8-10-2020

# Cyber-risk assessment model for smart cities: A time-series approach

Kalpit Sharma
*Indian Institute of Management Lucknow*, fpm18012@iiml.ac.in

Arunabha Mukhopadhyay
*Indian Institute of Management Lucknow*, arunabha@iiml.ac.in

# Cyber-risk assessment model for smart cities: A time-series approach

*TREO Talk Paper*

**Kalpit Sharma**
IIM Lucknow
kalpit@iiml.ac.in

**Arunabha Mukhopadhyay**
IIM Lucknow
arunabha@iiml.ac.in

Smart cities are the future of urban socio-economic ecosystems. Their success rests on the use of digital technologies, data and design thinking to increase the effectiveness and efficiency of city services. Cyber-attacks have risen by 32% in 2018 due to increased Internet penetration. Hackers attack every 39 seconds, on an average 2244 times a day (Pandey et al., 2019). To understand the intensity of damage to smart cities due to cyber-attacks, we need to understand the core concept of smart cities. Often smart cities are confused to be solely based on technological interventions. Decision-makers conveniently forget about the part where standalone systems must be integrated with each other without their temporal redundancy affecting the overall service desired from them. Generally, the attack lifecycle, that is, from breach to containment can take as long as 314 days. At this rate, cyber-enabled ecosystems can suffer from losses as large as US$ 6 trillion by 2021. In March 2018, Atlanta witnessed a cyberattack which resulted in US$ 10 million in losses by exposing poorly secured public computer systems (Hatmaker 2018). Earlier in 2019, city of Baltimore was under Ransomware attack where the city's system was frozen until a huge ransom of US$ 76,280 was paid to hackers but it is estimated that they lost US$ 18 million in the complete attack lifecycle (Eiten 2019).

We use *protection-motivation theory* and *rational choice theory* (Rogers 1975; Kahneman and Tversky 1979) to study cyber-risk associated with integrated traffic management system (ITMS) in smart cities. We try to investigate following research questions: (i) what is the probability of occurrence of cyber-attacks in a smart city, (ii) what is the expected loss for the smart city due to it, and (iii) what are the ways to mitigate cyber-risk? The average speed of vehicles over time either increases or decreases due to failure of ITMS orchestrated by cyber-attacks. The proportion of cases with anomalous speeds correspond to cyber-attacks and thus, probability of cyber-attack occurrence and associated expected loss can be estimated.

We use a dataset from Citypulse[1], a company that manages smart city projects in Scandinavian countries. The current dataset consists of data collected from traffic monitoring system in Danish city of Aarhus. The dataset consists of data from sensors employed across different streets. These sensors collect data every 5 minutes about the number of vehicles that passed, average speed, median & average time in last observation window. Data extends from months of February 2014 to November 2014 (excluding July 2014). Attributes namely average speed and average measured time are highly correlated and thus, we only study average speed to analyse abnormal congestion pattern. To simplify the analysis, we study only one sensor with 58321 data points which were condensed into 5077 hourly data points across 9 months. The proposed method uses Seasonal Autoregressive Integrated Moving Average (SARIMA) model (Box et al, 1994) to fit time-series model for each month. We analyse the residuals of each monthly time-series and tag data points which have residual value greater than $\pm 2\sigma$. The tagged data points correspond to anomalies due to cyber-attacks on traffic management system.

We observe that October is the riskiest month in terms of occurrence of cyberattacks with higher expected losses leading to congestion on roads. City government may follow undermentioned mitigation strategies: (i) They may implement technology pieces (like stringent firewalls, intrusion detection systems or divert excess/illegitimate traffic to backup servers, CDNs) which will help decrease the probability of an cyberattack and thus, lower the expected loss for riskiest months; (ii) Government can then subscribe to cyber-insurance policies and reduce the risk and severity. Our work, thus, contributes by helping government authorities decide whether to accept, reduce or pass the cyber-risks arising in integrated traffic management systems of smart cities.

[1] CityPulse Dataset Collection. Retrieved from http://iot.ee.surrey.ac.uk:8080/