This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

SHIELD: *S*ocial sensing and *H*elp *I*n *E*mergency using mobi*L*e *D*evices

Gautam S. Thakur, Mukul Sharma, Ahmed Helmy
Department of Computer and Information Science and Engineering,
University of Florida, Gainesville, FL
{gsthakur, msharma, helmy}@cise.ufl.edu

***Abstract*—School and College campuses face a perceived threat of violent crimes and require a realistic plan against unpredictable emergencies and disasters. Existing emergency systems (e.g., 911, campus-wide alerts) are quite useful, but provide delayed response (often tens of minutes) and do not utilize proximity or locality. There is a need to exploit proximity-based help for immediate response and to deter any crime. In this paper, we propose *SHIELD*, an on-campus emergency rescue and alert management service. It is a fully distributed infrastructure-less platform based on proximity-enabled trust and cooperation. It relies on nearby localized responses sent using Bluetooth and/or WiFi to achieve minimal response time and maximal availability thereby augmenting the traditional notion of centralized emergency services. Analysis of campus crime statistics and WLAN traces surprisingly show a strong positive correlation (over 55%) between on-campus crime statistics and spatio-temporal density distribution of on-campus mobile users. This result is promising to develop a platform based on mutual trust and cooperation. Finally, we also show a prototype application to be used in such scenarios.**

I. INTRODUCTION

The current emergency, alert and public safety systems take centralized approaches and do not tap any available local rescue service. For example, 911 and Emergency BlueTowers connect to centralized Public Safety Answering Point (PSAP), which then send rescuers at the crime site. Also, they require pre-established links and infrastructure, which may not be available everywhere especially in areas affected by earthquake and floods. On the other hand, decentralized and distributed approaches of small handheld devices with short communication (Bluetooth, WiFi) give new dimension to express human activities never seen before in terms of personal safety and rescue. They helped to realize great potential of service localization, proximity, participatory sensing and message relaying in multitude of ways, for example: inferring shared interest[8] and friendship networks[6], identifying social structure and; human behavior based message forwarding[7]. In a novel way, here we extend their underlying capabilities to augment current emergency rescue and alert response management systems.

We propose ideas to develop: (1) trust from mobile user encounters (2) context aware service localization and signaling of historical crime log statistics, all as measures to provide a preemptive response in averting the possibility of incident occurring via a system we called *SHIELD*. As a reaction to minimize the average response time of an already occurred event, SHIELD maximizes the use of available local help in the vicinity of incidence. SHIELD achieve operational independence and robustness in the process of distress signaling by providing a set of guidelines to ensure privacy, identify trusted entities of the network and increase the cooperation among them, hence regulating the flow of information/message in a controlled manner.

We develop trust and cooperation in the network based on (1) Number of Bluetooth encounters (2) Duration of Bluetooth encounters. Then, we propose a comprehensive trust model built on these and other contextual features. The trust model plays a vital role in privacy preservation of mobile users and sought to increase cooperation inside the network. We also propose a context aware energy efficient protocol that takes input from trust model and historical crime log statistics. Keeping in mind the limited resource of mobile devices, the protocol is adaptive and adjusts the parameter setting to better serve the nature of emergency and alert scenario. Finally, the proposed system can easily augment existing services (like 911) and bridge the gap to cater available localized services of first responder as quickly as possible. In all, our design goals to develop such infrastructure-less distributed system includes: (1) Maximum availability, (2) Minimum response time, (3) Reliability of communication via network trust generation, (4) Scalability and (5) Cross-platform functionality to mitigate response irrespective of the device manufacturers.

II. RELATED WORK

A. Emergency and Rescue Systems in General:

As mentioned, most of the existing systems are either centrally controlled or require third party support (Cell Towers etc). For example, university campuses deploy BlueTowers and standard text messaging systems like CampusED, e2Campus, Panic n' Poke to alert students and faculties. However, they have some shortcomings: BlueTowers are not available everywhere and the SMS text service are expensive, passive and incur lot of resources. Instead targeting affected users, these SMS are sent in thousands, which overload the central system and affect other voice-data services with delayed throughput and unacceptable percentage loss of total messages

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

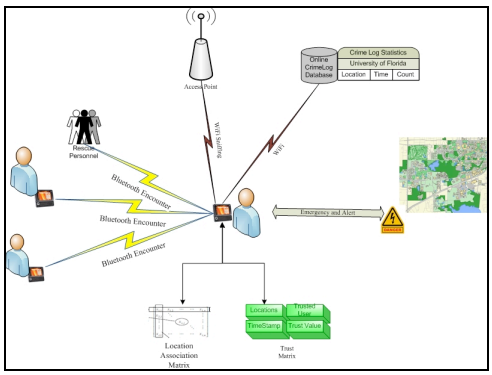


Figure 1: SHIELD Architecture

sent. Furthermore, affected mobile users lack any network driven trust and cooperation, but need to coordinate on their level. Finally, they cannot be used in situations of disasters, earthquake where infrastructure collapses.

B. *Other Approaches:*

The development of a robust and responsive system is critical to emergency management. Several prototypes have been proposed in the past. The authors in[14] proposed a dynamic data driven application framework that uses wireless call data to measure the abnormal movement patterns in the population. The need for a reliable communication and interoperability challenges among rescue teams from technological, sociological and organizational point of view are discussed in [9]. The barriers to technology adaption in emergency management and user capabilities are discussed in [10][11], which gives deployment level intricacies of systems. Finally, real time test beds and simulator are modeled in [12][13], to help develop a system that can actually react in reality.

C. *Understanding User behavioral patterns:*

Currently, numerous attempts are being made to understand user behavioral patterns from machine-sensed measurements [4,5]. They try to discover mobile users' social structures, periodic routines and spatio-temporal profiles. A detailed study on various expects of human patterns are done in [15-17]. On the same lines, authors in [1][2] investigate the social structures, community formation and derive expressions for the cooperation in the network based on similarity and density distribution. These works motivate us to develop a framework that uses behavioral patterns in the context of developing trust and cooperation from multi-sensing handheld devices.

D. *Using Human Mobility as a Communication Paradigm:*

To uncover user behavioral patterns is not enough; we need some compelling reasons to develop a communication paradigm based on these patterns. An important work in [7] proposes a mobility protocol that uses human behavior to transfer messages. In [18][19], authors consider the impact of mobility in designing communication protocols and provide ways to develop an effective communication system. These rationales give an important motivation that a system can be developed from user behavioral patterns. It can use those characteristics features as a medium to establish a secure and timely communication in DTN like environment. Next, we discuss SHIELD architecture.

III. SHIELD: RATIONALE AND ARCHITECTURAL OVERVIEW

In this section, we discuss the SHIELD architecture as shown in Fig.1. Here, we assume mobile users are carrying handheld devices equipped with RF-communication capability. The main components of the SHIELD are:

A. *The Encounter and Duration Matrix:*

Mobile encounters are the discovery of the Bluetooth devices present in the vicinity. Initially, we build two matrices: 1) An Encounter matrix that contains the number of encounters with other users. 2) A Duration matrix that contains the duration of these encounters with other users. We also record the timestamp and the location of encounter. The location is derived from the access point sniffing and used to co-locate a user with the incidence location and time.

B. *The Trust Matrix:*

The trust model discussed later uses these encounters and builds a wrapper of trust for the mobile host in form of a trust matrix. It first maps encounters in spatio-temporal dimension and then assigns them into various classes of trust that identifies other users influence in emergency rescue and alert. From the analysis of real traces and human surveys, we find that large number of encounters and longer encounter duration belong to known persons like friends, colleagues and spouse.

C. *Advisory Sub-System:*

To provide an optimal level of safety and self-preparation, we analyzed historical on-campus crime logs. We created an online database of these crimes statistics and ranked various campus location. The location ranking and vulnerability assessment is done using time and nature of the crime. The system gives a statutory threat warning to the mobile users whilst visiting a location at a particular time. The location is derived from the nearest Access Point. For example, the system flashes a cautionary signal to the students passing a parking garage at nighttime, if it has some recent crime history. As shown in Fig. 1, this data may be stored on the device, or accessed from a server using a WiFi connection.

D. *Context-aware Adaptive Protocol:*

We introduce a context-aware adaptive protocol to complement trust model and advisory sub-system. Its main task is to perform efficient routing and transmission of the distress signal. For example, during a critical time like passing a parking garage, the protocol increases Bluetooth scanning frequency to identify nearby trusted devices and notify them of its existence. However, in normal operations it tries to save resources (battery power etc), by reducing scanning frequency.

E. *Distress Signaling:*

In emergency situations the mobile user can use all available modes of communication to let nearby trusted nodes know of the situation. A user can select classes of trust to send the distress signal (automatically) based on their availability and also to a category of individuals who provide specialized services like doctors, security and rescue personnel, nighttime vigil guards etc. In the following text, we describe the details.

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

Table 1: Wireless Trace Measurements

Type of Trace	Duration	Statistics
Bluetooth	Fall 2009	135 Users on Nokia N810
WLAN Usage	Fall 2008	12000 User
Crime Log	1998-2010	17510 cases

IV. TRACE ANALYSIS

An important aspect in Ad Hoc Network research is the careful logging of mobility traces and empirical ways to understand large systems. In the past few years, we saw a significant effort by several universities[4][5] to collect large-scale measurement that logs Bluetooth encounters and WLAN users' network usage spatio-temporal information. The *TRACE* framework as mentioned in[1] helps to further refine and generate encounter matrices for our analysis. Table-1 shows the measurements used for our purpose of study. The above measurements are collected from the main university campus of University of Florida. Bluetooth encounters are collected from 135 students in Fall 2009 on Nokia N810s devices. To understand density, we also use WiFi measurements from Access Point (WLAN) connections. The crime log received from Police department of University of Florida contains ten years of on-campus incidences detailing the type, time, date and location of crime.

V. TRUST MODEL

Today mobile users frequently carry handheld (e.g. iPhones) devices that can be used to reflect their personality. Using the multi-sensor capability of these devices (e.g. Bluetooth, GPS and WiFi sniffing), we can capture vital statistics like frequency and duration of time spent at particular locations. Statistical analysis [2][3][16] of historical logging of mobility shows user behavioral pattern has location visiting preferences, periodic reappearances and preferential attachments. Another perspective in the study of behavioral patterns is the analysis of similarity that helps develop inter-connection between mobile users. In this regard, a fundamental work is done in [20][21], which provides significant evidences of socio-demographic, spatio-temporal regularity and social structures as a basis to develop homophilous relations and propinquity among users. It also shows people who know each other form a cohesive cluster with a small average shortest path length, and a large clustering coefficient. Using this rationale, we conducted an experiment to analyze user encounter patterns in University of Florida campus. For a period of ten weeks in Fall 2009, we distributed Nokia N810 and OpenMoko to 135 students. The devices were equipped to sniff nearby active Bluetooth devices in a range up to ~50 meters, localized by WiFi Access Point information. The analysis show that large number and duration of meetings belong to users who know each other very well (validated by the students carrying out the experiments), is shown in the Fig.2. The curves decrease for mobile users with known faces to completely strangers. The characteristic similarity brings people of the same nature together. Thus, the information flows relevant to one mobile

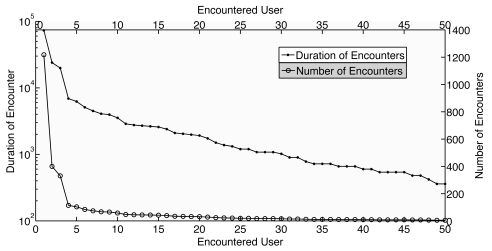


Figure 2: The distribution show users who know each other have large frequency and duration of encounters compared to strangers.

user more likely to be of the interest to another mobile user of same circle. Conversely, the same circle can be called for in the event of emergency and alert. Finally, the way to develop such a circle of trust and friendship can be derived from the mobile encounters. Using these results we can say that known mobile users with *frequent encounters* and *large meeting duration* most effectively are the ones trusted at first place. Furthermore, a co-operation network based on these two metrics can be developed and very well be used in the event of emergency and alert management. The formation of trust and cooperation between two mobile users i and j is defined as:

A. Number of Encounters $f(i,j)$:

We define the number of encounters (*n)* as the frequency of encounter (i.e., coming within radio range) between two mobile users and are the number of repeated meetings per unit time as

$$f(i,j) = \sum_{i,j=1}^{n} \delta(i,j)$$

B. Duration of Encounters $D(i,j)$:

We define duration of encounter as the amount of time spent by mobile users together. While the number of encounters provides an important criterion to quantify the active mobility of users in the network, it does not provide a minimum threshold time required to establish a connection and successfully transfer the messages. For example, say two mobile users often meet, but only for a fraction of a minute, despite a successful encounter, it is impossible for them to communicate effectively. Duration of encounters provides the requisite stability factor in a dynamic network environment. Qualitatively, it also defines the closeness between two mobile users, as a dimension to measure trustworthiness and an expected level of cooperation in the emergency and alert situation. We define the duration of encounter between two mobile user nodes i and j as:

$$D(i,j) = \sum_{i,j=1}^{n} d(\delta(i,j))$$

Where $d(\delta(i,j))$, is the individual duration of meeting between i and j while they encounter. These two metrics provide a foundation that led us to implement a comprehensive trust model. It effectively optimizes the distress signal transmission with trusted nodes. The trust model uses a rule-based classifier that recognize Bluetooth encounter and assigns them into various classes of trust. These classes of trust define the social

Figure 3: Application Protocol

proximity of a user in emergency and alert situations. The rule base classifier consists of a Rule set $R = \{r_1, r_2, r_3, ..., r_k\}$ such that each classification rule is of form:

$$r_j : (\text{Encounter, Condition}) = C_l(y)$$

Each rule consists of a condition statement that defines attributes pertinent to the encounter. The term $C_l(y)$ shows that node y is assigned to class $C_l \in C$, such that $C = \{C_1, C_2, C_3, ..., C_m\}$. These rules may not be mutually exclusive and sometimes more than one rule can apply to an encounter. Following condition statements are used to built classifier from environment sensed emergent properties:

1) Location and vicinity information of Bluetooth encounter.
2) Tags that define the level of trust with an encountered device. These tags are similar to ranks and status quo of a person, i.e. doctors, security personnel.
3) Duration, frequency and clock time of the encounter.
4) Activity based encounters, which describes the circumstances when Bluetooth encountered happened.

This classifier is easy to interpret and can be incrementally built on the existing rules.

VI. PROTOCOL DESIGN

The stack defines a process to send distress signals to a few trusted nodes. It achieves its goal by managing activities, sensing the emergent properties from the location of incidence, data of historical events and intelligently choosing the most effective form of available communication. The protocol stack is shown in Fig. 3 is divided into four main components as

A. The Scan Engine:

The top component contains scanner and profiler for mobile user encounters. The trust model generates a user's behavioral profile and aggregates the classification of its Bluetooth measurements into encounter matrix form. The device sensor provides detail on the historical crime log, location of the incident, duration & time to maximize efficiency of signal.

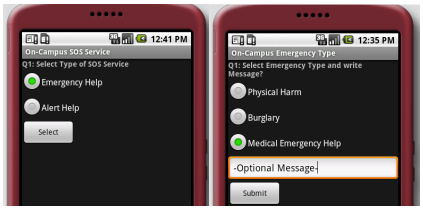


Figure 4: SHIELD Application Prototype

B. Protocol Adaption:

To provide optimal level of services and to ensure the limitation imposed by mobile device protocol adapts to environment by selectively changing the parameter space based on environment sensed input and crime log statistics.

C. Distress Signal Communication:

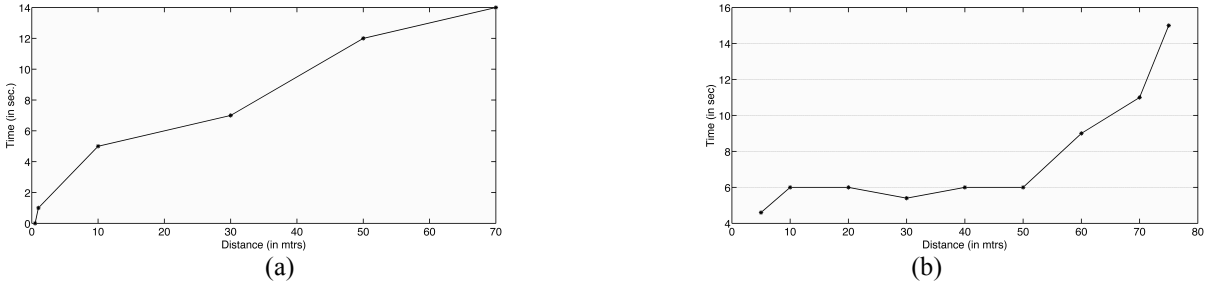
This component is responsible for deciding the level of trust. Based on the type of incident, the trust magnitude and severity is decided before sending the distress signal. We define various trust magnitudes: Friends, Strangers, Acquaintances, Tagged data. A distress signal can be bifurcated into emergencies and alerts. An *emergency* situation can be burglary, heart attack, while *alerts* might involve hurricane warning, earthquakes. The application decides the life span of the message, number of hops, type of forwarding method etc.

D. Discovering and Pairing:

The lower most component is responsible for message transmission to other mobile user devices and also performs important operations like pairing, discovering and relaying to other devices. This module is attached to hardware, which can use any of the available communication to send distress signal.

VII. APPLICATION PROTOTYPE

We developed a prototype application on Android Simulator based on SHIELD architecture. As show in Fig.4, this prototype can use Bluetooth to collect user encounters and to transmit distress signal. The core is the trust model, which is responsible for classifying and extracting the level of trust based on mobile user encounters and other machine sensed vicinity data. User interfaces provide graphical input capability to record victim response to a distress signal message. Finally, the protocol and its adaptation module are used along with message to send the distress signal.



(a) (b)

Figure 5: (a) The Bluetooth Scanning time varies with distance. (b) Connection and Transfer time for Bluetooth

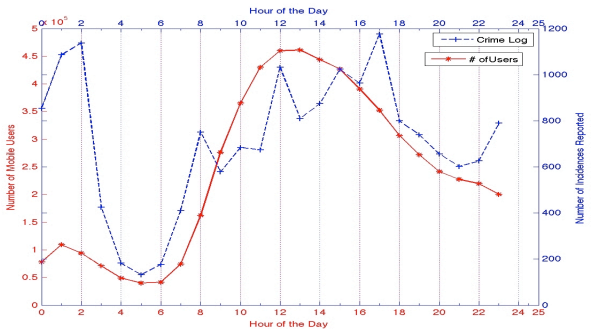


Figure 6: A graph showing crime log and density distribution of on-campus mobile users.

VIII. Test Bed Implementation Analysis

In this section, first we evaluate our test-bed results for Bluetooth performance using Nokia N810. We find that an average of 15-20 seconds is a good estimate for sending a distress signal to trusted nodes. Then, we analyzed over ten years of on-campus crime incidences against the density distribution of on-campus mobile users. Here, we find most of the incidences happen when mobile users are active. This correlation of 55% shows one good thing, incidences can be averted if a proper coordination and trust in the network exists.

A. Bluetooth Evaluation:

Since Bluetooth is a primary mode for distress signaling, it is very important to first evaluate its performance and effectiveness to communicate the message. We used Nokia N810 to measure the Bluetooth performance on scanning and connection time, delivery and message size. To ensure the quickest level of communication, we optimized the Bluetooth capability of these devices. The result for average scanning and connection time is shown in Fig. 5(a). The scan time of six to ten seconds is optimal to find trusted nodes within 50 meters of radius. As the emergency is relaxed, we can spend extra time in scanning and tracing the trusted nodes. We also define an efficient and useful Message format. We analyzed the connection and transfer time taken for a One Hop Transfer of message size of 184 bytes. As shown in Fig. 5(b), we found that low transfer times range between 0-60 meters. These results show great promise to use Bluetooth communication in designing rescue applications.

B. Crime Statistics and Mobile User Density:

Next, we analyzed the past ten years of the crime log statistics of University of Florida to understand the spatio-temporal distribution of the incidences happened on-campus and also the density distribution of active mobile users. As shown in Fig. 6, the crime statistics are high during the midnight and then increases as the daytime progresses. There is a positive correlation between the incidences and the number of active mobile users. Thus, these incidences can be very well averted given proper preparedness exists for the mobile users.

IX. Conclusion

In this paper, we propose a novel method to utilize handheld devices in emergency rescue and alert scenarios. We introduce SHIELD to establish spatio-temporal trust and cooperation for use in localized emergency alerts. An important sub-system of SHIELD is the proximity-enabled trust generation based on the number and duration of encounters among mobile users. Our analysis shows that a large number of encounters and high meeting duration occurs among users who know each other very well. Then, we introduce a context-aware adaptive protocol that is both energy efficient and social aware for signaling distress message. Our statistical analysis reveals a positive correlation (55%) between on-campus crime incidences and density distribution of users. The results indicate a need for a system based on mutual trust and cooperation to avert incidences and help controlled flow of information during alerts. To aid this, we also proposed an application prototype for iPhones and other handheld devices. We hope that SHIELD will augment the current safety infrastructure and its deployment help make a safe environment in schools and universities campuses.

References

[1] Wei J. Hsu, Debojyoti Dutta, and Ahmed Helmy. *Mining behavioral groups in large wireless LANs*, MobiCom, 2007.

[2] Hsu, W., Spyropoulos, T., Psounis, K., and Helmy, *A. Modeling spatial and temporal dependencies of user mobility in wireless mobile networks*. IEEE/ACM Trans. Netw. 2009

[3] Henderson, T., Kotz, D., and Abyzov, I. *The changing usage of a mature campus-wide wireless network.* MobiCom '04.

[4] MobiLib: Community-wide Library of Mobility and Wireless Networks Measurements. http://nile.usc.edu/MobiLib.

[5] CRAWDAD: A Community Resource for Archiving Wireless Data At Dartmouth. http://crawdad.cs.dartmouth.edu/index.php

[6] Nathan Eagle, Alex S. Pentland, and David Lazer. *Inferring friendship network structure by using mobile phone data*. PNAS 2009.

[7] W. Hsu, D. Dutta, and A. Helmy. *CSI: A Paradigm for Behavior-oriented Delivery Services in Mobile Human Networks*. Arxiv preprint arXiv:0807.1153, 2008.

[8] Terry, M., Mynatt, E. D., Ryall, K., Leigh, D. *Social net: using patterns of physical proximity over time to infer shared interests*. CHI '02.

[9] Manoj, B. and Baker, A. H. *Communication challenges in emergency response.* Communication, 2007

[10] Tierney, K. and Sutton, J. *Cost and culture: Barriers to the adoption of technology in emergency management*. RESCUE 2005.

[11] Zimmermann, H. *Availability of technologies versus capabilities of users*. ISCRAM, 2006.

[12] Jain, S. and McLean, C. *Simulation for emergency response: A framework for modeling, simulation for emergency response*. WSC 2003

[13] Sullivan, Thomas J. 1985. *Modeling and Simulation for Emergency Response*, Lawrence Livermore National Laboratory, 92001.

[14] Madey, G.R., Szabo, G., Barabási, A.-L.: *WIPER: The integrated wireless phone based emergency response system*. ICCS 2006

[15] Pentland, Alex (Sandy): *Automatic mapping and modeling of human networks,* Physica, 2007

[16] Akoush, S. and Sameh, A. *Mobile user movement prediction using bayesian learning for neural networks*. IWCMC '07.

[17] Andrew Miklas, Kiran Gollu, Kelvin Chan, Stefan Saroiu, Krishna Gummadi, and Eyal de Lara. *Exploiting social interactions in mobile systems*. UbiComp 2007.

[18] Augustin Chaintreau, Pan Hui, Jon Crowcroft, Christophe Diot, Richard Gass, James Scott, "*Impact of Human Mobility on Opportunistic Forwarding Algorithms*," MOBICOM, 2007

[19] Scott, J.; Crowcroft, J.; Hui, P. & Diot, C. (2006), *Haggle: a Networking Architecture Designed Around Mobile Users,* WONS 2006.

[20] Miller McPherson, Lynn Smith-Lovin, James M Cook, *Birds of a Feather: Homophily in Social Networks*, Sociology 2001

[21] Duncan J. Watts and Steven H. Strogatz. *Collective dynamics of 'small-world' networks*. Nature, 393(6684):440–442, June 1998.