

Accepted Manuscript

A dynamic prime number based efficient security mechanism for big sensing data streams

Deepak Puthal, Surya Nepal, Rajiv Ranjan, Jinjun Chen

PII: S0022-0000(16)00020-9
DOI: <http://dx.doi.org/10.1016/j.jcss.2016.02.005>
Reference: YJCSS 2957

To appear in: *Journal of Computer and System Sciences*

Received date: 28 August 2015
Revised date: 23 January 2016
Accepted date: 2 February 2016

Please cite this article in press as: D. Puthal et al., A dynamic prime number based efficient security mechanism for big sensing data streams, *J. Comput. Syst. Sci.* (2016), <http://dx.doi.org/10.1016/j.jcss.2016.02.005>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



A Dynamic Prime Number Based Efficient Security Mechanism for Big Sensing Data Streams

Deepak Puthal^{*}, Surya Nepal[†], Rajiv Ranjan^{**}, and Jinjun Chen^{*}

^{*}Faculty of Engineering and Information Technology
University of Technology Sydney, Australia

[†]CSIRO Data61, Australia

^{**}School of Computing Science
Newcastle University, UK

Abstract

Big data streaming has become an important paradigm for real-time processing of massive continuous data flows in large scale sensing networks. While dealing with big sensing data streams, a Data Stream Manager (DSM) must always verify the security (i.e. authenticity, integrity, and confidentiality) to ensure end-to-end security and maintain data quality. Existing technologies are not suitable, because real time introduces delay in data stream. In this paper, we propose a Dynamic Prime Number Based Security Verification (DPBSV)¹ scheme for big data streams. Our scheme is based on a common shared key that updated dynamically by generating synchronized prime numbers. The common shared key updates at both ends, i.e., source sensing devices and DSM, without further communication after handshaking. Theoretical analyses and experimental results of our DPBSV scheme show that it can significantly improve the efficiency of verification process by reducing the time and utilizing a smaller buffer size in DSM.

Keywords—Security; Sensor Networks; Big Data Stream; Key Exchange; Security Verification.

1. Introduction

1.1 Big Data Stream

A large number of applications, such as large scale sensors, information monitoring, web exploring, data from social networks like Twitter and Facebook, surveillance data analysis, and financial data analysis, deal with a large stream of data input, and consequently require an alternate ideal model of real-time data processing. As a result, a new computing paradigm based on Stream Processing Engines (SPEs) has appeared [15]. SPEs deal with the specific types of challenges and are intended to process data streams with a minimal delay [15-18]. In SPEs, data streams are processed in real time (i.e. on-the-fly) rather than batch processing after storing the data.

Several of these applications are approaching the bottleneck of current data streaming infrastructures and require real-time processing of very high-volume and high-velocity data streams (also known as *big data streams*). The complexity of big data is defined through V⁴'s: 1) *volume* – referring to terabytes, petabytes, or even exabytes (1000⁶ bytes) of stored data, 2) *variety* – referring to unstructured, semi-structured and structured data from different sources like social media (Twitter, Facebook etc.), sensors, surveillance, image or video,

¹The preliminary version of this paper is published in *14th IEEE International Conference on Trust, Security and Privacy in Computing and communications* (IEEE TrustCom-15) Helsinki, Finland. 2015. [47]

Download English Version:

<https://daneshyari.com/en/article/4951276>

Download Persian Version:

<https://daneshyari.com/article/4951276>

[Daneshyari.com](https://daneshyari.com)