

A Study on Securing Safety via Application of the Blind Spot Metrics for Report Cases of the Police

Benjamin Aziz^{†*}, Jeyong Jung^{*}

^{*}Department of Police Science, College of Social Sciences, University of Ulsan, Ulsan, South Korea

[†]School of Computing, University of Portsmouth, Portsmouth, United Kingdom

Abstract

One of the great challenges of Information and Communication Technology is the difficulty of measuring its efficiency. Previous literature mostly examined correlations between police response time and other features, but failed to quantitatively measure and study time related features themselves. This paper measures the efficiency of Information and Communication Technology on policing by using two cyber security metrics: Mean Blind Spot and the Approximate Mean Blind Spot metrics. Using a real dataset from a Korean police station, various time related features are used to evaluate these metrics. The results provide some insights into the police personnel management.

Keywords: Data analysis, police case studies, risk metrics, security

1. Introduction

Police response time is recognised as an important criterion when measuring police performance and effectiveness in many societies [1, 2]. It is emphasised to satisfy expectations of citizens regarding policing services [3, 4]. This is also the case in South Korea, where police are expected to respond to 112 calls within just a few minutes. However, both the police and citizens tacitly accept the reality that it is almost impossible to respond to a scene within such short period of time, due to various reasons such as traffic, uncooperative citizen attitudes, frequent demand for police services. However, as gaining public trust is of vital importance to the police organisation, reducing response time is deemed to be one of the priorities for the police.

In fact, there have been numerous approaches to address this issue within the Korean police. Those include training patrol officers, changing a patrolling strategy, revising the 112 system or redefining patrolling jurisdictions. There is a critical missing piece in all of these efforts; the fact that the police vaguely recognise the problem and failing to clearly define it. In other words, the police have not attempted to quantitatively measure the problem or the delayed police response. Without a

clear definition of the problem, no one can evaluate a solution in an objective and precise manner.

The orientation of this research is driven by a motivation towards the convergence of Information and Communication Technology (ICT) and real world policing. In this paper, we intend to fill this empirical gap by applying metrics to a Korean 112 dataset. This research aims to achieve two goals. The first is to pinpoint the problem as to the police responses by quantitatively measuring it. Unfortunately, the 112 dataset has not thus far been fully utilised by researchers due to accessibility difficulty and the perception that such datasets are of little/no use. By using some features related to time of the responses in the dataset, we could take a quantitative approach to formulating the problem. The second aim is to test existing theoretical metrics against a real dataset. This aim does not only validate the metrics that we proposed in [5], but also produces policy implications for the police fit for their working environment.

2. Related Work

In academic circles concerned with policing and security research, response time has been a core research subject for decades [6, 3, 1, 7, 8, 9, 10, 4, 11]. Response time refers to “the amount of time occurring between the time a police unit on the street received a call from the dispatcher and the time when that unit contacted the

*Corresponding author

Email addresses: benjamin.aziz@port.ac.uk (Benjamin Aziz[†]), pancon@ulsan.ac.kr (Jeyong Jung^{*})

citizen involved” - [12]. Many studies [9, 2, 11] examined the causal relationship between police performance and response time, as response time is considered as one of a number of crucial measures of efficient policing. Research on the response time has progressed in two distinctive streams: The first stream involved crime control. Research in this stream studied an effect of the response time on arresting of perpetrators. The main argument was that shortening the response time increased the probability of arrest at the scene [1, 7, 8]. In [8], the authors found a negative relationship between response time and burglary arrests after controlling significant incident characteristics such as workload, time of incident, whether a perpetrator was caught etc. Analysing data from Houston Police Department, [1] found a similar result. The second stream is related to public satisfaction. There is no doubt that citizens expect the police response to be within a “socially acceptable” period of time. According to [4], rapid police response increases the level of satisfaction among the public. On the other hand, [3] found that high responsiveness of the police reduced the chance of “being victimised”, which in turn also increased the victims’ satisfaction level.

Nonetheless, despite the above and other numerous studies on police response time, no research has adopted metrics as a framework in this context. The main reason could be that previous studies were within the domain of policing and criminal justice. In this study, we took an interdisciplinary approach to address the domain problem of policing by applying metrics from cyber security. Metrics are considered a valuable tool for decision-makers in any public or private organisations. Managers in organisations have a tendency to quantify their activities and issues by using metrics as a method to evaluate organisational goals and objectives [13, 14]. One great example is a Goal Question Metric approach, which emphasises the quantification of an organisational goal [15]. There are substantial advantages to using metrics; e.g. persuading decision-makers, facilitating communications with employees and calculating quantified impact on organisations.

To contribute to knowledge accumulation in this field, we use relevant metrics which incorporate recovery time from a prior incident until the next call for service. Our study does not intend to examine a relationship or causal effect of the response time, but takes the response time as a crucial element of security metrics we try to apply to the dataset. This interdisciplinary approach is expected to identify how ICT influences policing strategies or tactics in the real world.

3. Description of the 112 Dataset

This study uses an emergency (“112”) call dataset from one police station in Seoul in South Korea (there are 31 police stations in Seoul). The police station is located in the centre of Seoul. Its jurisdiction spans 9.96km². The dataset contains 48553 entries contained in a single file of size 4.3MB. It was recorded over a period of one year from 1st November 2017 to 31st October 2018. Of these entries, there are 40783 entries that are good for our analysis to follow. The other 7770 entries were excluded from the analysis as they lack data related to either the dispatch time or the finishing time of an incident. The dataset consists of the following features:

- F1. Date of reporting.* This is of type date, and it represents the date on which the 112 call was made.
- F2. Time of taking the call.* This feature is of type time, and it represent the time in the day at which the 112 call was taken by an operator.
- F3. Date and time of commanding dispatch.* This feature is of type date-time, and it represents the date and time at which a call taker commanded a patrol officer to respond to the incident.
- F4. Date and time of response - starting time.* This feature is of type date-time, and it represents the date and time at which a police patrol officer started to respond after receiving the command (whether to call the caller or drive to the scene itself).
- F5. Date and time of response - arrival time.* This is of type date-time, and it represents the date and time at which the patrol officer arrived at the scene.
- F6. Date and time of response - finishing the response.* This feature is of type date-time, and it represent the date and time the patrol officer finished the response.
- F7. Automatic arrival.* This feature is a binary Yes/No, where Yes means a patrol car arrived within 50m of the incident scene, a GPS attached to the police car automatically logged the F5 feature, and No means that the police officer did not need to go to the scene or that there was a malfunction of the GPS system in the car.
- F8. Code.* This is a text value representing the severity level of the incident. Its value ranges from Code0 to Code4, with Code0 being the most severe level and Code4 being the least severe level not requiring a patrol officer to physically go to the scene.
- F9. Type of incident.* This feature has a text value that represents the type of incident involved. There are six incident types: *traffic, miscellaneous work, other crime, public order management, coordination with other agencies* and *serious crime*.

F10. Jurisdiction of the police box. This feature has a character value that represents the police box. There are seven police boxes, A-G, each of which has its own jurisdiction. These police boxes are categorised into *Jigudae* (A, B, C), which are larger than *Pachulso* (D, E, F, G) in size, covering more geographical area.

F11. Type of response - treatment by officers. This feature has a text value that represents the response or treatment of the patrol officer. This includes *arrest, further investigation, finishing on the scene, non-treatment, responding without going to the scene, false report, transfer to other organization (i.e. to other police stations, agencies, or hospitals).*

F12. Caller gender. This feature has a text value that represents the caller's gender. This is either *male, female* or *unknown*.

Later, we write, Fi_j , for $i = 1 \dots 12$, to refer to the value of feature Fi for a specific entry j in the dataset. The following is a sample entry from the dataset:

```
'30/11/2017' '23:49:34' '30/11/2017 23:49'
'30/11/2017 23:51' '30/11/2017 23:52' '01/12/2017
03:30' 'N' 'C1' 'Other crime' 'A' 'Arrest' 'Male'
```

4. Analysis of the Dataset

4.1. Overview of the Metrics

We introduced in [5] two cyber security metrics: the Mean Blind Spot (MBS) and the Approximate Mean Blind Spot (AMBS) metrics. Informally, MBS is the mean of the differences between the dates and times of the finishing of responses of current incidents, and the dates and times of the commanding of dispatches of next incidents. There are $n - 1$ number of such blind spots, since the metric relates features of an incident to features of the following incident. We can define MBS in terms of the above features and an n number of valid entries, as follows:

$$MBS = \frac{\sum_{j=1}^{n-1} (F3_{j+1} - F6_j)}{n - 1} \quad (1)$$

Intuitively, the MBS metric represents a measure of *readiness* reflecting the efficiency at which current incidents are dealt with (in preparation for future incidents). A positive value for the MBS metric is good, since it indicates that there is a positive time margin, on average, between the occurrence and recovery of incidents.

On the other hand, the second metric, AMBS, was defined in [5] as the ratio of the MTIR (Mean-Time-to-Incident-Recovery) [16] to the MTBSI (Mean-Time-

Between-Security-Incidents) metrics [16]. Before proceeding further, we first adapt these metrics in terms of the dataset features. First, we redefine MTBSI as the mean time between any two incidents in terms of the $F3$ feature, as follows:

$$MTBSI = \frac{\sum_{j=1}^{n-1} (F3_{j+1} - F3_j)}{n - 1} \quad (2)$$

We chose the $F3$ feature as this represents the first point in which real action is taken (issuing the command to dispatch a police unit.) We then redefine MTIR:

$$MTIR = \frac{\sum_{j=1}^n (F6_j - F3_j)}{n} \quad (3)$$

as the mean time between dispatching a police unit to the time the action taken is finished. The AMBS is therefore defined:

$$AMBS = \frac{(\sum_{j=1}^n (F6_j - F3_j)) \times (n - 1)}{(\sum_{j=1}^{n-1} (F3_{j+1} - F3_j)) \times n} \quad (4)$$

as the ratio between the two aforementioned metrics. Intuitively, AMBS is a measure of the queue of incidents tied-in to some resource while that resource is dealing with an existing incident. Therefore, it gives an indication of how much *loaded* a resource (i.e. police unit, police box etc.) could be at any one point of time.

4.2. Results

Table 1 shows the results of the MBS and AMBS analyses, as well as the breakdown of the relevant (correct) data entries, for (i) Severity Codes from 0 to 4, (ii) Jurisdictions from A to G, and (iii) Incident Types of Traffic (T), Public order management (P), Miscellaneous work (M), Other crime (O), Coordination with other agencies (C) and Serious crime (S).

The MBS analyses imply that Code0 has the highest positive value which means there is a plenty of time to prepare for the next case, while Code2 has the highest negative value which signifies a serious lack of readiness. The MBS values of other codes are somewhere in between. In terms of the incident types, Serious Crime (S) - as expected - is handled with enough resources, while at the other end, Other Crime (O) is not. However, the results from these two classifications provide limited insight in practicality in that, in reality, 112 calls are dealt with by the time sequence of the occurrence of those calls. On the other hand, statistics by jurisdictions provide good information because actual police response is run within each jurisdiction regardless of severity code or incident type of a reported case.

	Number of relevant data entries	MBS (min.)	Approximate MBS
Severity Codes			
Code0	234	2162.75	1
Code1	9602	-9.78	2
Code2	28259	-28.86	3
Code3	2688	169.61	1
Code4	0	undefined	undefined
Jurisdictions			
A	7401	21.96	1
B	9786	3.77	1
C	8164	11.75	1
D	4735	54.22	1
E	3708	90.96	1
F	3985	90.26	1
G	3004	125.99	1
Incident Types			
T	5832	46.13	1
P	14824	-4.00	2
M	3585	65.53	1
O	11208	-4.87	2
C	3440	106.78	1
S	1894	182.03	1

Table 1
Results of the analysis

The MBS results by jurisdiction can be compared to the number of patrolling officers in a police box: A - 31, B - 29, C - 29, D - 20, E - 20, F - 21 and G - 22 officers, obtained outside of the dataset. This comparison shows that allocation of personnel would benefit from the MBS results, since the ratio of the MBS for highest jurisdiction (G) to the lowest (B) is over 33 times while B has only just over 30% more officers than G, which is inconsistent with the MBS metric. Jurisdictions with high MBS values (E, F and G) have lower numbers of personnel than those with low MBS values (A, B and C), therefore some balancing is required. Currently, personnel allocation is based on the status of the police box, whether it is *Jigudae* or *Pachulso*. If the police station takes the MBS results into consideration, allocation of field personnel can be made more efficient.

The AMBS results highlighted uniform load by jurisdiction, however, when it comes to incident types, we notice higher load for public order and other crimes, possibly due to fewer resources dedicated to these types.

5. Conclusion

This study has demonstrated how the use of data analysis can shed some light on the impact of police resourcing in reducing response times. The previous literature mostly studied impacts of response time on variables such as police performance, crime control, or public satisfaction, but not much on managing response time itself. Therefore, this study contributes to this research gap, through quantitatively evaluating existing MBS and AMBS metrics [5]. In this regard, our anal-

ysis is expected to generate policy implications in the future, which could be helpful to the concerning organisation from the human resources management point of view. As such, this study intends to enlarge the scope of research subjects, which concern the linkage between police management and risk metrics. This could be a contribution to knowledge in policing and risk studies.

For future research, we recommend that more real world datasets are used to test the (approximate) blind spot metrics. This will help us to not only see whether these metrics are applicable with high practicality, but also refine the metrics and contribute to the improvement of the efficiency of the real world scenarios.

References

- [1] A. Cihan, Y. Zhang, L. Hoover, Police response time to in-progress burglary: A multilevel analysis, *Police Quarterly* 15 (3) (2012) 308–327.
- [2] L. W. Sherman, Policing for crime prevention, in: L. W. Sherman, D. C. Gottfredson, D. L. MacKenzie, J. Eck, P. Reuter, S. D. Bushaway (Eds.), *Preventing crime: What works, what doesn't, what's promising*, U.S. Department of Justice, Washington, DC, 1998, pp. 295–336.
- [3] B. S. G., F. Horvath, Crime-victim evaluation of police investigative performance, *Journal of Criminal Justice* 19 (3).
- [4] T. J. McEwen, E. F. Connors, M. I. Cohen, Evaluation of the differential police response field test, US Department of Justice, National Institute of Justice, Washington, DC, 1986.
- [5] B. Aziz, A. Malik, J. Jung, Check your blind spot: a new cybersecurity metric for measuring incident response readiness, in: *Proceedings of the 4th International Workshop on Risk Assessment and Risk-driven Testing*, Vol. 10224 of Lecture Notes in Computer Science, Springer, 2017, pp. 19–33.
- [6] B. Vidal, Jordi, T. Kirchmaier, The effect of police response time on crime clearance rates, *The Review of Economic Studies* 85 (2).
- [7] C. Clawson, S. K. Chang, The relationship of response delays and arrest rates, *Journal of Police Science and Administration* 5 (1).
- [8] C. R. Timothy, L. Blake, The effects of patrol workloads and response strength on arrests at burglary emergencies, *Journal of Criminal Justice* 33 (3).
- [9] G. L. Kelling, M. H. Moore, The evolving strategy of policing, perspectives on policing, Tech. rep., US Department of Justice, National Institute of Justice (1988).
- [10] J.-S. Lee, J. Lee, L. T. Hoover, What conditions affect police response time? examining situational and neighborhood factors, *Police Quarterly* 20 (1).
- [11] J. M. Stevens, T. C. Webster, B. Stipak, Response time: Role in assessing police performance, *Public Productivity Review* 4 (3).
- [12] G. L. Kelling, T. Pate, D. Dieckman, C. E. Brown, The kansas city preventive patrol experiment, Tech. rep., Police foundation (1974).
- [13] T. Kayworth, D. Whitten, Effective information security requires a balance of social and technology factors, *MIS Quarterly Executive* 9 (3).
- [14] J. Kwon, J. R. Ulmer, T. Wang, The association between top management involvement and compensation and information security breaches, *Journal of Information Systems* 27 (1) (2013) 219–236.

- [15] V. R. Basili, G. Caldiera, H. D. Rombach, The goal question metric approach, *Encyclopedia of software engineering* (1994) 528–532.
- [16] T. C. for Internet Security, *Cis security metrics v1.1.0* (Nov. 2010).