Estudo do Consumo de Energia do Protocolo DTLS para Internet das Coisas

Daniele Freitas de Jesus, João Henrique Kleinschmidt

Programa de Pós-Graduação em Engenharia da Informação – Universidade Federal do ABC (UFABC)
Caixa Postal 09210-580 - Santo André - SP - Brasil

{daniele.freitas,joao.kleinschmidt}@ufabc.edu.br,

Abstract. *The term Internet of Things refers to the interconnection of networks of smart objects and technologies on the global Internet, as well as a set of technologies that make up these objects and their applications and services. The Internet of Things has great limitations on their resources and there are many challenges to enable security of the transmitted information. Every security implementation should take these limitations into account, which motivated this research. This research aims to propose different security architectures, using standardized protocols for the Internet of Things, analyzing the energy consumption of the network when using the security protocol DTLS. We use the Contiki simulation environment to test the DTLS protocol in a client/server scenario to verify the energy consumption of the handshake process.*

1. Introdução

O termo Internet das Coisas (IoT - *Internet of Things*) vem sendo amplamente utilizado para se referir à interconexão da rede formada por objetos inteligentes e as tecnologias globais na Internet, além do conjunto das tecnologias que compõem esses objetos e o conjunto de suas aplicações e serviços. Algumas características chaves identificam esse paradigma: dispositivos heterogêneos, a troca de dados onipresente por meio de tecnologias sem fio, seus recursos escassos de processamento, energia, armazenamento e banda de transmissão, para economizar eventuais custos na construção da arquitetura [Miorandi 2012].

Os recursos escassos na Internet das Coisas ainda são os grandes limitantes para possibilitar segurança das informações transmitidas, mas a falta de padronização na segurança para Internet das Coisas é um sério problema, já que por enquanto só existe o protocolo *Datagram Transport Layer Security* (DTLS) disponível. Alguns trabalhos propõem o uso desse protocolo com outros presentes nas outras camadas existentes, mas não analisam a pilha de protocolos nos principais cenários da Internet das Coisas.

O objetivo principal desta pesquisa é analisar o consumo de energia do protocolo DTLS para a Internet das Coisas, utilizando a ferramenta Power Trace do Contiki para mensurar o consumo de energia.

2. Estudo do Consumo de Energia do DTLS na IoT

Estruturalmente, a IoT requer arquiteturas de software que sejam capazes de lidar com grandes quantidades de informações, consultas e computação, fazendo uso de novos paradigmas de processamento de dados e de fluxo, filtragem, agregação e mineração de dados, todos sustentados por padrões de comunicação, tais como HTTP e IP. Entretanto, a energia é desperdiçada por transmissão de dados desnecessários, por conta de sobrecarga de protocolo e padrões de comunicação não-otimizados. Por isso, a necessidade em se padronizar protocolos para a IoT [Palattella 2013].

Os protocolos disponíveis e atualmente usados em cada camada, de acordo com [Kothmayr, Et Al. 2013] são: na camada de Aplicação, *Constrained Application Protocol* (CoAP) entre outros; em Segurança, o *Datagram Transport Layer Security* (DTLS); na camada de Transporte e Rede, o UDP, IPv6 e *Routing Protocol for Low-power* (RPL); na camada de Acesso e Física, o IEEE 802.15.4.

O DTLS é um protocolo de segurança usado para proteger o tráfego de *datagramas* para aplicações cliente/servidor, automatizando o gerenciamento de chaves, a autenticação e a encriptação dos dados. É composto de um protocolo *Record* que carrega outros protocolos como o *Alert, ChangeCipheSpec, Handshake*, e *Data.*

O *Handshake* é organizado em *flights*, usadas para negociar chaves de segurança, conjuntos de codificação e métodos de compressão [Raza, Et Al. 2013]. Em resumo, nos *fligths* 1, 2 e 3 são trocadas as mensagens *Hello* entre cliente e servidor para iniciar a conexão, nos *fligths* 4 e 5 são definidos o tamanho da chave, métodos de compressão e/ou certificados, caso tenha, e no *fligth* 6 é enviada a mensagem de finalização do *Handshake*, permitindo o envio de dados criptografados.

Para verificar o desempenho energético da rede com o uso da pilha de protocolos estudado, foi utilizado o Sistema Operacional *Contiki*, que é um open source pioneiro para a Internet das Coisas, orientado a eventos. Possui a capacidade de carregar e descarregar aplicações no equipamento em execução, ou ser emulado em seu simulador *Cooja*, antes de ser gravado [Dunkels 2004].

Foram realizados testes no *Cooja* usando uma arquitetura cliente/servidor com a pilha de protocolos e o DTLS-Lithe - uma ferramenta disponibilizada por [Raza, Et Al. 2013], que implementa o DTLS com a opção de *Handshake* completo ou comprimido - habilitados, para mensurar o impacto energético inicial deste protocolo de segurança neste cenário de rede.

3. Considerações Finais

Esta primeira fase da pesquisa buscou estudar os conceitos gerais de Internet das Coisas, Segurança, e os protocolos disponíveis para ela, além de iniciar os testes na plataforma de simulação.

Os primeiros resultados com o DTLS no cenário cliente/servidor, já apresentaram uma considerável redução de consumo energético no servidor, conforme apresentado na Figura 1. Propostas como o *Lithe* reduzem o consumo de energia em seu *Handshake*, o que permite nortear as próximas etapas para abordar outras arquiteturas de segurança para a Internet das Coisas.

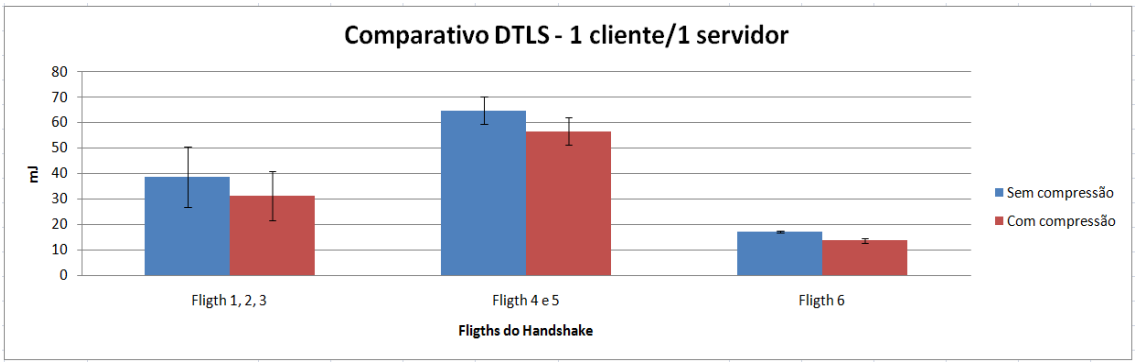

Figura 1 - Análise de Consumo DTLS no Servidor Com e Sem Compressão de *Handshake*

4. Referências

Dunkels, Adam, Et Al. (2004) Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors. Swedish Institute of Computer Science.

Kothmayr, Thomas, Et Al.(2013) DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Networks. Elsevier.

Miorandi, Daniele, Et Al.(2012) Internet of things: Vision, applications and research challenges. Ad Hoc Networks 10 1497–1516.

Palattella, Maria Rita, Et Al.(2013) Standardized Protocol Stack for the Internet of (Important) Things. IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter.

Raza, Shahid, Et Al. (2013) Lithe: Lightweight Secure CoAP for the Internet of Things. IEEE Sensors Journal, Vol. 13, No. 10, Oct 2013.

Rescorla, E., Et Al.(2006) Datagram Transport Layer Security. RFC 4347: Datagram Transport Layer Security. Internet Engineering Task Force (IETF).