Safe Cities. A Participatory Sensing Approach

Jaime Ballesteros, Mahmudur Rahman, Bogdan Carbunar, Naphtali Rishe
School of Computing and
Information Sciences
Florida International University
Miami, Florida 33199
Email: {jball008, mrahm004, carbunar, rishen}@cs.fiu.edu

Abstract—**Smart cities combine technology and human resources to improve the quality of life and reduce expenditures. Ensuring the safety of city residents remains one of the open problems, as standard budgetary investments fail to decrease crime levels. This work takes steps toward implementing smart, safe cities, by combining the use of personal mobile devices and social networks to make users aware of the safety of their surroundings. We propose novel metrics to define location and user based safety values. We evaluate the ability of forecasting techniques including autoregressive integrated moving average (ARIMA) and artificial neural networks (ANN) to predict future safety values. We devise iSafe, a privacy preserving algorithm for computing safety snapshots of co-located mobile device users and integrate our approach into an Android application for visualizing safety levels. We further investigate relationships between location dependent social network activity and crime levels. We evaluate our contributions using data we collected from Yelp as well as crime and census data.**

I. Introduction

Smart cities exploit synergies between their social components and technological advances to improve the quality of life of residents, while reducing expenditures. Safety is an issue of particular concern: While billions of dollars are invested annually, a significant reduction in crime levels has not been successfully achieved [1].

In this paper we use a combination of mobile technologies and online social networks to address this problem. The overarching goal of our work is to make mobile device users aware of the safety of their surroundings. Drawing inspiration from participatory sensing, our approach uses mobile devices as sensors, to gauge and share the safety level of their location.

Previous attempts of making people safety-aware include the use of social media as a means to distribute information about unreported crimes [2], or web based applications for visualizing unsafe areas [3], [4]. The main drawback of these solutions stems from the difficulty of integrating their use in the everyday life of users.

To this end, we propose a suite of techniques for defining the safety of locations and users. We first define location centric, static safety labels, based on crime levels recorded at those locations. Then, taking advantage of observed crime level periodicities, we investigate and compare the ability of auto-regressive integrated moving average (ARIMA), linear (double) exponential smoothing (LES) and artificial neural network (ANN) models to predict future location-based safety values based on the recorded crime history. To define finer grained and more accurate safety values, we exploit the insight that the safety of a user depends not only on the intrinsic history of her current location, but also on the people with whom she is currently co-located. We propose then the notion of user safety profiles, encoding the safety values of locations visited by users.

We further devise iSafe, a distributed algorithm that takes advantage of the wireless capabilities of mobile devices to compute real-time snapshots of, and aggregate the safety profiles of co-located users. Since safety profiles are sensitive information, we are particularly interested in preserving the privacy of users involved. iSafe uses secret splitting and secure, multi-party computation techniques to aggregate safety profile without learning the private information of participants.

Finally, we investigate relationships between the quality and quantity of social network user feedback and crime levels.

We have implemented iSafe as an Android application and present snapshots of its functionality. We provide extensive evaluations of our contributions using crime and census data from the Miami-Dade county (FL) as well as data we have collected from both users and participating businesses in Yelp [5], a popular geosocial network centered on user feedback.

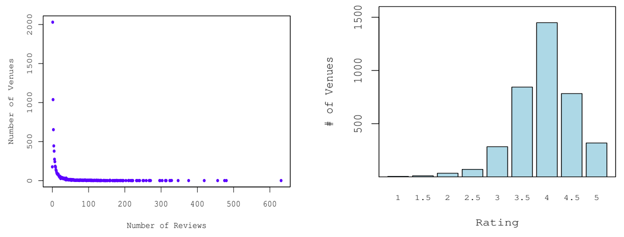
The paper is organized as follows. Section II presents the model considered as well as the datasets and tools used in this work. Section VI investigates relationships between social networks and crime levels. Section III proposes a static, location centric safety labeling technique and Section IV compares the ability of ARIMA, LES and ANN models to predict future safety values. Section V combines these contributions into iSafe. Section VIII presents evaluation results. Section IX describes related work and Section X presents our conclusions.

II. Background and Model

We begin by briefly describing the geosocial network concept and the crime and census datasets that we use in our work. Subsequently, we describe our system model and detail several forecasting tools we use.

A. Geosocial Networks

Geosocial networks (GSNs) such as Yelp and Foursquare extend classic social networks with the notions of (i) venues, or businesses and (ii) *check-ins*. That is, besides user accounts, GSNs provide also accounts for businesses (e.g., restaurants, yoga classes, towing companies, etc). Users then employ



(a) (b)

Fig. 1. Statistics of Miami venues: (a) Distribution of number of reviews per venue. (b) Distribution of venue ratings. Venues recording less than 4 reviews were filtered out.

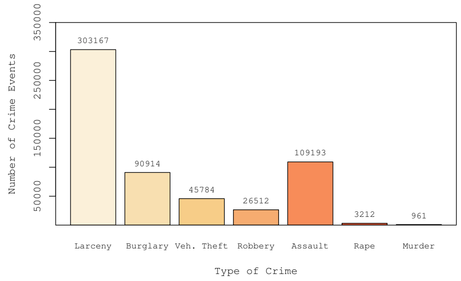


Fig. 2. Outcome of DT classifier – statistics of crime in Miami-Dade county. Distribution of number of crime events per type of crime.

check-ins to report their location, in terms of their presence at one of the venues supported by the GSN. Users can share check-in information with friends and also use it to achieve special status (badges, mayorships) and receive frequent customer discounts from participating venues. In addition, geosocial networks encourage and reward user feedback, in the form of ratings and reviews, left for visited venues. Users ratings range from 1 to 5 stars and are aggregated to produce an overall venue rating.

Figure 1(a) shows the distribution of the number of reviews left for a venue, with a logarithmic y scale. It shows a long tail distribution, with around 2000 venues having 1 review but only 1000 venues having 2 reviews. We emphasize the low number of venues without reviews - only 177. Figure 1(b) shows the distribution of the number of venues with an aggregated rating ranging between 1 and 5. As expected, it shows that Yelp reviews are mostly positive: most aggregate ratings are at or above 4 stars.

B. Crime Data

We use a historical database of more than 2.3 million crime incidents reported in the Miami Dade county area since 2007 [6]. Each record is labeled with a crime type (e.g., homicide, larceny, robbery, etc), the time and the geographic location where it has occurred. We briefly document two problems we encountered when pre-processing this data. First, since records come from different Police departments, the crime type labels are non-uniform, (e.g., *murder* in Miami Beach vs. *homicide* in North Miami). Second, crime reports include many minor incidents (e.g., fire alarms issues), resulting in over 140 different crime types.

In order to standardize and eliminate ambiguities, we mapped crimes into 7 categories: Murder, Forcible Rape, Aggravated Assault, Robbery, Larceny/Theft, Burglary/Arson, Motor Vehicle Theft. We removed minor crime reports that did not fall into these categories. Due to the large number of records in the database, manual mapping was infeasible. Instead, we have experimented with two machine learning techniques for classifying each record: the Naive-Bayes (NB) classifier and the Decision Trees (DT) classifier [7]. In order to build our training and test sets, we manually annotated a random sample of 2000 records from different police departments. Then, we split this subset of records into training and test datasets, each containing 1000 records. We built our classifiers using the NLTK library [8]. The accuracy was measured using a simple metric that measures the percentage of inputs in the test set that the classifier correctly labeled. For instance, a crime type classifier that predicts the correct crime type 60 times in a test dataset containing 100 crime types, would have an accuracy of 60%. On our crime dataset, the NB classifier achieved an accuracy of 91% and the DT classifier an accuracy of 98%. Thus, we have used the outcome of the DT classifier. Figure 2 shows the crime set's distribution of the crime categories following the DT classification.

In the following, let c denotes the number of crime types. In our case, c = 7. Let $\bar{CT} = \{CT_1, .., CT_c\}$ denote the ordered set of crime types.

We also used Census data sets [9], reporting population counts and demographic information. The data is divided into geographical extents e.g. polygons, called *census block groups*. Each block contains information about the population within (e.g., population count, various statistics). According to the data, Miami Dade county has a population of $2,496,435$.

C. System Model

We assume users own mobile devices equipped with wireless interfaces, enabling the formation of transient, ad hoc connections with neighboring devices. Devices also have Internet connectivity, which, for the purpose of this work may be intermittent. Users may take advantage of Internet connectivity to report to geosocial networks as well as to retrieve crime information (both described in the following). Each user is required to install an application on her mobile device, which we henceforth denote as the *client*.

Besides a client application, the framework we propose also consists of a service provider that centralizes crime and census information and provides it upon request to clients. In the following, we denote the service provider by S.

D. Forecasting Tools

We briefly describe several time series forecasting tools.

ARIMA Model. ARIMA models have been successfully used in forecasting time series in a variety of domains, including economics, marketing and sales, power systems, social problems, etc. ARIMA incorporates autoregressive (p),integration(d) and moving average terms(q) to provide higher fitting and forecasting accuracy. ARIMA uses the input data to determine the appropriate model form. The ARIMA forecasting procedure consists of four steps [10], (1) identifying the ARIMA(p, d, q) structure, (2) estimating the unknown parameters, (3) fitting tests on the estimated residuals and (4) forecasting future outcomes based on the historical data.

The formulation of the ARIMA model depends on the characteristics of the series. Generally, it is originated from the autoregressive model AR (p), the moving average model MA (q) and the combination of AR (p) and MA (q), the ARMA (p, q) model [11]. Like most time series, ours is non-stationary. Hence we cannot apply stationary ARIMA processes directly. One way of handling non-stationary series is to apply *differencing* (d) so as to make them stationary. Then, to find the best ARIMA model, we used the autocorrelation (ACF) and partial autocorrelation (PACF) functions for preliminary estimations of the AR(p) and MA(q) components. The ACF function is a set of correlation coefficients between the series and lags of itself over time while the PACF function is the partial correlation coefficients between the series and lags of itself over time. We use the Corrected Akaike Information Criterion (AICc) [10] as the primary criterion in selecting the orders of a fitted ARIMA model which acts as an estimator of the expected discrepancy between the true model and a fitted candidate model. We choose the ARIMA model that has the minimum AICs value. We use T-statistics with 95% confidence interval to test the significance of the parameters in the fitted ARIMA model.

Linear (Double) Exponential Smoothing (LES) Model. Brown's linear (double) exponential smoothing [12] includes trend variations of the time series without a significant seasonal component. The process is controlled by a smoothing parameter α whose value ranges between 0 and 1. α decides the weight placed on the most recent observations during the forecast process. We determine the value of α by minimizing the root mean squared error(RMSE) [13] (see below) from one step-ahead forecasts and repeating the process for all forecast values.

Artificial Neural Network (ANN). ANNs are data-driven self-adaptive methods that learn and generalize from experience and capture subtle functional relationships among the empirical data even if the inherent relationships are unknown or difficult to describe. In this paper we focus on the multilayer perceptrons (MLP) ANN model, which is particularly suitable for forecasting, due to its ability for input-output mapping.

The ANN we consider consists of an input layer (of the same size as the input vector), two layers of hidden nodes and an output layer providing the forecast value. Two hidden layers are sufficient to learn any complex nonlinear function [14]. Before the training phase, we normalize the input data to a $(-1, 1)$ range; following the prediction step we map the output back to the initial range. For the training phase we use a multilayer feedforward network trained using back propagation and the Levenberg-Marquardt algorithm to perform function fitting (nonlinear regression). We have split the data into training and test vector sets.

Crime Type	Weight
Assault	0.176
Robbery	0.180
Rape	0.307
Homicide	0.336

TABLE I
CRIME WEIGHT ASSIGNMENT USING THE FCPC.

Error Measurement. We use the root mean squared error (RMSE) and mean absolute percent error (MAPE) [13] as error measurements to evaluate the accuracy of different models. MAPE can be easily affected by the magnitude of series but it does provide information about the relative magnitude of the forecast error. On the other hand, RMSE is a more objective measure in absolute magnitude. Thus, in our evaluation, the RMSE is used as the primary and MAPE as the secondary accuracy measure.

III. LOCATION BASED SAFETY

We take advantage of the crime dataset to define the notion of safety as it relates to location. We use the census blocks to divide space, and assign each a *safety index*.

Block Safety Index. For a census block B and time interval ΔT, let $C(B, \Delta T)$ denote a c-dimensional vector, where the i-th entry denotes the number of crimes of type $CT[i]$ recorded in block B during interval ΔT. Let $\bar{W}$ denote a c-dimensional vector of weights – each type of crime has a weight proportional to its seriousness (defined shortly). Let $BC(\Delta T)$ denote the population count recorded for block B. Then, we define the *crime index* of block B during interval ΔT as

$$CI(B, \Delta T) = min\{C(B, \Delta T)\bar{W}/BC(\Delta T), 1\} \qquad (1)$$

where $C(B, \Delta T)\bar{W}$ denotes the vectorial product of the number of crimes per type and the crime weights. That is, B's crime index is the per-capita weighted average of crimes recorded during time interval ΔT. The safety index SI of block B during interval ΔT is then defined as

$$SI(B, \Delta T) = 1 - CI(B, \Delta T) \qquad (2)$$

Note that the CI and SI metrics both take values in the [0, 1] interval. Higher values of $SI(B, \Delta T)$ denote safer blocks.

Crime Weight Assignment. We propose a weight assignment approach where each crime is assigned a weight proportional to its seriousness, as defined in the criminal punishment code, i.e., the Florida Criminal Punishment Code (FCPC) [15]. The FCPC is divided into *levels* ranging 1-10, and each level L_k contains different types of felonies. The higher the level, the more serious is the felony. Also, each felony has a *degree*, (i.e., capital, life, first, second and third degree, sorted in decreasing order of seriousness), with an associated punishment (years of imprisonment) [16].

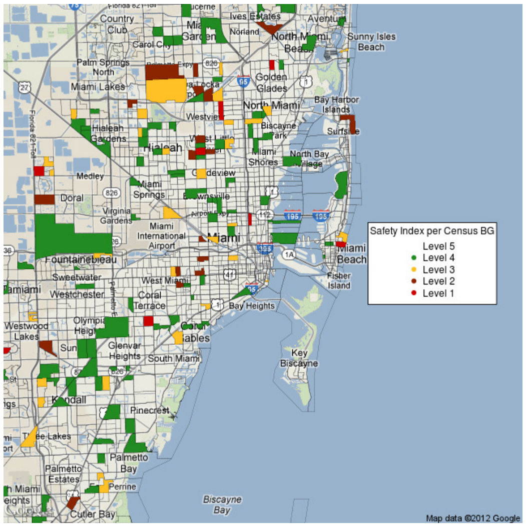


Fig. 3. Safety Index in Miami-Dade county: $SI(B, \Delta T)$ values are mapped into Safety Levels. The higher the level, the safer the Block

Let L_k denote the set of felonies within level k and let P_k denote the set of corresponding punishments. Let $l_k = |L_k|$ denote the number of felonies within level k. Then, we define the weight of crime type $CT[i]$, $\bar{w}_i$, as

$$\bar{w}_i = \sum_{k=1}^{10} \rho_k \sum_{j=1}^{l_k} P_k[j], \; where \; CT[i] \in L_k[j],$$

where $\rho_k = k/\sum k$ is the weight assigned to level k (normalized to the number of levels). The weight of crime type $CT[i]$ is the weighted sum of the per-level sum of the punishment values ($P_k[j]$) associated with each occurrence of $CT[i]$ within the felonies of level k.

For instance, consider the impact of level L_8 on the weight of the "Robbery" crime. L_8 has 51 types of felonies, so $l_8 = 51$. Out of those 51 felonies, two are related to "Robbery" : $L_8[23]$ is "Robbery with a weapon" and $L_8[24]$ is "Home-invasion robbery". Both of them are first degree felonies, therefore punishable with up to 30 years of imprisonment. Thus, the contribution of level 8 to the weight of "Robbery" is $8/55 \times 2 \times 30$.

Table I shows the resulting normalized weights.

Illustration. We use the Miami-Dade crime set to illustrate the geographic distribution of block-level safety index information, where ΔT consists of the year 2010. We use the census dataset to extract the population count $BC(\Delta T)$. Figure 3 shows the color-coded safety index for each block group in the Miami-Dade county (FL) where crimes have been reported during 2010. The safety index considers crimes against person only. Blocks without color have a very low reported crime level. Green blocks denote safer locations while darker yellow and red blocks denote areas with more reported crimes.

Answering Safety Queries. Crime and census data are stored by the service provider S. In order to provide safety information to the user efficiently, S indexes blocks using an R-Tree [17] spatial data structure, that enables the fast retrieval of SI values. A safety query made by a client consists of a point p in the space, e.g, two geographical coordinates, and queries the R-Tree structure using a best-first traversal approach [18]. Once the corresponding block is found, S returns the SI value to the client.

IV. Predicting Safety

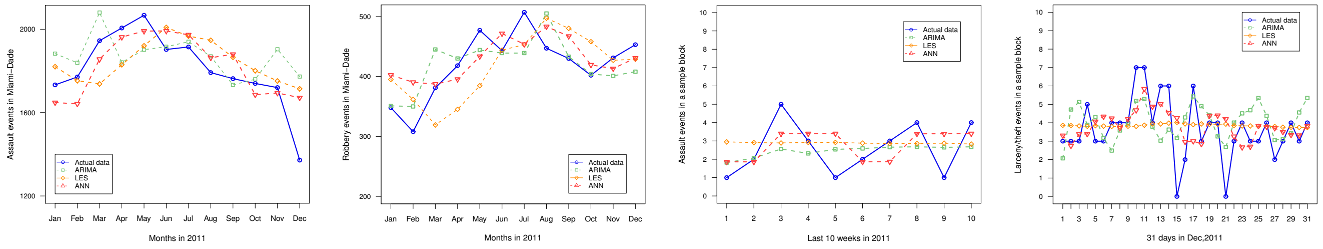
The static crime index does not take into consideration seasonal, weekly or even daily fluctuations. As such, a static safety index may include unnecessary errors – e.g., higher number of crimes in a past August may introduce inaccuracies in the crime index considered in the current month of April. In this section we address this issue. We explore the performance of the time series forecasting techniques discussed in Section II-D in predicting the number of crimes to occur at a location during the near future, based on the recorded history.

We used the R statistical software package [19] to generate the ARIMA model and MATLAB toolboxes [20] for LES and ANN models. In the following, we analyze separately three crime types, aggravated assault, robbery and larceny/theft that make up for more than 75% of the total amount of crimes. As we show later in this section, predicting categorized event counts enables the prediction of future safety values.

In the first two experiments, we used crime data recorded between 2007 and 2010 to predict per-month categorized event counts for the year 2011, for the entire Miami-Dade county. Figure 4(a) compares the predictions for the number of assaults made by ARIMA, LES and ANN against the recorded values. Table II shows the RMSE and MAPE values for the three methods. All three models correctly predict the downward trend from May until December, with ANN achieving a slightly better accuracy than LES and ANN. Figure 4(b) shows a similar plot for robberies. While all models accurately predict the initial increase followed by a slight decrease in the number of robberies, ARIMA and ANN outperform the LES model, as also shown by the RSME and MAPE values (see Table II). ARIMA slightly outperforms ANN.

We focus then on finer grained spatial and temporal predictions: per-block, weekly events. For ANN, we partition the input data into 95 training vectors and 10 test vectors. Figure 4(c) compares the recorded data against the ARIMA, LES and ANN predictions of assault events in the last ten weeks of 2011, for one block in the Miami-Dade county. We emphasize the accuracy of the prediction (see Table II), which is similar for ANN and ARIMA. Finally, we focus on daily crime predictions. For the same block used in the previous experiment, using a time window of events recorded between Jan 1, 2010 and Nov 30, 2011, we predict the 31 days of December 2011. Fig 4(d) shows the comparison between the recorded data and the ARIMA, LES and ANN forecast, for the daily number of larceny/theft events. ANN slightly outperforms ARIMA and LES, but all models exhibit good accuracy - except for the unexpected zero crime incidents observed during a couple of days.

Predicting the Safety Index. At the beginning of each day (i.e., at midnight), for each block B we compute predictions for each type of crime. This enables us to construct the



(a) (b) (c) (d)

Fig. 4. Crime Forecasting Experiments in Miami-Dade: (a) Prediction of assaults, 2011 monthly basis. (b) Prediction of robberies, 2011 monthly basis. (c) Prediction of assaults in a given block for the last 10 weeks of 2011. (d) Prediction of larcenies in a given block for the last 31 days of 2011.

predicted version of the vector $C(B, \Delta T)$, which we denote by $PC(B, \Delta T)$. ΔT is now defined as the next 24 hours. We then define the predicted safety index:

$$PSI(B, \Delta T) = 1 - min\{PC(B, \Delta T)\bar{W}/BC(\Delta T), 1\} \quad (3)$$

V. iSafe: Context-Aware Safety

When the number of recorded events is low, accurately predicting values within a short time interval is difficult - the difference between 0 and 1 is significant, as the safety of a block is greatly influenced by a single homicide. In this section we propose to address this issue, by exploiting the intuition that the safety of a place depends not only on its history but also on the people currently located at that place. We take advantage of the wireless communication capabilities of most mobile devices (e.g., smartphones, tablets), which allow them to form short lived, ad hoc communities.

Our approach is the following. First, we assign each user a static safety index, based on the locations she has visited. We then aggregate the safety index values of co-located users, to obtain an overall sense of the present company. Since such values are sensitive information (may be unflattering, or may even leak the locations visited by the user), we introduce iSafe, a distributed algorithm that allows the aggregation of safety index values while preserving the privacy of involved participants. iSafe combines this information with the predicted safety of the user's current location to construct an overall safety value.

A. User Safety Profiles

We extend the safety index definition from locations to users. We define here the safety profile of a user as an aggregate of the safety values of locations visited by the user. We assume a user device can capture the user's location, e.g., using GPS, a combination of celltower and Wi-Fi access point localization techniques or simply using check-in information available from geosocial networks.

Let $H_U = \{[B_i, T_i] | i = 1..h\}$ denote the location history of user U, consisting of recorded [block, time] pairs. That is, we assume a block level localization precision. We then define the safety profile of user U, SP_U, as the average over the safety indexes of all the blocks visited by the user:

$$SP_U = (\sum_{i=1}^{h} SI_{B_i})/h \quad (4)$$

The intuition is that the safety of a user is a function of the safety of all the places the user visits. If the location sampling process is done periodically, the formula naturally ensures that blocks where the user spends more time have more impact on the user's safety index. Moreover, to prevent users who work in unsafe areas (e.g., law enforcement officers, social workers, etc) from having low safety indexes, the safety profile of a user should not be computed over locations where the user is working.

B. Putting it All Together

The client running on the wireless-enabled mobile device of a user U contacts the service provider S, storing the crime and Census datasets. U retrieves (potentially privately, using a private information retrieval technique [21]) the predicted safety index of the block B where U is located. The value PSI_B is defined according to Equation 3. Subsequently, U sets up ad hoc connections with co-located users. It then retrieves their safety profiles and computes an aggregated value - the user's safety index in real time. We define the safety index of U within a block B, $SI_U(B)$, to be

$$SI_U(B) = \alpha(\sum_{i=1}^{k} SP_{U_i})/k + (1 - \alpha)PSI_B \quad (5)$$

where $U_1, .., U_k$ are the co-located users, SP_{U_i} is the safety profile of user U_i, defined according to Equation 4 and $\alpha \in [0, 1]$ is a weight. The value of α is a function of the number of co-located users as well as the amount of crime history for B: When one component is likely to be inaccurate, its weight will be low.

C. iSafe

We use a multi-party, secure function evaluation to allow k users to combine their aggregate safety indexes, without allowing any participant to learn somebody else's safety index.

Model	Fig. 4(a)		Fig. 4(b)		Fig. 4(c)		Fig. 4(d)	
	RMSE	MAPE	RMSE	MAPE	RMSE	MAPE	RMSE	MAPE
ARIMA	158.80	6.42	38.77	7.08	1.27	43	1.57	34.52
LES	151.03	6.79	53.57	11.89	1.41	42.08	1.61	30.07
ANN	116.48	5.32	40.44	8.23	1.3	35.72	1.49	27.02

TABLE II
ERROR MEASUREMENT DATA.

Algorithm 1: iSafe pseudocode.

```
1.  Object implementation iSafe;
2.  neighbor[] N;                 #set of neighbors
3.  double SP;                    #safety profile
4.  string R;                     #random value
5.  string[] shares;              #set of shares
6.  string[] NShares;             #shares of neighbors
7.  Operation computeSI()
8.      N := discoverNeighbors();
9.      B := getCurrentBlock();
10.     R := getRandom();
11.     shares := split(R, |N|);
12.     for i := 1 to |N| do
13.         send(N[i], shares[i]); od
14.     getNeighborShare(NShares);
15.     int order := electLeaderOrder();
16.     int S := 0; int count := 0;
17.     while (count < |N|) do
18.         count := count + 1;
19.         if (count = order) then
20.             S := S + SP + R;
21.             for i := 1 to |N| do S := S − NShares[i]; od
22.             mcast(S);
23.         else S := recv(); fi
24.     od
25.     double SI := $\alpha$S/|N| + (1 − $\alpha$)S.getSI(B);
26      return SI;
27. end
```

Algorithm 1 shows the pseudocode of iSafe. iSafe achieves privacy through the use of secret splitting. Each client generates a random value (line 10) and splits it into shares – one for each neighbor. That is, if the random value is R, the shares $sh_1, .., sh_k$ are generated randomly such that $\sum_{i=1}^{k} sh_i = R$. The client sends each share to one neighbor (lines 12-13) and receives a share from each neighbor (line 14). The clients engage in a leader election/order selection distributed algorithm (line 15), where each client is assigned a unique identifier, between 1 and k. When a client's turn comes, according to the order established, it adds the safety profile of its user and its random value R to the overall sum (S), (line 20), subtracts all the shares of secrets of its neighbors (line 21) and sends a multicast of the result (line 22). Otherwise, each client blocks to receive the multicast values of its neighbors (line 23). At the end of the process, the client combines the result, averaged over the number of its neighbors, with the safety index of its current location, retrieved for its current block B from the service provider S (line 25).

D. Analysis

We now prove the following result.

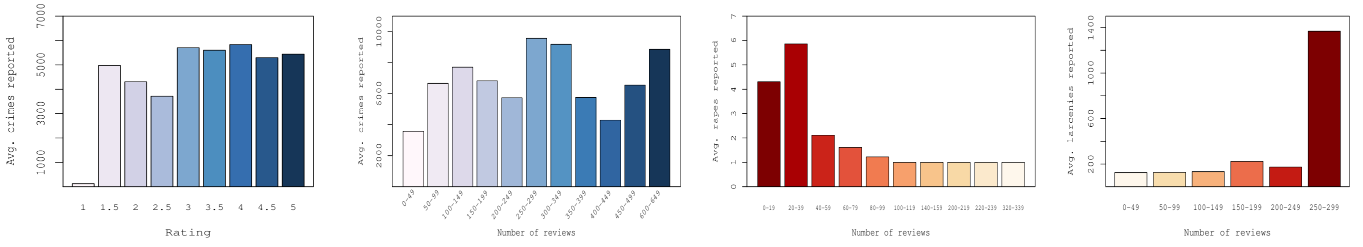
Theorem 1: An adversary $\mathcal{A}$ controlling c out of k participants in the iSafe algorithm, can only find the sum of the SP values of the remaining $k - c$ honest participants.

Proof: Secret splitting is information theoretical secure: Without knowing *all* the shares of a secret, no information can be inferred about the secret. The adversary $\mathcal{A}$ has access to all intermediate values multicast in Algorithm 1, as well as c shares of the secret of each of the remaining $k - c$ honest participants. Let R_i denotes the random value of the i-th (honest) participant and let $s_{1i}, s_{2i}, .., s_{ki}$ be the shares received by that participant from all the other participants. Then, the sum $R_i + s_{1i} + s_{2i} + .. + s_{ki}$ is random and cannot be predicted by $\mathcal{A}$: $\mathcal{A}$ only controls c shares of R_i (out of $k - 1$ shares), but not R_i, thus the other $k - c$ values in the sum are random and not under the control of $\mathcal{A}$. Thus, $\mathcal{A}$ cannot infer the SP_i by looking at the value of S before and after R_i's multicast. Moreover, at the end of the protocol, the combination of the random values and shares controlled by $\mathcal{A}$ is the inverse of the combination of the random values and shares controlled by the honest participants. Thus, the statement of the theorem follows. ■

VI. SOCIAL NETWORKS AND CRIME

Finally, in an effort to define the safety of a location, we study the relationship between data collected from social networks and crime. To achieve this, we rely on the user feedback data we collected from Yelp and on the crime dataset. One initial hypothesis was that venues with many positive reviews are located in safer areas. To test this hypothesis, for each venue in Miami-Dade, we used the Yelp provided street address, geocoded it to GPS coordinates, and collected the number of crimes within an area of 200m (standard size of a neighborhood block in the United States). Figure 5(a) plots the dependency between venue rating values (average over all user feedback) and total crime levels, over all venues and crimes in Miami-Dade. Figure 5(b) plots the dependency between the total number of reviews, grouped in buckets of 50 (e.g., 0-49), received by a venue, and total crime levels, also for the Miami-Dade county. Our results were negative. Rating and review counts have no relation with total crime levels: 5 star and 2 star venues as well as venues with 500 and with 100 reviews had similar crime counts in their vicinity.

We then studied a specialized view of this data - the relationship between review counts and crime types (see Section II-B). One finding is depicted in Figure 5(c), showing the relationship between reported rapes and review counts: rapes occur more frequently in places with low number of reviews. Furthermore, we have studied the relation between crime types and number of reviews received from visitors vs. locals. This information is publicly available, as Yelp users need to



(a) (b) (c) (d)

Fig. 5. Statistics of Miami venues: (a) Average number of crimes per rating. (b) Average number of crimes per number of reviews. (c) Number of rapes per number of venue's reviews. Locals and visitors. (d) Number of larcenies/thefts per number of venue's reviews. Local users only.

specify a home city/state. Figure 5(d) shows that the number of larcenies is high around venues with many local reviews. A potential explanation is that local yelpers (Yelp users) are more likely to choose venues in good neighborhoods, and good neighborhoods are more likely to attract thieves.

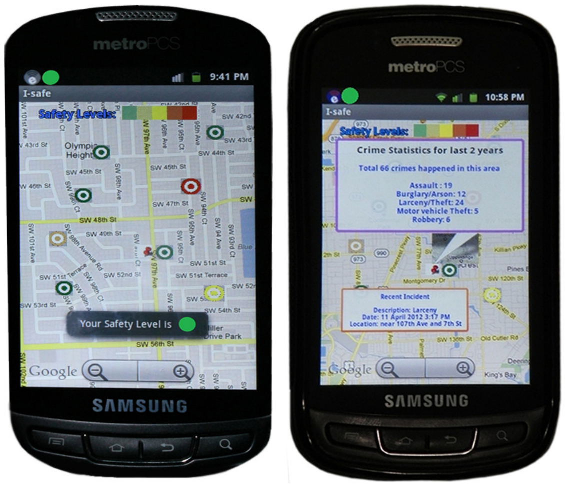
VII. Attacks and Defenses

Safety profiles of co-located users are aggregated to obtain a safety image of locations. Since that image impacts user decisions, it can become the target of malicious attacks. For instance, malicious users may attempt to incorrectly (i) improve the safety of desired locations, for instance to attract unsuspecting users to unsafe locations or to (ii) decrease the safety image of target locations. We now describe several mechanisms that could be exploited to perform these attacks, and suggest defenses.

Reporting incorrect locations. Malicious users may report incorrect locations, corresponding to safe areas. Even with GPS verification mechanisms in place, committing location fraud has been largely simplified by the recent emergence of specialized applications for the most popular mobile ecosystems (LocationSpoofer [22] for iPhone and GPSCheat [23] for Android). To prevent this attack, location verification mechanisms can be used [24], [25], [26]. For instance, in previous work [24], one of the authors has developed venue-centric location verification techniques, that rely on devices installed by venue owners within their venues. In the scenario considered in this paper, the owners' incentive for participation is to prevent the tampering of the safety image of their neighborhood.

Turning off devices in bad areas. Users could turn off their iSafe application when entering bad areas. While we cannot prevent this behavior, we propose two solutions to alleviate this problem. In the first solution, we use rewards and game mechanics to encourage people to report as many locations as possible. For instance, users gain points for each reported location, perhaps more for the occasional unsafe location. Points are used to acquire badges, similar in principle to those used by mobile social networks like Foursquare [27] or Yelp [5].

In the second solution, iSafe keeps track of the user's battery level and cellular signal strength. Furthermore, iSafe periodically persists the current time stamp. If the last committed time stamp is more than one period behind the current one, iSafe detects an *offline* interval. With the exception of the user entering into a blind coverage spot (including underground transportation) or running out of battery power, iSafe penalizes the user's safety profile with an amount proportional to the length of the offline interval.



Your Safety Level is

Crime Statistics for last 2 years

Total 66 crimes happened in this area

Assault : 19
Burglary/Arson: 12
Larceny/Theft: 24
Motor vehicle Theft: 5
Robbery: 6

Recent Incident

Description: Larceny
Date: 11 April 2012 3:17 PM
Location: near 107th Ave and 7th St

(a) (b)

Fig. 6. Snapshots of iSafe on Android.

VIII. Experiments

iSafe Implementation. We have implemented the location centric static safety labeling component of iSafe using Android. We used a Samsung Admire smartphone running Android OS Gingerbread 2.3 with an 800MHz CPU as the testing platform. We used the Android Maps API to facilitate the location based service employed by our approach. We represent safety using five color labels ranging from green (safe) to red (unsafe). iSafe retrieves the current geo-location of the user, then computes and displays the safety labels of the current location and of surrounding blocks. A separate service runs in the background, displaying in the status bar of the Android device, the safety color label of the user's current location. Figures 6(a) and 6(b) show snapshots of iSafe's functionality.

Safety profiles for Yelpers. We have collected public information from the accounts of 2025 Yelp users, all residents of the

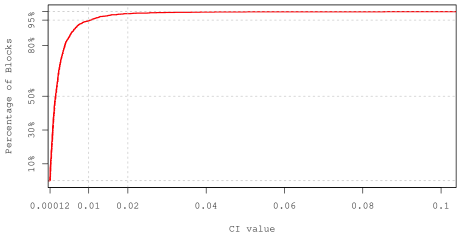


Fig. 7. Safety index values: Distribution of CI values (Crime Index) on blocks in Miami-Dade County.

Miami-Dade county. The information collected for each user includes the number of reviews, the venues reviewed, existing check-ins at any venues, and the date when each review and check-in was recorded. We build the crime index, CI, value for each Census block from the Miami-Dade county in 2010. Figure 7 shows the cumulative distribution function of the CI values (Figure 3 shows their spatial distribution). It shows that for the Miami-Dade county, most blocks experience relatively low levels of crime per-capita: 50% of blocks have a CI value smaller than 0.0015 and only 5% of blocks have CI values exceeding 0.01.

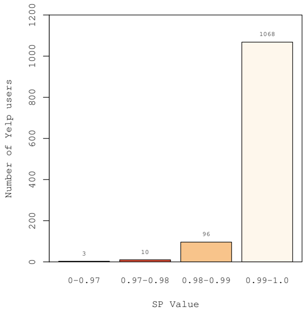


Fig. 8. Distribution of SP values of Yelp users.

Given the CI values of the blocks containing the venues visited (reviewed or subject of a check-in) by a yelper (Yelp user), we compute the user's SP value, as defined by Equation 4. Out of the 2025 collected yelpers, 1194 had written reviews in 2010. Figure 8 shows the distribution of SP values of these 1194 yelpers. It shows that most Miami-Dade county yelpers are safe: all have an SP value larger than 0.96 (1 is the maximum value), with 90% of them having an SP that exceeds 0.99. This shows that local yelpers are capable of visiting (or reviewing) mostly venues in areas with low numbers of crimes per-capita.

We further compare the evolution in time of the safety index SI_B of a block B with the average of the SP values of yelpers that visited B (and left feedback). From Section V we note that these two metrics are the building blocks of Equation 5. To this end, based on the crime database, for each month we calculate the SI values of all the blocks in the Miami-Dade county. Then, for each block B we calculate the monthly average of SP values of yelpers that visited B. Figure 9 shows the monthly evolution of the SI_B value of a Miami-Dade block and the average SP value of the 339 Yelp users that visited the block during 2010. It shows that for this block, the two components of Equation 5 have similar values, thus will have a similar impact on a user's safety.

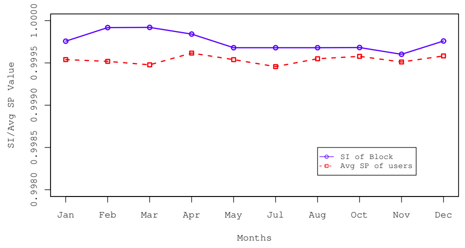


Fig. 9. SI value of a Miami-Dade block and the average of SP values of Yelp users that visited the block w.r.t time.

IX. Related Work

Smart cities have been the focus of recent efforts at IBM [28] and several academic research groups at MIT [29] and UCLA [30]. Caragliu et. al. [31] present a study on the factors that determine the performance of a "smart city". They focus specifically on European cities by analyzing urban environments, levels of education and different accessibility modalities that are positively correlated with urban wealth. Since one important aspect of smart cities is safety, Patton [32] emphasizes the use of audio sensors and cameras that allow authorities to quickly respond in an emergency event without receiving a 911 call. We note that we consider a different angle: making users aware of their surroundings.

Furtado et. al. [2] propose the use of social media in a collaborative effort to inform people about crime events that are not reported to police. Their wiki website spots areas on the map where participant users have reported crime events. Police departments also release tools to make citizens aware of their safety, e.g., the Miami-Dade police department, deployed an web application [33] that identifies crime areas based on current crime reports. We note however that our solution seamlessly integrates context and time sensitive safety metrics into the everyday user experience.

Participatory sensing is receiving increasing attention due to the popularity of mobile devices. The multimodal sensing capabilities of devices enable a broad range of applications that leverage collected data from participants, sensed from their surroundings. Estrin [34] discuss advantages of participatory sensing in health and transportation and provide insights on the architecture of participatory sensing applications. Thiagarajan et. al. [35] propose cooperative transit tracking using mobile phones. Privacy becomes a serious concern when the user personal information may be compromised. Christin et. al. [36] present a survey on the efforts made to preserve privacy in participatory sensing systems. In contrast, our work does not collect user information, but instead allows devices to aggregate information collected from co-located users without learning personal information.

Dynamic safety practices leveraging social networks and GPS mobile phones have been introduced in [37] to create a system for personalized safety awareness. The system exploits sensors available in mobile phones to enhance the personal safety of users by aggregating community. Our work is different in that we predict future crime levels, define a safety index that includes the impact of crimes on locations and on the profiles of users and propose a distributed algorithm that privately aggregates safety indexes of co-located users.

The problem of crime prediction has been explored in several contexts. Hotspot mapping [38] is a popular analytical technique used by law enforcement agencies to identify future patterns in concentrated crime areas. Different methods and techniques have been analyzed to review the utility of hotspot mapping in [39], [40], [41], [42]. Hot spot analysis however, often lacks a systematic approach, as it depends on human intuition and visual inspection.

A variety of univariate and multivariate methods have been used to predict crime. Univariate methods range from simple random walk [43] to more sophisticated models like exponential smoothing. While exponential smoothing offers greater accuracy to forecast "small to medium-level" changes in crime [44], we have shown that ARIMA and ANN models outperformed it on our data. In [45], Ediger et al. show the effectiveness and reliability of ARIMA and SARIMA models in predicting the total primary energy demand of Turkey from 2005 to 2020. Olligschlaeger [46] showed that ANNs were able to predict drug markets. We note that the goal of our work is not intrinsically crime forecasting. Instead, we incorporate crime forecasting techniques into our safety metrics, in an attempt to provide to participating users a dynamic framework for safety awareness.

X. Conclusion

In this paper we have proposed several techniques for evaluating the safety of users based on their spatial and temporal dimensions. We have shown that data collected by geosocial networks bears relations with crimes. We have proposed a holistic approach toward evaluating the safety of a user, that combines the predicted safety of the user's location with the aggregated safety of the people co-located with the user.

XI. Acknowledgments

We thank Melissa Ballesteros for her help with the graphics. This research was supported in part by NSF grants CNS-0821345, CNS-1126619, HRD-0833093, IIP-0829576, CNS-1057661, IIS-1052625, CNS-0959985, OISE-1157372, IIP-1237818, IIP-1215201, IIP-1230661, IIP-1026265, IIP-1058606, and IIS-1213026.

References

[1] Justice Policy Institute. Fact Sheet on The Obama Administrations 2011 Budget: More Policing, Prisons, and Punitive Policies. http://www.justicepolicy.org/research/1923, February 2010.

[2] Vasco Furtado, Leonardo Ayres, Marcos de Oliveira, Eurico Vasconcelos, Carlos Caminha, Johnatas DOrleans, and Mairon Belchior. Collective intelligence in law enforcement the wikicrimes system. *Information Sciences*, 180(1):4 – 17, 2010.

[3] James Cridland. Mapping the riots. http://james.cridland.net/blog/mapping-the-riots/.

[4] The Guardian. Uk riots: every verified incident. http://www.guardian.co.uk/news/datablog/2011/aug/09/uk-riots-incident-listed-mapped.

[5] Yelp. http://www.yelp.com.

[6] Terrafly Project. Crimes and Incidents Reported by Miami-Dade County and Municipal Police Departments. http://vn4.cs.fiu.edu/cgi-bin/arquery.cgi?lat=25.81&long=-80.12&category=crime_dade.

[7] Pang-Ning Tan, Michael Steinbach, and Vipin Kumar. *Introduction to Data Mining*. Addison Wesley, 1 edition, May 2005.

[8] NLTK Project. Natural Language Toolkit. http://nltk.org/.

[9] United States Census. 2010 census. http://2010.census.gov/2010census/, 2010.

[10] Fang-Mei Tseng and Gwo-Hshiung Tzeng. A fuzzy seasonal arima model for forecasting. *Security Journal*, 126:367 – 376, 2002.

[11] George E.P. Box, Gwilym M. Jenkins, and Gregory C. Reinsel. *Time series analysis forecasting and control*. John Wiley and sons, 1994.

[12] Robert F. Nau. Decision 411 forecasting. http://www.duke.edu/ rnau/411avg.htm.

[13] H.Brian Hwarng and H.T Ang. A simple neural network for arma(p,q) time series. *Omega*, 29(4):319 – 333, 2001.

[14] Jonathan J. Corcoran, Ian D. Wilson, and J.Andrew Ware. Predicting the geo-temporal variations of crime and disorder. *International Journal of Forecasting*, 19(4):623 – 634, 2003.

[15] Florida Department of Corrections. Florida criminal punishment code. http://www.dc.state.fl.us/pub/sen_cpcm/cpc_manual.pdf.

[16] Richard Hornsby. Florida criminal penalty chart. http://www.richardhornsby.com/criminal/penalties/.

[17] Antonin Guttman. R-trees: a dynamic index structure for spatial searching. In *Proceedings of ACM SIGMOD*, 1984.

[18] Gisli R. Hjaltason and Hanan Samet. Distance browsing in spatial databases. *ACM Transactions on Database Systems (TODS)*, 24(2):265–318, 1999.

[19] R Development Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria, 2011. ISBN 3-900051-07-0.

[20] MATLAB. *version 7.10.0 (R2010a)*. The MathWorks Inc., Natick, Massachusetts, 2010.

[21] William I. Gasarch. A survey on private information retrieval (column: Computational complexity). *Bulletin of the EATCS*, 82:72–107, 2004.

[22] Big Boss. Location spoofer. http://goo.gl/59HMk, 2011.

[23] Gpscheat! http://www.gpscheat.com/.

[24] Bogdan Carbunar and Rahul Potharaju. You unlocked the Mt. Everest Badge on Foursquare! Countering Location Fraud in GeoSocial Networks. In *To appear in Proceedings of the 9th IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS)*, 2012.

[25] Stefan Saroiu and Alec Wolman. Enabling New Mobile Applications with Location Proofs. In *Proceedings of HotMobile*, 2009.

[26] Z. Zhu and G. Cao. APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services. In *Proceedings of IEEE INFOCOM*, 2011.

[27] Foursquare. https://foursquare.com/.

[28] IBM. Ibm smarter cities. http://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/index.html.

[29] MIT Media Lab. Smart cities. http://cities.media.mit.edu/.

[30] Urban Sensing CENS UCLA. Walkability project. http://urban.cens.ucla.edu/projects/walkability/.

[31] A. Caragliu, C. Del Bo, and P. Nijkamp. Smart cities in europe. Serie Research Memoranda 0048, VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics, 2009.

[32] Z. Patton. Sensors make cities smarter. http://www.governing.com/topics/public-justice-safety/Sensors-Make-Cities-Smarter.html, April 2010.

[33] Miami-Dade Police Department. Crimeview community. http://crimemaps.miamidade.gov.

[34] Deborah L. Estrin. Participatory sensing: applications and architecture. In *Proceedings of the 8th international conference on Mobile systems, applications, and services*, 2010.

[35] A. Thiagarajan, J. Biagioni, T. Gerlich, and J. Eriksson. Cooperative transit tracking using smart-phones. In *8th ACM Conference on Embedded Networked Sensor Systems*, pages 85–98, 2010.

[36] D. Christin, A. Reinhardt, S. Kanhere, and M. Hollick. A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software*, 84(11):1928 – 1946, 2011.

[37] Anna Yu, Athanasios Bamis, Dimitrios Lymberopoulos, Thiago Teixeira, and Andreas Savvides. Personalized Awareness and safety with mobile phones as sources and sinks. In *International Workshop on Urban, Community, and Social Applications of Networked Sensing Systems (UrbanSense08)*, 2008.

[38] Spencer Chaineya, Lisa Tompson, and Sebastian Uhlig. The utility of hotspot mapping for predicting spatial patterns of crime. *Security Journal*, 21:4 – 28, 2008.

[39] John E. Eck, Spencer Chainey, James G. Cameron, Michael Leitner, and Ronald E. Wilson. Mapping crime: Understanding hot spots. Special, U.S. Department of Justice, Office of Justice Program, National Institute of Justice, August 2005.

[40] S. Chainey and J. Ratcliffe. *GIS and Crime Mapping*. Wiley, 2005.

[41] E. Jefferis. A multi-method exploration of crime hot spot: A summary of findings. Technical report, U.S. Department of Justice, Office of Justice Program, National Institute of Justice, 1999.

[42] S Chainey, S Reid, and N Stuart. *When is a Hotspot a Hotspot? A Procedure for Creating Statistically Robust Hotspot Maps of Crime*. Kidner, D and Higgs, G and White, S, 2002.

[43] N. Barberis, A. Shleifer, and R Vishny. A model of investor sentiment. *Journal of Financial Economics*, 49:307–243, 1998.

[44] Gorr and A. Olligschlaeger. Crime hot spot forecasting: Modeling and comparative evaluation. Draft final report, U.S. Department of Justice, Office of Justice Program, National Institute of Justice, 2001.

[45] Volkan S. Ediger and Sertac Akar. Arima forecasting of primary energy demand by fuel in turkey. *Energy Policy*, 35:1701–1708, 2007.

[46] A.M Olligschlaeger. Artificial neural networks and crime mapping. Studies/research report, U.S. Department of Justice, Office of Justice Program, Drug Market Analysis Program, 1997.