An Internet of Things Solution for Intelligence Security Management

Short Paper

Xiaotong Sun
School of Information, Renmin University of China
59 Zhongguancun Street, Beijing 100872, China
sun_xiao_tong@ruc.edu.cn

Qili Wang
School of Information, Renmin University of China
59 Zhongguancun Street, Beijing 100872, China
wql@ruc.edu.cn

Abstract

Digital governance undertaken by government combines information and communication technologies (ICTs) and government services to accomplish government functions in an effective and efficient way. Information systems can facilitate digital governance through desirable technology choices. With ubiquitous, integrated, intelligent and universal devices surrounding us as foundations, we introduce Internet of Things (IoT) technology, a newcomer in ICTs, to fulfill digital governance while simultaneously assure the innovative technology to have its intended effect. In this study, we develop an IoT-based solution for intelligence security governance (ISG), a critical branch of digital governance. We use situational crime prevention (SCP) approach, an achievement of criminology research, to describe, explain and predict events in ISG and extend the context of SCP to IoT environment. Synthesizing SCP with IoT technologies contributes to the theory development of SCP and offers powerful tools for public sectors such as police forces.

Keywords: Digital government, digital governance, Internet of Things, design science, situational crime prevention

Introduction

Digital governance is an evolving concept for government in digital age, which combines information and communication technologies (ICTs) and government services (Dawes 2009). Governments are considered to be "smart" when they offer responsive, efficient and accountable public services relying on communication networks and information technology infrastructures. Information systems (IS) facilitate realization of digital governance through digital service design (Williams et al. 2008). Design efforts made to radically rethink how government services work aim at making desirable technology choices. Among existing government information systems, appropriate contemporary ICTs, such as wireless telecommunications, mobile internet, and big data analysis, play a central role in reorganizing services in a digital way (Andrade and Doolin 2016). Adoption of these technology innovations holds the potential to attain information-sharing, interaction-enabled and transparent digital governance.

As a result of ICT's development towards the direction of ubiquity, integration, intelligence and universality, many of the devices all around us will be on the communicating-actuating network in one form or another, which indicates the advent of the Internet of Things (IoT) era (Gubbi et al. 2013). Multiple devices and techniques have been developed to collect information by utilizing senses such as sight, sound and touch, which constitute the foundation and core part of IoT technology. Government and public agencies have upgraded to IoT devices to collect data of higher quality. However, the integrity and intelligence characteristics of IoT are still inadequately understood by government agencies. In other words, the IoT

techniques are utilized independently of each other and play no role of processing and leveraging information. Although introducing widespread ICT-based communication applications, such as social networking website, into digital government has been proved an effective way to improve governance (Hong and Kim 2016), how IoT can make it easier for governance to fulfill its functions while simultaneously assure the regulation have its intended effect is still unclear. To fill this knowledge gap, we propose an IoT solution to improve the capacity of governments to conceive and implement innovative IoT approach.

We establish strategies for IoT implementation in digital governance of crime detection, which refers to as intelligence security governance (ISG). ISG is a critical branch of digital governance since governments are responsible for the preservation of public order and safety. To better describe, explain and predict crime commitment, we introduce situational crime prevention (SCP) approach, an achievement of criminology research, into ISG and extend its context to IoT environment. Synthesizing SCP with IoT technologies contributes to the theory development of SCP and offers powerful tools for police forces to detect criminal act (Gregor and Hevner 2013). Prior studies show that identifying local problems to solve, generating specific solutions, and promoting governance effectiveness help create more feasible IoT-based solutions (Lal Das et al. 2017). In this study, we examine the smuggling vehicle detection problem in ISG.

Both governments and citizens can benefit from a more efficient and effective ISG. Our study can provide several practical implications for these stakeholders. From the perspective of government, our proposed solution can help reap the significant potential benefits of IoT such as streamlined regulatory processes and reduced regulatory burden. For instance, the IoT-based automatic detection systems can greatly alleviate the physical burden of human monitoring in the security branch of the government through substituting manual inspections. From the perspective of citizens, the improvement of ISG can bring a safer and more peaceful life environment since real-time detection can act as prevention measures with a purpose to stop the commission of crimes.

Related Research

Digital governance refers to a new form of government practice that shifts from bureaucratic mode to ICT-enabled innovative mode (Kraemer and King 2006). The application of digital ICTs to promote the transformation of government functions and the adjustment of governmental structures is widely viewed as the enlightened way to improve internal efficiency and effectiveness (Milakovich et al. 2012). Beyond the concerns typically in association with digital governance, research problems encompass the benefits of tools developed for governance in digital age as an open and dynamic socio-technical system (Dawes 2009). How public sectors can respond to some of the challenges arising from societal problems such as crime, migration and climate change using ICT-based systems is considered to be a critical issue (Millard 2015). Misuraca et al. (2012) proposed a solution of scenario design framework defined according to two key impact dimensions: extent of openness and transparency and extent of integration in strategy intelligence. Based on an analysis conducted on research literature in the digital government field (Janowski 2015), digital governance has evolved into contextualization stage which shows its dependency on a particular application scenario.

However, there is still a lack of growth in the number of digital governance articles focusing on the contextualization stage (Janowski 2015). Viewed from research domain in information system, digital governance research is closely related to the design science paradigm, a problem-solving paradigm, that focuses on evaluating and determining the utility of information technology and ICT-based systems (Gregor and Hevner 2013). As stated by Hevner et al. (2004), this stream of research proactively seeks problem solving, creation and innovation. To continue with further research of digital governance, researchers are facing a perennial problem that there is no consolidated approach to integrate, use and process new sources of quantitative and qualitative data (Misuraca et al. 2012).

In the dawning age of the “Internet of things”, researchers began to utilize data collected from a wide variety of gadgets and devices, such as infrared sensor, weight sensors and other sensing elements (Stankovic 2014). Fueled by the prevalence of IoT devices whose number was expected to reach 24 billion in 2020, an unprecedented expansion in the amount of data and the number of data sources leads to the emergence of various kinds of application systems going up one after another (Buckley 2006). IoT-based systems have been proved supportive to high-risk industries including environment (Lee and Shim 2007), health (Nadj et al. 2016), and safety (Yang et al. 2013). Even though features derived from IoT data are demonstrated as

useful in predictive analysis (Sun et al. 2019) and decision support (Monteiro and Parmiggiani 2019), how to apply these technologies in digital governance remains to be explored. Frameworks that connect technological innovations to the creation of public value are the key motives for the adoption of innovative technologies in digital governance (Meijer 2015). The interconnectivity, real-time capability and being measurement of real-world activities are three characteristics of IoT that may facilitate to realize the unity of motives and effects in digital governance (Ransbotham et al. 2016).

The Proposed Methodology

The digital governance problem we tackle in this study is the lack of artifacts that extend ISG capabilities by incorporating IoT technologies. Artifact design for ISG focuses on predictive analyses of criminal activities. In light of criminology, we propose to use Situation Crime Prevention (SCP) to extract information from environmental sensing data to reconstruct the real-world events and support crime detection. In the case of detecting smuggling vehicles in China, we combine traffic and crime data obtained from the public security bureau to achieve accurate detections. Figure 1 illustrates the concrete steps of our proposed methodology: how to prepare data observed by "Things" for further analysis, how to model interconnected data as features, and how to deploy the features to spot suspects for further investigation.

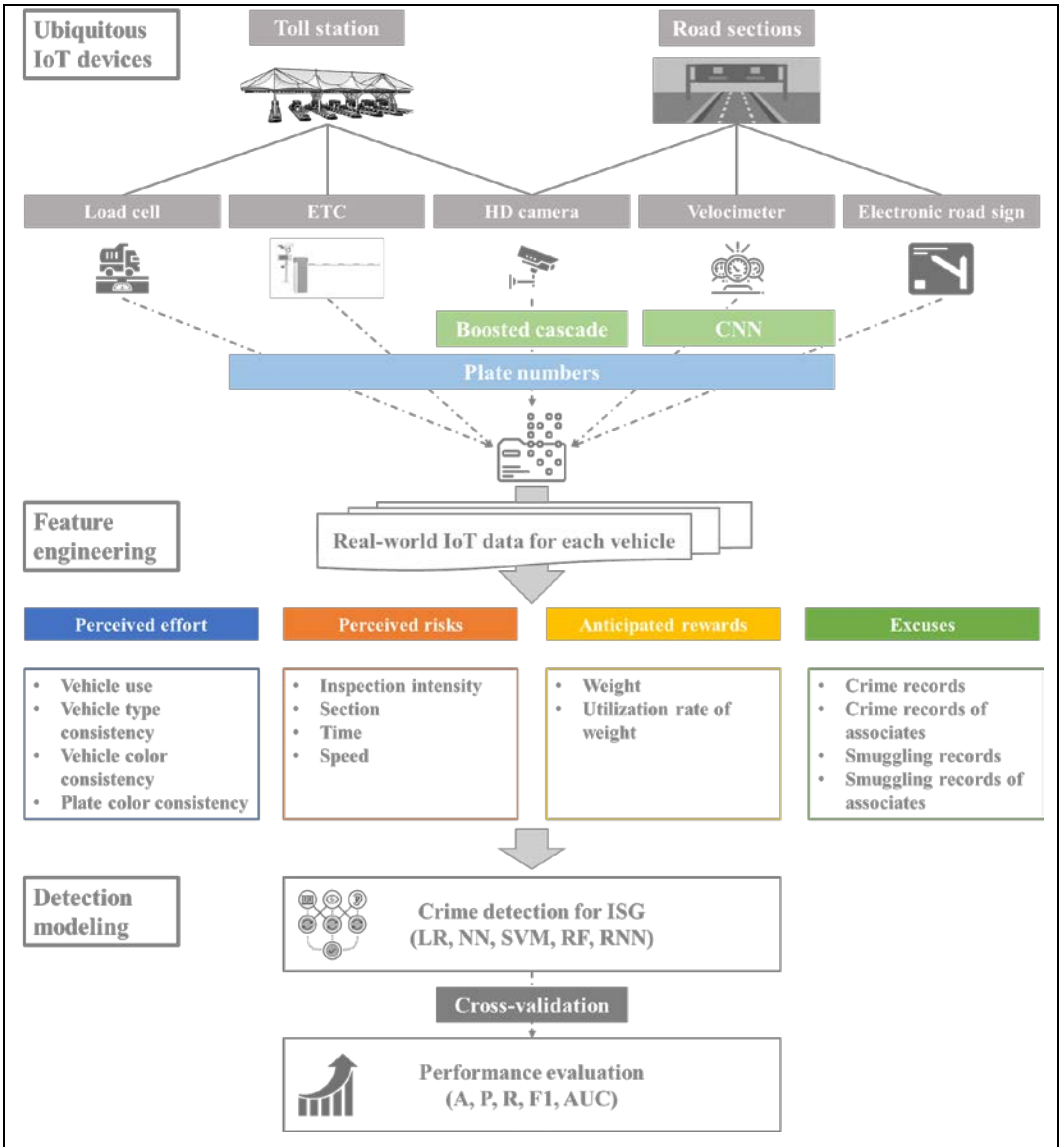

Figure 1. The Proposed Methodology for ISG

Ubiquitous "Things" for Data Preparation

Opportunities to improve efficiency and optimization of ISG exist in the almost imperceptible but prevalent "things" in our lives. These "things" are physical objects which are embedded with sensors and able to transmit data within a network. Connected devices, such as radio frequency identification (RFID) readers, wireless cameras, and sensors, are typical "things" that constitute IoT. Sheer growth in the range of IoT devices leads to a tremendous amount of data unceasingly generated with unprecedented richness. A real-time monitor system using IoT devices can interpret, analyze and predict based on a wealth of information contained in IoT data. The IoT-based monitoring allow rendering of reality since the IoT devices mimic embodied perception when they sense the lifeworld. As IoT devices are increasingly approximating human sensory capacity (Monteiro and Parmiggiani 2019), public security departments can know what is happening while reducing their burden of human monitoring with the assistant of IoT-based monitoring.

Efforts should be paid to seize the opportunities IoT brings to ISG. Security monitoring departments will have to face the challenge how to correspond the numbers generated by sensors or other devices to the reality events and how to be acutely aware of the crimes that is taking place. Addressing this challenge requires specific data preparation including integration and preprocessing for data collected by IoT devices. We focus on IoT devices embedded in public infrastructure (such as roads, street lights, and public spaces) since governments can obtain data flowing from these devices timely and directly. These data obtained directly from public sectors themselves usually has higher primitiveness, accuracy, integrity and reliability and lower cost than those acquired indirectly from private sectors.

Table 1. Common IoT Devices in Public Infrastructure

Location	Road Toll Station			Road Section		
Device	Bayonet HD Camera	Electronic Toll Collection (ETC)	Load Cell	Section HD Camera	Velocimeter	Electronic Road Sign
Technology	Video	RFID		Strain Gauge	Video	Radar
Data Type	Unstructured (Video)	Structured		Structured	Unstructured (Video)	Structured and Unstructured (Image)
Preprocessing Method	Boosted Cascade				Boosted Cascade	Convolutional Neural Networks

Table 1 lists common IoT devices in public infrastructure and describes their properties including the technology applied, position located, type of generated data and method selected to preprocess the data. Overall, scaled implementation of IoT devices are mainly concentrated in road area, especially highways with access control (Lal Das et al. 2017). RFID is an important, relatively mature and highly applied technology in IoT devices. RFID tags mounted on vehicles contain electronic vehicle registration data, such as the plate number, plate color, vehicle type, vehicle color, and owner id. RFID readers located on both sides of road sections and toll stations aid to collect data of vehicles and to achieve better than 99% identification rate of vehicle (Gubbi et al. 2013). There is accordingly a set of coordinate data in time order for each vehicle, collected by electronic road signs distributed in road sections. The time-series data can facilitate the fulfilling of path-identifying function. Sensors are another core component of IoT devices. Different types of sensors enrich data for IoT-based monitoring: radar sensor-based velocimeters obtaining travel speed data, strain gauge sensor-based load cells obtaining vehicle weight data, and video sensor-based camera networks obtaining real-time video of moving vehicles. We adopt state-of-art algorithms for information extraction from the video and image data, including boosted cascade method (Viola and Jones 2001) and convolutional neural networks (Krizhevsky et al. 2012). By analyzing integrated data obtained through IoT technologies, security agents can conjure up states and trajectories of vehicles and profiles of

drivers. It is worth noting that license plate numbers play a key role in the process of integrating data from different data sources.

Criminological Perspective for Feature Engineering

Checkpoints for ISG, which operate automatic monitoring systems, do not require physical observations in regulatory inspections but call for strong analytical capabilities to make sure losing no opportunity to identify criminals. Accordingly, there is a need to create effective IT artifacts for crime detection based on relevant criminology theory (Hevner et al. 2004). To effectively and efficiently tap into the capacity of IoT data to reflect realistic environments, we refer to SCP. SCP provides a theoretical basis to investigate how immediate environments impact criminal acts. Clarke (1995) suggests that SCP could help analyse the circumstance fostering specific kinds of crime, and such an examination could help reduce the opportunity for targeted crimes to occur by environmental change. SCP first identifies factors involved with a specific type of crime from four elements, including perceived effort, perceived risks, anticipated rewards and excuses. Varying variables will be taken as proxy measures for these four elements when studying different types of crime. Then, it seeks to reduce the immediate opportunities for committing crime by altering the identified situational factors. According to SCP, quantifying crime opportunities effectively needs a thorough consideration of the above four elements.

Guided by SCP, we propose a feature extraction framework that measures criminal tendencies from the above four aspects. Since SCP notes that measures should be directed at specific crimes, we take smuggling as an example to illustrate the proposed framework. Smuggling is one of the criminal activities that poses great threats to the state's economic prosperity and the order of its market economy. One of the most feasible way to combat smuggling is intercepting the vehicles used to transport contraband in transit. IoT data, as previously described, collected by "things" embedded in road area offer new insights into feature engineering for smuggling detection. Hence, features are constructed with application of SCP and IoT data, as shown in Table 2.

Perceived Effort

We consider the perceived effort as the physical and mental energy that need be consumed to evade crime detections. Camouflage is one of the most common way for smugglers to make their illegal transports appear legal (Thursby et al. 1991). Most cases of smuggling accompanied with identity theft behaviors that conceal smugglers' true identity by disguising the numbers or color of the registration plate using someone's motor vehicle registration information (Koops et al. 2009). Accordingly, people who show intentional concealment of identity hold strong potential to become an offender since they often tend to underestimate the effort involved in a criminal act to an acceptable level. To disclose the delinquent tendencies, we establish a set of features which examine the consistency between recognized vehicle attributes extracted from camera video data and registered vehicle attributes obtained from information containing in RFID tags. We also apply vehicle use to measure the opportunities for crimes to occur, from the fact that latent criminals are most likely to pretend to drive official vehicles for the convenience of avoiding inspections. These perceived effort features, targeting to disguises of criminals, are used to measure the extent to which effort is believed to be required in the commission of crime.

Perceived Risks

We consider the perceived risks as offenders' perceptions of the possibility of being caught and penalized. From the current view, the main deterrent threat to potential offenders is furnished by formal surveillance provided by police. For smuggling activities, intercepting the vehicles used to transport contraband in transit is the common method used by public security departments. Study shows that smugglers are likely to carefully choose the route for illegally transport to avoid spot checks in transit (Kaza et al. 2007). We measure the perceived risks of smugglers through the security surveillance intensity along the route. Factors influencing the risk of offenders' transporting plan include time, sections and inspection intensity of the route. Additionally, high speed driving is a common tactic for smugglers increasing interception difficulty and mitigating risks. Vehicle speed, which can be measured by velocimeters on different road sections, is incorporated into our constructed features to confront the tactic. These perceived risks features serve to capture the immediate risk that potential offender is facing in ongoing transportation activities.

Table 2. SCP-Based Features and Measurement

Components	Feature	Measurement
Perceived Effort	Vehicle Use	A discrete variable representing vehicle use, which can be converted from license plate colors or other specific combination of numbers and letters in plate numbers.
	Vehicle Type Consistency	A Boolean variable whose value is 1 when the recognized type of the vehicle is same with the registered type obtained by the license plate number, and 0 otherwise.
	Vehicle Color Consistency	A Boolean variable whose value is 1 when the recognized color of the vehicle is same with the registered color obtained by the license plate number, and 0 otherwise.
	Plate Color Consistency	A Boolean variable whose value is 1 when the recognized color of the license plates is same with the registered color obtained by the license plate number, and 0 otherwise.
Perceived Risks	Inspection Intensity	Inspection intensity is measured by average check ratio which is the average of check ratios of all the checkpoints the vehicle passes through. Check ratio is the ratio of total number of vehicles subjected to thorough check to that of vehicles passing through the checkpoint.
	Section	A Boolean variable whose value is 1 when the vehicle passes through sensitive sections, and 0 otherwise. Sensitive sections are road segments marked as sensitive by agents who are experts in related crimes.
	Time	A Boolean variable whose value is 1 when the vehicle arrives the checkpoint at a sensitive time, and 0 otherwise. Sensitive time is the time point which falls in time intervals marked as sensitive by agents who are experts in related crimes.
	Speed	A continuous variable whose value is the average of vehicle speed throughout whole itinerary.
Anticipated Rewards	Weight	A continuous variable whose value is the weight of the vehicle.
	Utilization Rate of Weight	A continuous variable whose value is the ratio of the actual weight of vehicle divided by the limit weight of it.
Excuses	Crime Records	A Boolean variable whose value is 1 when the owner of the vehicle has committed a crime, and 0 otherwise.
	Crime Records of Associates	A Boolean variable whose value is 1 when any relative of the vehicle owner has committed a crime, and 0 otherwise.
	Smuggling Records	A Boolean variable whose value is 1 when the owner of the vehicle has committed smuggling, and 0 otherwise.
	Smuggling Records of Associates	A Boolean variable whose value is 1 when any relative of the vehicle owner has committed smuggling, and 0 otherwise.

Anticipated Rewards

We consider anticipated rewards as spiritual and material returns that criminals expect to get from their perpetration of crime. The high return, which comes from price disparity due to high levies on imported goods, is a critically important incentive for smuggling (Norton 1988). As smugglers face significant risk of penalties if they caught with contraband in each illegal transport, they may act in a greedy way that they can get as much proceeds as possible from the risk they take. It is evident that the more goods are transported in a single transport, the higher the potential profits of smugglers. Correspondingly, we regard

the total weight of vehicle and goods, which can be collected by strain gauge sensors, as a feature to represent the anticipated rewards. Considering the limited interior space in vehicles, smugglers will seek to make full use of them. To reflect this attempt, we add weight utilization rate of vehicles as a cue to the feature set. These anticipated rewards features can exhibit the characteristic of typical vehicles for smuggling as heavy weight and high weight utilization rate.

Excuses

We consider excuses as events that happened around criminals and used to rationalize their conduct. Intuitively, things happened both to criminals themselves and to anyone to whom they are related can impact their feelings of own illegal conducts. Criminal records are a strong indicator of re-implementation of criminal acts since material reward, euphoria or other benefits obtained by past delinquencies can consolidate criminal will. We investigate the criminal records of vehicle owners to describe their will to commit an offense. We also consider the criminal records of vehicle owners' relatives when constructing the crime detection features. In addition, it is likely to form an intention to commit the same crimes as friends or oneself having engaged in (Thomas 2015). Thus, we introduce features focusing on smuggling records to reveal the intention. These excuses features aim at the psychological preparation that are required prior to criminal activities.

Machine Learning Methods for Predictive Modeling

A high hit rate crime detection mechanism can facilitate ISG in a cost-effective manner. Recent developments in machine learning techniques have elevated the potential for solving security governance problems (Dawes 2009). The serious consequences of crime detection failure put forward strict request to model performance. Given the key requirement on prediction accuracy, machine learning approaches are better suited than traditional regression methods which emphasize interpretability (Lin et al. 2017). We use machine learning methods to predict the opportunity that a vehicle is smuggling contraband by applying the variables constructed based on SCP as shown in the bottom of Figure 1. Since there has no method been acknowledged as the best one for ISG so far, we use common machine learning methods including logistic regression (LR), neural networks (NN), support vector machine (SVM), random forest (RF), and recurrent neural network (RNN) in this study.

Table 3. Description of the Data Set

Systems	Data Content	No. of Variables
Highway Toll System	Plate number, entry time, entry section, exit time, exit section and vehicle weight	6
Digital Archive System	Plate number, owner id, plate color, vehicle type, vehicle color, owner criminal records	6
Radar Speed Measurement Snapshot System	Plate number, time, position, speed	4
Video Monitoring System	Plate number, time, position, recognized plate color, recognized vehicle type, recognized vehicle color	6
The number of normal travel process is 902,958; the number of smuggling travel process is 397.		

Preliminary Analysis

We will use large real-world datasets obtained from the public security bureau of a border city with a population over one million people in China to test the performance of our proposed methodology. The IoT datasets in different information systems span about six months from January 1, 2018, to July 7, 2018. Vehicle travel processes from entry into a highway to exit are regarded as detection objects. A record in highway toll system including plate number, entry time, entry section, exit time, exit section and vehicle weight represents a travel process. All travel processes for smuggling were identified and labeled by

matching the criminal records in digital archive system with highway toll records; The timing of arrests and information on arrested persons and related vehicles in criminal records were used for the purpose of data matching. We also applied the plate numbers in highway toll records to retrieve the basic information on vehicles and their owners from the digital archive system. Speed records for a vehicle travel process were collected from the radar speed measurement snapshot system, first by screening out the speed records of recording time in the range of travel beginning and ending time and then by searching the selected records by the plate number. The vehicles' conditions in real-time were recorded with the form of video in video monitoring system. We extracted the required information such as when and where the vehicle was and what color the vehicle plate and vehicle itself were using the rapid object detection algorithm proposed by Viola and Jones (2001). Table 3 describes the summary statistics of the datasets.

Further Evaluation and Expected Contribution

Consistent with the design science paradigm (Hevner et al. 2004), we will conduct a series of experiments to test and demonstrate the effectiveness of our proposed methodology for ISG. The detection performance will be quantified using standard metrics including accuracy, recall, F1 score, and the area under the receiver operating characteristics (ROC) curve (AUC). Cross-validation as the most common approach for parameter adjustment and model selection will be employed to evaluate detection models on the holdout data. For further evaluation, we design three sets of experiments to assess our proposed methodology. In the first set of experiments, five classifiers (LR, NN, SVM, RF, RNN) will be used to detect smuggling activities. We will also investigate each of the four categories of SCP-based features independently. In the second set of experiments, we will examine the incremental effect of including each set of SPC-based features and a full combination of SCP-based features. The classifiers using features adapted from existing rule-based ISG method will be used as baseline methods. In the third set of experiments, we will compare our proposed methodology with those smuggling detection methods that have attained state-of-the-art results. Since the Perceived Effort variables are constructed based on the findings of previous studies and the Anticipated Rewards variables are derived from the practical experience of police officers, we speculate that these two sets of SCP-based features will perform well independently. As for the Excuses variables, we suppose that they can achieve great performance when measuring the incremental effects of each set of features in a comprehensive consideration of the high relevance of variables and the imbalance of data.

The underlying contributions of our study are threefold. Firstly, the technology and equipment of IoT which can be used for ISG are sorted out, and an innovative IoT-based crime detection method is proposed. Secondly, in the ISG field, we introduce criminology—SCP approach—as a basis to construct features, and take the detection of smuggling as an example to illustrate the feature engineering. Finally, large real data sets will be used to demonstrate the effectiveness of the proposed methodology and its application value in practical scenarios.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (Grant No. 71771212, U1711262), Humanities and Social Sciences Foundation of the Ministry of Education (No. 14YJA630075, 15YJA630068), and Fundamental Research Funds for the Central Universities, and Research Funds of Renmin University of China (No. 15XNLQ08). Qili Wang is the corresponding author.

References

Andrade, A.D., and Doolin, B. 2016. "Information and Communication Technology and the Social Inclusion of Refugees," MIS Quarterly (40:2), pp. 405-416.

Buckley J. (Ed.) 2006. The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, NY.

Clarke, R. V. 1995. "Situational Crime Prevention," Crime and justice (19), pp. 91-150.

Dawes, S. S. 2009. "Governance in the Digital Age: A Research and Action Framework for an Uncertain Future," Government Information Quarterly (26:2), pp. 257-264.

Gregor, S., and Hevner, A. R. 2013. "Positioning and Presenting Design Science Research for Maximum Impact," MIS Quarterly (37:2), pp. 337-355.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. 2013. "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future generation computer systems (29:7), pp. 1645-1660.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," MIS Quarterly (28:1), pp. 75-105.

Hong, S., and Kim, S. H. 2016. "Political Polarization on Twitter: Implications for the Use of Social Media in Digital Governments," Government Information Quarterly (33:4), pp. 777-782.

Janowski, T. 2015. "Digital Government Evolution: From Transformation to Contextualization," Government Information Quarterly (32), pp. 221–236.

Kaza, S., Wang, Y., and Chen, H. 2007. "Enhancing Border Security: Mutual Information Analysis to Identify Suspect Vehicles," Decision Support Systems (43:1), pp. 199-210.

Koops, B. J., Leenes, R., Meints, M., van der Meulen, N., and Jaquet-Chiffelle, D. O. 2009. "A Typology of Identity-Related Crime: Conceptual, Technical, and Legal Issues," Information, Communication & Society (12:1), pp. 1-24.

Kraemer, K., and King, J. L. 2006. "Information Technology and Administrative Reform: Will E-Government be Different?" International Journal of Electronic Government Research (2:1), pp. 1-20.

Krizhevsky, A., Sutskever, I., and Hinton, G. E. 2012. "ImageNet Classification with Deep Convolutional Neural Networks," in Proceedings of the Annual Conference on Neural Information Processing Systems, pp. 1097-1105.

Lal Das, P., Beisswenger, S. C., Mangalam, S., Yuce, M. R., and Lukac, M. 2017. Internet of Things : The New Government to Business Platform - A Review of Opportunities, Practices, and Challenges (English), Washington, D.C. : World Bank Group.

Lee, C. P., and Shim, J. P. 2007. "An Exploratory Study of Radio Frequency Identification (RFID) Adoption in the Healthcare Industry," European Journal of Information Systems (16:6), pp. 712-724.

Lin, Y. K., Chen, H., Brown, R. A., and Li, S. H. 2017. "Healthcare Predictive Analytics for Risk Profiling in Chronic Care: A Bayesian Multitask Learning Approach," MIS Quarterly (41:2), pp. 473-495.

Meijer, A. 2015. E-Governance Innovation: Barriers and Strategies," Government Information Quarterly (32:2), pp. 198-206.

Milakovich, M. 2012. Digital Governance, New York: Routledge.

Millard, J. 2015. "Open Governance Systems: Doing More with More," Government Information Quarterly (35:4), pp. s77-s87.

Misuraca, G., Broster, D., and Centeno, C. 2012. "Digital Europe 2030: Designing Scenarios for ICT in Future Governance and Policy Making," Government Information Quarterly (29), pp. s121-s131.

Monteiro, E., and Parmiggiani, E. 2019. "Synthetic Knowing: The Politics of the Internet of Things," MIS Quarterly (43:1), pp. 167-184.

Nadj M., Jegadeesan H., Maedche A., Hoffmann D., Erdmann P. 2016. "A Situation Awareness Driven Design for Predictive Maintenance Systems: The Case of Oil and Gas Pipeline Operations," in Proceedings of the 24th European Conference on Information Systems, pp. 1–10.

Norton, D. A. 1988. "On the Economic Theory of Smuggling," Economica (55), pp. 107-118.

Ransbotham, S., Fichman, R. G., Gopal, R., and Gupta, A. 2016. "Special Section Introduction—Ubiquitous IT and Digital Vulnerabilities," Information Systems Research (27:4), pp. 834-847.

Stankovic, J. A. 2014. "Research Directions for the Internet of Things," IEEE Internet of Things Journal (1:1), pp. 3-9.

Sun, P., Li, J., Bhuiyan, M. Z. A., Wang, L., and Li, B. 2019. "Modeling and Clustering Attacker Activities in IoT through Machine Learning Techniques," Information Sciences (479), pp. 456-471.

Thomas, L. C. 2000. "A Survey of Credit and Behavioural Scoring: Forecasting Financial Risk of Lending to Consumers," International Journal of Forecasting (16:2), pp. 149-172.

Thursby, M., Jensen, R., and Thursby, J. 1991. "Smuggling, Camouflaging, and Market Structure," The Quarterly Journal of Economics (106:3), pp. 789-814.

Viola, P., and Jones, M. 2001. "Rapid Object Detection using a Boosted Cascade of Simple Features," in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 511-518.

Williams, K., Chatterjee, S., and Rossi, M. 2008. "Design of Emerging Digital Services: A Taxonomy," European Journal of Information Systems (17:5), pp. 505-517.

Yang, L., Yang, S. H., and Plotnick, L. 2013. "How the Internet of Things Technology Enhances Emergency Response Operations," Technological Forecasting and Social Change (80:9), pp. 1854-1867.