Mehanizmi izmenjave zaupanja in ugleda

David Jelenc

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Laboratorij za e-medije
Večna pot 113, 1000 Ljubljana, Slovenija
E-pošta: david.jelenc@fri.uni-lj.si

Abstract

Trust and reputation systems are systems that estimate the trustworthiness of entities as they roam virtual communities and applications. But while entities can traverse application boundaries their trust and reputation information cannot: it remains locked to the application in which it was generated which forces entities to build trust and reputation anew in every application they join. We describe the issue of trust and reputation system information exchange. We define the problem, outline the set of desired features that a exchange mechanism ought to have and analyze the existing solutions through the lens of required features. We conclude that only a few solutions exist that address the issue of trust and reputation information exchange and all of them are in some aspect limited.

1 Uvod

Z nenehno rastjo omrežja Internet postajajo aplikacije, v katerih raznovrstne entitete—bodisi ljudje, naprave ali avtonomne storitve—zasledujejo svoje cilje s sodelovanjem, čedalje bolj razširjene. A v tovrstnih aplikacijskih okolij je sodelovanje težko vzpostaviti, saj ne vemo, ali bo entiteta, s katero smo v interakciji, dejansko spoštovala svoje obveze. Takšni pomisleki so še posebej izraziti v odprtih okoljih, ki nimajo razsodnikov, ki bi tovrstne spore razreševali, ali v primerih, kadar so si entitete neznane. V takih primerih se pogosto uporabijo modeli zaupanja in ugleda, ki zbirajo, ocenjujejo in razpečujejo podatke o zaupanju in ugledu entitet. Ti podatki se lahko nato uporabijo v raznovrstnih odločitvah, kot so denimo s kom stopiti v kupo-prodajno interakcijo, od koga pridobiti podatke in podobno. In čeprav se zavedamo, da imata besedi zaupanje in ugled različen pomen, bomo v tem prispevku uporabljali pojma model zaupanja in model ugleda kot sinonima; razlog je v tem, da sta v znanstveni literaturi pogosto pomešana.

Primerov uporab sistemov za obvladovanje zaupanja in ugleda je precej in posledično se taki sistemi zelo razlikujejo. Z vidika arhitekturnega pristopa poznamo centralizirane in porazdeljene storitve. Primer prvih so ocenjevalni sistemi, s katerimi kupci ocenjujejo prodajalce na centraliziranih elektronskih tržnicah [18, 17], primeri drugih pa porazdeljena okolja P2P (angl. peer-to-peer) za izmenjavo računskih virov [14]. Nadaljnje lahko sisteme za obvladovanje zaupanja in ugleda ločimo glede to, komu so v pomoč: bodisi podpirajo odločanje ljudi bodisi prispevajo vhodne podatke v povsem avtomatizirane procese, kot je denimo usmerjanje omrežnega prometa [9]. A vsi taki sistemi imajo enak cilj, ki je neodvisen od arhitekturnega pristopa ali končnega uporabnika: oceniti stopnjo zaupanja entitet in izboljšati odločanje.

Eden izmed odprtih problem sistemov za obvladovanje zaupanja in ugleda je njihova nezmožnost izmenjave podatkov. Medtem ko entitete prosto prehajajo med različnimi platformami, so njihovi podatki o zaupanju in ugledu vanje tesno zasidrani in dostopni le aplikaciji, ki jih je ustvarila. In čeprav lahko včasih poslovna odločitev povzroči nastanek takšnih podatkovnih silosov (primeri neuspelih poskusov združitve podatkov s platforme Amazon in eBay [19]), lahko velik del zaslug pripišemo tudi pomanjkanju rešitev in standardiziranih pristopov, ki bi takšno izmenjavo omogočali. Denimo, v preglednem prispevku o sistemih zaupanja in ugleda Hendrikx et al. [5] ugotavljajo, da je zmožnost uvoza in izvoza tovrstnih podatkov eden izmed odprtih izzivov.

Celovita rešitev izmenjave podatkov o zaupanju in ugledu bi prinesla trojno korist [4]. Prvič, omogočila bi aplikacijam, da ocenijo stopnjo zaupanja in ugleda z večjo mero natančnosti; tako kot vsak algoritem za podajanje napovedi, tudi sistemi za zaupanje in ugleda delujejo bolje, če imajo na razpolago več podatkov. Drugič, izmenjava podatkov bi omogočila entitetam, da prenašajo pridobljen ugled in zaupanje med različnimi sistemi. Tako entitetam ne bi bilo treba le-teh znova vzpostavljati v vsakem sistemu posebej. In tretjič, izmenjava podatkov bi omogočila hitrejšo rast in razvoj novih sistemov. Tak primer je paradigma Internet Stvari (angl. Internet of Things), v kateri se večje število vsakodnevnih naprav (značke RFID, senzorji, aktuatorji, mobilne naprave) povezuje in omogoča nove primere uporabe. Če želimo, da bodo interakcije med tovrstnimi entitetami uspešne, se bodo morale take *stvari* naučiti medsebojno zaupati in mnogi vidijo rešitev v sistemih za obvladovanje zaupanja in ugleda [12, 23].

2 Funkcionalne zahteve za izmenjavo

Rešitev za izmenjavo informacij o zaupanju in ugledu mora nasloviti štiri vidike: vsebino in strukturo sporočil,

vmesnik storitve, oceno zaupanja podatkov in prevajanje podatkov.

2.1 Določiti vsebino in strukturo sporočil

Prvi vidik zadeva vsebino in strukturo sporočil, ki kodirajo informacije o zaupanju in ugledu. Ob tem je velika raznolikost obstoječih sistemov težavna. Pri tovrstni analizi so pomembni vhodni podatki, iz katerih se izračun zaupanja vrši, in tip podatka, v katerem je izračun zaupanja izražen. Večina sistemov za obvladovanje zaupanja in ugleda vrši izračune na podlagi ocen, ki jih je entiteta pridobila v preteklih interakcijah, in ocen izpeljanih iz mnenj, ki so jih o tej entiteti podale druge entitete [15, 2, 5, 22]. Nekateri modeli še dodatno v izračun vključijo sistemske informacije, kot so struktura družbenega omrežja [20], kateremu entiteta pripada, tip vloge, ki jo entiteta opravlja [6] in podobno. V tem prispevku se bomo omejili le na najpogostejše modele tj. take, ki vršijo izračune na podlagi ocen: bodisi takih iz preteklih informacij bodisi takih, ki so izpeljane iz mnenj.

Podobno se sistemi razlikujejo tudi pri načinih, kako je ocena zaupanja izražena. Nekateri definirajo stopnjo zaupanja kot skalarno vrednost z nekega intervala, denimo število z intervala $[0,1]$, celo število z lestvice med 1 in 10, ali kvalitativna vrednost z urejenostne lestvice. Drugi podatke o zaupanju in ugledu kodirajo kot terko, kjer posamezna komponenta označuje del ocene: denimo sistemi, ki temeljijo na ogrodju subjektivne logike [8] uporabljajo trojico števil (b,d,u), ki označujejo količino prepričanja, dvoma in negotovosti zaporedoma; vsaka od komponent je z intervala $[0,1]$ in njihova skupna vsota znaša 1. Idealna rešitev bi bila taka, ki se jo da aplicirati na čim več obstoječih sistemov.

2.2 Določiti vmesnik storitve

Rešitev mora opredeliti jasen vmesnik storitve in načine za realizacijo. Potrebno je definirati, kako sistemi medsebojno zahtevajo podatke, v kakšnem obsegu ter s kakšno pogostostjo. Prav tako mora rešitev imeti mehanizem za sporočanje napak.

2.3 Določiti zanesljivost izmenjanih informacij

Tretji vidik rešitve zadeva oceno zanesljivosti izmenjanih informacij. Vsak sistem ni enako zaupanja vreden in dobra rešitev mora informacije o tem, kako zaupanja (ne)vredni posamezni sistemi so, pri integraciji upoštevati. V nasprotnem primeru se lahko zgodi, da so izračuni po izmenjavi slabši. Pri tem dodajmo, da večina sistemov za obvladovanje zaupanja že ima osnovne mehanizme za naslavljanje potencialno lažnih informacij, saj gre za temeljno funkcionalnost tovrstnih sistemov.

2.4 Prevesti podatke ob izmenjavi

Zadnji vidik pokriva mehanizme za prevajanje (angl. translation) podatkov med sistemi. Velika raznolikost med obstoječimi modeli zaupanja in ugleda pomeni, da ti operirajo z zelo različnimi tipi podatkov. Te razlike je potrebno pri integraciji upoštevati. Pri tem gre lahko bodisi zgolj za manjša odstopanja kot je denimo drugačen interval, na katerem so vrednosti izražene (denimo uporaba intervala $[0,1]$ ali $[0,100]$) bodisi za večje razlike, kot je denimo sistemska pristranskost (angl. bias) tj. nagnjenost sistema, da uporablja pretirano pozitivne (ali negativne) ocene.

3 Pregled obstoječih rešitev

Znanstvena literatura o pričujoči tematiki je precej skopa; dosedanje delo je večinoma skoncentrirano na razvoj modelov zaupanja in ugleda, integracija sistemov pa je bila zapostavljena. Eden izmed prvih poskusov izmenjave podatkov o zaupanju in ugledu prihaja s strani Trčka [21], ki predlaga definicijo tipov v jeziku XML (XML DTD) za opis vmesnika izmenjave. Predlagani sta dve sporočili, `trustResponse` in `trustRequest`, ki se uporabita za pošiljanje zahtevkov in podajanje odgovorov. Rešitev je dokaj osnovna in specifična za v istem članku predlagan model zaupanja in se ga ne da uporabiti širše. Prav tako rešitev ne vsebuje mehanizmov, s katerimi bi lahko omejili količino izmenjanih podatkov (rešitev implicira, da vsak `trustResponse` vsebuje vse podatke sistema)

V sorodnem delu Kovač in Trček [10] predlagata spletno storitev, ki implementira vmesnik za izmenjavo. Vmesnik omogoča agentom pridobiti oceno stopnje zaupanja drugih agentov kot tudi shranjevanja ocen iz preteklih interakcij. Čeprav se omenjeno delo ne osredotoča na integracijo, kljub temu podaja definicijo vsebine in strukturo sporočil ter vmesnik storitve. A prav tako so definicije prilagojene specifičnemu modelu zaupanja in v rešitvi manjkajo poizvedovalni mehanizmi. Vmesnik storitve in sporočila so definirana s pomočjo sheme XML.

Marienfield et al. [13] predlagajo ontologijo za podajanje ocen. Avtorji podajo strukturo sporočila, ki vsebuje šest komponent, in sicer `about`, ki pove, na katero entiteto se ocena navezuje, `submittedBy`, ki pove, kdo je oceno podal, `creationTime`, ki poda čas oddaje ocene, `hasAspect` govori o kontekstu oz. storitvi, za katero je bila ocena podana, ter komponenti `hasScale` in `hasValue`, s katerima je ocena definirana. Prva komponenta govori o tipu ocene oz. o ocenjevalni lestvici (nominalna, urejenostna, intervalna, razmerostna), druga pa o sami vrednosti. Takšna definicija ocene je precej bolj splošna od prejšnjih, a pokriva zgolj modele, kjer so ocene skalarji; večvrednostnih ocen s tem sporočilom ni mogoče izraziti. Na podoben način so ocene podane tudi v okolju za testiranje modelov zaupanja Alpha Testbed [7], kjer posamezna ocena sestoji iz petih komponent: `source`, `target`, `service`, `date` in `value`, ki zaporedoma označujejo ocenjevalca, ocenjenca, tip storitve, datum ocenjevanja in podano oceno, ki je izražena kot decimalno število z intervala $[0,1]$.

Grinshpoun et al. [4] predlagajo mehanizem za deljenje ugleda v virtualnih skupnostnih, ki so ga poimenovali CCR (angl. cross-community reputation). Delo primarno naslavlja problem določanja zanesljivosti in prevajanja podatkov ob izmenjavi. Delovanje sistema lahko opišemo sledeče: ko sistem A pošlje poizvedbo v sistem B in ko slednji vrne odgovor, se nad izmenjanimi podatki opravi zaporedje transformacij. Najprej se prejeti podatki preslikajo iz domene, ki jo uporablja sistem

Tabela 1: Ocena splošnosti obravnavanih rešitev glede na kriterije iz sekcije 2. Pomen ocen je sledeč: 0 - rešitev ni podana; 1 - rešitev je primerna le za specifične modele; 2 - rešitev je širše uporabna; 3 - rešitev je povsem splošna.

Delo	Sporočila	Vmesnik	Zanesljivost	Prevedba
Trček [21]	1	1	0	0
Kovač in Trček [10]	1	1	0	0
Marienfeld et al. [13]	2	0	0	0
CCR in TRIC [4, 3]	1	1	2	2

B, v domeno, ki jo uporablja sistem A. Zatem se podatki preslikajo glede na kontekst, v katerem so nastali: sprva se preslikajo iz kontekstov, ki jih uporablja sistem B, v univerzalne kontekste, nakar se ocene iz univerzalnih kontekstov preslikajo v kontekste, ki jih uporablja sistem A. Avtorji predpostavljajo, da vse ocene vsebujejo še podatek o zanesljivosti; sama ocena je par vrednost-zanesljivost. Zanesljivost ocene se ob vsaki taki transformaciji zniža glede na obseg spremembe; uporabljena je različica Pinyolovega prevajanja ocen [16].

Gal-Oz et al. [3] podajo implementacijski vidik pristopa CCR imenovan sistem TRIC (angl. Trust and Reputation In virtual Communities). Avtorji zasnujejo centralizirano arhitekturo, v kateri strežnik TRIC igra vlogo posrednika za izmenjavo informacij. Posledično je strežnik TRIC zadolžen za vsa prevajanja in za izvajanje varnostnih politik. V delu avtorji obravnavajo tri vidike izmenjave: kdo jo prične, kdaj se zgodi in kakšen je njen obseg.

Sistema CCR in TRIC sta obetavna poskusa za izmenjavo informacij o zaupanju in ugledu v centraliziranih okoljih kot so denimo spletne tržnice. Žal pa avtorji predpostavljajo vnaprej določeno obliko ocen (par vrednost-zanesljivost) ter obstoj univerzalno določenih kontekstov, kar omejuje splošnost rešitve.

Z vidika funkcionalnih zahtev iz sekcije 2 lahko povzamemo, da Trčkov in Kovačev [21, 10] predlog le delno naslavljata vsebino in strukturo sporočil ter določata vmesnik storitve, Marienfield et al. [13] določa srednje napredno vsebino in strukturo sporočil, predloga CCR in TRIC [4, 3] pa v glavnem naslavljata zanesljivost in prevedbo pri izmenjavi; povzetek primerjav je podan v Tabeli 1. Pri tem poudarjamo, da nobena od obravnavanih rešitev ni v celoti splošna in da problem izmenjave ostaja odprt.

Pri koncu pregleda podajamo še lasten pogled na vsebino in strukturo sporočil ter mehanizme poizvedovanja (definicijo vmesnika). Na izmenjavo med različnimi sistemi zaupanja lahko gledamo tudi kot na integracijo podatkov iz porazdeljenih podatkovnih baz, pri čemer ima vsaka podatkovna baza svoje specifike, kot je struktura ocen. Rešitev se tako ponuja v domeni semantičnih tehnologij, kjer lahko uporabimo tehnologiji Resource Description Framework (RDF) [11] in SPARQL Protocol and RDF Query Language (SPARQL) [1]. Prvo lahko uporabimo za definicijo sporočil oz. ocen, drugo pa za pošiljanje prilagojenih poizvedb. Pri tovrstni rešitvi vsak sistem skrbi za svoj imenski prostor, v katerem definira sporočila in določi atribute, po katerih lahko ostali sistemi poizvedujejo, poizvedbe pa se vršijo preko tehnologije SPARQL

4 Zaključek

V prispevku smo obravnavali izziv izmenjave podatkov, ki jih uporabljajo sistemi za obvladovanje zaupanja in ugleda. Identificirali smo funkcionalne zahteve, ki jih mora rešitev imeti, in skozi njihovo prizmo obravnavali obstoječe rešitve. Ugotovili smo, da obstaja zgolj nekaj parcialnih rešitev in da izziv izmenjave podatkov med sistemi za obvladovanje zaupanja in ugleda ostaja odprt.

Literatura

[1] SPARQL 1.1 overview. W3C recommendation, W3C, March 2013. http://www.w3.org/TR/2013/REC-sparql11-overview-20130321/.

[2] Gennaro Costagliola, Vittorio Fuccella, and Fernando A Pascuccio. Towards a trust, reputation and recommendation meta model. *Journal of Visual Languages & Computing*, 2014.

[3] Nurit Gal-Oz, Tal Grinshpoun, Ehud Gudes, and Ingo Friese. Tric: An infrastructure for trust and reputation across virtual communities. In *Fifth International Conference on Internet and Web Applications and Services (ICIW)*, 2010.

[4] Tal Grinshpoun, Nurit Gal-Oz, Amnon Meisels, and Ehud Gudes. Ccr: A model for sharing reputation knowledge across virtual communities. In *IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technologies*, 2009.

[5] Ferry Hendrikx, Kris Bubendorfer, and Ryan Chard. Reputation systems: A survey and taxonomy. *Journal of Parallel and Distributed Computing*, 2015.

[6] Ramón Hermoso, Holger Billhardt, Roberto Centeno, and Sascha Ossowski. Effective use of organisational abstractions for confidence models. In *Proceedings of the 4th European Workshop on Multi-Agent Systems EUMAS*, 2006.

[7] David Jelenc, Ramón Hermoso, Jordi Sabater-Mir, and Denis Trček. Decision making matters: A better way to evaluate trust models. *Knowledge-Based Systems*, 2013.

[8] Audun Jøsang. *Subjective logic*. Springer, 2016.

[9] Rida Khatoun, Youcef Begriche, Juliette Dromard, Lyes Khoukhi, and Ahmed Serhrouchni. A statistical trust system in wireless mesh networks. *Annals of Telecommunications*, 2016.

[10] Damjan Kovač and Denis Trček. Qualitative trust modeling in soa. *Journal of Systems Architecture*, 2009.

[11] Markus Lanthaler, Richard Cyganiak, and David Wood. RDF 1.1 concepts and abstract syntax. W3C recommendation, W3C, February 2014.

http://www.w3.org/TR/2014/REC-rdf11-concepts-20140225/.

[12] Margaret L Loper and Brian Swenson. Machine to machine trust in smart cities. In *IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, 2017.

[13] Florian Marienfeld, Edzard Höfig, Andrea Horch, Maximilien Kintz, and Jan Finzen. Making sense of ratings: a common quantitative feedback ontology. In *Proceedings of the 7th International Conference on Semantic Systems*, 2011.

[14] Xianfu Meng, Tianjiao Li, and Yu Deng. prefertrust: An ordered preferences-based trust model in peer-to-peer networks. *Journal of Systems and Software*, 2016.

[15] Isaac Pinyol and Jordi Sabater-Mir. Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review*, 2011.

[16] Isaac Pinyol, Jordi Sabater-Mir, and Guifre Cuni. How to talk about reputation using a common ontology: From definition to implementation. In *Ninth Workshop on Trust in Agent Societies*, 2007.

[17] Ansley Post, Vijit Shah, and Alan Mislove. Bazaar: Strengthening user reputations in online marketplaces. In *Proceedings of NSDI'11: 8th USENIX Symposium on Networked Systems Design and Implementation*, 2011.

[18] Kevin Regan, Pascal Poupart, and Robin Cohen. Bayesian reputation modeling in e-marketplaces sensitive to subjectivity, deception and change. In *Proceedings of the National Conference on Artificial Intelligence*, 2006.

[19] Paul Resnick, Ko Kuwabara, Richard Zeckhauser, and Eric Friedman. Reputation systems. *Commun. ACM*, 2000.

[20] Jordi Sabater, Mario Paolucci, and Rosaria Conte. Repage: Reputation and image among limited autonomous partners. *Journal of artificial societies and social simulation*, 9:3, 2006.

[21] Denis Trček. Towards trust management standardization. *Computer Standards & Interfaces*, 2004.

[22] Sokratis Vavilis, Milan Petković, and Nicola Zannone. A reference model for reputation systems. *Decision Support Systems*, 2014.

[23] Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A survey on trust management for internet of things. *Journal of network and computer applications*, 2014.