Optimizing Message Verbosity and Energy Consumption in Secured Wireless Mobile Networks

P. P. Abdul Haleem, National Institute of Technology Calicut, India
M. P. Sebastian, National Institute of Technology Calicut, India

ABSTRACT

This article presents a method for reducing the verbosity of messages in the constrained wireless mobile networks. Wireless mobile devices, especially low cost devices are stifled by the limited resources such as battery power, screen size, input, memory and processors. The relevance of low cost wireless mobile devices in penetrating to the third world market demands for a cost effective messaging format that fits in the constrained wireless environment. The proposed scheme is based on YAML Ain’ Markup Language (YAML), a user friendly and light weight messaging format. Measures to reduce the message size and energy consumption together with secure processing are proposed. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: Knowledge Representation; ECC; Mobile Computing, Signcryption; Verbosity Reduction; Wireless Mobile Networks; XML

INTRODUCTION

In the recent years, both the number and capabilities of wireless mobile devices have increased rapidly in such a way that the mobile world is becoming a significant part of the Internet. This sudden upsurge also resulted in the increase of applications and user base. Applications and users, accustomed to the luxury of larger systems are forced to work within the daunting constraints of the devices and the network.

A major constraint in wireless mobile devices is power. Even with latest processors and memory chips, the rechargeable battery attached to the wireless mobile devices still tends to fall behind the expectations. The RF part of cellular engine, which is responsible for transmission and reception of messages, is the biggest consumer of energy in a mobile device (Michael, 2005). Security protocols also consume power - number of packets transmitted or received and the size of the keys are two...
important factors to be taken care to conserve energy. Wireless environment also imposes several constraints such as (i) networks are less reliable and expensive (ii) transmission errors and message latency are higher than in the wired world, and (iii) any information transmitted over wireless links is subjected to possible interception.

Available studies indicate that verbosity reduction of messages is an urgent concern in the constrained wireless mobile environment (Kangasharju, Lindholm, & Tarkoma, 2008). Thus reducing the verbosity of messages can have an impact cutting across several layers of the wireless networking protocols. Coupled with this, the application of a lightweight cryptographic system suitable to the wireless mobile environment can reduce the power consumption considerably. We propose the application of an Elliptic Curve Cryptography (ECC) based technique to address this problem.

ECC is already in use in the wireless mobile security arena due to its dramatic decrease in the key size and running time without compromising the security. A 160-bit ECC key offers the same level of security as a 1024-bit RSA key (Chou, 2003). The energy analysis on various cryptographic algorithms and key exchange protocols reveals considerable savings with ECC without compromising in security (Potlapally, Ravi, Raghunathan, & Jha, 2003). ECC is used in the design of the elliptical curve variations of Integrated Encryption Scheme (IES) and Signcryption. Elliptic Curve Integrated Encryption Scheme (ECIES) is a public-key encryption scheme based on ECC which provides semantic security against chosen-plaintext and chosen-ciphertext attacks (Certicom-Research, 2000). Signcryption is a method to reduce the cost of the signature-then-encryption method, by combining the functions of digital signature and public key encryption in a logically single step (Zheng, 1997a). Signcryption costs 58% less in average computation time and 70% less in message expansion than does signature-then-encryption, and it costs on the average 50% less in computation time and 91% less in message expansion than signature-then-encryption with RSA (Zheng, 1997b). Thus, IES and Signcryption with ECC appear to be better mechanisms in the constrained wireless mobile environment.

XML is generally considered as the protocol for messaging (SOAP-Tutorial, 2007). XML faces many problems when used in the wireless mobile environment (Kangasharju, 2005). The number of bytes required for data representation is huge. Due to this verbosity, XML buffers need to be flushed more often at the time of input and output, leading to lesser throughput. Also, larger messages are vulnerable to retransmissions. The highly textual nature of XML makes the string parsing compulsory for further processing. XML documents are structured and this adherence of the document to the accompanying structure is to be verified by parsers. It has been one of the easy targets for hackers, due to its long term use and universality.

There is an argument that the designers of wireless mobile devices are competing to pack more facilities into the devices and hence there is no scope for energy conserving measures, especially for messaging. But in reality, these features are used only by the top 10% of the customers. At the same time, low-cost devices are steadily increasing their market share, especially in developing countries. The projected shipments of ultra-low cost devices is estimated to be 24.3 million in the Asia Pacific region, as opposed to 0.6 million in the North America region (Gokran, 2007).

Thus, a messaging standard that performs well within the constraints of wireless mobile environments is needed. This article presents a messaging standard that reduces some of the limitations of XML (relevant in the wireless mobile environment) retaining its good aspects. We suggest a messaging format with the following features: (i) simple and flexible, both for the user and the application programmer (ii) editable and easily readable (iii) less verbosity for the message without compression/binary encoding (without affecting the readability) (iv) facility for a schema definition (v) consumes less bandwidth and short transmission time (by
Component Agent Systems: Building a Mobile Agent Architecture That You Can Reuse
www.igi-global.com/chapter/component-agent-systems/26725?camid=4v1a

A Probabilistic Routing Protocol in VANET
www.igi-global.com/article/probabilistic-routing-protocol-vanet/47329?camid=4v1a