A Framework for the Smart-City Nerve Center

Ankur Gupta and Purnendu Prabhat
Model Institute of Engineering and Technology - Jammu
Deepak Garg
Bennet University -Noida

The smart-city concept represents an inter-domain application of internet-of-things, cloud computing and big data. To realize the vision of a smart-city, novel integration and application of new advances in Software-Defined Networking, Machine Learning, Real-Time Stream Processing, Social Network Analysis and High-Performance Computing are envisaged. We propose a Smart-City Nerve Centre (SCNC) which collates data from diverse sources to create a single control center for the effective and efficient management of real-time IoT traffic. The SCNC is a cloud-based big-data analysis framework receiving large volumes of structured and unstructured data from geographically diverse sensors, streams from social media, inputs from mobile devices of citizens among others. The SCNC processes the received data, derives insights, enables automated actions and escalates issues to human managers for real-world interventions. This paper establishes the need of the SCNC, lists major technical challenges involved and describes a novel SCNC framework that addresses the stated challenges.

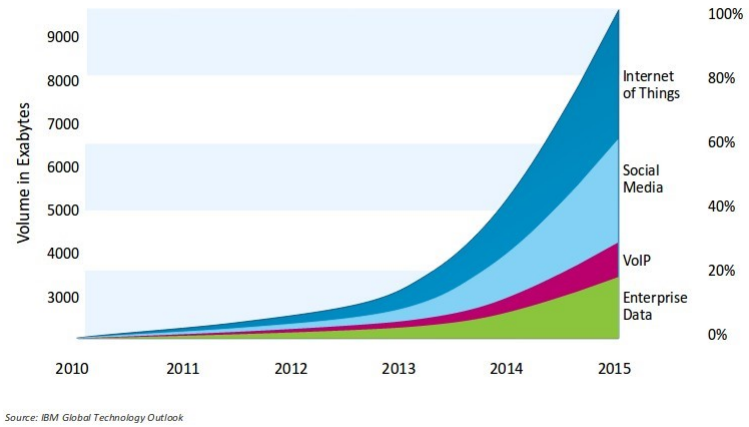
Keywords: Internet of Things, Smart-city, Software Defined Networking, Traffic Engineering.

1. INTRODUCTION

Smart-city encompasses IoT devices installed at different strategic locations, handheld smart devices and a plethora of computing nodes streaming high volumes of real-time data to data-centers for processing and initiating necessary actions. The data can either be sent directly to the cloud or aggregated by intermediate servers which can also help in data authentication and validation. The sheer volume of IoT data threatens to exceed the computing capacity and bandwidth of private data-centers. Thus, smart and efficient handling of IoT traffic is a major challenge which needs to be addressed to enable the next-generation of smart-cities. We propose the Smart-City Nerve Centre (SCNC), a cloud-based big-data analysis framework receiving large volumes of structured and unstructured data from geographically diverse sensors, streams from social media, inputs from mobile devices of citizens among others. The SCNC processes the received data, derives insights, enables automated actions and escalates issues to human managers for real-world interventions, while performing traffic engineering through a multi-tier P2P-SDN architecture.

Smart Cities can be envisaged to handle critical data pertaining to national security, disaster management, road-traffic management, emergency management, e-governance, large scale automation and the like. Thus, it becomes necessary to overcome the network latency and reduce the processing time to the minimum through efficient stream processing while ensuring security and validation of data. These streams potentially burden the storage and computational capacities of smart-city data centers which are typically managed by local Governments through private data centers. In the smart-city Barcelona, the predicted internet data generated by sensors is around 8GB per day; which does not contain the data generated by event driven sources [Sinaeepourfard et al. 2016]. Moreover, the big-data generated by smart-city is characterized to be of high volume, velocity and variety [Kitchin 2014].

Thus, IoT and social media streams are seen as major enablers for smart-city. According to IDC FutureScape, IoT applications will merge streaming analytics with machine learning [IDC]. This directly relates to network congestion and overloaded data-centers. Interestingly, IBM estimates that only 10% of the data is used or actionable [IBM]. Thus, potentially, around 90% of data needs to be filtered out otherwise it will overwhelm the data-center. The sensor data is also known to be highly redundant and can be filtered out or compressed by orders of magnitudes



. Figure 1:Data volume generated by different applications over the years [mqug.org.uk]

[Chen et al. 2014] [IETF]. Authenticity of sensors is another important to ensure privacy and security as Gartner expects a billion-dollar black market by 2020 that sells fake sensors and video data to mask criminal activities. The major challenges in creating efficient IoT data processing architectures include:

—IoT traffic shaping and management

—Addressing security issues such as authentication in IoT environments

—Determining data quality and eliminating noise

—Devising functional redundancy and fault management strategies

—Resource and energy-efficiency

Several researchers have proposed schemes and mechanisms to move processing of sensor data to the end nodes of the network, i.e. the sensors itself or the devices that are directly connected to the sensors. This paradigm is known as Edge computing [Satyanarayanan et al. 2015]. As the edge nodes in a network are not computationally powerful enough to perform high-end data analysis and prediction, research has been done to make small resource sharing networks of the nodes called a fog [Cisco]. Both edge computing and fog computing reduce the bandwidth requirement, network latency and hence enhance QoS. Software-Defined Networking (SDN) is a key enabler for both Edge and Fog computing paradigms.

Frameworks for collating and analysing data from diverse IoT streams are needed to manage data. Cisco's Jasper [Jasper] is a cloud based control platform which is used to manage IoT devices through a user-friendly interface and a dashboard to provide insights. However, it does not provide analysis capabilities for processing inputs from the web, mobile and social networks. Social Internet of Things (SioT) [Atzori et al. 2012] is another platform where the devices have a social network and communicate among each other. These provide opportunity for high QoS augmented reality through pervasive intelligence and analytics.

The rest of the paper is organized as follows: Section 1 provides an overview of the traffic-related challenges for IoT applications in the smart-city concept, justifying the need for SCNC. Section 2 explains the SCNC framework along with its architecture and important algorithms it encompasses. Early results are also provided based on simulation on Mininet. Section 3 concludes the paper and provides some ideas for future work.

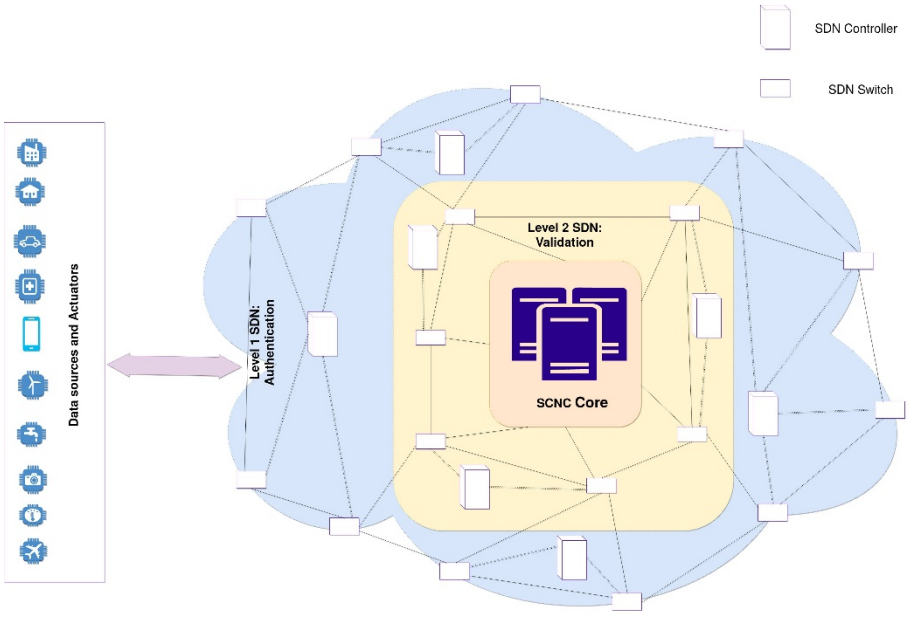
2. SMART CITY NERVE CENTRE (SCNC)

2.1 SCNC Framework

We propose a novel Software Defined Network (SDN) based SCNC framework for traffic engineering to handle the big data generated by smart-city data sources. The framework also performs authentication, noise elimination and guarantees data quality while incurring minimal overhead. Figure 1 shows high-level architecture of the SCNC framework. The architecture contains 2 levels of SDN, Level 1 SDN (L1-SDN) for authentication and Level 2 SDN (L2-SDN) for validation, surrounding the core of SCNC. The SCNC core is responsible for crucial decision making and action initiation.

Data sources like sensors installed at varied locations, hand-held devices etc. generate data packets that enters the L1-SDN. The L1-SDN checks authenticity of the packet by using the Digital Signature Algorithm [Kravitz 1993]. Authentication information is stored in Authentication DB which is a peer-2-peer database and is hosted on the controllers of L1-SDN. It forwards the packet to L2-SDN if they are authentic. Inauthentic packets are dropped. L2-SDN filters the data using Distributed Kalman Filter (DKF) [Olfati-Saber 2007] technique which validates the data based on the history and consensus with other sources. Once validated the packet is sent to the SCNC core. Invalid packets are dropped.

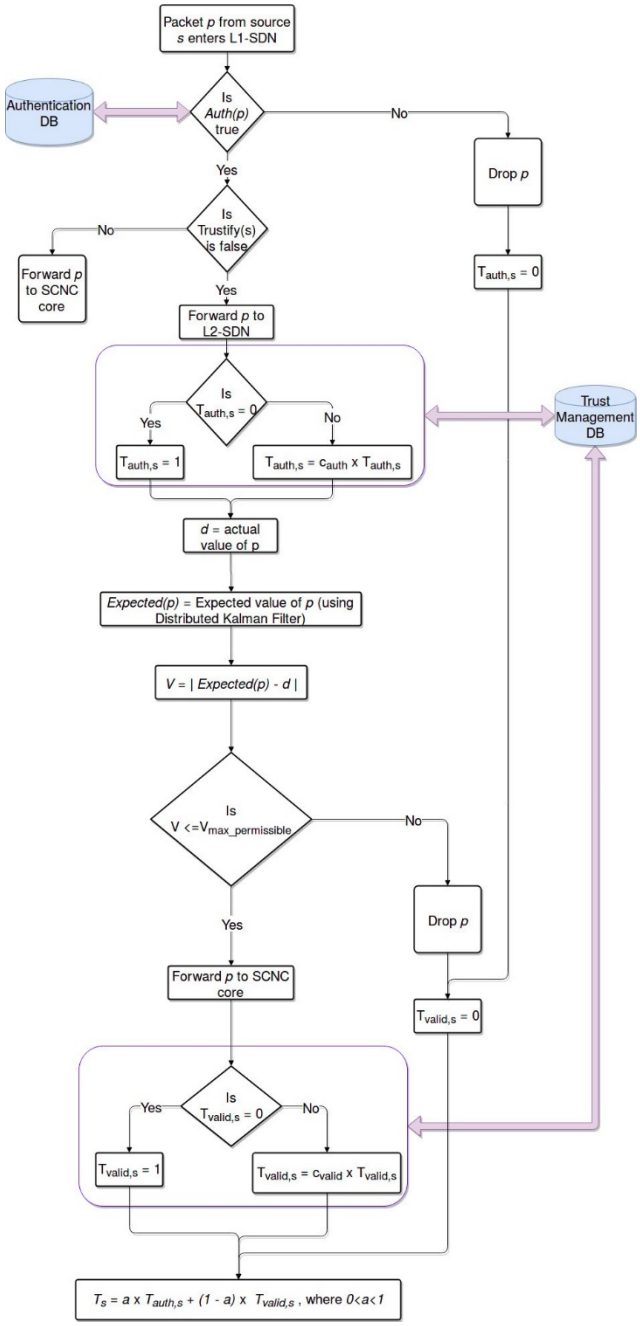
To make this scheme scalable for the size and velocity of data generated we need to allow high-speed channeling of authentic and valid data packets to the core. To achieve this, we do not validate each and every packet, instead we assign trust index to sources; higher the trust index, lower is the need to validate it each time. We maintain trust index of the sources in TrustedDB which is a peer-2-peer database hosted on the SDN controllers. Based on the trust index of a packet's source, the Trustify algorithm decides if the packet will be sent for filtering or directly sent to the SCNC core for analysis. The trust index of the sources is managed by the Trust Expansion Algorithm (TEA) which runs on the controllers.



. Figure 2:High-level architecture of SCNC framework

2.2 Trust Expansion Algorithm (TEA)

The TEA is a distributed algorithm runs both on the controllers of L1 and L2 SDNs and its primary goal is to filter IoT traffic, validate data and forward the most clean and actionable data to the SCNC core. TEA is described in the flowchart of figure 2.



. Figure 3:Flowchart for TEA

The expressions used in TEA are described below:

—$T_{auth,s}$ = Trust index of authentication for source s

—$T_{valid,s}$ = Trust index of validation for source s

—T_s = Overall trust index for source s

—$Auth(p)$ = True if p is authentic, false otherwise. The authenticity of p is determined by DSA.

—$Expected(p)$ = Expected value of data packet p obtained through DKF of the the data series generated by s

—$Random(0, 1)$ = A random number generated between 0 and 1

—c_{auth} = Factor by which the $T_{auth,s}$ is incremented

—c_{valid} = Factor by which the $T_{valid,s}$ is incremented

We briefly describe the algorithms used. The Trustify algorithm is invoked every time a data packet is authenticated. It decides if the trust of the source is to be checked or not. The pseudocode for Trustify is written in Algorithm 1.

Algorithm 1: Trustify

```
input  : source s
r ← Random(0, 1);
if r > 0.8 then
    return false;
else
    if T_s < 1 then
        return false;
    else
end
return true;
```

The packet is to be passed through another level of validation (return false), if the random number generated is greater than 0.8 (can be increased for higher time intervals between trust verification and vice-versa) or if the trust index of the source is less than 1. Otherwise (return true) the packet is directly sent to the core of SCNC.

The TEA increases the trust index of the sources if the packets are authentic and valid, and reduces it to 0 if they are inauthentic. If the packets are authentic but invalid, the trust index is increased or decreased depending upon the constants a, $c_{auth} and c_{valid}$. Thus, it is possible that the trust index of sources go on increasing which may lead to very long times after which the packet's data is validated. To overcome this problem, we define a Trust Decay Algorithm (TDA) which decreases the trust index of sources with time by a factor of 2 every half-life time. The half-life time is preconfigured. Its pseudocode is written in Algorithm 2.

Algorithm 2: TrustDecay

```
input  : sources, Trust index of sources
while 1 do
    for s in sources do
        n ← (time − s.timestamp) / s.half_life;
        T_s ← 2 − n × T_s;
    end
end
```

The TDA runs parallely on controllers and updates the P2P Trust Management Database hosted on the controllers. We have implemented a 2-level P2P-SDN architecture on Mininet [Mininet] modeling Openflow [ONF] controllers connected to each other. We have modelled an IoT workflow using normal distribution. Initial results are tabulated below:

Feature	*Value*
Average Authentication Time (L1-SDN)	0.56 ms
Average Validation Time (L2-SDN)	0.41 ms
Average latency for traffic reaching core	0.64 ms
% of traffic reaching core	72%

Table I. Initial results from Mininet simulation

3. CONCLUSION AND FUTURE WORK

We present a novel framework to design the Smart City Nerve Centre which will be able to efficiently manage large volumes of data in a secure manner without incurring significant overheads. Our P2P-SDN based framework provides authentication and data validation services based on a trust computation and expansion logic without the need to inspect all traffic leading to significant latency and computation savings. Future work shall involve detailed testing using real-world IoT workloads to derive further insights and refine the algorithms to meet real-world requirements. We also intend to build intelligence into the L1and L2 SDNs through advanced analytics and the use of baselining to be able to predict IoT traffic patterns and help the system adapt accordingly.

REFERENCES

Atzori, L., Iera, A., Morabito, G., and Nitti, M. 2012. The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Computer networks 56,* 16, 3594–3608.

Chen, M., Mao, S., and Liu, Y. 2014. Big data: A survey. *Mobile networks and applications 19,* 2, 171–209.

Cisco. rfc3272. http://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf.

IBM. Ibm press release. http://www-03.ibm.com/press/us/en/pressrelease/46453.wss.

IDC. Idc futurescape: Worldwide internet of things 2017 predictions. https://www.idc.com/research/viewtoc.jsp?containerId=US40755816.

IETF. rfc3272. https://www.ietf.org/rfc/rfc3272.txt.

Jasper. rfc3272. https://www.jasper.com/control-center-for-iot.

Kitchin, R. 2014. The real-time city? big data and smart urbanism. *GeoJournal 79,* 1, 1–14.

Kravitz, D. W. 1993. Digital signature algorithm. US Patent 5,231,668.

Mininet. Mininet homepage. http://mininet.org/.

mqug.org.uk. The hyperconnected enterprise briefings. http://mqug.org.uk/downloads/201407/201407 - MQM03 - Smarter Business by Unlocking IoT.pdf.

Olfati-Saber, R. 2007. Distributed kalman filtering for sensor networks. In *Decision and Control, 2007 46th IEEE Conference on.* IEEE, 5492–5498.

ONF. Openflow. https://www.opennetworking.org/sdn-resources/openflow.

Satyanarayanan, M., Simoens, P., Xiao, Y., Pillai, P., Chen, Z., Ha, K., Hu, W., and Amos, B. 2015. Edge analytics in the internet of things. *IEEE Pervasive Computing 14,* 2, 24–31.

Sinaeepourfard, A., Garcia, J., Masip-Bruin, X., Marín-Tordera, E., Cirera, J., Grau, G., and Casaus, F. 2016. Estimating smart city sensors data generation. In *Ad Hoc Networking Workshop (Med-Hoc-Net), 2016 Mediterranean.* IEEE, 1–8.

Prof. Ankur Gupta is the Director at the Model Institute of Engineering and Technology, Jammu, India, besides being a Professor in the Department of Computer Science and Engineering. Prior to joining academia, he worked as a Technical Team Lead at Hewlett Packard, developing software in the network management and e-Commerce domains. He obtained B.E (Hons) Computer Science and MS Software Systems degrees from BITS, Pilani and his PhD from the National Institute of Technology in India. His main areas of interest include peer-to-peer networks, network management, software engineering and cloud computing. He has published over 40 peer-reviewed papers in reputed international journals and conferences and is a recipient of the AICTE's (All India Council for Technical Education) Career Award. He has filed 14 patents in diverse technical domains and is the founding managing editor of the International Journal of Next-Generation Computing (IJNGC). He is a senior member of both the IEEE and ACM and a life member of the Computer Society of India.
Email-ID: ankurgupta@mietjammu.in.

Purnendu Prabhat is an Assistant Professor at Model Institute of Engineering and Technology, Jammu in the Department of Computer Science & Engineering. He received his Bachelors degree in Computer Science & Engineering from Kalasalingam University, Tamil Nadu in 2012 and Masters degree (gold medalist) in Computer Science from Central University of South Bihar in 2014. His research interests include Network Management, Software Defined Networking, Internet of Things and their application in Smart Cities. He has filed 2 patents and published 8 research papers and is also a mentor in Center for Research Innovation and Entrepreneurship (CRIE), MIET Jammu. He is a member of IEEE and Python Software Foundation. He is also an Amazon Web Services Certified and Accredited Instructor. Besides research he enjoys programming and teaching.
Email-ID: purnendu.cse@mietjammu.in.

Prof. Deepak Garg is the Head of Department of Computer Science and Engineering at Bennet University, Noida. He received his bachelors degree in Computer Science and Engineering from Punjab Technical University and PhD from Thapar University, Patiala. His main areas of interest include Data Science, Data Analytics, Deep Learning, Advance data structures and algorithms, Approximation algorithms, OptimizationMOOCs and Transformations in Higher Education with quality perspective. As an academician he has over 18 years of experience at leading academic institution. He has an experience in automating and implementing the technology solution on a larger scale in education sector.
Email-ID: deepak.garg@bennett.edu.in