A Secure IoT Architecture for Smart Cities

Shaibal Chakrabarty, Daniel W. Engels, *Senior Member, IEEE*

***Abstract*—We present a secure Internet of Things (IoT) architecture for Smart Cities. The large-scale deployment of IoT technologies within a city promises to make city operations efficient while improving quality of life for city inhabitants. Mission-critical Smart City data, captured from and carried over IoT networks, must be secured to prevent cyber attacks that might cripple city functions, steal personal data and inflict catastrophic harm. We present an architecture containing four basic IoT architectural blocks for secure Smart Cities: Black Network, Trusted SDN Controller, Unified Registry and Key Management System. Together, these basic IoT-centric blocks enable a secure Smart City that mitigates cyber attacks beginning at the IoT nodes themselves.**

I. Introduction

The Internet of Things (IoT) is growing pervasively around us. IoT systems encompass a broad range of technologies from small radio frequency identification (RFID) systems to large battery powered or mains powered sensor and control systems integrated into the everyday things around us. The primary role of IoT systems include the ability to monitor the environment, such as through ad-hoc sensor networks, to monitor things, such as through reading an RFID tag identifier, and to control things, such as through actuators.

With over 50% of the worlds population now in cities, significant strains are placed on city resources and infrastructures. The use of Information and Communications Technologies (ICT) to modernize cities promises to create Smart Cities that mitigate the impacts of increased city populations while improving the quality of life for all inhabitants [1]. Smart Cities are large, complex, distributed and continuous systems containing and using mission-critical data that must be secured end-to-end. Smart Cities are increasingly becoming IoT-enabled and IoT dependent [2], while their security is dependent upon the security of the underlying IoT protocols that have well-documented vulnerabilities [3].

In this paper, we present a secure IoT architecture for Smart Cities that addresses the vulnerabilities in traditional IoT systems. The building blocks of the architecture include Black Networks, Trusted SDN Controllers, a Unified Registry and a Key Management System. The security services provided through this architecture extend beyond the basic security provided by IoT protocols. The security services provided mitigate the vulnerabilities of basic IoT networks, especially for mission-critical data, at the Link and Network layers in addition to supporting standard services at the Transport and Application layers.

The remainder of this paper is organized as follows: In Section II we present the building blocks for a secure IoT framework for a Smart City. We draw relevant conclusions and suggest future areas of research in Section III.

II. A Secure IoT Architecture for Smart Cities

Figure1 shows the basic components of a secure Smart City IoT architecture. These basic components include Black Networks, Trusted SDN Controllers (noted as TTP), Unified Registry and Key Management System.

Smart City IoT networks operate over heterogeneous technologies and across multiple device types. The basic security building blocks enable secure communications and authentication across these heterogeneous technologies [4]. Not all security can be embedded within the IoT nodes because of IoT node resource constraints. We present four fundamental building blocks of a secure IoT architecture for a Smart City. They are: *Black Networks* for data privacy, confidentiality, integrity and authentication;*Trusted Third Party (TTP)* for efficient and anonymous routing across IoT nodes that sleep upto 90% of the time; *Unified Registry* for a database of devices (sensors, gateways and nodes) and their attributes; *Key Management* for an external key management system for IoT networks. Table I summarizes these security services.

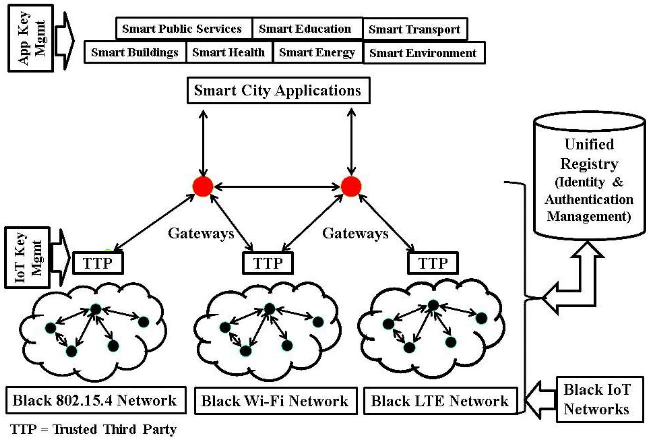

Fig. 1. Basic Components of a Secure IoT Architecture for Smart Cities

A. Black Networks

Black Networks are networks that secure all data, including the meta-data, associated with each frame or packet in an IoT protocol[5]. Black Networks encrypt the payload and the meta-data within an IoT protocol Link layer communications. Similarly, the meta-data is independently secured in the Network layer. Encryption can be done via Grain128a or AES in the EAX or OFB modes. The resulting compatible frame, allows the intended recipient to correctly receive and decode the message, via a shared secret. Black Networks mitigate a broad range of both passive and active attacks, providing

978-1-4673-9292-1/16/$31.00 ©2016 IEEE

TABLE I. SECURE IOT SMART CITY ARCHITECTURE SERVICES

IoT-based Smart City Security	
Security Component	*Security Services*
Black Networks	Confidentiality, Integrity, Privacy
Trusted SDN Controller	Secure Routing (Black packets), Availability
Unified Registry	Identity Management, Node Authentication, Authorization, Accounting, Availability and Mobility
Key Management	External Key Management

confidentiality, integrity and privacy in IoT networks due to the authenticated and secured communications at both the Link layer and the Network layer. However, encrypting the header creates routing challenges for IoT nodes which are asleep a majority of the time.

B. Trusted SDN Controller

Trusted SDN (Software Defined Networking) Controllers manage and orchestrate the flow of communications between and amongst IoT nodes and the rest of the networking infrastructure. SDN is a networking paradigm that separates the control flow from the data packet flow. The primary motivation for an SDN Controller is to resolve the routing challenges presented in privacy preserving IoT Black Networks [5]. In an IoT Black Network, Node A wishes to send a packet to Node B without an adversary knowing the packet is destined for Node B, and the packet from Node A must traverse the IoT network successfully even when the nodes sleep a majority of the time. We propose two general methods to resolve this. The SDN controller, maintaining an IoT network topology view and a sleep/wake timing view, can predetermine the packet's route and synchronize the nodes for routing. Therefore, the SDN controller can create flow tables for any Black packet to be routed from Node A to Node B and assist in synchronizing the wake times for the intermediate nodes. Another approach is for the SDN Controller to create a random, dynamic route for each hop, routing through awake intermediate nodes. The Trusted SDN Controller maintains a global IoT network view, manages sleep/wake cycles, along with other network states.

C. Unified Registry

A Unified Registry is used to consolidate the heterogeneous technologies, addressing schemes and devices that make up the IoT networks for a Smart City. The concept can be extended to a Visiting Unified Registry for IoT nodes that are mobile and cross networks. This is important from a security standpoint a majority of IoT networks assume fixed nodes communicating using wireless technologies. In a Smart City environment there are multiple wireless technologies in use (e.g. WiFi, LTE), there are multiple protocols in use (such as ZigBee, 6LoWPAN, WirelessHART, Bluetooth Low Energy), and there are multiple addressing schemes in use (e.g. IPv6 128-bit addressing, Bluetooth 48-bit addressing, RFID addressing and E.164). All of these identities need a unified attribute set for identity management, authentication, authorization and accounting. In addition, translations between wireless technologies, protocols and addressing schemes may have to be done, and the Unified registry facilitates the conversion. For multiple regulatory, practical and security (honeypot) reasons, a Unified Registry is difficult to implement in practice. What can be implemented, in a highly distributed manner, is a logical entity that points to the data and attribute set of the IoT node within the Smart City network.

D. Key Management System

Resource-constrained IoT nodes communicate securely by means of a shared key. Symmetric keys are used for simplicity and resource efficiency. Key management is a critical part of all security architectures. Keys must be generated, stored, communicated and used in a secure fashion. Key distribution is a critical problem for symmetric keys in a distributed mobile system. The use of a hierarchical Key Management System enables for efficient key distribution while providing for secure use of the symmetric keys by authorized devices.

We propose an independent hierarchical key management and distribution system for each layer of the communication protocol. Given multiple functions, access technologies, protocols and node types, Smart Cities need a secure Key Management System for generating, distributing, storing, revoking, changing and using keys.

III. CONCLUSIONS AND FUTURE WORK

Smart City IoT networks are increasingly widespread and carrying mission-critical data over IoT networks that have well-known vulnerabilities. Our secure IoT Smart City architecture adds privacy (through Black Networks), identity management and authentication (by the Unified Registry), secure routing (via a Trusted SDN) and a secure Key Management System. These four fundamental security architectural components can be deployed across all Smart City functions. Future research areas include extending the secure IoT architecture using address translations, defining location privacy and characterizing mobility.

REFERENCES

[1] B Bowerman, J Braverman, J Taylor, H Todosow, and U Von Wimmersperg. The vision of a smart city. In *2nd International Life Extension Technology Workshop, Paris*, volume 28, 2000.

[2] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities. *Internet of Things Journal, IEEE*, 1(1):22–32, 2014.

[3] Hui Suo, Jiafu Wan, Caifeng Zou, and Jianqi Liu. Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, volume 3, pages 648–651. IEEE, 2012.

[4] Henrich C Pohls, Vangelis Angelakis, Santiago Suppan, Kai Fischer, George Oikonomou, Elias Z Tragos, Rodrigo Diaz Rodriguez, and Theodoros Mouroutis. Rerum: Building a reliable iot upon privacy- and security-enabled smart objects. In *Wireless Communications and Networking Conference Workshops (WCNCW), 2014 IEEE*, pages 122–127. IEEE, 2014.

[5] Shaibal Chakrabarty, Daniel W. Engels, and Selina Thathapudi. Black SDN for the Internet of Things. In *Mobile Ad Hoc and Sensor Systems (IEEE MASS), Oct 2015 IEEE International Conference on*. IEEE, 2015.