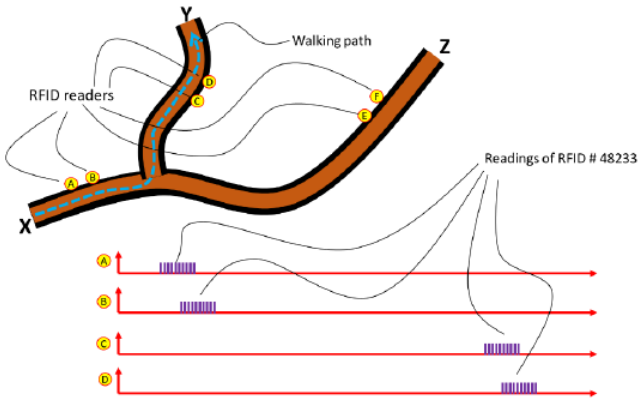

Fig. 2. RFID reader locations and Possible walking path

Every pair of person/tag that are not reasonably co-located are declared as suspicious and a security officer is assigned to check them (possibly in a method that was disclosed in another of our submissions to this RFI) Every RFID tag that is found to be too stationary is assumed to have been ditched and the control tries to identify its owner (typically by face recognition or by calling his phone number) and check him.

Determination of stationarity of an RFID can be done in several ways, and there is a distinction between "micro stationarity" and "macro stationarity".
Macro stationarity is stability in one location. Micro stationarity is lack of motion.
An RFID is macro-stationary if the wearer does not change its location in the venue.
An RFID is micro-stationary if it is not carried on a human body.
Macro-stationarity is checked by tracking the location of the RFID throughout the event. It is a simple matter of data processing. The macro stationarity can be classified to 4 operational categories: Stationary, piece-wise stationary, restless and moving:

A. Stationary – does not change location throughout the event

B. Piece-wise stationary – changes location from time to time, and stationary in each location for reasonable time.

C. Restless – changes location frequently, but stationary in each location

D. Moving – changes location all the time throughout the event.

The stationarity attribute is a significant security intelligence that, together with other indications, helps to investigate and alert.
Micro stationarity is checked by analysis of the phase and amplitude stability of the signal received from the RFID at the reader. If the RFID is on a person, the natural movement of the body and the frequent changes of obstacles on the multipath between the RFID and the reader, change the amplitude and phase of the received signal and indicate that the RFID is not at rest. IF the RFID is ditched, it will have much less variations in multipath and will have long periods of stable signal. The method is described in this flowchart

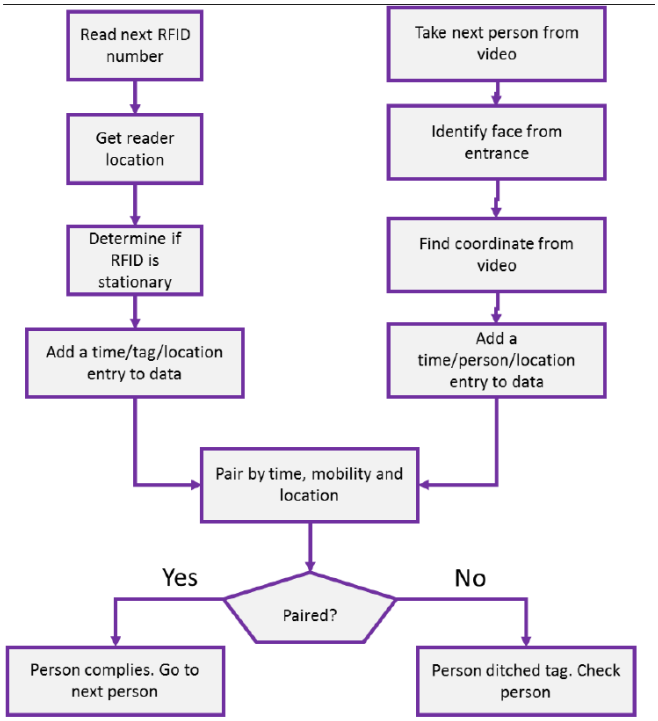

Fig. 3. Flowchart of proposed method.

In the second drawing the disturbance is easily identified. Some additional non-frontal vectors that are detected by various cameras were added as reference for non-significant vectors. Normally there will be many more such vectors as people do look around occasionally, but they will be dispersed more or less equally over the entire area of the event, they will not be oriented in any specific direction, and they will only deviate from the front direction for short periods. The vectors around a disturbance, on the other hand, will (a) be concentrated around a common center, and (b) be present for much longer durations. Statistic filtering can easily remove most of the non-significant vectors and leave for further analysis only vector sets that may point to a disturbance.

Each vector starts at the location of the pair of eyes that were detected by the camera, and its length may be proportional to the density of people in that area – where the denser the people the shorter the visible range of each person and hence the shorter the vector.

IV. Conclusion

The following alerts can be generated by this system:
1. "This RFID is micro-stationary and macro-stationary for too long. It may have been ditched by the attendee. This badge was purchased by the following person and was worn by the following face. Please seek him in the video and check him"
2. "This person is detached from his RFID tag. We did not sense his RFID when the reader was in his vicinity. Please approach and check him".
3. "This person is not identical to any of the people who entered legally. Probably a sneaker. Please check him".
4. "This person is in a restricted area that is not allowed for his RFID tag. He could only enter this area if he has ditched his tag. Please check him".
5. "This RFID tag changes its macro-location at a rate that is not reasonable for an innocent spectator. Please check him".
6. "This RFID does not seem to be on a live person. This is the face of the person who is supposed to wear it. Please check this person".

In order to have good coverage of RFID reading in a crowd, where no stationary readers infrastructure are naturally distributed and no personnel are typically distributed, a mobile RFID reader can be used, carried by a balloon, a drone or a cable as in the following illustration

Fig. 4. Example for better RFID reader coverage.

This solution is "non-invasive" to innocent attendees, it can detect suspects upon macro-motion, it can serve multiple event types (sports, performances, conventions,

etc.) and it is portable and does not require significant infrastructure.

While there is no assurance that all people in the crowd will be recognized in the video, and as the travelling readers will not reach every point in the crowd, this is an excellent supplement to other methods and it will deter people from ditching their tags and becoming anonymous.

ACKNOWLEDGMENT

This research was originally submitted to Xinova, LLC by the author in response to a Request for Invention. It is among several submissions that Xinova has chosen to make available to the wider community. The authors wish to thank Xinova, LLC for their funding support of this research.
More information about Xinova, LLC is available at www.xinova.com.