Use of encryption for secure communication plays an important role in building applications in mobile computing environments. With the emergence of more and more heterogeneous devices and diverse networks, it is difficult, if not impossible, to use a one-size-fits-all encryption algorithm that always has the best performance in such a dynamic environment. We envision that the only way to accelerate the deployment of encryption algorithms is providing a flexible adaptation of choosing an appropriate encryption algorithm from multiple diverse algorithms according to the characteristics of heterogeneous mobile computing environments.

Based on the Fractal framework [1], we propose and implement an adaptive encryption protocol, which can dynamically choose a proper encryption algorithm based on application-specific requirements and device configurations. Performance evaluation results show that in the divergent environment with different devices and applications, the adaptive encryption protocol successfully selects the best encryption algorithm from the candidate algorithms, and minimizes the total time overhead and insures the security as well.

1. INTRODUCTION

Use of encryption for secure communication is important for building distributed applications. With the development of computer and communication technologies, more and more heterogeneous devices, like desktops, laptops, PocketPCs, and cellular phones are connected to the Internet using diverse networks, like Ethernet, Wi-Fi, Bluetooth, 3G/4G wireless technology. On one hand, different technologies have different characteristics. On the other hand, a heterogeneous environment makes it possible to dynamically change between different devices and network environments. For instance, a person uses a laptop with a cable modem at home, a cell phone with 3G/4G or Bluetooth on the way to the office, a desktop with Ethernet LAN in the office and a PDA with Wi-Fi in the meeting room. Diverse network connections and heterogeneous
devices demand the adaptation functionality in a distributed fashion because no one-size-fits-all single function or protocol can perform well over all these networks and devices. Although many symmetric or asymmetric encryption algorithms have been proposed, none of them takes the diversities of device and network into the design. It is difficult, if not impossible, to build a one-size-fits-all encryption protocol which can run well in the dynamic environment. The only way to accelerate the deployment of encryption algorithms is to provide a flexible adaptation of choosing multiple diverse algorithms.

Adaptation has been considered as a general approach to address the mismatch problem between clients and servers [2, 3, 4, 5]. From the perspective of adaptation locations, some of them propose the in-network adaptation, such as CANS [2], Rover [3], Odyssey [4], and Active Names [5], which focus on how to do the adaptation step by step across an overlay path. From the network OSI model’s point of view, some of them work in the network layer [6], which adapts the TCP/IP protocol dynamically according to the changing situations on both ends. The Fractal framework [1], a dynamic application level protocol adaptation approach, utilizes the mobile code technology for protocol adaptation and leverages existing content distribution networks (CDN) for protocol adaptors (mobile codes) deployment. The protocol adaptation in Fractal is based on the assumption that an application protocol is composed of a series of components, also called protocol adaptors (PAD). When a protocol needs to be adapted, the application simply needs to add or remove some PADs into or from it. We will give a brief introduction about the Fractal framework in Section 3.

Based on the Fractal framework, we propose and implement an adaptive encryption protocol, which dynamically chooses a proper encryption algorithm based on application-specific requirements and device configurations. Evaluation results show that the adaptive encryption protocol can choose the best encryption algorithm from the candidates to minimize the total time overhead and ensure the security as well.

The rest of the chapter is organized as follows. After a brief introduction of background in Section 2, the Fractal framework and platform of the adaptive encryption protocol are depicted in Section 3. Section 4 describes the adaptation model for the adaptive encryption protocol. Performance evaluation and related work are described in Section 5 and Section 6 respectively. We summarize the chapter in Section 7.

2. BACKGROUND

In the design and implementation of the adaptive encryption protocol, several background topics are involved, such as: mobile code [7, 8], content distribution network [9, 10], protocol adaptation [11, 6, 12], and encryption algorithms. In this section, we explain the general background of each related research field.

2.1. Mobile Code

Mobile code [8] is defined as the data that can be executed as a program. The code can be pre-compiled for immediate execution on the recipient’s processor, compiled