LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities

Travis Mick, Reza Tourani, and Satyajayant Misra, *Senior Member, IEEE*

***Abstract*—Recent literature suggests that the Internet of Things (IoT) scales much better in an information-centric networking (ICN) model instead of the current host-centric Internet protocol (IP) model. In particular, the named data networking (NDN) project (one of the ICN architecture flavors) offers features exploitable by IoT applications, such as stateful forwarding, in-network caching, and built-in assurance of data provenance. Though NDN-based IoT frameworks have been proposed, none have adequately and holistically addressed concerns related to secure onboarding and routing. Additionally, emerging IoT applications such as smart cities require high scalability and thus pose new challenges to NDN routing. Therefore, in this paper, we propose and evaluate a novel, scalable framework for lightweight authentication and hierarchical routing in the NDN IoT. Our ns-3 based simulation analyses demonstrate that our framework is scalable and efficient. It supports deployment densities as high as 40 000 nodes/km^2 with an average onboarding convergence time of around 250 s and overhead of less than 20 kibibytes per node. This demonstrates its efficacy for emerging large-scale IoT applications such as smart cities.**

***Index Terms*—Information-centric networking (ICN), Internet of Things (IoT), networking, secure onboarding, secure routing, smart cities.**

I. Introduction

THE NEW emerging concept of smart cities applies concepts from the Internet of Things (IoT) to the management of diverse municipal infrastructure and assets [1]. Smart cities will involve large numbers of IoT devices installed in a range of settings from individual homes to critical infrastructure, potentially in a very dense deployment. Considering many of these devices will have limited computational and memory capacities, and will communicate over low-power lossy networks (LLNs), the feasibility of such applications will require advances in efficiency and scalability of IoT networking and communications. Additionally, smart cities will require strong guarantees of security: networked devices will handle large volumes of sensitive information and control valuable assets such as utility infrastructure, thus widening the attack surface for potential compromise. Therefore, strong end-to-end security and privacy mechanisms between smart devices and the cloud are imperative.

Manuscript received May 30, 2017; accepted June 29, 2017. Date of publication July 11, 2017; date of current version April 10, 2018. This work was supported by the NSF under Grant 1719342, Grant 1345232, and Grant 1248109. *(Corresponding author: Satyajayant Misra.)*

The authors are with the Department of Computer Science, New Mexico State University, Las Cruces, NM 88003-8006 USA (e-mail: tmick@cs.nmsu.edu; rtourani@cs.nmsu.edu; misra@cs.nmsu.edu).

Digital Object Identifier 10.1109/JIOT.2017.2725238

Recent literature suggests that information-centric networking (ICN) is a more appropriate approach than Internet protocol (IP) for IoT [2]. Named data networking (NDN) [3], in particular, is a strong architecture for creating scalable and efficient smart city networks, by employing features such as stateful forwarding and in-network caching. In addition, it offers security benefits such as enforced provenance through mandatory network-layer signatures.

Several ICN-based IoT deployments have been announced in the literature, however, no holistic NDN of Things (NDNoT) architecture and protocol suite has yet been proposed. In particular, existing literature tends to neglect concerns related to secure routing and onboarding. Works that do address routing or onboarding do so separately, neglecting the fact that they are closely coupled. As a result, the proposed solutions are limited in scalability, and lack applicability to highly demanding applications such as smart cities. We believe that by exploiting the coupling between routing and onboarding and addressing them *simultaneously*, high degrees of network efficiency and scalability, which are demanded by such applications become achievable.

In addition to introducing a combined approach to routing and onboarding, we employ a hierarchical network structure, a design which has previously been suggested to enable scalability in IoT [4]. Such an architecture allows us to offload much of the burden of routing onto a few less-constrained "anchor" nodes (which may also serve as fog nodes as in [4]), while other devices need only form destination-oriented trees. This approach is similar to that of the IPv6 routing protocol for low-power and lossy networks (RPL) [5], which is currently favored for the IP-based IoT. This is in contrast to previous proposals for the NDNoT, which employed reactive, rather than proactive, routing protocols.

In our framework, secure onboarding is made a prerequisite to routing, in order to help protect the network against routing attacks such as blackholes [6]. Each node in the network is authenticated prior to commencing routing, and in turn a node also authenticates the network it is joining. Since asymmetric cryptography is typically infeasible on IoT devices, we use symmetric cryptography. Our onboarding protocol is based on preshared keys (PSKs) between each node and a designated authentication manager in the infrastructure.

We have combined our approaches to routing and onboarding into a single holistic framework for lightweight authentication and secured routing (LASeR). The combined authentication and onboarding processes are very lightweight, requiring only three round trips and few cryptographic operations.