Considerations for Designing Private and Inexpensive Smart Cities

Jasmine DeHart
Department of Computer Science
University of Oklahoma
Norman, Oklahoma, USA
Email: dehart.jasmine@ou.edu

Corey E. Baker
Department of Computer Science
University of Kentucky
Lexington, KY, USA
Email: baker@cs.uky.edu

Christan Grant
Department of Computer Science
University of Oklahoma
Norman, Oklahoma, USA
Email: cgrant@ou.edu

***Abstract*—The expectation of people and futurists is that all respectable cities will become Smart Cities in the near future. Two main barriers stand in the way of the evolution of cities. First is cost, the transformation into a smart city is expensive (e.g., between $30 Million and $40 Billion) and only a few cities are able to obtain the resources required for upgrades. Second, many citizens equate the data collection and surveillance of smart city technology with aggressive infringements on privacy. In this paper, we describe how citizens, city planners, and companies can develop smart cities that do not require crippling loans and are respectful of privacy.**

Keywords–smart city; privacy; networks.

I. INTRODUCTION

Ubiquitous technology has long been an expectation of the 21st century. Recently, the concept of a Smart City has led cities, developers, and citizens to pursue idyllic improvements to municipal infrastructure. Smart city designs tend to require Internet of Things (IoT) devices to be connected in order to retrieve the data generated by the devices. Unfortunately, significant costs are incurred when deploying sensors equipped with 5G or WiFi connectivity due to data subscription fees [1] [2]. As the number of cities that want to become "smart" increases, innovative ways of transforming a conventional city into a smart city need to be investigated. Aspiring smart cities are predicated on the belief that socioeconomic impact will yield a return on investment for smart cities, but financiers have been apprehensive [3].

While innovations in technology continue, citizens are critical about how unvetted smart cities can violate intrinsic rights [4]. People are inventing methods to disguise themselves from surveillance systems using fashionable masks [5]. Citizens also depend on other products to curtain themselves from other devices, such as smart speakers [6] [7]. However, laws are consistently being passed to ensure the responsibility of the city or company protects the privacy of the citizens [8] [9].

In remainder of this paper, we introduce and discuss the concepts of low-cost and privacy-enabled smart cities. In Section 2, we focus on defining what a smart city is and the requests of the top seven applicants that were apart of the 2015 Smart City Challenge [10]. In Section 3, we discuss the large monetary costs smart cities have invested to become "smart" along with some opinions on how to reduce cost. In Section 4, we discuss the infringements of privacy that smart cities produce and then, we propose innovative ways cities can protect their citizens. Lastly, we conclude by summarizing the insights and future direction of this research.

II. HOW CAN A CITY BECOME "SMART"?

Establishing what technologies create a smart city can include many intricate components. To define the essence of a Smart City, we start by establishing the basic universal technologies that all smart cities require. In 2015, the United States Department of Transportation announced the Smart City Challenge which asked cities in America to create an integrated, smart, and efficient transportation system built on data, applications, and technology in an effort improve the lives of its citizens [10]. Figure 1 displays U.S. cities that are currently smart cities or are interested in becoming "smart" (the circle area denotes the population size). Of these, the Smart City Challenge received 78 applicants describing what a smart city looked like for their community.

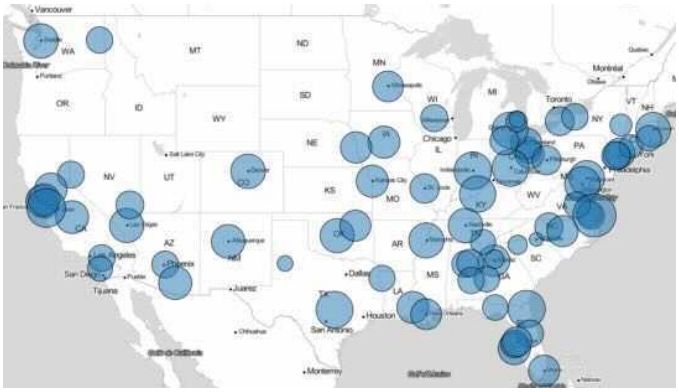

Figure 1. Current and potential smart city locations in the United States.

The list of technologies have been derived from the top seven applications from the Smart City Challenge. From this challenge, the seven cities were chosen as finalist include: Columbus (Ohio), Austin (Texas), Denver (Colorado), Kansas City (Missouri), Pittsburgh (Pennsylvania), Portland (Oregon), and San Francisco (California). Following this competition, these finalist serve as a foundation for cities hoping to become smarter. These cities request several technologies and components, such as:

- Electric vehicle charging stations
- Electric/autonomous public transportation vehicles
- Connected vehicles using a smart grid
- User mobile applications
- Traffic signaling priority

To integrate these technologies, the cities use sensors, video, Global Positioning Systems (GPS), and radio signals from

 ISBN: 978-1-61208-794-8

pedestrians, vehicles, and equipment. These cities also use these video and GPS feeds for license plate recognition and to track crime related incidents. The goal of becoming a smarter city revolves around connecting under-served communities to opportunities, decreasing health disparities, reducing air pollution, and increasing the mobility of citizens by relieving congestion of roadways.

Assisting low socioeconomic and disabled citizens has risen to the forefront of smart city development strategies. In an effort to make these advancements more inclusive of those communities, the smart cities have proposed the use of:

- *Smart kiosks* enable advanced payment options by incorporating additional features, such as braille and voice feedback
- *Electronic signs* provide visual and audio cues to pedestrians
- *Autonomous car sharing* allows commuters first and last mile transportation with a reduction in costs
- *Information screens* provide real-time transportation updates through audio and video

With the incorporation of these additional technologies, we see these cities become more inclusive and smarter for all. On top of an already costly smart city, these specialized technologies raise an additional cost along with continually maintaining all aspects of these technologies.

III. Low-Cost Smart Cities

Smart City projects can be extremely expensive to deploy and manage. Cities around the world such as San Diego, New Orleans, London, and Songdo have either proposed or invested in Smart City projects that cost between $30 Million and $40 Billion. In addition to the cost of deploying and maintaining the IoT devices themselves, a significant portion of the expense is a result of providing Internet connectivity via 5G or WiFi to those devices. These costs are a major barrier to the widespread deployment of Smart City technology and the social benefits that may ensue from that technology [11].

To alleviate the costs, opportunistic communication, such as Delay Tolerant Networks (DTNs) can be used as a backbone for Smart City communication to facilitate data that does not have real-time Quality of Service (QoS) constraints. DTNs traditionally provide opportunistic networking connections in areas with little to no infrastructure. Messages are delivered with some delay which is directly correlated with the layout, density, and mobility of nodes in the network [12] [13]. Recognizing that some data are needed in real-time, edge-computing can be utilized as long as the placement of internet-connected nodes are optimized in the network. For data that can tolerate delays, the natural movement of people and vehicles through a city to transfer data between nodes. In this way, the citizens become an integral part of the smart city network itself.

In order for low-cost Smart Cities to flourish and DTNs as backbone to be practical, both the technology questions related to the devices and the network itself, as well the social aspects of how people and vehicles move through a city must be addressed. For almost 20 years there has been a substantial amount of research in opportunistic communications and delay tolerant networks; unfortunately real-world deployments traditionally fall short of their simulated counterparts [14]. Related efforts, [13], [15]–[22], have proven the ability to deliver messages when connections are intermittent, but generally are limited to performing within simulation environments [23].

IV. Privacy-Enabled Smart Cities

With the use of smart city technologies, how does a city ensure privacy and security for its citizens? Cities will become a 24 hour hub for collecting information about the mobility and efficiency of transportation, but also personally identifying information of its' travellers [24]. In the Smart City Challenge [10], the applicants describe the possible risks and mitigation strategies with the deployment of these cities. From these concerns, we focus on the risks associated with the citizens in those environments. The main concerns for smart city citizens revolve around data sharing, individual privacy, system security, data privacy, and data management. In Table I, we explore each smart city and if these smart city risks will be addressed in the development of their city.

TABLE I. OVERVIEW OF THE MAIN SMART CITY CONCERNS FOR CITIZENS SELF-IDENTIFIED BY THE CITIES.

City	Data Sharing	Individual Privacy	System Security	Data Privacy	Data Management
Columbus, OH	–	–	–	–	–
Austin, TX	√	–	√	√	√
Denver, CO	–	–	√	√	–
Kansas City, MO	√	√	√	–	–
Pittsburgh, PA	–	√	–	√	√
Portland, OR	√	–	–	√	√
San Francisco, CA	√	√	–	–	–

Each city (rows) either discusses (√) or does not mention (–) the privacy risk of a technology (columns). Data sharing and data privacy concerns are addressed by the majority (4 of 7) of the cities. Individual privacy, system security, and data management are each addressed by three of the cities. In Table II, we reviewed these Smart City proposals and assessed a score based on a Likert Scale (Excellent, Average, Poor) from these five categories (Data Sharing, Individual Privacy, System Security, Data Privacy, & Data Management). From the proposal and discussion, a city will receive:

- Excellent: The proposal has thorough discussion about the risks and mitigation strategies related to topic and a solid plan of action.
- Average: The proposal has moderate to little discussion about the risks and mitigation strategies related to topic and a general plan of action.
- Poor: The proposal has little to no discussion about the risks and mitigation strategies related to topic and no plan of action.

Columbus is the only city without a risk analysis in their proposal. This city will develop their plan during the implementation of their city, but would this be enough? Immediately after winning, Columbus created the Smart City Program Office to assess possible risks and mitigate them. Of the finalists, none of these cities provide a detailed description

 ISBN: 978-1-61208-794-8

of the protection they will provide their citizens in their proposals. To mitigate the proposed risks these cities seek to: (1) implement standards from government and industry, (2) anonymize or mask sensitive personal data, and (3) partner with cyber-security experts and government.

TABLE II. RATING OF PRIVACY DISCUSSION BY CITY.

City	Data Sharing	Individual Privacy	System Security	Data Privacy	Data Management
Columbus, OH	Poor	Poor	Poor	Poor	Poor
Austin, TX	Poor	Poor	Excellent	Excellent	Excellent
Denver, CO	Poor	Poor	Poor	Average	Poor
Kansas City, MO	Poor	Average	Excellent	Poor	Poor
Pittsburgh, PA	Poor	Poor	Poor	Average	Poor
Portland, OR	Average	Poor	Poor	Average	Average
San Francisco, CA	Poor	Poor	Poor	Poor	Poor

Beyond security breaches and attacks, what protection will these cities use to ensure the privacy of those who want to remain anonymous in an "always on" city? Researchers have investigated the concerns of privacy leaks and the types of privacy leaks on social media [25]. These privacy leak concerns can be expected in a smart city where citizens are continually being monitored. To help cities protect their citizens, we propose the use of a visual mitigation library used for videos and images based on existing literature [26]. This work provides a foundation for several mitigation techniques used for social media networks, however these same technologies can be implemented to protect the citizens from surveillance concerns and privacy issues. Beyond the citizen's concern for anonymity or protection of minors, there is a concern for the type of information that is leaked in a public setting.

A. *ViperLib: Mitigation Library*

We seek to expand this work as a foundation for the need of mitigation techniques in video surveillance. Everyday people purchase items with their credit or debit cards, carry identification, or use keys (virtual and physical passcodes). This type of sensitive content will be captured in those videos and image feeds [27] [28], with the use of a redaction spectrum we can ensure that content will not be leaked to others. Studies have shown that the use of obfuscation methods [29]–[31] can protect individual privacy.

To address this concern, we suggested the deployment of the *ViperLib*. This mitigation library will allow the Smart Cities to choose how and where they want to integrate this technology. As proposed by [26], mitigation techniques can be integrated into mobile applications, servers, IoT devices, and comprehensive systems. Techniques, such as obfuscation (e.g., adversarial noise, blurring, blocking), interception, and blind vision can be integrated into this library easily ready for use. The library can also facilitate active engagement strategies for alerting authorized personnel about pertinent privacy concerns and suggesting the possible mitigation strategies for that visual content. These types of alerting strategies are similar to *Chaperone Bot or Privacy Patrol* from previous works [26]. The *ViperLib* open-source library can be integrated into existing "off-the-shelf" packages. Citizens can select the privacy protection features that must be integrated into deployed systems. Such libraries can provide safety, security, and peace of mind to the citizens that reside in those areas.

V. CONCLUSION & FUTURE WORK

In summary, this paper argued that Smart Cities have the capability to be both private and inexpensive in deployment and for long term sustainability. During planning and implementation of these cities, officials along with citizens should further consider the high cost and privacy concerns associated with their development choices. The need for privacy mitigation in Smart Cities extends from the protection of personally identifying information to the choice of anonymity and protect of minors. Beyond the deployment of the *ViperLib*, we proposed the use of DTNs to lower the cost of Smart Cities and allow citizens assist the in the transmission of data across the city. Deploying traditional IoT infrastructure is prohibitively expensive for most cities and expanded developments introduces privacy risks. However, low-cost smart cities and privacy-enabled technologies can achieve the goals of smart cities while allowing citizens to feel secure and protected.

Future research considers the potential effects of security for cyber-physical systems in real IoT deployments. To do this, we will collaborate with Louisville, Kentucky, a Smart City Applicant, to discuss future strategies and deployment plans for *ViperLib* as part of NSF Grant (#1952181).

ACKNOWLEDGMENT

This material is based upon work supported by the National Science Foundation under Grant No. 1952181.

REFERENCES

[1] J. Paradells, C. Gómez, I. Demirkol, J. Oller, and M. Catalan, "Infrastructureless smart cities. Use cases and performance," *2014 International Conference on Smart Communications in Network Technologies, SaCoNeT 2014*, pp. 1–6, 2014.

[2] E. Max-Onakpoya *et al.*, "Augmenting cloud connectivity with opportunistic networks for rural remote patient monitoring," in *2020 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2020, pp. 920–926.

[3] Deloitte, "The challenge of paying for smart cities projects," Deloitte, Tech. Rep., 2018, last accessed on 09/01/2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-ps-the-challenge-of-paying-for-smart-cities-projects.pdf

[4] J. E. Smith, "As San Diego increases use of streetlamp cameras, ACLU raises surveillance concerns," Aug. 2019, last accessed on 09/01/2020. [Online]. Available: https://lat.ms/33AzG7I

[5] A. Harvey, "Cv dazzle: Camouflage from computer vision," *Technical report*, 2012.

[6] J. Morse, "There's a privacy bracelet that jams smart speakers and, hell yeah, bring it," last accessed on 09/01/2020. [Online]. Available: https://mashable.com/article/bracelet-jams-alexa-smart-speakers/

[7] Y. Chen, H. Li, S.-Y. Teng, and S. N. Z. Li, "Wearable microphone jamming," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2020, pp. 1–12.

[8] C. Doctorow, "The case for ... cities that aren't dystopian surveillance states," *The Guardian*, Jan. 2020, last accessed on 09/01/2020. [Online]. Available: https://www.theguardian.com/cities/2020/jan/17/the-case-for-cities-where-youre-the-sensor-not-the-thing-being-sensed

[9] H. Devlin, "AI systems claiming to 'read' emotions pose discrimination risks," *The Guardian*, Feb. 2020, last accessed on 09/01/2020. [Online]. Available: https://www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks

 ISBN: 978-1-61208-794-8

[10] U. D. of Transportation, "Smart city challenge," Jun 2017, last accessed on 09/01/2020. [Online]. Available: https://www.transportation.gov/smartcity

[11] O. Madamori, E. Max-Onakpoya, C. Grant, and C. Baker, "Using delay tolerant networks as a backbone for low-cost smart cities," in *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 2019, pp. 468–471.

[12] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for dtn protocol evaluation," in *Proceedings of the 2nd international conference on simulation tools and techniques*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, p. 55.

[13] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: Social-based forwarding in delay-tolerant networks," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 11, pp. 1576–1589, 2011.

[14] C. E. Baker, A. Starke, T. G. Hill-Jarrett, and J. McNair, "In vivo evaluation of the secure opportunistic schemes middleware using a delay tolerant social network," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2017, pp. 2537–2542.

[15] R. Cabaniss, S. S. Vulli, and S. Madria, "Social group detection based routing in delay tolerant networks," *Wireless networks*, vol. 19, no. 8, pp. 1979–1993, 2013.

[16] P. Costa, C. Mascolo, M. Musolesi, and G. P. Picco, "Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 5, pp. 748–760, 2008.

[17] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant manets," *Mobile Computing, IEEE Transactions on*, vol. 8, no. 5, pp. 606–621, 2009.

[18] W. Gang, W. Shigang, L. Cai, and Z. Xiaorong, "Research and realization on improved manet distance broadcast algorithm based on percolation theory," in *Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference on*. IEEE, 2012, pp. 96–99.

[19] W.-j. Hsu, D. Dutta, and A. Helmy, "Csi: A paradigm for behavior-oriented profile-cast services in mobile networks," *Ad Hoc Networks*, vol. 10, no. 8, pp. 1586–1602, 2012.

[20] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in *Service Assurance with Partial and Intermittent Resources*. Springer, 2004, pp. 239–254.

[21] M. Musolesi and C. Mascolo, "Car: context-aware adaptive routing for delay-tolerant mobile networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 2, pp. 246–260, 2009.

[22] A. K. Gupta, J. K. Mandal, and I. Bhattacharya, "Comparative performance analysis of dtn routing protocols in multiple post-disaster situations," in *Contemporary Advances in Innovative and Applicable Information Technology*. Springer, 2019, pp. 199–209.

[23] A. Picu and T. Spyropoulos, "Dtn-meteo: Forecasting the performance of dtn protocols under heterogeneous mobility," *IEEE/ACM Transactions on Networking*, vol. 23, no. 2, pp. 587–602, 2014.

[24] R. Sánchez-Corcuera, A. Nuñez-Marcos, J. Sesma-Solance, A. Bilbao-Jayo, R. Mulero, U. Zulaika, G. Azkune, and A. Almeida, "Smart cities survey: Technologies, application domains and challenges for the cities of the future," *International Journal of Distributed Sensor Networks*, vol. 15, no. 6, p. 1550147719853984, 2019.

[25] J. DeHart, M. Stell, and C. Grant, "Social media and the scourge of visual privacy," *Information*, vol. 11, no. 2, p. 57, 2020.

[26] J. DeHart and C. Grant, "Visual content privacy leaks on social media networks," *arXiv preprint arXiv:1806.08471*, 2018.

[27] R. Hoyle, R. Templeman, D. Anthony, D. Crandall, and A. Kapadia, "Sensitive lifelogs: A privacy analysis of photos from wearable cameras," in *Proceedings of the 33rd Annual ACM conference on human factors in computing systems*. ACM, 2015, pp. 1645–1648.

[28] M. Korayem, R. Templeman, D. Chen, D. Crandall, and A. Kapadia, "Enhancing lifelogging privacy by detecting screens," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 4309–4314.

[29] T. Orekondy, M. Fritz, and B. Schiele, "Connecting pixels to privacy and utility: Automatic redaction of private information in images," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 8466–8475.

[30] Y. Li, N. Vishwamitra, B. P. Knijnenburg, H. Hu, and K. Caine, "Blur vs. block: Investigating the effectiveness of privacy-enhancing obfuscation for images," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE, 2017, pp. 1343–1351.

[31] T. E. Boult, "Pico: Privacy through invertible cryptographic obscuration," in *Computer Vision for Interactive and Intelligent Environment (CVIIE'05)*. IEEE, 2005, pp. 27–38.

 ISBN: 978-1-61208-794-8