# Person Detection Techniques for an IoT Based Emergency Evacuation Assistance System

Prasad Annadata
Dept. of Computer Science
University of Denver
2280 South Vine Street
Denver CO 80210 USA
prasad@cs.du.edu

Wisam Eltarjaman
Dept. of Computer Science
University of Denver
2280 South Vine Street
Denver CO 80210 USA
wisam@cs.du.edu

Ramakrishna Thurimella
Dept. of Computer Science
University of Denver
2280 South Vine Street
Denver CO 80210 USA
ramki@cs.du.edu

## ABSTRACT

Emergency evacuations during disasters minimize loss of lives and injuries. It is not surprising that emergency evacuation preparedness is mandatory for organizations in many jurisdictions. In the case of corporations, this requirement translates to considerable expenses, consisting of construction costs, equipment, recruitment, retention and training. In addition, required regular evacuation drills cause recurring expenses and loss of productivity. Any automation to assist in these drills and in actual evacuations can mean savings of costs, time and lives. Evacuation assistance systems rely on attendance systems that often fall short in accuracy, particularly in environments with lot of "non-swipers" (customers, visitors, etc.,). A critical question to answer in the case of an emergency is "How many people are still in the building?". This number is calculated by comparing the number of people gathered at assembly point to the last known number of people inside the building. An IoT based system can enhance the answer to that question by providing the number of people in the building, provide their last known locations in an automated fashion and even automate the reconciliation process. Our proposed system detects the people in the building automatically using multiple channels such as WiFi and motion detection. Such a system needs the ability to link specific identifiers to persons reliably. In this paper we present our statistics and heuristics based solutions for linking detected identifiers as belonging to an actual persons in a privacy preserving manner using IoT technologies.

## CCS Concepts

**•Security and privacy → Human and societal aspects of security and privacy; •Networks → Mobile ad hoc networks;** *Sensor networks;* Physical topologies; **•Human-centered computing → Ambient intelligence;** *Empirical studies in ubiquitous and mobile computing;*



*IoTSEC '16 Nov 28, 2016, Hiroshima, Japan*



DOI: http://dx.doi.org/10.1145/3004010.3004019

## Keywords

Internet of Things; IoT; Privacy; Security; Human Safety; Emergency Evacuation; Mobile ad hoc Networks

## 1. INTRODUCTION

Disasters like fires or earth quakes happen and take a huge toll both in terms of money and life. The priority during those disasters is to save lives first. While some disasters cannot be avoided, being prepared to handle a disaster in such a way that loss of lives and injuries is minimized is paramount. Emergency preparedness is a popular paradigm across governments and corporations. Emergency evacuation preparedness is a major component of any entity's emergency preparedness practice. In fact, most governments have special organizations that handle disasters (e.g. FEMA[1] in the USA) and in most jurisdictions, they mandate that medium to large scale companies with high density work location structures have an ongoing emergency preparedness practice[10]. Corporations do this by creating emergency preparedness plans and train employees in evacuation procedures by conducting regular drills. These corporations usually have a dedicated or volunteer employee teams that are formally trained in disaster handling procedures. These teams then train some employees to be emergency response coordinators (ERCs). They ensure that there is enough coverage of each building and each floor where an ERC will be available in case of a disaster. While other employees practice locating nearest exit, remembering assembly points and exiting swiftly during emergency drills, the ERCs practice their tasks by coordinating these evacuation drills. An ERC's first task is to direct people to calmly leave the building and gather at a predetermined assembly point far enough away from the building. In the case of a real emergency, these ERCs also ensure that the disaster is reported to proper emergency responders or ERs (usually fire fighters) as soon as possible. Some corporations also suggest that ERCs, to the extent possible, have current attendance list on hand and take it with them to the assembly point. Once in the assembly point, they perform the task of accounting for every person that was in the building prior to the disaster as indicated per the attendance list. This process is termed as reconciliation. Using the attendance list and list of reconciled persons prepared at the assembly point, they arrive at a list of persons that are still not accounted for. These persons are assumed to be trapped in the building. This list

[1]Federal Emergency Management Agency.

is given to the ERs when they arrive. This way, the ERs can focus their valuable immediate response time on getting the trapped people out and not on searching for people that are already accounted for. In modern implementations these emergency evacuation systems are linked to electronic attendance systems that give the ERCs and ERs a baseline of the number of people that were actually in the building prior to the disaster.

## 1.1 Problem Statement & Motivation

The process of accounting for all persons at the assembly point is still a manual task in most cases, and hence error prone and time consuming. In the case of large evacuations usually multiple assembly points, multiple ERCs and multiple exit points are involved. In the case of major disasters, centralized electronic attendance systems may go offline or become inaccessible. This causes confusion and even more delays in the reconciliation process, often forcing ERs to perform a room to room search. Clearly, the more time the reconciliation task consumes, the more risk it is for people trapped in the building. In the case of evacuation drills, this confusion and delay translates to more lost productivity. More importantly it causes lack of confidence in the emergency preparedness process, which leads to people not really following the evacuation procedures in the case of a real disaster. While no attendance system can be perfect, major inaccuracies can be costly. Even a small number of false negatives (the person wrongly counted as not-trapped) can be dangerous to those trapped people and too many false positives (too many people wrongly reported as trapped) can mean wasting of valuable response time.

Solutions proposed both in the industry and research community do rightfully suggest the automation of as many tasks as possible in the evacuation process. Most of the automation is achieved in the attendance systems[11, 12] using technologies such as RFIDs, NFC etc., The idea is these systems give a quick reliable baseline of how many people were actually in the building. In the case of registered users (e.g. employees) that adhere to the process of performing arrival action (e.g. card swipe), these systems are very accurate. In other words, in the case of mostly registered populations, these systems save time in getting the baseline on who was in the building prior to the disaster. But, as one can imagine, more time is spent on the reconciliation process than getting the baseline of who was present in the building, especially in the case of large evacuations, even if the attendance systems are automated.

Most attendance system still fall short in accounting for "non-swipers" such as visitors and even employees that follow a courteous colleague that holds the door open. In the case of establishments with lot of non-employee traffic such as shopping malls, banks, big box stores and government offices, these attendance systems are naturally inaccurate. Some attendance system that do not require specific IDs to be carried[7] still require specific action to be performed by registered users in order to be recognized. These systems are only as reliable as how strictly the users adhere to the arrival action processes such as a card swipes. These inaccuracies in attendance systems lend itself to two distinct problems. First problem is not having an accurate count that includes the non-swipers in the baseline i.e, not being able to accurately answer "How many people were in the building?". Second, slightly bigger problem is the inability to automatically reconcile the non-swipers such as visitors at the assembly point, i.e., not able to answer "How many people are still not accounted for?".

To alleviate both problems, we are of proposing and implementing a robust, cost effective, practical and novel solution that takes advantage of advances in IoT and supporting technologies. In addition to assisting with the two main questions, our solution has the ability to provide *last seen* location of the trapped persons. Clearly, the last seen location information can be of immense help to the ERs, probably making their rescue procedures faster, thus help reducing the loss of life or injury. This solution combines various technologies such as WiFi, passive WiFi, Bluetooth, motion detection, triangulation and ad hoc networking to have an as accurate as possible count of currently present persons in the building.

The system works by detecting the various electronic identifiers, such as MAC addresses using ad-hoc networked IoT devices spread across the building. The system relies on emitted identifiers without requiring specific actions (such as card swipes) from the people. To do that, it has to have the following abilities. Firstly, the ability to differentiate IDs that belong to persons from those belonging to other static objects. As one can imagine various identifiers are emitted not only by devices carried by people but also by devices that stay put in the building (e.g. printers, routers). A way to differentiate and narrow down identifiers that truly represent presence of persons is needed. Secondly, in this day and age people carry mobile devices that emit multiple identifiers across multiple channels such as WiFi and Bluetooth while some people carry multiple devices. These situations increase risk of over-counting and false positives i.e., mapping IDs to multiple persons even though they belong to a single person. Ability to determine multiple IDs that belong to the same person and mark them as belonging together is needed. In this paper we present statistical and heuristic techniques that normalizes identifiers from different technologies, narrow down the ones that can be linked to presence of a person, link multiple IDs that belong to the same person and to track the location of the person in a privacy preserving manner. We also present techniques that link non-identifying technologies such as motion and vision to enhance the accuracy of person detection. We have implemented these techniques in simulated environments and present the results we achieved. There are a few proposals and implementations in the automated attendance systems area that report number of employees that were present in the building. To our knowledge, there are no other proposals or systems that are designed specifically to assist in emergency evacuations. Our systems reports the last seen locations, that too of even unregistered persons (non-employees) and also assist in the reconciliation process while ensuring reasonable privacy to the people. Our proposals save considerable time in the reconciliation process that translates to saved money and saved lives.

# 2. PROPOSED SOLUTION & MODEL

In this section, we describe our solution interspersed with precise description of the model. The solution depends on the fact that most people carry with them smart devices (such as smartphones) or backscatter systems (such as RFID embedded cards) that actively or passively emit unique enough identifiers (such as a MAC address). Some technologies such

as WiFi, Bluetooth actively emit their identifiers that are reasonably unique, anonymous detection of which is already used in various applications[14, 5]. Most people that carry smartphones emit identifiers that can be scanned using antennas attached to IoT devices. There are other identifiers that are emitted by backscatter systems such as RFID[2] or WiFi backscatter[8] that can be read using specialized equipment. This equipment can be integrated into our proposed system by attaching IoT devices to them. When IoT devices are used to scan for available identifiers, there is of course concerns of loss of privacy[4]. We propose to minimize these concerns using a ID normalization technique explained in section 3. Some IDs such as MAC addresses are inherently unique by design. Even in the case of other application specific IDs such as RFIDs we assume them to be *unique enough*. This is a reasonable assumption considering the localized nature of our proposed system. The application will be built[3] with fault tolerance and to work in a distributed manner across all the IoT devices that get connected via an adhoc network. In environments where safety is critical enough to override privacy, the proposed solution can in fact be integrated with attendance systems to gather more accurate information.

The IoT devices are built using small single board computers (Raspberry Pi) with accessories that include WiFi and Bluetooth antennae. Some of the devices are equipped with motion detectors and camera based on their location. Each of the technologies used such as WiFi, Bluetooth, motion etc., are termed as channels. Some channels can detect unique enough IDs (simply called IDs from now on) such as MAC addresses or RFID tag numbers. The devices scan for visible identifiers on all their available channels. The scanning process occurs frequently at configured times and also can be event driven (e.g motion detected). The time stamps when the scanning is done is denoted by $T = \{t_1, t_2, t_3, ...\}$. These IoT devices, also known as scanners, scan across multiple channels and any detected IDs are normalized, merged and stored simply as $ID_{t_n} = \{id_1, id_2, id_3, id_4...\}$, representing the normalized set of identifiers discovered at time $t_n$. People detected (using techniques presented in this paper) are denoted by $P_{buillding} = \{p_1, p_2, ....\}$. The devices, $D = \{d_1, d_2...d_n\}$ are located strategically through out the building in all floors with approximate coordinates of the location of device in 3D space denoted by $L_{d_k} = (x_{d_k}, y_{d_k}, z_{d_k})$. The origin $(0, 0, 0)$ located at the ground floor bottom left of the building to make visualization easy. Please note that some coordinates can be negative based on the placement of devices in the basement floors or outside the building. Among the devices, there are some devices denoted as entry points $D_n$ and exit points $D_x$. Even though few devices can act as both, the device placement is strategically done to reduce $|D_n \cap D_x|$. Although this is not a strict requirement, it does make assessment of whether someone safely exited the building much simpler. Physical location of each of the IDs scanned is determined by triangulation and tracked for each ID using the tuple $L_{id_k} = \{(x_1, y_1, z_1), (x_2, y_2, z_2)...(x_n, y_n, z_n)\}$, where $(x_n, y_n, z_n)$ is the last known location. Please note that to improve readability of the discussions below, too deep subscripting and superscripting is omitted if referred items are obvious from the context.

The IoT based emergency evacuation assistance system has several modules and features that encompasses several facets of the evacuation drills. In this paper, we present techniques that achieve the following goals.

1. Scan for IDs efficiently and determine whether a detected ID belongs to a personal device or a static device, i.e. if the presence of that ID at a location can be reasonably equated to presence of a person. This goal can be satisfied by producing a map that associates person numbers to the IDs that were detected. $M = \{\langle p_1 : id...\rangle, \langle p_2 : id...\rangle, ...\}$. E.g. Let's say a scanning device detected IDs as follows at time, $t_n$, $ID_{t_n} = \{id_1, id_2, id_3, id_4\}$ and a different device at time $t_{n+p}$ observes another ID set $ID_{t_{n+p}} = \{id_3, id_4, id_5, id_6\}$, then we know that $id_3$ and $id_4$ have motion and they will be assigned to persons, e.g $\langle p_1 : id_3\rangle, \langle p_2 : id_4\rangle$.

2. Determine the list of IDs that belong to stationary entities such as desktops that rarely move and be safely eliminated as not belonging to a person. This goal can be satisfied by producing a set of stationary IDs, $ID_{stationary} = \{id...\}$ where each $id$ in the set has only one location in $L_{id}$ for a threshold amount of time or last location in $L_{id}$ has not changed for a threshold amount of time.

3. Determine multiple IDs that belong to the same person (e.g. WiFi mac address and Bluetooth mac address emitted by the same personal mobile device) and associate them to the same person so as to avoid overcounting the number of people. Satisfying this goal involves enhancing the person-to-ID map $M$ to ensure that within the map, if two IDs $id_j$ and $id_k$ belong to the same person $p_i$, then there exists an entry $< p_i : id_j, id_k... >$ in $M$.

4. Determine the last known location of a person as accurately as possible and save the information in an accessible manner. This is satisfied by performing triangulation of the ID after the scans and keeping the location sets $L_{id}$s up to date. Last known location will be the last entry in this location set for that ID. If the person has multiple IDs and if for whatever reason, their last seen locations are different then all those locations are reported in reverse chronological order of their scan times.

5. Come up with a list of number of people that were present in the building prior to disaster. Satisfying this goal involves reporting $P$, $M$ and $L_{id}$ data sets in a easily readable format in the user interface.

6. During a drill or an actual disaster, being able to quickly determine the presence of person at the assembly point and automatically add them to the "accounted for list". This is done by the IoT devices taken to the assembly point by ERCs and the exit devices, that are instructed to run in "reconcile mode". Satisfying this goal involves coming with a suitable efficient algorithm (and data structure) so as to they quickly correlate the list seen IDs in the assembly point and produce set of persons $P_{assembly\,point}$.

7. Produce a list of possible trapped people and their last seen locations. Satisfying this goal is a trivial exercise of doing $P_{building} - P_{assembly\,point}$ and report their last known locations using $L_{id}$ and presenting it in the user interface.

## 3. TECHNIQUES & ALGORITHMS

All the scanner devices placed through out the building are expected to form a robust enough ad hoc network and share data. They also implement distributed algorithms for storage of data, intermediate calculations, data structures representing $M$, $L_d$, $L_{id}$, $P$ in redundant fashion and perform indexing and triangulation. The actual discussion of ad hoc protocols, fault tolerance, triangulation algorithms are beyond the scope of this paper. Techniques employed in the IoT devices is explained below and presented briefly in Algorithm 1.

**Normalization of IDs** Depending on the channel, revealing of IDs can lead to loss of privacy. For example, employees often carry identity cards with RFID chips that identify themselves with their employee ID and/or name. Employee ID is commonly considered non-public proprietary information. Even if the IDs are pretty unique, such as MAC addresses, combined with other information, they can lead to loss of privacy[4]. So we propose that whenever IDs are detected these raw IDs are immediately normalized as follows, on the IoT device itself. The raw IDs are padded with a predetermined string and use one of the hashing algorithms such as SHA-1. The resultant hash is stored in the IDs set $ID$ and the raw ID discarded immediately. This secure hashing after padding with a predetermined salt ensures that privacy is not easily breached even if the data sets $M$, $ID$, $L_{id}$ are compromised. There is still some risk involved if an attacker has unfettered access to the IoT devices themselves and can directly manipulate the channel specific modules on it. Additional advantage of this process is it makes the rest of the proposed algorithms work on IDs in a channel agnostic manner.

**Detecting Movement** One straight forward way to determine that a scanned ID belongs to a person is to detect movement. This assumes that the building does not have lot of moving machinery that emit IDs. But if building does have lot of moving machinery that emit IDs (e.g. factory floor), we propose that the set $ID_{stationary}$ is pre-populated with IDs of these moving machinery. Absence of any detected ID in $ID_{stationary}$ is verified before performing further movement detection process. The movement is detected in two ways. When a scanner sees the ID for the first time it can assume the ID seen belongs to a person and maps it so. If the ID turns out to belong to a static entity, it will be cleared from the list. The second way to detect movement is if the ID is detected by multiple devices that are geographically apart. Let $ID_{t_n}$ be the set of IDs detected by a device at $t_n$ and $ID_{t_{n+p}}$ be the set of IDs detected by a device at different location at a later time $t_{n+p}$, then IDs belonging to $ID_{t_n} \cap ID_{t_{n+p}}$ can be assumed to have movement. These IDs are added to person-to-ID map $M$ after appropriate checks.

**Appearance at entrance and disappearance at exit** If an ID is seen for the first time at an entrance scanner, it is given a higher probability of being a personal device. Even if a static device's ID is detected by an entrance scanner when it was being brought in, it will initially be added to the person-to-ID map, $m$. But it will be eventually stops moving and will removed from $M$ and added to $ID_{stationary}$. Similarly if an ID is noticed to go out of range via an exit scanner, i.e the clean up routine detects the last seen location of an ID that no longer is in the building is an exit, then it is assumed to be a personal device. In normal situations when an exit is detected $P_{building}$ is decremented to indicate normal exit of a person. But, during a drill or an actual emergency, exit nodes behave slightly differently. When an exit of an ID in the person-to-ID is detected by an exit node during an emergency, that person is added to the $P_{assembly\,point}$, assuming that person is headed straight to the assembly point.

**Motion Detection & Cameras** Please note that in this paper we use the term motion detection to specifically mean the motion detected by the motion detection hardware and software that some scanners are equipped with. It is different from movement detection discussed above, which refers to the algorithmic detection of movement of an ID in the building. Motion detection or cameras do not recognize any IDs. If motion is determined or camera detects a moving person, the device immediately invokes the scan of other channels on the same IoT device. The IDs scanned at that moment, $ID_{detected}$ are then analyzed. If a previously not seen ID is detected in $ID_{detected}$, it is given a higher probability of belonging to a person. Similarly if no new ID is detected in $ID_{detected}$, i.e. all the $ID_{detected}$ already exist in either $M$ or $ID_{stationary}$, it will be noted as a potential electronically silent person as explained below. Although some proposals do exist that use cameras for detecting people directly[7], because they require people to pre-register and perform specific arrival actions like looking into a camera, we disregard them here.

**Co-occurrence of IDs & merging** The person to id Map $M$ and $ID_t$ are scrutinized to check, if pairs of IDs occur commonly. i.e. when any two IDs, $id_1$ and $id_2$ always occur together in ID sets and rarely occur on their own, then it will be noted that both IDs belong to same person and their tuples in the map $M$ are merged. The routine that detects the co-occurrence of IDs and merges the tuples in $M$ runs periodically on fixed intervals (configurable). The idea is to process the ID sets to identify pairs of IDs that occur together often more than a threshold percentage of time. When this percentage (configurable) is high, the corresponding tuples are merged. A brute force method on lists of ID sets, assuming we are dealing with $n$ sets of average $d$ IDs across these sets would be $O(n.d.k^2)$, where $k$ is the number of unique IDs across all the sets. In order to improve the performance, we maintain a reverse index[1] of IDs. Even though indexing costs $O(nd + k)$, since it is distributed and run across several devices before being merged. The system may go back routinely and verify the validity of merged maps by making sure the IDs still come in together.

**Clean-up routines** There are several clean up routines that are run at configurable intervals, usually daily or intervals that coincide with working shifts. These routines do the following tasks (1) Detect exited persons by tracking last seen times of IDs and mark them exited after configurable amount of time. (2) resolve conflicts such as same ID belonging to different persons, by letting the latest entry win, followed by majority opinion. (3) Even if a device has movement earlier, but if it has not moved for a while, then mark those devices as stationary (configurable) (4) Expire IDs that have not been seen in a while and remove them (5) validate the entries the person-to-ID maps ($M$), stationary IDs ($ID_{stationary}$) by checking them against latest ID sets (6) Send notifications to administrators on performance, unresolved conflicts, failed devices, storage full events etc., **Electronically Silent Person Detection** Be-

cause safety of life is involved, it is important to try to account for persons that do not carry any electronically detectable IDs. Popular way to mitigate this in the case of corporate work locations such as offices and factories is to mandate that all visitors obtain a visitor ID and they carry it with them as long as they are in the premises. We propose to place devices equipped with motion detection and camera be placed strategically at the entrance(s) and exit(s). If a motion/image that corresponds to a person is detected[2], then an immediate scan using other channels on the device is performed. Let's say the resultant ID set is $ID_{t_{detected}}$. Two situations can arise here. One: all ids from $ID_{t_{detected}}$ are all previously known i.e. each $id \in ID_{t_n}$ has been deemed stationary (i.e. $id \in ID_{stationary}$) or belonging to a person whose location is known be away from the current device. In this case, it is assumed that this detected event (motion or camera) belongs to an electronically silent person. $M$ is updated with a "null" person without any linked IDs and the $P_{building}$ is updated appropriately. Two: a new ID, i.e,, not previously recorded in the system is detected in $ID_{t_{detected}}$. In this case, it is detected as movement of that ID, and is noted as belonging to a non electronically silent person and mapped so. This process is explained in Algorithm 2.

**Algorithm 1** Person Detection Algorithm

```
1: t ← 0
2: ID_stationary ← prepopulate
3: ID_prev ← DetectAllIDs()  ▷ Collect Normalized IDs
4: while True do
5:     t ← t + 1
6:     ID_now ← DetectAllIDs()
7:     ID_moved ← DetectMovement()
8:     ID_struct ← MergeAndIndex()
9:     M ← UpdatePersonToIdMap()
10:    for all id in ID_struct do
11:        if last moved time of id > thershold then
12:            Add id to ID_stationary
13:        end if
14:    end for
15:    ID_prev ← ID_now
16: end while
```

**Algorithm 2** Motion Detection Event Handler

```
1: ID_detected ← ScanOtherChannels()
2: ID_new ← ID_detected − ID_struct
3: if ID_new = ∅ and ID_detected ∈ ID_stationary or away
   then                          ▷ electronically silent persons
4:     Add null-person to M
5: else                          ▷ detected persons with IDs
6:     M ← UpdatePersonToIdMap()
7: end if
```

## 4. IMPLEMENTATION & RESULTS

As the complete implementation is part of a larger effort by the authors and that work is in progress, the implementation of the proposed techniques in this paper were confined to simulated situations to prove the merit of these techniques. However, care has been taken to use realistic simulated data such as generating valid MAC-ids, assigning realistic multiple number of devices to persons and making sure arrivals and departures of people imitate typical business days. Simulations are a standard practice in evaluating theories in emergency evacuation situations[13, 6].

We ran several simulations in two different sets with different random seed values. We ran a set of smaller simulations to validate our code, typically with 100 people for 3600 time intervals. Our larger simulations were run with 1000 people for 36000 time intervals. Each run simulates a single 10 hour business day. Each person was assigned between 0 and 4 identifiers using a normal distribution so that most people get assigned two or three identifiers. All the people enter the simulated building through a single entry point. The building is simulated with locations that are equal to the number of people (assuming the building's are usually built and occupied to capacity) with no restriction placed on having multiple people being at a single location. Devices are placed uniformly across the locations. Each device is assumed to be able detect IDs carried by people at locations that are between itself and its neighboring devices. Movement of people is done randomly using an uniform distribution with slight bias towards forward movement. Even though there is a single entry point, multiple exit points are simulated. Since we do not have real data to use, arrival time of people in the building is controlled by a beta distribution ($\alpha_1 = 1.5, \alpha_2 = 5$) that ensures majority of people entering the building in the morning[9]. Similarly people exiting the building is done using another beta distribution ($\alpha_1 = 5, \alpha_2 = 1.5$) skewed to ensure majority of people leave in the afternoon. As people enter the building and move randomly around the building, the IDs they carry are detected by the devices. We realize that random movement is not a realistic imitation of actual people's behavior in a work location[13]. But we chose this to ensure the detection techniques still work even in high movement scenarios. The devices are assumed to share this information and the algorithms are run on aggregated data. When IDs are detected by the devices, initially each ID that is moving is assumed to belong to a different person and counted so. Every several iterations, a *merge* process is performed. In this process, IDs

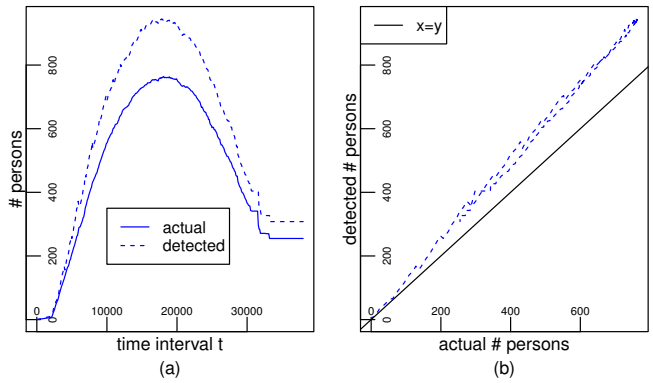


**Figure 1: (a) The number of people detected and actual number of people, both numbers tracked against time $t$. (b) The number of detected persons against the actual number of people.**

[2]Algorithms for inference of a human from motion or image are beyond the scope of this paper.

that have stayed together over the last several time periods are merged. This detection process is optimized by tracking the locations as sequences of strings and available optimized duplicate detection libraries are used to detect IDs moving together. Since the initial path taken by all people will be the same as they all enter using a single entrance, the duplicate detection process detects a large number of duplicates. But we know that these large number of duplicates cannot be merged as they they are not likely belong to the same person. So, a threshold is used to set the upper limit to the number of duplicates IDs that will be merged.

Through out the simulation process the number of actual people and number of people detected by the algorithms is tracked. Figure 1(a) shows the actual and detected number of persons as the time progresses. During the study, we tried to tune the parameters to eliminate false negatives (most dangerous) while minimizing the number of false positives. It is observed that the max duplicate threshold parameter (max number of similarly path-ed IDs that can be merged) has an impact on false negative rate. Hence we performed several simulations with varying value of this threshold to ensure that the algorithm does not produce false negatives. We have not seen any false negatives produced during the studies when the this threshold is set to 3 or below. This threshold is realistic considering, a person carrying more than 3 IDs is rare, and even so, those IDs will eventually be detected as duplicate pairs. Figure 1(b) shows that the detected number of persons is always equal or above the number of actual persons.

However the following limitations of the simulation do exist. All persons are assumed to have same speed of movement. Motion detection and camera channels are not used. Some other features such as introduction of noise in ID detection, simulating assembly point ID detection and electronically silent persons is planned for future work.

# 5. CONCLUSION & FUTURE DIRECTION

In this paper we proposed several techniques to be used by a IoT based system that helps in emergency evacuation and reconciliation. We have presented a mathematical model and clearly defined the goals our presented methods intend to achieve. We showed that our methods do work by using simulations and presented the results. Based on the results, we conclude that, detection of persons using IoT technologies even in scenarios where there is lot of unregistered traffic is a worthwhile pursuit. Building a system that can report not only the number of unaccounted persons, but also their last known location is possible. Automatic reconciliation methods that these techniques can support can save both money and lives.

Future direction of this effort is very clear. These methods become part of an overall IoT based evacuation assistance system that is in the process of being implemented. Once the rest of the system gets proven out on simulated data in the lab, real data sets need to be used before pursuing prototyping and beta testing. In real life scenarios, this system can be integrated with automated attendance systems to improve (and complement) the results during emergency drills and actual emergencies. Special situations such as semi-stationary devices such as WiFi capable projectors, multiple people always moving together, frequent visitors such as delivery and cleaning staff, frequent comers-goers such as smokers, need to be modeled. When the system is operating in emergency mode, current person detection techniques need to be suspended and other algorithms are needed to efficiently assist ERCs, which are also left for future work. Another direction for this effort, once proven, will be to extend the paradigm to public places by utilizing big data and cloud technologies to be utilized in major public disasters such as earth quakes or explosions.

# 6. REFERENCES


[1] Inverted index — wikipedia, the free encyclopedia, 2016.

[2] R. Brideglall. Rfid device, system and method of operation including a hybrid backscatter–based rfid tag protocol compatible with rfid, bluetooth and/or ieee 802.11 x infrastructure, 2007.

[3] S. Chauhan, P. Patel, F. C. Delicato, and S. Chaudhary. A development framework for programming cyber–physical systems. In *Proceedings of the 2nd International Workshop on Software Engineering for Smart Cyber–Physical Systems*, 2016.

[4] M. Cunche. I know your mac address: Targeted tracking of individual using wi–fi. *Journal of Computer Virology and Hacking Techniques*, 2014.

[5] S. Goel, T. Imielinski, and K. Ozbay. Ascertaining viability of wifi based vehicle–to–vehicle network for traffic information dissemination. In *Intelligent Transportation Systems, 2004. Proceedings. The 7th International IEEE Conference on*, 2004.

[6] S. Gwynne, E. Galea, M. Owen, P. J. Lawrence, and L. Filippidis. A review of the methodologies used in the computer simulation of evacuation from the built environment. *Building and environment*, 1999.

[7] N. Kar, M. K. Debbarma, A. Saha, and D. R. Pal. Study of implementing automated attendance system using face recognition technique. *International Journal of computer and communication engineering*, 2012.

[8] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall. Wi–fi backscatter: internet connectivity for rf-powered devices. *ACM SIGCOMM Computer Communication Review*, 2015.

[9] A. M. Law, W. D. Kelton, and W. D. Kelton. *Simulation modeling and analysis*. 1991.

[10] C. J. Lehtola and C. M. Brown. Emergency action plans – osha standard 1910.38.

[11] T. Lim, S. Sim, and M. Mansor. Rfid based attendance system. In *Industrial Electronics & Applications, 2009. ISIEA 2009. IEEE Symposium on*, 2009.

[12] O. Shoewu and O. Idowu. Development of attendance management system using biometrics. *The Pacific Journal of Science and Technology*, 2012.

[13] V. Tabak, B. de Vries, and J. Dijkstra. Simulation and validation of human movement in building spaces. *Environment and Planning B: Planning and Design*, 2010.

[14] T. Tsubota, A. Bhaskar, E. Chung, and R. Billot. Arterial traffic congestion analysis using bluetooth duration data. 2011.