Accepted Manuscript

A realistic performance evaluation of privacy-preserving protocols for smart grid AMI networks

Samet Tonyali, Ruben Munoz, Kemal Akkaya, Utku Ozgur

PII: S1084-8045(18)30219-4

DOI: 10.1016/j.jnca.2018.06.011

Reference: YJNCA 2161

To appear in: *Journal of Network and Computer Applications*

Received Date: 16 December 2017

Revised Date: 3 May 2018

Accepted Date: 19 June 2018

Please cite this article as: Tonyali, S., Munoz, R., Akkaya, K., Ozgur, U., A realistic performance evaluation of privacy-preserving protocols for smart grid AMI networks, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.06.011.

A Realistic Performance Evaluation of Privacy-Preserving Protocols for Smart Grid AMI Networks

Samet Tonyali[a,*], Ruben Munoz[a], Kemal Akkaya[a], Utku Ozgur[a]

[a] *The Department of Electrical and Computer Engineering, Florida International University, Miami, FL, 33174 USA*

Abstract

The proliferation of ubiquitous communication with the Internet of Things has led to advancement in wireless communication technologies. Today, they have become an indispensable component of smart city applications thanks to the lower cost and easiness of the installation and the maintainability. For example, they are a promising alternative of the wired solutions used in Smart Grid Advanced Metering Infrastructure (AMI) networks. However, wireless communication networks are more vulnerable to cyber-attacks and easier to be eavesdropped, so researchers have proposed a number of secure protocols. In addition to being vulnerable to cyber-attacks, AMI also exposes consumer power data which poses privacy issues. While there has been a lot of research to address these issues, the validation efforts mostly utilized simulators and actual overhead due to these approaches have not been captured in a realistic setup. Therefore, in this paper, we chose two open-source wireless mesh networking standards, IEEE 802.11s and ZigBee, and built an AMI testbed at FIU Engineering Center that will be able to collect power readings from smart meters. Then, we used the testbed to assess and compare the performance of the two standards under fully homomorphic encryption and secure multiparty computation-based privacy-preserving protocols that can provide computation on the encrypted

*Corresponding author

Email addresses: stony002@fiu.edu (Samet Tonyali), rmuno039@fiu.edu (Ruben Munoz), kakkaya@fiu.edu (Kemal Akkaya), uozgu001@fiu.edu (Utku Ozgur)