2011

Managing Trust in Provenance-Aware Water Information Systems

Quan Bai
Tasmanian ICT Center, Australian Commonwealth Scientific and Research Organization (CSIRO), quan.bai@csiro.au

Qing Liu
Tasmanian ICT Center, Australian Commonwealth Scientific and Research Organization (CSIRO)

Corné Kloppers
Tasmanian ICT Center, Australian Commonwealth Scientific and Research Organization (CSIRO)

Xing Su
Tasmanian ICT Center, Australian Commonwealth Scientific and Research Organization (CSIRO)

Heiko Mueller
Tasmanian ICT Center, Australian Commonwealth Scientific and Research Organization (CSIRO)

See next page for additional authors

Follow this and additional works at: https://scholarsarchive.byu.edu/openwater

Managing Trust in Provenance-Aware Water Information Systems

Authors
Quan Bai, Qing Liu, Corné Kloppers, Xing Su, Heiko Mueller, and Andrew Terhorst

Managing Trust in Provenance-Aware Water Information Systems

Quan Bai, Qing Liu, Corné Kloppers, Xing Su,
Heiko Mueller and Andrew Terhorst

Tasmanian ICT Center,

Australian Commonwealth Scientific and

Research Organization (CSIRO), Hobart, Australia

Email: Quan.Bai@csiro.au

Introduction

Open water information systems such as the South Esk Hydrological Sensor Web[1] allow easy access to, and sharing of, hydrological information. Because important decisions may be based on the shared information, it is necessary to provide a trust management mechanism that allows users to evaluate the trustworthiness of such information. Trust can be defined as a belief a party has that the other party will fulfil its commitments [1][2].

Trust and Trust Management

Trust is a well-studied topic in computer science, spanning areas as diverse as security, multi-agent systems and distributed systems. For a water information system, we define trust as an assessment of the likelihood that a piece of information is accurate and reliable. There are a number of trust management mechanisms, which can be classified into two categories [3]:

1. **Reputation-Based Trust Mechanisms** normally use explicit and topic-specific trust ratings to represent the reliability or quality of a service (e.g., the rating system in the on-line auction site eBay). Service consumers are required to generate and maintained trust ratings based on their experience. Obviously, subjective trust evaluations from different users are introduced in Reputation-Based Trust Mechanisms, especially since there is no standard and shared evaluation criterion among users.

2. **Context-Based Trust Mechanisms** use meta-information to describe the circumstances in which information has been claimed (e.g., who published what, when and why), then evaluate information trustworthiness

---

[1] http://wron.net.au/au.csiro.OgcThinClient/OgcThinClient.html

based the roles of information providers. For example people may be inclined to trust the flood warnings published by the Australian Bureau of Meteorology rather than warnings from other authorities/organisations. Context-Based Trust Mechanisms encode trust policies from society into trust evaluation rules. This reduces subjective biases from individual users but at the cost of flexibility.

Provenance-Based Trust Evaluation

Provenance describes the origins and processes that relate with the generation of a piece of data. Provenance is considered as one of the most promising methods to help users assess the trustworthiness of shared data. The Tasmanian ICT Centre is currently incorporating a Provenance Management System (PMS) into the South Esk Hydrological Sensor Web. Not only does the PMS provide detailed descriptions about generation of information products, it also provides domain-specific information about sensors and model parameters. Provenance enables hydrologists and decision-makers to make judgements about the trustworthiness of information based on a wide range of criteria. Provenance information can be an order of magnitude more than the information it describes. There is a need to develop a trust model which can automatically extract trust information from huge amounts provenance information.

We have investigated popular trust management mechanisms and propose a provenance-based trust evaluation model that allows users to define key trust criteria. The proposed model inherits the advantages in both Reputation- and Context-Based Trust Mechanisms. The richer context provided by provenance information allows users to make more accurate assessments about data trustworthiness. Furthermore, users can include the explanation about their trust judgements as provenance information. Trust information (such as rating scores) can be associated with meta-annotations which include data consumption curriculum, data usage and reasoning behind trust judgements. This helps reduce risk of using information unfit for purpose and remove bias in trust assessments.

From the above two aspects, it can be seen that we can build a more reasonable and objective trust management mechanism based on provenance information. For water information systems, such a trust management mechanism will help users to estimate the trustworthiness of water information without introducing too much overheads.

References

[1] S. D. Ramchurn, D. Huynh, and N. R. Jennings, "Trust in multi-agent systems," *The Knowledge Engineering Review*, vol. 19, pp. 1–25, 2004.

[2] D. Artz and Y. Gil, "A survey of trust in computer science and the semantic web," *Journal of Web Semantics*, vol. 5, pp. 58–71, 2007.

[3] C. Bizer and R. Oldakowski, "Using context- and content-based trust poli-
cies on the semantic web," in *Proceedings of the 13th World Wide Web
Conference*, New York, NY,USA, 2004, pp. 228–229.