IOT-1-PASS-SECURITY: 1(ONE)-PASS AUTHENTICATED KEY AGREEMENT PROTOCOL FOR ENERGY CONSTRAINT IOT APPLICATIONS

Mehrdad Aliasgari, Garrett Chan, and Mohammad Mozumdar
Department of Computer Engineering and Computer Science,
Department of Electrical Engineering
California State University, Long Beach
Emails: mehrdad.aliasgari@csulb.edu, gchan310@gmail.com,
mohammad.mozumdar@csulb.edu

Submitted: Nov. 30, 2015 ***Accepted: Mar. 22, 2016*** ***Published: June 1, 2016***

Abstract- IoT data security is one of the core unresolved challenges in IoT community. Lack of resource-efficient authenticated secure key exchange methods among resource- constrained IoT devices makes man-in-the-middle attacks a serious vulnerability. In this regard, we propose 1(One) pass Authenticated Key Agreement (AKA) protocol for IoT applications. This protocol requires only one round of communication among the sender and receiver to establish a secure session, providing a balance between security (data confidentiality with integrity) and performance. We implemented and performed comprehensive power consumption and timing analysis of our implementation on Contiki platform to demonstrate the efficiency of the proposed protocol.

Index terms: IoT, Sensor Networks, Security, Identity Based Encryption, Elliptic Curve Cryptography.