Security and Privacy in Smart City Applications: Challenges and Solutions

Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen

The authors investigate security and privacy in smart city applications. Specifically, they first introduce promising smart city applications and architecture. Then they discuss several security and privacy challenges in these applications. Some research efforts are subsequently presented to address these security and privacy challenges for intelligent healthcare, transportation, and smart energy.

ABSTRACT

With the flourishing and advancement of the IoT, the smart city has become an emerging paradigm, consisting of ubiquitous sensing, heterogeneous network infrastructure, and intelligent information processing and control systems. A smart city can monitor the physical world in real time, and provide intelligent services to both local residents and travelers in terms of transportation, healthcare, environment, entertainment, and energy. However, security and privacy concerns arise, since smart city applications not only collect a wide range of privacy-sensitive information from people and their social circles, but also control city facilities and influence people's lives. In this article, we investigate security and privacy in smart city applications. Specifically, we first introduce promising smart city applications and architecture. Then we discuss several security and privacy challenges in these applications. Some research efforts are subsequently presented to address these security and privacy challenges for intelligent healthcare, transportation, and smart energy. Finally, we point out some open issues for future research.

INTRODUCTION

With the rising economy and social transformation, people have been moving from the country to cities, resulting in the largest wave of urbanization throughout the world. By 2030, the urban population is estimated to reach 5 billion (about 60 percent of the world population), which produces massive opportunities for the economic and social development of cities [1]. Due to the ever growing demands of local residents, the development of fundamental infrastructure and policies are not correspondingly ensured. Moreover, this unplanned and overly fast urban growth brings excessive burdens to climate, energy, the environment, and even living. These problems slow down the sustainable development of urban cities as a consequence. To mitigate the problems of rapid urbanization, it is urgent to improve governance and service delivery, offer swift seamless mobility, and achieve easy access to urban public facilities, affordable housing, quality healthcare, education, and living in highly populated areas [2]. A special spotlight is needed, covering urbanization trends in innovative management of urban operations and a variety of "smart" services to local residents, visitors, and the government to satisfy the ever increasing and diverse demands [3]. The advancement and flourishing of the smart city shed light on materializing these value-added services and tackling the problems of urbanization.

As an emerging paradigm, the smart city leverages a variety of promising techniques, such as the Internet of Things (IoT), cyber-physical systems, big data analysis, and real-time control, to enable intelligent services and provide comfortable life for local residents [4]. It integrates ubiquitous sensing components, heterogeneous network infrastructure, and powerful computing systems to sense the physical changes from cities and feed back to the physical world. Specifically, RFID devices, sensors, and versatile wearable devices are promoted to offer real-time monitoring and ubiquitous sensing, from energy to environments, from road traffic to healthcare, from home area to public venues, and so on. Then this sensing information is transmitted to a control center via heterogeneous networks. This control center takes comparative advantage of powerful computing systems, such as cloud servers, to process and analyze the collected data. Fueled by human intelligence, the control center makes optimal decisions and manipulates the urban operations via feedback components, such as actuators [3]. Having the advanced information, communication, and control technologies as backbones, a smart city can offer various applications, including intelligent transportation, smart energy, intelligent healthcare, and smart homes. Not only can this up-and-coming connected city quickly identify the demands of people and a city, but it can also manipulate urban operations to improve urban living quality in an intelligent and sustainable way. It is expected that the global smart city market will exceed US$1200 billion by 2020, which is almost triple that in 2014 [1].

When cities become smarter, people may suffer from a series of security and privacy threats due to the vulnerabilities of smart city applications [5]. For example, malicious attackers may generate false data to manipulate sensing results such that services, decisions, and control in a smart city are influenced and not "intelligent" enough. Moreover, these malicious attackers could also launch denial-of-service attacks, disrupting the sensing, transmission, and control to degrade the quality of intelligent services in a smart city.

Digital Object Identifier:
10.1109/MCOM.2017.1600267CM

Kuan Zhang, Jianbing Ni, Kan Yang, and Xuemin (Sherman) Shen are with the University of Waterloo; Xiaohui Liang is with the University of Massachusetts at Boston; Ju Ren is with Central South University, China.

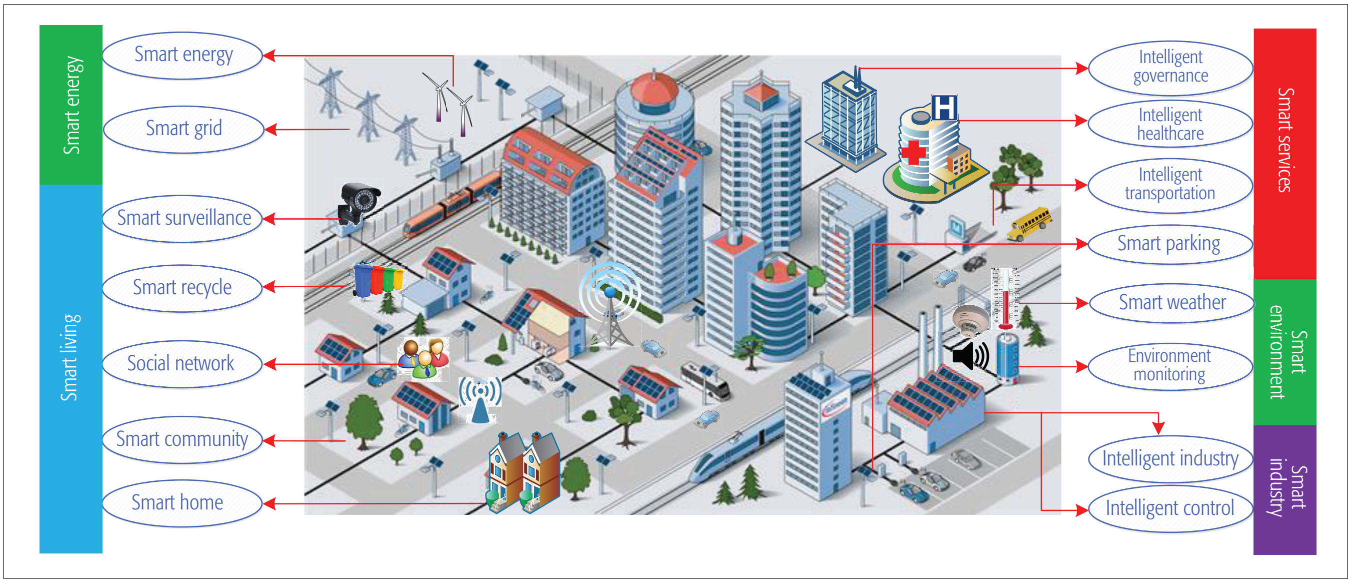

Figure 1. Smart city applications.

In addition, the pervasive video surveillance in a smart city captures a tremendous number of images and video clips, which may be utilized to infer local residents' trajectories and inherently endanger their privacy. The home area information collected and managed by smart home applications may pave the way to disclosing residences' highly privacy-sensitive lifestyle and even cause economic loss. Although some off-the-shelf techniques (encryption, authentication, anonymity, etc.) and policies might be directly applied to avert these problems [5], the emerging "smart" attackers could still infer and violate privacy in many other ways, such as side channel attack and cold boot attack [6]. Without sufficient security and privacy protections, users may refrain from accepting the smart city, which would remain as a far-off futuristic idea.

These emerging trends motivate our research investigating the not-for-profit global initiative of security and privacy for the smart city. In this article, we first introduce smart city applications and a heterogeneous architecture. Then we discuss several challenging security and privacy issues, including privacy leakage, secure information processing, and dependability in control. Some innovative research efforts are presented to address these challenges in various smart city applications. Finally, we point out several open research directions and the outlook of the smart city from the security and privacy perspective.

Smart City Applications and Architecture

As a smart city connects the physical world and the information world, many intelligent applications are emerging, from local to global, from sensing to control, as shown in Fig. 1. In this section, we introduce smart city applications and the heterogeneous architecture.

Smart City Applications

Smart city applications benefit people and the city in a variety of aspects: energy, environment, industry, living, and services.

We introduce several key applications as follows.

Smart Energy: Exploiting the widely deployed sensors to monitor energy generation, transmission, distribution, and consumption, smart energy [7] leverages utility usage, electric vehicle charging, smart grid, and so on. Not only can it reduce the energy consumption in many aspects, but it can also prevent blackout of power grid and failure of individual energy usage.

Smart Environment: The mart environment is promoted to support a comfortable climate and sustainable environment for the smart city. Ubiquitous sensing and intelligent climate management are jointly applied in smart environment applications [4]. They can monitor waste gas, greenhouse gas, city noise, air and water pollution, forest conditions, and so on, to afford intelligent and sustainable development.

Smart Industry: With the main driver of industrial sustainable development in the smart city, smart industry is being rolled out to optimize industrial production and manufacturing, while achieving efficiency and robustness. On one hand, it curtails the material and resource consumption (e.g., labor, time, and production lines) during the industrial process; on the other hand, it prevents industrial heat and gas waste from excessive emission. Both sensing and control are equally arresting components in smart industry, which requires real-time feedback and precise operations. Finally, servo actuators, motors, and robots are adopted to enable precise control and operations of consequence in smart industry.

Smart Living: In home areas, smart living offers intelligent management of various appliances and utilities to create comfortable homes and improve energy efficiency simultaneously [6]. It can enable remote control of home appliances, climate adjustment, energy saving, surveillance, entertainment, and education. In the community (or building), smart living applications also intelligently manage waste recycling, social networking, and parking to provide a smart community (or building) with comfortable lives, intimate service, wonderful experiences, and sustainable environment and energy.

To achieve ubiquitous sensing and finesse city management, smart city manipulates the information sensed from the physical world, the information transmitted in the communication world and the information processed in the information world for intelligent services.

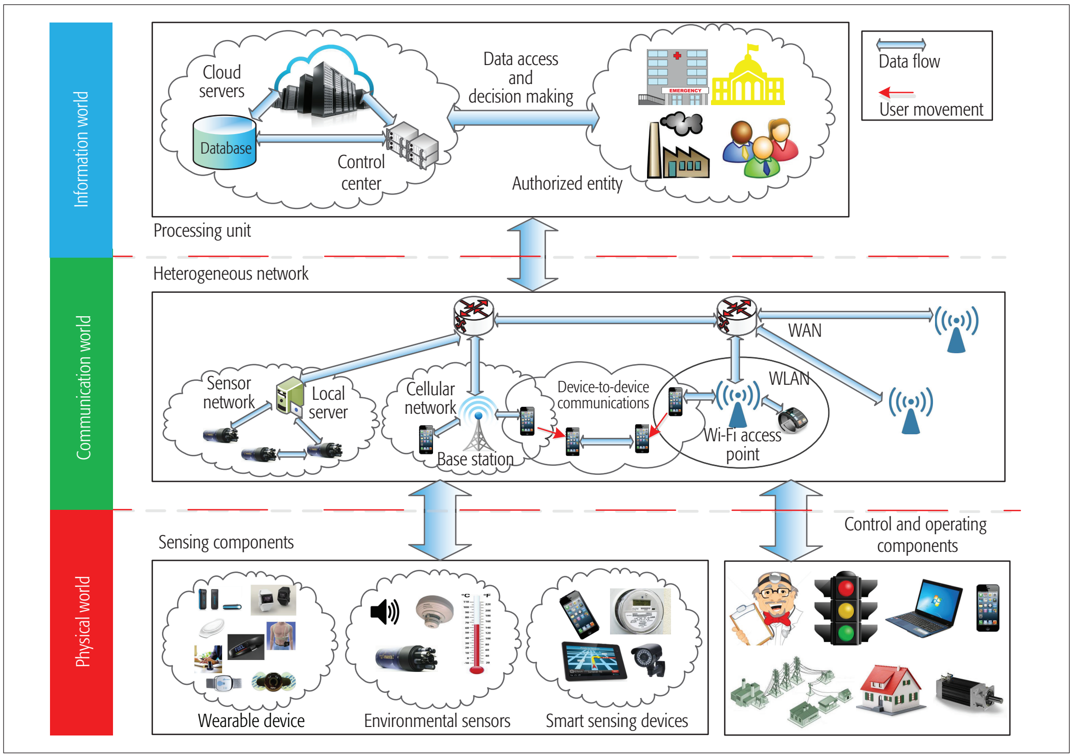

Figure 2. Architecture for smart city: physical world, communication world, and information world.

Smart Service: Smart service enables the public facilities and services to benefit people in a wide range of aspects [1]. For example, intelligent transportation [8] can help local residents and travelers to avoid road traffic congestion, enable road navigation, discover points of interests, manage the travel planning, and so on. The road traffic information can be collected by deployed sensors, cameras at the intersections, GPS, smartphones from people on the road, and so on. The control center adjusts travelers' road plans and feedback to their smartphones or GPS. In addition, road traffic can be adjusted by managing the traffic light and public transportation tools, such as buses, trains, and shared bicycles.

To provide quality healthcare, intelligent healthcare enables continuous health monitoring and timely diagnosis (including health warnings) to the people in a smart city [9]. It relies on wearable devices and medical sensors to measure users' health conditions, and sends health data to the processing unit for doctors' further diagnosis. It also provides easy access to a user's historical comprehensive health information, considerably increasing the chance to diagnose chronic or infectious diseases in the early stage. In addition, intelligent healthcare contains various health-related applications, such as home care, emergency alarm, and intelligent fitness and training.

Smart City Architecture

To achieve ubiquitous sensing and finesse city management, the smart city manipulates the information sensed from the physical world, the information transmitted in the communication world, and the information processed in the information world for intelligent services. It incorporates sensing components, heterogeneous network infrastructure, processing units, and control and operating components as shown in Fig. 2.

Sensing Components: Sensing components exploit wearable devices, industrial sensors, and smart devices (e.g., smartphones, smart meters, and video surveillance cameras [4]) to measure information from the physical world and transmit this information to the processing unit for decision making. In other words, sensing components are the bridge connecting the physical and information worlds. The sensing devices are either deployed by the government, departments, and companies, or carried by users as discussed above. In addition, due to the limitations of device size, battery, and processing capabilities, these resource-constrained sensing devices usually pre-process or compress the real-time and granular data before sending it to the network.

Heterogeneous Networks: With the coexistence of massive sensing devices and various applications [9], the sensing information is collected in different ways such that the heterogeneous network infrastructure plays an instrumental role in supporting the smart city. Heterogeneous networks incorporate cellular networks, wireless local area networks (WLANs), wide area networks (WAN), device-to-device (D2D) communications, millimeter-wave communications, sensor networks, and so on, and enable seamless switching among different types of networks. Heterogeneous networks represent the communication world in a smart city to connect the physical and information worlds.

Processing Unit: The processing unit exploits the powerful cloud computing servers, abundant databases, and dedicated control systems to analyze and process the collected sensing information from the physical world for decision making. The processing unit manages the information world in a smart city. Authorized entities, such as the government, hospitals, factories, users, and so on, have certain privileges and authorizations to access the collected information. They can also determine the requirements or policies for decision making and control in a smart city.

Control and Operating Components: Leveraging the optimization and decisions of the processing unit, a smart city feeds back to manipulate the physical world via the control and operating components, such as servo actuators or smartphones. These control and operating components optimize and make adjustments to the physical world such that a good quality of life can be offered in a smart city. They also implement the two-way flow of the smart city (i.e., sensing and control). Not only can his two-way flow acquire the knowledge about the physical world; it can also monitor and manage every device or component in a smart city to make it operate properly and "smart."

Security and Privacy Issues in a Smart City

Although cities are seeking to become "smarter," smart city applications raise a series of concerns and challenges in terms of security and privacy. As an information and networking paradigm, the smart city should be able to defend the involved information from unauthorized access, disclosure, disruption, modification, inspection, and annihilation. Underlying security and privacy requirements, including confidentiality, integrity, non-repudiation, availability, access control, and privacy [5], should be satisfied in the information, communication, and physical worlds. Besides these general requirements, securing a smart city still faces a set of unique challenges. On one hand, a smart city collects granular-scale and privacy-sensitive information from people's lives and environments; on the other hand, it processes this information, and manipulates and impacts people's lives. Due to these unique characteristics, security and privacy issues become challenging and prevent the smart city from being tempting enough to encourage more use.

Although cities are seeking to become "smarter," smart city applications raise a series of concerns and challenges in terms of security and privacy. As an information and networking paradigm, a smart city should be able to defend the involved information from unauthorized access, disclosure, disruption, modification, inspection, and annihilation.

Privacy Leakage in Data Sensing

A smart city is vulnerable to privacy leakage and information inferring by outside attackers, since private information is collected, transmitted, and processed. The disclosed privacy in a smart city may contain a user's identity and location in transportation, health condition in healthcare, lifestyle inferred from intelligent surveillance, smart energy, home and community, and so on. It would be a major oversight to disclose this privacy-sensitive information to untrusted or unauthorized entities in both the physical and communication worlds. To preserve user privacy during data sensing, some off-the-shelf security and privacy techniques, such as encryption, anonymity, and access control, can be applied [10, 11]. Martinez *et al.* [5] propose a set of privacy concepts and general privacy requirements toward smart city applications. The privacy of identity, query, location, footprint, and owner is identified and provided with some basic ideas to solve the general problems.

However, a portion of private information may still be unconsciously disclosed to untrusted entities. For example, intelligent surveillance may capture local residents' daily life hints, style, or even privacy, although it was originally designed for monitoring criminal behaviors in the real and cyber worlds. Similarly, a smart home also utilizes a surveillance camera to detect theft or abnormal events. The intruding attackers in a smart home may acquire private information about the home area, which is prejudicial to the residence's privacy. Most existing security and privacy protection [10] are developed against outside eavesdroppers and attackers. But potential inside attackers, such as agents, employees, and security guards, who can access surveillance records may either steal users' data or leave a gap for outside attackers. In addition, the data in a smart city are on a highly granular scale and of diverse types such that the privacy requirements vary with different types. It is challenging to develop adjustable privacy protection mechanisms in a smart city to balance the trade-off between privacy and efficiency.

Privacy and Availability in Data Storage and Processing

As a smart city takes comparative advantage of powerful cloud servers for data storage and processing in the information world, it faces security threats due to the untrusted cloud servers. If the smart city data are in clear text during storage and processing, they are directly revealed to the cloud server [12]. An alternative is to encrypt the smart city data and send ciphertexts to the cloud server for storage and processing [13]. Although this method prevents the untrusted cloud server from directly accessing the collected data, the cloud server cannot process the encrypted data and perform effective analytical operations for smart city applications. The latest breakthrough on fully homomorphic encryption sheds light on the processing, such as summation and comparison, over encrypted data. The computational overhead poses another impending challenge in terms of efficiency, especially when massive data are involved in a smart city.

Another challenging issue of securing a smart city is data sharing and access control. For example, road traffic data can be collected by deployed cameras or travelers' smartphones and GPS in a crowdsourcing way. During global road planning, it is challenging to define the access policy and enable privacy-preserving data sharing among the collaborators. Therefore, smart city data storage and sharing require extensive research efforts.

Trustworthy and Dependable Control

A smart city, having a two-way control flow, relies on the control system and actuators to materialize the operations determined by the control center. The control and feedback systems in the physical world, especially public and industrial infrastructure, become highly attractive targets for attackers, criminals, and even terrorists [14]. Denial-of-service attacks, spoofing attacks, malicious data injection, and so on would disrupt the smart city such that the management, control, and operation are either biased and incorrect or disabled. Most of these malicious attacks and misbehaviors are detected based on third party inspection and auditing. In [15], data integrity functionality and digital signatures are adopted in software defined networks to achieve data integrity, access control, and so on. Meanwhile, trusted computing is

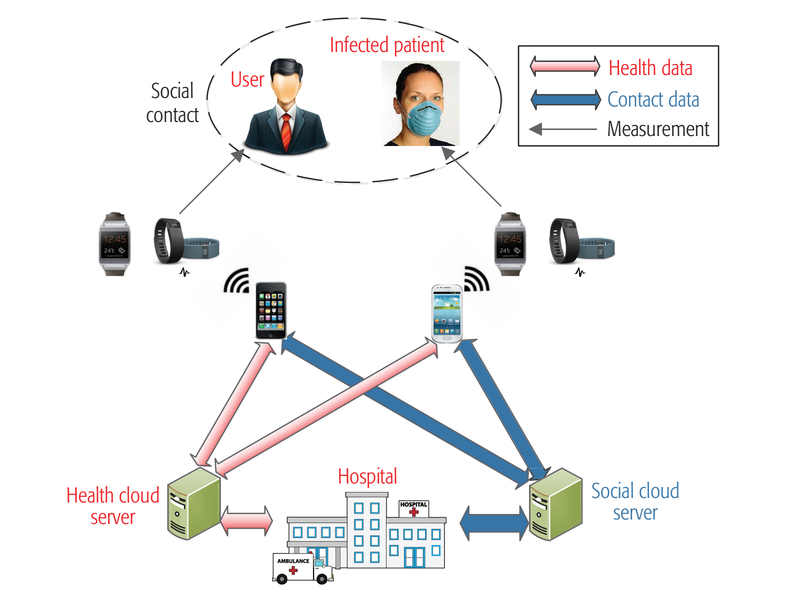

Figure 3. Intelligent healthcare integrating social networking and health data for infection analysis.

a state-of-the-art solution to resist operating system and software framework alterations. However, these schemes consume large latency and a high false rate to detect "smart" attacks in a smart city. As dependability of control is considered as the topmost priority in a smart city, efficient and fast detection of malicious attacks and misbehaviors becomes challenging, requiring collaborative efforts among various parties and stakeholders.

Security Solutions for Smart City Paradigms

To materialize the notion of security and privacy in a smart city, balanced and pragmatic solutions are desired. In this section, we introduce state-of-the-art security and privacy protection schemes for several emerging smart city paradigms, including intelligent healthcare, intelligent transportation, and smart grid.

Privacy-Preserving Infection Spread Analysis for Intelligent Healthcare

Intelligent healthcare, fueled by connected biomedical sensors, and health data storage and processing units, provides preventive, curative, and palliative health services. It can collect a wide range of real-time health data from users, and analyze and defend severe healthcare issues city-wide, such as infectious disease spread. Infectious diseases (e.g., Ebola, flu, and acute respiratory infection) could be rapidly spread in the population via human-to-human contact, especially when the infected patients cough and sneeze in a crowd. People having frequent contact or strong social relationships with a patient (e.g., students studying in the same classroom or families living in the same house) are usually considered susceptible from the perspectives of biomedicine and sociology. An old-fashioned prevention approach is to isolate the susceptible people for a certain period. However, this approach does not consider their health condition and susceptibility in terms of negative impacts, including massive healthcare expense, economic loss of the isolated people, and panic or anxiety among the society.

To tackle the infection spread problem, intelligent healthcare would provide efficient diagnosis and health condition (or emergency) warning, by analyzing in real time the infectiousness during outbreak season. Suppose a junior school student, Bob, is continuously monitored from both the health and social perspectives during the outbreak of an infectious disease. Once Bob's immunity goes very low and he frequently contacts an infected student, he may be inferred as a susceptible patient in the early stage. In general, the spread of infectious disease depends on users' social contacts and health conditions. Specifically, this spread process can be affected by several key factors of infection, that is, susceptibility of the infected patient, immunity strength of the contacted user, contact duration, and social ties.

The fusion of social network data together with real-time health data facilitates a novel paradigm of infection analysis, as shown in Fig. 3. On one hand, a social network employs a variety of applications to mine users' social contacts during their social interactions. For example, the Wechat friend discovery program can find users in physical proximity and record social interactions; speech recognition can detect if some people cough or sneeze; a face-tagging function can identify a user's face from images. On the other hand, wearable devices and medical sensors can measure a user's real-time health condition [3, 9].

However, health and social network data are collected by multiple independent service providers, such as hospitals and social network vendors (e.g., Facebook and Wechat). The collaboration of these service providers is the key challenge of enabling this enhanced infection analysis, and poses a series of security issues. Both social and health cloud servers are considered to be honest but curious [5] in intelligent healthcare applications. To preserve the user's data privacy and achieve data availability, homomorphic encryption [9] can be adopted to make both social network and health data invisible to the untrusted cloud servers. The collaboration of different untrusted cloud servers is achieved via the authorized entity (i.e., a hospital authorized by users as shown in Fig. 3). However, when the hospital queries the infected patient's data on the social cloud server, the social cloud server may infer that the queried user is infected even though the query content is still invisible. In addition, any entity without the authorization of the data owner should not be able to query the owner's data. State-of-the-art security and privacy protections are essential for intelligent healthcare. Without effective protections, users may not be willing to share their social and health data with others such that the infection analysis would be disabled.

To this end, conditional oblivious transfer protocol is developed for the privacy-preserving data query [9]. On one hand, it allows an authorized entity, such as a doctor, to access a patient's social network data from the social cloud server; on the other hand, it prevents the social cloud server from accessing the data and inferring any information about the query, such as the patient's identity. Users or data owners are able to grant authorization to the trusted entity before the query. Any

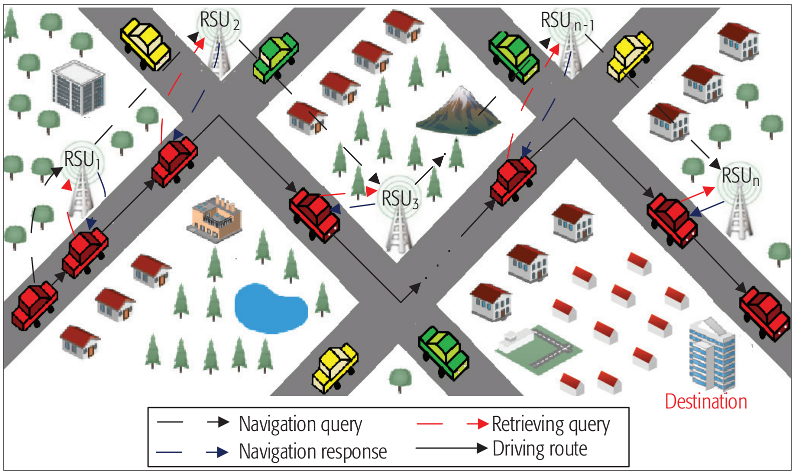

Figure 4. Intelligent navigation with privacy preservation.

entity without user authorization cannot query any data. In addition, secure multi-party computation based on homomorphic encryption [9] is utilized to prevent the untrusted health cloud from learning any private social and health data.

Secure Navigation for Intelligent Transportation

A smart city offers intelligent transportation services to local residents and visitors in various aspects, including road traffic adjustment, navigation, point of interest recommendation, parking, and so on. As an integral part of intelligent transportation, navigation attracts intensive attention [5]. Existing GPS devices can provide static navigation by showing the route on pre-downloaded maps. However, it lacks real-time road traffic adjustment such that the calculated fastest route may be delayed by dynamic congestion. Dynamic navigation exploits human intelligence and dynamic road traffic sensing from travelers on the road and roadside units (RSUs) in a crowdsourcing way [3].

As shown in Fig. 4, a querier, that is, the querying vehicle in the navigation service, sends a navigation query to the closest RSU. The query contains the current location, destination, and expired time. Then the RSU forwards this query to the RSU that covers the destination through the network among RSUs. Upon receiving the navigation query, RSUs send the crowdsourcing task to the vehicles in its coverage area to find the fastest driving route for the querier. The querier retrieves a response from the RSUs when entering the coverage area of each RSU, and finally reaches the destination.

During this type of distributed navigation, the private location information of both the querying vehicle and responding vehicles may be disclosed. To this end, the Elgamal and Advanced Encryption Standard (AES) schemes [8] are utilized to encrypt the querier's location and destination in each hop from the querier to the last RSU, preserving a vehicle's query privacy. To prevent RSUs from linking the navigation query and retrieving query to a specific vehicle, each vehicle randomizes the credential issued by the trusted authority to generate a group signature. In addition, to prevent the sensitive information in the navigation response being disclosed, the driving route is encrypted by Elgamal and AES schemes associated with a zero-knowledge range proof, which proves that the time cost is less than the given threshold, without exposing the exact value [8]. Finally, the traceability of group signature allows the trusted authority to trace any malicious vehicle that does not honestly follow the rules.

In summary, this privacy-preserving navigation scheme relies on the distributed RSUs to complete the road planning task in a crowdsourcing way. During the querying, crowdsourcing, and navigation phases, both querier and responding vehicles can preserve location privacy.

Adaptive Key Management for Smart Grid

Smart grid relies on millions of smart meters to measure the real-time power consumption in residential areas or buildings, as shown in Fig. 5. These metering data are aggregated to the control center to optimize the power distribution in return. However, a series of attacks attempt to tamper smart meter records and upload modified data to the control center [15]. Moreover, the ever increasing volume of metering data poses a new challenging issue of managing secret keys for each device [6]. Predominantly, the data integrity and authentication should be achieved during the aggregation of smart metering. In addition, the metering data of a home area may reflect the residence's lifestyle, condition (e.g., very low power consumption over a long duration indicates that residents are out), and preferences [6]. If the untrusted aggregators learn and reveal this private information, the residents' privacy would be jeopardized, and economic loss may even be caused.

In [7], Zhang *et al*. propose a privacy-preserving aggregation scheme (PARK) to improve the computational efficiency and protect smart metering data from disclosure to untrusted aggregators. An adaptive key management scheme is developed based on bidirectional hash chains, generating the encryption keys for every smart meter during each period. The trusted authority calculates the decryption key for the aggregator as the summation of encryption keys from a group of *N* smart meters. It is only when having all *N* ciphertexts that the aggregator can decrypt the summation of *N* smart meters. If no smart meter joins or leaves the smart grid, every smart meter's encryption key is automatically updated. The aggregator's decryption key is updated in a synchronous way. The trusted authority determines the length of hash chains, which reflects the reputation of smart meters. A meter with a high reputation receives a key with long expiry time. When some meters join or leave the smart grid, the trusted authority only needs to update the aggregator's decryption key. The revocation overhead is mainly from the re-distribution of the decryption key. As shown in Fig. 6, the proposed PARK scheme costs one-time key distribution in every key update, while other schemes (distributed key management and a naive scheme [7]) cost higher key update overhead. In addition, forward and backward secrecy is achieved based on the security of a one-way hash function.

Future Research Directions

Since some off-the-shelf security and privacy solutions [4] may not conquer all the challenges in a smart city, we discuss several open research directions including, but not limited to, the following.

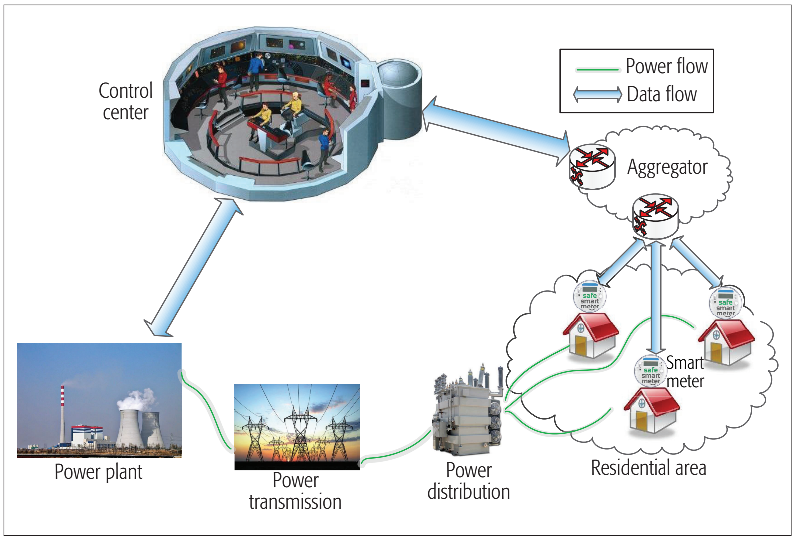

Figure 5. Smart grid architecture, including power flow and data flow.

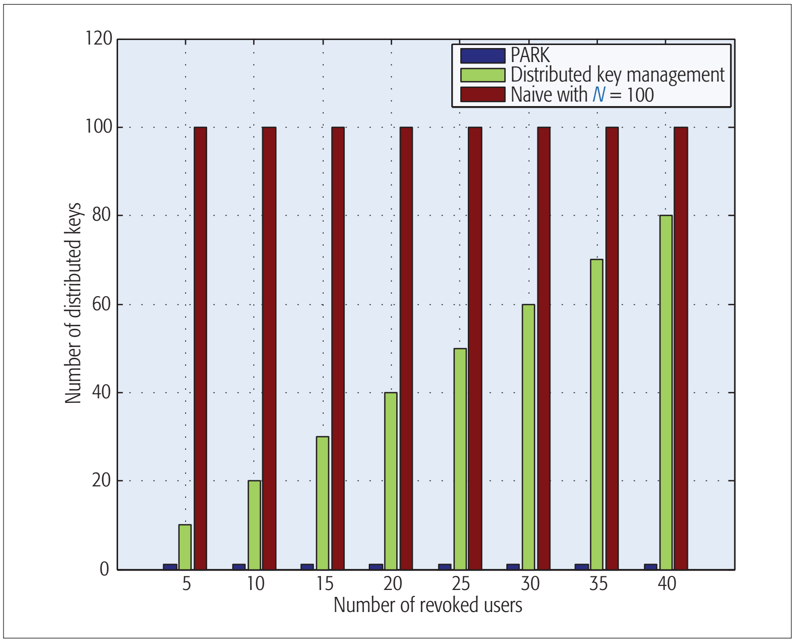

Figure 6. Comparison of key management overhead in smart grid.

First, crowdsensing, which exploits smart sensing devices of local residents, can provide improved sensing capability for the smart city rather than purely relying on pre-deployed fixed sensors. However, the crowdsensing accuracy may vary with a contributor's knowledge, preference, selfishness, and so on. An initial idea of stimulating citizens to contribute for crowdsensing is to develop incentives for them. Moreover, trustworthiness should also be considered when designing incentive schemes. In addition, crowdsensing contributors' privacy hidden in the sensing results may be jeopardized by "smarter" attackers. In particular, when multiple contributors pool their sensing results together, an individual contributor's private information is likely to be collaboratively inferred by others. Therefore, how to achieve incentive and privacy remains as a challenge for crowdsensing in smart city.

Second, a smart city is vulnerable to false data injection in both sensing and control phases. Digital signature techniques [9] cannot prevent the data from being tampered from the origination. An insight into detecting false data injection is to leverage machine learning and data mining to come up with a boundary of reasonable sensing data. Abnormal detection techniques may be an alternative to identify the false data. However, it is still an open issue requiring multidisciplinary knowledge and efforts to address.

Last but not least, the ever growing volume of data and devices in a smart city poses open problems for intelligent services and privacy. Inside attackers exploit human intelligence and have access to big data such that the privacy of data owners may be inferred and violated; even the traditional cryptographic schemes have been applied to big data. An alternative to detect these inside attackers is to enhance the traceability and allow a trusted third party to monitor and audit. Meanwhile, collaborative efforts among municipalities, regulation departments, industry, academia, and business companies are necessary to set up privacy policies and regulations. In addition, data privacy, availability, and management should be achieved simultaneously.

Conclusions

In this article, we have investigated the smart city, and discussed the security and privacy challenges in emerging smart city applications. We have first introduced smart city applications in different aspects and discussed the architecture. Then we have presented the general security and privacy requirements and identified several security challenges for the smart city. In addition, we have dwelled in greater depth on state-of-the-art security and privacy solutions for smart city applications. Several open research directions are also discussed.

We hope this article sheds more light on the security and privacy for smart cities, where more ground-breaking research efforts along this emerging line will be seen in the future.

Acknowledgment

This research has been supported by a research grant from the Natural Science and Engineering Research Council (NSERC) and Care In Motion (CIM) Inc., Canada.

References

[1] P. Neirotti *et al.*, "Current Trends in Smart City Initiatives: Some Stylised Facts," *Cities*, vol. 38, 2014, pp. 25–36.

[2] R. G. Hollands, "Will the Real Smart City Please Stand Up? Intelligent, Progressive or Entrepreneurial?" *City*, vol. 12, no. 3, 2008, pp. 303–20.

[3] J. Liu *et al.*, "Software-Defined Internet of Things for Smart Urban Sensing," *IEEE Commun. Mag.*, vol. 53, no. 9, Sept. 2015, pp. 55–63.

[4] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things J.*, vol. 1, no. 1, 2014, pp. 22–32.

[5] A. Martinez-Balleste, P. Perez-Martinez, and A. Solanas, "The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible," *IEEE Commun. Mag.*, vol. 51, no. 6, June 2013, pp. 136–41.

[6] X. Li *et al.*, "Smart Community: An Internet of Things Application," *IEEE Commun. Mag.*, vol. 49, no. 11, Nov. 2011 pp. 68–75.

[7] K. Zhang *et al.*, "PARK: A Privacy-Preserving Aggregation Scheme with Adaptive Key Management for Smart Grid," *Proc. IEEE ICCC*, 2013, pp. 236–41.

[8] J. Ni *et al.*, "Privacy-Preserving Real-Time Navigation System Using Vehicular Crowdsourcing," *Proc. VTC-Fall*, 2016, pp. 1–6.

[9] K. Zhang *et al.*, "Security and Privacy for Mobile Healthcare Networks — From Quality-of-Protection Perspective," *IEEE Wireless Commun.*, vol. 22, no. 4, Aug. 2015, pp. 104–12.

[10] A. S. Elmaghraby and M. Losavio, "Cyber Security Challenges in Smart Cities: Safety, Security and Privacy," *J. Advanced Research*, vol. 5, no. 4, 2014, pp. 491–97.

[11] R. H. Weber, "Internet of Things — New Security and Privacy Challenges," *Computer Law & Security Review*, vol. 26, no. 1, 2010, pp. 23–30.

[12] M. Naphade *et al.*, "Smarter Cities and Their Innovation Challenges," *IEEE Computer*, vol. 44, no. 6, 2011, pp. 32–39.

[13] J. Gubbi *et al.*, "Internet of Things (IoT): A Vision, Architectural Elements, And Future Directions," *Future Gen. Comp. Sys.*, vol. 29, no. 7, 2013, pp. 1645–60.

[14] R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Comp. Net.*, vol. 57, no. 10, 2013, pp. 2266–79.

[15] A. Akhunzada *et al.*, "Securing Software Defined Networks: Taxonomy, Requirements, and Open Issues," *IEEE Commun. Mag.*, vol. 53, no. 4, Apr.2015, pp. 36–44.

Biographies

Kuan Zhang [S'13] received his B.Sc. degree in communications engineering and M.Sc. degree in computer science from Northeastern University, China, in 2009 and 2011, respectively. He received his Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2016. Currently, he is a postdoctoral fellow with the Department of Electrical and Computer Engineering, University of Waterloo. His research interests include security and privacy for mobile social networks, e-healthcare systems, and cloud computing.

Jianbing Ni received his Bachelor and Master degrees from the University of Electronic Science and Technology of China in 2011 and 2014, respectively. Currently, he is pursuing his Ph.D. degree at the Broadband Communications Research (BBCR) Group, Department of Electrical and Computer Engineering, University of Waterloo. His research interests include security and privacy for crowdsouring, vehicular ad hoc networks, cloud computing, and fog computing.

Kan Yang received his B.Eng. degree in information security from the University of Science and Technology of China in 2008 and his Ph.D. degree in computer science from the City University of Hong Kong in August 2013. From September 2013 to July 2014, he was a postdoctoral fellow in the Department of Computer Science, City University of Hong Kong. From July 2014 to June 2016, he was a postdoctoral fellow and the coordinator of the security group of the BBCR Group in the Department of Electrical and Computer Engineering, University of Waterloo. He will join the Department of Computer Science at the University of Memphis soon. His research interests include cloud security, big data security, mobile security, applied cryptography, and distributed systems.

Xiaohui Liang [M'15] received his Ph.D. degree from the Department of Electrical and Computer Engineering of the University of Waterloo, and his Master and Bachelor degrees from the Computer Science Department of Shanghai Jiao Tong University. He was also a postdoctoral researcher at the Department of Computer Science, Dartmouth College, New Hampshire. Since 2015, he has been an assistant professor with the Computer Science Department at the University of Massachusetts Boston. His research interests include security, privacy, and trustworthiness in medical cyber physical systems, cyber security for mobile social networks, and applied cryptography.

Ju Ren [S'13] received his B.Sc., M.Sc., and Ph.D. degrees, all in computer science, from Central South University, China, in 2009, 2012, and 2016, respectively. From August 2013 to September 2015, he was a visiting Ph.D. student with the Department of Electrical and Computer Engineering, University of Waterloo. Currently, he is a Distinguished Professor with the School of Information Science and Engineering, Central South University. His research interests include wireless sensor networks, mobile sensing/computing, transparent computing, and cloud computing. He is the corresponding author of this article.

Xuemin (Sherman) Shen [M'97, SM'02,F'09] received his B.Sc. degree from Dalian Maritime University, China, in 1982, and his M.Sc. and Ph.D. degrees from Rutgers University, Newark, New Jersey, in 1987 and 1990, respectively, all in electrical engineering. He is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. He was the Associate Chair for Graduate Studies from 2004 to 2008. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He was a recipient of the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo; the Premier's Research Excellence Award in 2003 from the province of Ontario; and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He served as the Technical Program Committee Chair/Co-Chair for ACM MobiHoc '15, IEEE INFOCOM '14, IEEE VTC-Fall '10, the Symposia Chair for IEEE ICC'10, the Tutorial Chair for IEEE VTC-Spring '11 and IEEE ICC '08, and the Technical Program Committee Chair for IEEE GLOBECOM '07. He also serves/has served as Editor-in-Chief for *IEEE Network*, *Peer-to-Peer Networking and Application*, and *IET Communications*. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology and Communications Societies.

The collaborative efforts among municipalities, regulation departments, industry, academia and business companies are necessary to set up privacy policies and regulations. In addition, data privacy, availability and management should be achieved simultaneously.