Estudo de Mecanismos de Gerenciamento de Confiança no Contexto da Internet das Coisas

Carolina V. L. Mendoza[1], João H. Kleinschmidt[1]

[1]Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas Universidade Federal do ABC (UFABC) Santo André – SP – Brasil

clezamen@hotmail.com, joao.kleinschmidt@ufabc.edu.br

Abstract. *Internet of Things (IoT) is the interconnection of a large number of devices or "things". One challenge in the IoT is the security and privacy. Managing trust is a mechanism that allows the nodes to establish connections with a predefined level of trust between them. The aim of this study is to address the main characteristics of the trust management in IoT. Most existing studies do not meet the needs of the IoT, due to the greater heterogeneity of network nodes and different requirements of IoT. As future work, strategies of trust management will be implemented in the Contiki COOJA simulator.*

1. Introdução

A Internet das Coisas é a interconexão de um grande número de dispositivos, ou seja, entidades heterogêneas ou "coisas" [Atzori et al 2010]. Esses objetos são identificáveis e possuem uma tarefa específica em um determinado ambiente. Este novo paradigma implica uma comunicação não só entre os seres humanos e as coisas, mas também entre os próprias objetos, sem intervenção humana. Entre as redes que prometem uma melhor adaptação a este novo paradigma são as redes ad hoc móveis, RFID (Identificação por Rádio Frequência) e as redes de sensores, graças ao seu baixo custo e capacidade de comunicação[Cho et al 2011]. A IoT traz grandes desafios para a implementação no mundo real. Um desses desafios é a segurança e privacidade [Lacuesta et al 2012]. O gerenciamento de confiança é um mecanismo que permite que os nós estabeleçam conexões com um nível pré-definido de confiança entre eles e contribui para a segurança da IoT[Cho et al 2011]. Devido a limitações de recursos, tais como capacidade de processamento, memória e energia, heterogeneidade dos dispositivos e requisitos específicos da Iot, não é possível implementar mecanismos de confiança tradicionais das redes existentes. O objetivo deste estudo é abordar as principais características do gerenciamento de confiança no contexto da Internet das Coisas.

2. Gerenciamento de confiança

Gerenciamento de confiança são os mecanismos para avaliar, estabelecer, manter e revogar a confiança entre dispositivos que formam parte de uma rede. O parâmetro de confiança pode ser usado para o controle de acesso, roteamento seguro, detecção de intrusos, entre outros. Geralmente a noção de confiança está relacionada a reputação, sendo que a primeira (confiança) é uma derivação da segunda (reputação). Reputação é a opinião de um nó sobre outro e é formada baseada no histórico de comportamento do nó [Cho et al 2010]. Foram analisados os trabalhos de pesquisas de maior relevância,

abordando os sistemas de gerenciamento de confiança para redes ad hoc, assim como para RFID e redes de sensores. As metodologias utilizadas para a modelagem de confiança entre nós, assim como a identificação dos fatores e métricas que afetam o parâmetro de confiança foram estudados. Em geral, as estratégias propostas usam observações diretas e indiretas, recomendações, evidências (certificados digitais, infraestruturas de chaves públicas, etc) ou políticas locais e globais [Cho et al 2010]. A maioria dos estudos existentes para redes ad hoc e de sensores não satisfaz as necessidades da IoT, devido a maior heterogeneidade dos nós da rede. Existem poucos trabalhos na literatura que tratam do gerenciamento de confiança especificamente para IoT e muitos estudos ainda precisam ser feitos [Bao et al 2012; Fritsch et 2012; Lacuesta et al 2012; Lu et al 2012]. Outra dificuldade encontrada é a falta de análise comparativa entre os mecanismos propostos e os diferentes cenários utilizados por cada trabalho.

Neste contexto, este trabalho pretende incorporar os principais mecanismos de gerenciamento de confiança existentes na literatura e avaliá-los no contexo da IoT, considerando seus diferentes requisitos e heterogeneidade. Para isso, estão sendo implementados no simulador Cooja, que faz parte do sistema operacional Contiki [Contiki 2013]. Modificando o código do simulador para incorporar as características de confiança entre nós, os quais também serão avaliados em cenários próprios para a IoT. Este simulador foi desenvolvido especificamente para o ambiente da IoT e permite a comparação de diversos algoritmos. Outra vantagem é que é possível a simulação de diversos hardwares reais, que estão implementados no Contiki. Isto permite, por exemplo, avaliações mais precisas do consumo de energia dos nós da rede.

3. Referências

Atzori, L., Iera, A., & Morabito, G. (2010). “The internet of things: A survey”. Computer Networks, 54(15), 2787-2805.

Bao, F., & Chen, I. R. (2012). “Dynamic trust management for internet of things applications”. Proceedings of the 2012 International Workshop on Self-aware Internet of Things (pp. 1-6).

Contiki O.S developed for the Internet of Things <www.contiki-os.org> (acessado em 01.11.13).

Cho, J. H., Swami, A., & Chen, R. (2011). “A survey on trust management for mobile ad hoc networks”. Communications Surveys & Tutorials, IEEE, 13(4), 562-583.

Fritsch, Lothar; Groven, Arne-Kristian; Schulz, Trenton, (2012). “On the Internet of Things, Trust is Relative”. Communication in Computer and Information Science - Contructing Ambient Intelligence. Springer Berlin Heidelberg. p. 267-273.

Lacuesta, R., Palacios-Navarro, G., Cetina, C., Peñalver, L., & Lloret, J. (2012). “Internet of things: where to be is to trust”. EURASIP Journal on Wireless Communications and Networking, 1-16.

Liu, W., Yin, L., Fang, B., & Yu, X. (2012). “An Efficient Trust Evaluation Approach in Attacker Dominated Networks in Internet of Things”. In Future Information Technology, Application, and Services (pp. 559-567). Springer Netherlands.