Enhancing Trust-based Data Analytics for Forecasting Social Harm

Nahida Sultana Chowdhury, Rajeev R. Raje, Saurabh Pandey, George Mohler, Jeremy Carter
Indiana University Purdue University Indianapolis
Indianapolis, Indiana, USA
{nschowdh, rraje, pandey, gmohler,

***Abstract* First responders deal with a variety of “social harm” events (e.g. crime, traffic crashes, medical emergencies) that result in physical, emotional, and/or financial hardships. Through data analytics, resources can be efficiently allocated to increase the impact of interventions aimed at reducing social harm T CDASH (Trusted Community Data Analytics for Social Harm) is an ongoing joint effort between the Indiana University Purdue University Indianapolis (IUPUI), the Indianapolis Metropolitan Police Department (IMPD), and the Indianapolis Emergency Medical Services (IEMS) with this goal of using data analytics to efficiently allocate resources to respond to and reduce social harm. In this paper, we make several enhancements to our previously introduced trust estimation framework T CDASH. These enhancements include additional metrics for measuring the effectiveness of forecasts, evaluation on new datasets, and an incorporation of collaborative trust models. To empirically validate our current work, we ran simulations on newly collected 2019 and 2020 (Jan April) social harm data from the Indianapolis metro area. We describe the behavior and significance of the collaboration and their comparison with previously introduced stand alone models.**

***Keywords-Social* harm; Subjective logic; Trust management; Hotspots; Collaborative patterns.I**

I. Introduction

Devising a strategy for a smart city is a challenging task, as it requires a combination and an in depth exploration of a number of domains. In [1], six domains of smart cities are described one of the key domains indicated in that report is Safety and Security. That report indicates that technology and data will play significant roles in preventing crimes by assessing multiple streams of community and crowdsourced information. One concept, related to Safety and Security of smart cities, that can be mitigated by the use of such multiple streams of data is social harm. Social harm is “a concept that enables criminology to move beyond legal definitions of ‘crime’ to include immoral, wrongful and injurious acts that are not necessarily illegal” [2]. Social harm incidents may lead to physical harm (e.g. injury sus tained from an assault or traffic crash), financial (e.g., fraud), or emotional/psychological harm [3]. Many social harm incidents require first responders (e.g., law enforcement and emergency personnel) to coordinate together to prevent or quickly respond in order to lessen their impact. One way of quantifying the impact of social harm is by determining the economic burden carried by society due to such incidents.

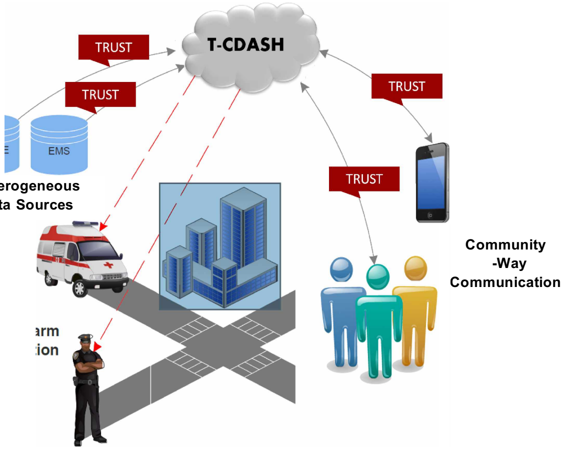

Figure 1: T CDASH System Architecture.

Social science experts view costs associated with crimes from two perspectives, quantifiable and unquantifiable costs [4] , Quantifiable costs point to direct monetary cost to the society, including the loss in business, damage to property, medical expenses, and others. Unquantifiable costs refer to psychological impacts resulting in anxiety and loss of productivity among victims.

One way of dealing with social harm is by using statistical models combined with software tools for forecasting social harm and directing resources to places and times where interventions are needed. For this purpose crime mapping [5] , “risk terrain” regression models [6], [7], point processes [8] and deep learning [9] are some of the approaches that have been considered. For a comprehensive review of spatial crime forecasting see [10]. Defining high risk areas help police, social service providers, and community stakeholders to allocate their resources efficiently.

One challenge that arises in modeling social harm is the integration of 1) real time data from 911 that is un verified and subject to label noise and 2) verified incident reports that may take several days or weeks to enter the records management system. Methods are needed for associating these data and correcting mislabeled real time data that can lead to misleading alarms, thereby allowing for a more optimal allocation of resources. To accomplish this, there is a need for a platform where various stakeholders, including the law-enforcement agencies, community organizations and citizens, can quickly and anonymously report live social harm incidents. To this effect, in our past work, we have developed and deployed the Trusted Community Data Analytic for Social Harm Prevention (T-CDASH) system [11] – a web-based system for capturing, analyzing, forecasting, and thereby, alleviating social harm. Figure 1 shows an overview of the T-CDASH system. The T-CDASH system can bring together various stakeholders, including law-enforcement agencies, community organizations, emergency medical services, and citizens to provide integrated data sharing and analytics in near real-time. The T-CDASH system uses a Hawkes Point Process Service (HPPS) [12] for generating social harm forecasts and provides a user interface to different stakeholders in the community to allocate resources for targeted interventions.

The T-CDASH system incorporates a trust framework consisting of several models that assign different degrees of trust to each social harm event. In our previous research [11], we empirically evaluated these trust models and compared their accuracy using 2012-2013 UCR (Uniform Crime Reporting) [13] and CAD (Computer Aided Dispatch) [14] datasets obtained from the IMPD. In this paper, we enhance this past work by:

- evaluating the effectiveness of the T-CDASH system by applying its trust models to the most recent (Jan to Apr. 2019 and Jan to Apr. 2020) RMS (Records Management System) [15] dataset, again, received from the IMPD.
- considering the frequency of a social harm event along with its average cost to identify top hotspots for a given geographical region ("policing beat") – in our previous work [11], the top hotspots for each policing beat were selected based solely on the average cost associated with a social harm incident in that beat.
- devising and experimenting with different collaborative patterns amongst trust models and empirically validating these patterns using both the new RMS and the old datasets (used in [11]).

The rest of the paper is organized as follows: The second section presents related research work on modeling trust. Section III explains the details of the T-CDASH trust models and the data management process along with pre-processing and correlation operations performed on the RMS dataset. Section IV presents results from several experiments indicating the performance of different trust models developed as part of the framework on 2012-2013 and 2019 & 2020 (Jan-April) datasets. The paper concludes by discussing the insights gained and presents directions for future work.

II. RELATED WORK

To generate reliable forecasting, it is important for the data to be reliable – i.e., there is a need to consider the trust associated with the data. This paper focuses on the trust viewpoint of social harm events. Significant research is available on establishing trust in distributed systems. Jøsang [16] established an opinion model for estimating the trust of events based on *belief (b)*, *disbelife(d)*, and *uncertainty(u)*. Here, opinions regarding a proposition/event translate in degrees of belief, disbelief and uncertainty. The belief, disbelief and uncertainty are calculated based on evidential analysis. For any proposition/event, positive evidences supporting the proposition trigger the belief. Also, negative evidences opposing the proposition contribute to the disbelief. Uncertainty is mainly attributed to the lack of evidences. Ceolin et al. [17] created a trust algorithm for computing b, d, and u as introduced by Jøsang in [16]. The algorithm was applied in the maritime domain for estimating trust of messages to track ships. The T-CDASH system used Jøsang's opinion model for estimating trust of social harm events.

Another common way of integrating trust with events is through the reputation model. Furtado et al. [18] used this reputation model to describe the reputation-based trust management methodology in WikiCrimes [19] system for generating reputation scores for the registered users. The reputation score increases with each genuine crime reported and it is used by the application for associating trust with the live reported events – preserving anonymity of users is a critical requirement for such reputation-based systems. However, limited work has been done in creating a comprehensive system that combines the forecasting of future social harm incidents while allowing users to report live incidents. In the T-CDASH system, instead of reputation model, we have used crime-related attributes such as incident types, location, and days and historical data to associate trust with reported events.

III. TRUST MODELS AND DATA MANAGEMENT

A. Trust Models

Due to the presence of many stakeholders (e.g., IMPD, community organizations, and citizens) in the T-CDASH system, there is a need to manage the trust associated with their interactions with the T-CDASH system. Any malicious or incorrect interaction with the T-CDASH system may affect its hotspot forecasting. One way of ensuring and maintaining the accuracy of forecasting is to pre-process and filter out live user-inputs (especially from untrusted users such as citizens) before they are considered for generating hotspots. This pre-processing and filtering stage helps in assigning a trust value to each live interaction – to achieve this objective, in our previous work [11], we proposed six trust models, and empirically evaluated and compared their effectiveness. The trust models are:

- Ground-truth model: in this model, all the inputs are assumed to be trustworthy and passed to the HPPS service for generating the hotspots.

- Optimistic model: this model considers a high percentage (80% to 90%) of all the live user-inputs (randomly chosen) to be trustworthy and passes them to the HPPS service; others are ignored.
- Pessimistic model: it is opposite of the Optimistic model. Here, only a small percentage (10% to 20%) of all the live user-inputs (randomly chosen) are considered to be trustworthy and passed on to the HPPS service; others are ignored.
- Average model: in this model, half of all the live user-inputs (randomly chosen) are considered as trustworthy and passed on to the HPPS service.
- Random model: in this model, a set of live user-inputs are randomly chosen in the process of hotspots generation; others are ignored.
- Opinion-based model: this model selects or rejects the live inputs based on the trust tuple made up of belief (b), disbelief (d) and uncertainty (u) values. The b, d and u values are computed in two ways by this model.
    - Random: it randomly assigns values to b, d and u.
    - Heuristic: it utilizes the correlation created between live and historical data. This is based on actual event attributes and its correlation with historical incidents.

In this research, these trust models are composed with following four different collaboration patterns:

- 'OR' Collaboration: The T-CDASH system considers, for the forecasting purposes, only those social harm events that are generated by at least one of the above-mentioned trust models.
- 'AND' Collaboration: The T-CDASH system considers, for the forecasting purposes, only those social harm events that are generated by all the above-mentioned trust models.
- 'MAJORITY' Collaboration: The T-CDASH system considers, for forecasting purposes, only those social harm events that are generated by the majority ($>= 3$) of the above-mentioned trust models.
- 'XOR' Collaboration: The T-CDASH system considers, for forecasting purposes, only those social harm events that are generated by exactly one of the above-mentioned trust models.

B. Data Management

We considered, for this research, data from three different sources: RMS, UCR and CAD system. As explained by the Law Enforcement Information Technology Standards Council (LEITSC) in [14], the CAD system assists in performing public safety operations in an automated manner. It includes incident reporting, emergency vehicle dispatch, along with incident tracking and management capabilities. Information captured by CAD assists in creating the RMS reports. LEITSC [15] describes RMS as an agency-wide system for recording, persisting, and retrieving information and documents related to law enforcement operations. Although the RMS allows multiple incident reporting mechanisms, it records only a single entry for each incident. The RMS datasets (2019 & 2020 (Jan-April)) were made available, to us, by the IMPD for the Indianapolis metropolitan area. On the other hand, the UCR consists of data collected from four different systems [13] (2012-2013). In this section, we will mainly focus on the recently available RMS dataset mapping mechanism and trust association with the T-CDASH system. In our previous paper [11], details about UCR and CAD were provided [1].

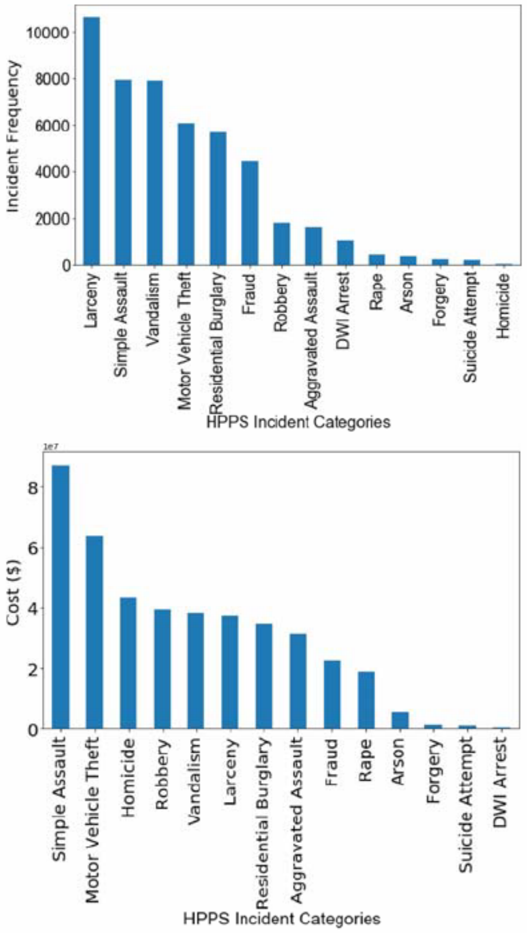

Figure 2: Statistics for Indianapolis social harm 2019 & 2020 (Jan-April) RMS dataset.

RMS Data. A report is made by the IMPD whenever an incident is investigated. This RMS data is available from Socrata [20] – Socrata is a Database-as-a-Service (DaaS)

[1] At the time of the submission of this paper, we received the CAD dataset for 2020 (Jan-April) for Indianapolis. This dataset contains 2,60,980 reported incidents along with 412 unique incident types. The received data is unstructured and has been collected on a daily basis. Hence, it will need additional preprocessing and mapping before it can be used with the T-CDASH system. We will pursue that work as a future direction.

Table I: RMS to HPPS input incident Mapping

RMS - Incident description	HPPS - Incident description	HPPS - Incident Code
DRIVING UNDER THE INFLUENCE	DWI Arrest	1
DAMAGE TO PROPERTY	Vandalism	3
CREDIT CARD/AUTOMATIC TELLER MACHINE FRAUD	Fraud	4
ATTEMPTED OR THREATENING SUICIDE	Suicide Attempt	5
COUNTERFEITING/FORGERY	Forgery	6
ALL OTHER LARCENY	Larceny	8
ATTEMPTED BURGLARY	Residential Burglary	9
MOTOR VEHICLE THEFT	Motor Vehicle Theft	11
FIGHT	Simple Assault	12
ARSON	Arson	13
AGGRAVATED ASSAULT	Aggravated Assault	14
ATTEMPTED ROBBERY	Robbery	15
FORCIBLE FONDLING	Rape	17
MURDER AND NONNEGLIGENT MANSLAUGHTER	Homicide	18

platform that helps in managing government data. Since these entries are recorded post police investigations, they can be considered highly trustworthy. The statistics for the Indianapolis social harm 2019-2020 (Jan-April) RMS dataset is presented in Figure 2. It indicates the frequency and the cost (unit $10 millions) associated with each social harm event for the 2019 and 2020 datasets. It is worth noting, from this figure, that some categories of the incidents, such as homicide, occur less frequently but are associated with a high cost.

Data Mapping. Different social harm reporting and management systems store data in different formats, and each has their own schema. To analyze, correlate, and process these data records, in T-CDASH, it is necessary to convert them in a schema used by the Hawkes Point Process Service (HPPS). To achieve this, each record of the RMS is preprocessed. Currently, the T-CDASH system supports hotspot forecasting for 18 different incident types [12]. It is, thus, necessary to map the RMS records to these 18 categories.

The RMS records maintained by the IMPD are analyzed and mapped to the HPPS input categories. For the RMS, incident descriptions closely resemble the type of incident and are used for generating the mapping. Table I provides the mapping between various RMS incident descriptions (collected from 2019 & 2020 (Jan-April) datasets) and the corresponding HPPS input incident categories. For the mapping, we followed the similar mechanism [11] that was used to map the UCR and CAD reported incident categories (2012-2013) to HPPS input incident categories.

Data Correlation. Trust, as indicated earlier, is an important feature associated with the T-CDASH system. To maintain reporter's anonymity and to avoid misuse of reporter's historical reputation, this trust is computed by using Jøsang's opinion model [16] consisting of belief (b), disbelief (d) and uncertainty (u) tuples – in a similar way as utilized by Ceolin et al. [17]. Through the opinion model, a certain degree of trust is assigned to each live incident reported to the T-CDASH system. These b, d, u values are calculated by the T-CDASH system using the number of positive evidences, negative evidences, and total evidences [21] that it has received. In the T-CDASH system, to gather these evidences, geo-coordinates, the type, and the reported date of the incident are considered. For calculating the total evidences, the geo-coordinates (circular range 110 m) and/or day (4 days), are considered. Based on these features, each live social harm incident is correlated with historical social harm incidents. If there is a positive correlation between the historical incidents and the current incident then reported incident is deemed trustworthy.

IV. Experimental Results

This section discusses various experiments performed to empirically validate the accuracy of different trust models proposed within the T-CDASH system with recent and previous datasets. This section also presents different approaches to generate the top hotspots (e.g., hotspots based on the incident frequency and combination of incident frequency and average cost) and their impact on accuracy. In addition, the usage of collaboration patterns between different trust models is discussed here.

Table II: Training and Testing Years for Evaluating Trust Models

Training Year	Testing Year
2012-2013	2013
2019-2020	2020

A. Training the Hawkes Point Process Service (HPPS)

While evaluating the trust models and make forecasting about the top social harm hotspots, in a policing beat, it is crucial to train the HPPS properly. Since the UCR and RMS data are highly trustworthy, the HPPS is trained on the UCR data (2012-2013) and the RMS data (2019 and 2020). Also, real-time data is required to test the trust models – the CAD data are considered for evaluating the trust models as those

Table III: Different approaches to generate to hotspots using 2012-2013 dataset

Model	Location?	Day?	Avg cost-based Hotspots Matched (%)	Incident freq.-based Hotspots Matched (%)	Combination of Incident freq. and Avg cost based Hotspots Matched (%)
Optimistic (80%)	yes	yes	37.46	58.1	43.06
Pessimistic (5%)	yes	yes	49.66	65.07	58.13
Average	yes	yes	42.93	60.7	50.22
Random	yes	yes	42.85	60.68	50.06
Random Heuristic	yes	yes	42.03	67.97	63.16
Heuristic (50% - 50%)	yes	yes	49.59	67.33	61.75

data contain the real-time reporting of social harm incidents. However, the CAD data for 2019 or 2020 was not available for our experiments. Hence, we generated synthesized CAD data based on the RMS data of 2020 and CAD data of 2016 (most recent CAD data that are available). It is worth noting that many incidents included in the CAD dataset are not reported in the RMS dataset in the same way. One of the reasons for such a difference is that an incident may have never happened. To synthesize a CAD dataset for testing, we considered two different strategies: (a) two-third data is randomly obtained from the CAD records of 2016 and one-third is randomly taken from the RMS data of 2020, and (b) one-third data has randomly selected from the 2016 CAD dataset whereas the remaining data was randomly picked from the RMS records of 2020. On examining the UCR and CAD data of 2013, it is observed that approximately $2/3^{rd}$ of CAD data is reflected in the UCR reported records. Therefore, based on this observation, we initially selected the strategy (a). We also wanted to experiment with the opposite scenario and hence, we then selected the strategy (b). Our experiments, hence, involve two combinations of yearly data for training and testing the trust models as shown in Table II. All the experiments are performed on the monthly data of the testing period and then equated out over the entire span (2012-2013 dataset the duration is entire year and 2019 and 2020 dataset the duration is 4 months).

B. Experiments with 2012-2013 Dataset

Based on our previous [11] experiments and associated insights, we selected the following parameters for the experiments with the RMS dataset.

- **Time series data cross-validation**. In our previous experiments [11], two different cross-validation techniques were utilized: Rolling Origin (RO) and Rolling Windows (RW) [22] [23]. The experimental results indicated that performance of RO, as indicated by accuracy, was less accurate than that of RW. Therefore, in our current experiments, we have used only the RW cross-validation technique.
- **Allowed Input (%)**. For the Optimistic and Pessimistic models, with the increase of allowed input percentage, the accuracy of matched hotspots was reduced. Therefore, in our current investigation, while using the Optimistic model, 80% of inputs were considered trustworthy. Similarly, for the Pessimistic model, 5% of inputs were considered trustworthy.
- **Trust Aspects**. Trust tuples (b, d, and u), associated with an incident, depend on the positive and negative evidences available for that incident [11]. To gather these evidences, in our past work, we considered three aspects of each incident: Location, Day, and Incident Type. Hence, in our experiments, we have considered all these three aspects.
- **Trust Threshold Value**. The Opinion-based model, in our past experiments, used different predefined threshold percentages of *belief* and *disbelief*. Here, if the generated *belief* value of an incident is higher than a selected *belief*'s threshold value, then the incident is considered for generating hotspots. Again, if the generated *disbelief* value of an incident is higher than a selected *disbelief*'s threshold value, then the incident is ignored. Based on the results of those experiments, we decided to apply only 50% as the trust threshold value for both *belief* and *disbelief*.

C. Approaches to generate the top hotspots

In our experiments, the Ground-truth model acts as a baseline model, and the accuracy of all the other models is defined in terms of the *hotspots matching percentage*. The hotspots matching percentage is the percentage of top hotspots for each policing beat, generated by a model, that match (have the same location and incident type and within the day range) with the top hotspots generated by the Ground-truth model. In the T-CDASH system, the top hotspots for each beat are selected based on their average cost associated with the social harm incident. In the current research, we have also explored additional criteria, which are: incident frequency and combination of both (incident frequency followed by the average cost).

Using these parameters, we carried out various experiments (using all the 6 trust models indicated in Sect. III-A) with the T-CDASH system using the 2012-2013 and 2019 and 2020 datasets to investigate the impact of the additional criteria (mentioned above) in terms of hotspot matching percentage. The results of these experiments are presented in Table III.

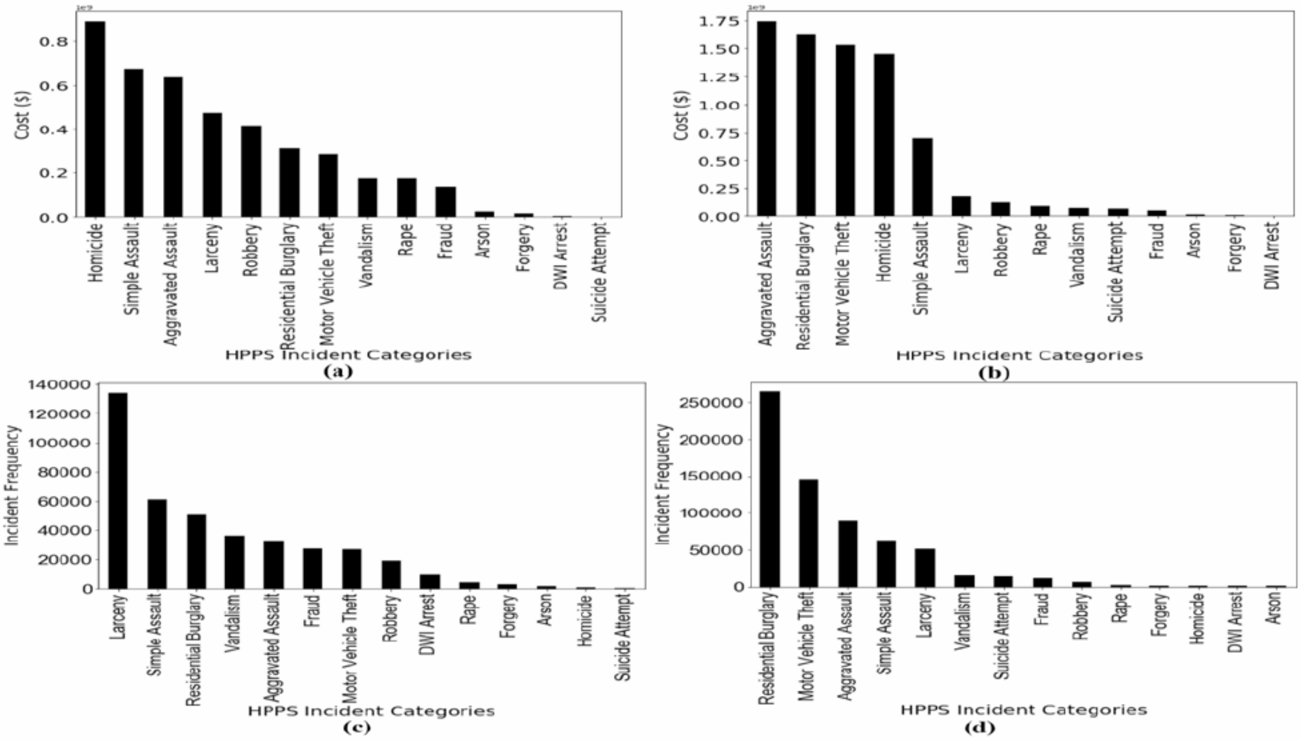

Figure 3: Statistics for Indianapolis social harm 2013 UCR and CAD dataset based on Incident's cost and frequency.

As seen from Table III, the inclusion of the incident frequency has significantly boosted the accuracy percentage of matched hotspots percentages when compared with other two criteria (cost and a combination of cost with frequency) for all six models. On analyzing the UCR and CAD data of 2016, we observed that three incidents categories (Homicide, Simple Assault, and Aggravated Assault) out of the top 5 categories matched based on the cost metric. Whereas, four incidents categories are matched (Larceny, Simple Assault, Residential Burglary and Aggravated Assault) out of the top 5 categories based on the incident frequency metric (as presented in Figure 3). Here, Figures 3(a) and (b) outline the UCR and CAD dataset statistics based on the cost feature. Similarly, Figures 3(c) and (d) represent the UCR and CAD dataset statistics based on the incident frequency feature. Hence, *to select the top hotspots in a policing beat, the incident frequency should be the most suitable criteria to consider.*

Another experiment, using the same parameters, was conducted for the RMS (2019 and 2020) datasets as well. The results of that experiment are provided in Table IV. Here, we can observe the same trend in terms of the performance of trust models. However, the accuracy percentage is much higher than the 2012-2013 dataset – a possible reason for this higher accuracy is that these RMS datasets are of a shorter duration (only four months Jan to April). Another possible reason could be related to the way we created the synthesized the CAD data for testing. In Table IV, as indicated earlier, the synthesized CAD data is a combination of two-third CAD data from the year 2016, and remaining

Table IV: Different approaches to generate to hotspots using 2019 and 2020 (Jan-April) dataset

Model	Location?	Day?	Avg cost-based Hotspots Matched (%)	Incident freq.-based Hotspots Matched (%)	Combination of Incident freq. and Avg cost based Hotspots Matched (%)
Optimistic (80%)	yes	yes	60.1	68.69	63.29
Pessimistic (5%)	yes	yes	67.05	78.01	72.38
Average	yes	yes	64.34	71.8	68.93
Random	yes	yes	64.01	71.35	67.56
Random Heuristic	yes	yes	51.83	64.82	57.96
Heuristic (50% - 50%)	yes	yes	58.22	69.57	61.72

data is obtained from the RMS 2020 dataset. In addition, we have experimented with the other approach, where only one-third of synthesized data was obtained from previous CAD data and remaining from the RMS 2020 dataset. For, both approaches the performance of all the trust models varies insignificantly excluding the Heuristic model. For second approach, the Heuristic model hotspots matched percentage rises to 73.57% based on the incident frequency.

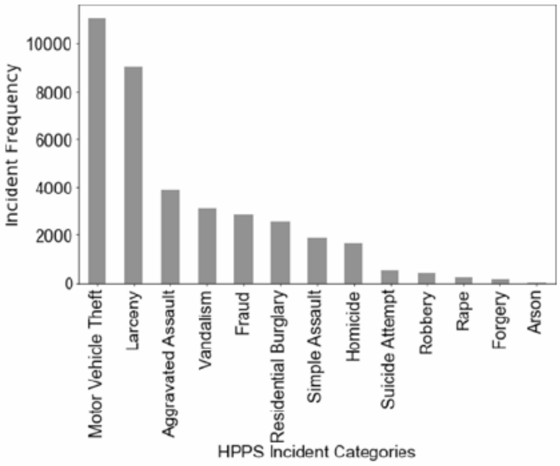

Figure 4: Statistics for Indianapolis social harm 2020 (Jan-April) CAD dataset based on Incident's frequency.

As indicated above, our existing CAD mapping scheme, in the T-CDASH system, uses 38 different reported incident types. We wanted to check the applicability of this mapping scheme to the recently received CAD data for 2020. Hence, as a preliminary investigation, we identified incidents (from the newly received CAD dataset for 2020) which belong to these 38 CAD categories and plotted them using the frequency-based incidents' statistics. Those details are presented in Figure 4.

D. Collaborative Trust Models

Instead of using each of the trust models in a linear manner, as indicated earlier, we employed different collaborative patterns among the trust models. The rationale for such collaborative (and hence, parallel forecasting) is twofold – (a) real-time events may be generated asynchronously and a user of the T-CDASH system may decide to employ a certain trust models for a certain type (e.g., use the heuristic model where there is lot of past data available for a particular beat) of incident data stream, and (b) parallel execution of trust models will result in a short turn-around time than a sequential execution of 6 trust models. In this study, we did focus only on the first part as the size of all the datasets are not very large – in future, if we can obtain large datasets and use them for training purposes, we could reduce both the training and forecasting times by collaborative executions of the trust models. The collaborative patterns are applied to all the 6 trust models. However, from previous experiment findings [11], we had observed that the Pessimistic and Heuristic models always outperformed than other trust models. Therefore, as an additional experiment, we applied the 'OR', 'AND', and 'XOR' collaboration patterns only to the Pessimistic and Heuristic models. The resulting outcomes are presented in Table V and Table VI. Here, for 2012-2013 dataset, we observed that the collaboration between two trust models (Pessimistic and Heuristic) performed better than the collaboration between all the 6 models. However, a different scenario was observed for the 2019 and 2020 datasets – the collaboration between the Heuristic and the Pessimistic models resulted in a lower matching percentage than compared to the collaboration between all 6 models. A possible reason for this change of behavior is that the stand-alone matching percentage of the Heuristic model is

Table V: Performance of Collaborative Trust Models with 2012-2013 dataset

Model	Location?	Day?	Avg cost-based Hotspots Matched (%)
AND Compose (All)	yes	yes	40.75
OR Compose (All)	yes	yes	37.86
MAJORITY Compose (All)	yes	yes	41.35
AND Compose (Pessimistic & Heuristic)	yes	yes	43.57
OR Compose (Pessimistic & Heuristic)	yes	yes	42.64
XOR Compose (Pessimistic & Heuristic)	yes	yes	44.59

Table VI: Performance of Collaborative Trust Models with RMS (2019 and 2020 (Jan-April)) dataset

Model	Location?	Day?	Avg cost-based Hotspots Matched (%)
AND Compose (All)	yes	yes	61.33
OR Compose (All)	yes	yes	57.4
MAJORITY Compose (All)	yes	yes	65.81
AND Compose (Pessimistic & Heuristic)	yes	yes	59.27
OR Compose (Pessimistic & Heuristic)	yes	yes	55.17
XOR Compose (Pessimistic & Heuristic)	yes	yes	62.76

lower than other models and that contributes to the different behavior. Comparing with the stand-alone performance of each trust model, we can conclude that the collaboration between all the 6 trust models, for the 2019 and 2020 datasets, does not yield any significant improvement. A possible reason for such a low performance is that the 2019 and 2020 dataset is small in size (only 4 months).

V. Conclusion and Future Work

This paper describes enhancements made to our past work, using the T-CDASH system, for forecasting social harm events using various datasets (CAD, RMS, and UCR). These enhancements include: (a) addition of the frequency of incidents, to the average cost, while computing the hotspots for each policing beat, (b) apply the six trust models to new datasets (2019 and 2020) obtained from the IMPD, and (c) investigation of different collaborative patterns amongst the six trust models. For the new (2019 and 2020) dataset, we observed, quite surprisingly that the Pessimistic model outperforms all the other trust models. One possible reason, in addition to the small size of the dataset, for this behaviour, is the lack of actual CAD data for the same time period.

Moreover, in our experiment, we also observed that for both the datasets, the collaborative patterns do not yield any significant improvement in the hotspot matching percentage when compared with the stand-along models. However, for the 2012-13 dataset, a collaboration between only two models outperformed the collaboration between all the models. Experimenting with additional datasets, such as the CAD data for 2020 that we recently received, is necessary to generalize matching percentages and the collaborative behavior between the models. In the future, different machine learning techniques can also be incorporated for generating trust models. Additionally, other comparison metrics, such as Earth Mover's Distance, can be applied to the results of the standalone and collaborative outcomes. Although, in this paper, we have described the applicability of T-CDASH on the data related to Indianapolis, T-CDASH can be easily adapted to any other city's social harm data. Such an adaptation will require the mapping of the reported incidents to the HPPS incident codes and run similar experiments. Therefore, an experimentation with other datasets associated with different cities is an interesting direction to explore in future.

VI. Acknowledgements

This project is supported in part by NSF grants CNS-1737585, SES-1343123, and DMS-1737996. G.M. is a co-founder and serves on the board of PredPol, a predictive policing company.

References

[1] "Define Your Smart City Strategy," https://www2.deloitte.com/us/en/pages/consulting/solutions/smart-cities-strategies.html.

[2] "Criminology beyond crime," *The Open University*, 2016.

[3] D. Dorling, D. Gordon, P. Hillyard, C. Pantazis, S. Pemberton, and S. Tombs, "Criminal obsessions: Why harm matters more than crime," *Centre for Crime and Justice Studies*, 2008.

[4] J. R. Greene, "New directions in policing: Balancing prediction and meaning in police research," *Justice quarterly31.2*, 2014.

[5] S. Chainey and J. Ratcliffe, *GIS and crime mapping*. John Wiley & Sons, 2013.

[6] J. H. Ratcliffe, R. B. Taylor, A. P. Askey, K. Thomas, J. Grasso, K. J. Bethel, R. Fisher, and J. Koehnlein, "The philadelphia predictive policing experiment," *Journal of Experimental Criminology*, pp. 1–27, 2020.

[7] J. M. Caplan, L. W. Kennedy, and J. Miller, "Risk terrain modeling: Brokering criminological theory and gis methods for crime forecasting," *Justice quarterly*, vol. 28, no. 2, pp. 360–381, 2011.

[8] G. O. Mohler, M. B. Short, S. Malinowski, M. Johnson, G. E. Tita, A. L. Bertozzi, and P. J. Brantingham, "Randomized controlled field trials of predictive policing," *Journal of the American Statistical Association*, vol. 110, no. 512, pp. 1399–1411, 2015.

[9] e. a. Wang, Bao, "Deep learning for real time crime forecasting," 2017.

[10] O. Kounadi, A. Ristea, A. Araujo, and M. Leitner, "A systematic review on spatial crime forecasting," *Crime Science*, vol. 9, no. 1, pp. 1–22, 2020.

[11] S. Pandey, N. S. Chowdhury, R. R. Raje, G. Mohler, and J. Carter, "Trust estimation of historical social harm events in indianapolis metro area," in *2019 IEEE International Smart Cities Conference (ISC2)*, 2019.

[12] G. Mohler, J. Carter, and R. Raje, "Improving social harm indices with a modulated hawkes process," *International Journal of Forecasting*, vol. 34, no. 3, pp. 431–439, 2018.

[13] "Uniform Crime Reporting," https://www.fbi.gov/services/cjis/ucr.

[14] "Standard Functional Specifications for Law Enforcement Computer Aided Dispatch (CAD) Systems," https://it.ojp.gov/documents/LEITSC_Law_Enforcement_CAD_Systems.pdf.

[15] "Standard Functional Specifications for Law Enforcement Records Management Systems (RMS)," https://it.ojp.gov/documents/LEITSC_Law_Enforcement_RMS_Systems.pdf.

[16] A. Jøsang, "Artificial reasoning with subjective logic," vol. 48, p. 34, 1997.

[17] D. Ceolin, P. T. Groth, and W. R. Van Hage, "Calculating the trust of event descriptions using provenance." 2010.

[18] V. Furtado, L. Ayres, M. De Oliveira, E. Vasconcelos, C. Caminha, J. D'Orleans, and M. Belchior, "Collective intelligence in law enforcement–the wikicrimes system," *Information Sciences*, vol. 180, no. 1, pp. 4–17, 2010.

[19] e. a. Furtado, Vasco, "Collective intelligence in law enforcement–the wikicrimes system," *Information Sciences180.1*, 2010.

[20] "Socrata," https://moto.data.socrata.com/dataset/Indianapolis-Metropolitan-Police-Department/n3wc-t646.

[21] B. Skoric and N. Zannone, "Flow-based reputation with uncertainty: Evidence-based subjective logic," *International Journal of Information Security*, 2015.

[22] L. J. Tashman, "Out-of-sample tests of forecasting accuracy: an analysis and review," *International journal of forecasting*, vol. 16, no. 4, pp. 437–450, 2000.

[23] "Time Series Cross-Validation," https://cran.r-project.org/web/packages/greybox/vignettes/ro.html.