Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών
Τομέας Επικοινωνιών, Ηλεκτρονικής και
Συστημάτων Πληροφορικής

Κοινωνικός Αποκλεισμός και Επανένταξη Εικονικών Οντοτήτων στο Διαδίκτυο των Πραγμάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΛΕΥΘΕΡΙΟΣ ΚΟΚΟΡΗΣ - ΚΟΓΙΑΣ

Επιβλέπων : Θεοδώρα Βαρβαρίγου
Καθηγήτρια ΕΜΠ

Αθήνα, Ιούνιος 2015

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών
Τομέας Επικοινωνιών, Ηλεκτρονικής και
Συστημάτων Πληροφορικής

Κοινωνικός Αποκλεισμός και Επανένταξη Εικονικών Οντοτήτων στο Διαδίκτυο των Πραγμάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΛΕΥΘΕΡΙΟΣ ΚΟΚΟΡΗΣ - ΚΟΓΙΑΣ

Επιβλέπων : Θεοδώρα Βαρβαρίγου
Καθηγήτρια ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 16η Ιουνίου 2015.

Θεοδώρα Βαρβαρίγου Καθηγήτρια ΕΜΠ	????????????? Αναπ. Καθηγητής Ε.Μ.Π.	ΑΣΔΔΔΔΔ Επίκ. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2015

Ελευθέριος Κόκορης - Κόγιας

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Στον 21ο αιώνα, ο ψηφιακός κόσμος έχει ενσωματωθεί στην καθημερινότητά μας. Έξυπνες συσκευές θα είναι σύντομα σε θέση να αποφασίζουν μόνες τους πώς θα ενεργήσουν ώστε να διευκολύνουν την ζωή μας. Οι δράσεις αυτές θα πρέπει να βασίζονται στην χρήση γνώσης που αποκτήθηκε από παρόμοιες συσκευές που αντιμετώπισαν παρόμοια προβλήματα. Ωστόσο, καθώς αυτές οι συσκευές γίνονται όλο και ποιο αυτόνομες, πιθανές επιθέσεις μπορεί να οδηγήσουν σε προβλήματα όχι μόνο στον ψηφιακό κόσμο αλλά και στον πραγματικό

Ο σκοπός της παρούσας διπλωματικής εργασίας είναι, ο σχεδιασμός και η υλοποίηση ενός decentralized συστήματος για την διαχείριση της εμπιστοσύνης των συσκευών μεταξύ τους στο πλαίσιο του Κοινωνικού Διαδικτύου των Πραγμάτων (ΚΔτΠ) όπως αυτό απεικονίζεται από το project Cosmos .

Οι μέθοδοι διαχείρισης εμπιστοσύνης βασιζόμενη στη φήμη(reputation-based) έχουν χρησιμοποιηθεί με επιτυχία την προηγούμενη δεκαετία κυρίως σε Peer-to-Peer συστήματα. Για το λόγο αυτό, η εργασία αυτή χτίστηκε επάνω σε state-of-the-art αλγορίθμους που χρησιμοποιούνται σε τέτοια συστήματα, με στόχο την περαιτέρω ανάπτυξη και τροποποίηση των ιδεών ώστε να μπορούν να ενσωματωθούν στο πλαίσιο του Διαδικτύου των Πραγμάτων.

Αυτή η μελέτη προσδιορίζει τις πιθανές απειλές που μπορούν να προκύψουν στο ΚΔτΠ. Στην συνέχεια αναλύεται η προτεινόμενη αρχιτεκτονική του συστήματος διαχείρισης εμπιστοσύνης, η οποία είναι χτισμένη σε δύο παρατηρήσεις πάνω στης κοινωνικές αλληλεπιδράσεις των ανθρώπων. Πρώτον, όταν κάποιος θέλει να έχει πρόσβαση σε μια νέα υπηρεσία ζητά προτάσεις από τους φίλους του. Αυτή η διαδικασία χτίζει την φήμη (reputation) κάποιου. Δεύτερον, όταν κάποιος έχει αρκετές αλληλεπιδράσεις με κάποιον άλλο, η φήμη δεν έχει σημασία πια. Εκεί έχει χτιστεί εμπιστοσύνη.

Μετά από κατάλληλη μοντελοποίηση αυτών των εννοιών χρησιμοποιώντας ιδέες από την Θεωρία των Πιθανοτήτων, προσθέσουμε χαρακτηριστικά, όπως η ικανότητα μίας κακόβουλης Εικονική Οντότητα (ΕΟ) να εξιλεωθεί , η γρήγορη αναγνώριση αλλαγών στη συμπεριφορά των ΕΟ από αξιόπιστες σε κακόβουλες και η δυναμική ενσωμάτωση νέων ΕΟ στο σύστημα. Στο τέλος τρέξαμε μια προσομοίωση και παρουσιάζουμε τα αποτελέσματα.

Λέξεις κλειδιά

εμπιστοσύνη, φήμη, ασφάλεια , Διαδίκτυο των πραγμάτων, Εικονική οντότητα, Cosmos, ασφάλεια κατανεμημένων συστημάτων, Κοινωνικό Διαδίκτυο των Πραγμάτων, κλιμάκωση

Abstract

In the 21st century the digital world is incorporated on everyday life. Smart devices will soon be able to decide on their own of actions needed to be taken in order to facilitate our lives. These actions will be based on acquiring knowledge from similar devices that have encountered similar problems. However, as these devices are becoming autonomous, potential attacks can result in problems not only in the digital world but also in the physical one.

The purpose of this thesis is the design and implementation of a decentralized system for Trust Management in the context of the Social Internet of Things as seen by the Cosmos project.

Reputation-based trust management methods have been successfully used in the past decade mostly on Peer-to-Peer systems. For this reason, this study is built upon state-of-the-art algorithms used on such systems, with the aim of further developing the ideas proposed and modifying them to fit the context of the Internet of Things.

This study identifies the potential threats that can emerge in SIoT. After that the proposed architecture is analyzed. It is built upon two observations of the social interactions of humans. Firstly, when someone wants to access a new service he asks for referrals from his friends. This feedback is called Reputation. Secondly, when someone has enough interactions with someone else, the reputation does not matter any more. There has been built Trust.

After appropriately modeling these notions using Probability Theory we add features like the ability of a malicious Virtual Entity (VE) to get redemption, the quick identification of behavioural changes of VE's from trustworthy to malicious and the dynamic integration of new VE's in the system. In the end we run a simulation and present the results.

Key words

Internet of Things, trust, reputation, scalability, security, Cosmos, Social Internet of Things, Distributed Systems security

Ευχαριστίες

==========

TODO

==========

Ελευθέριος Κόκορης - Κόγιας,

Αθήνα, 16η Ιουνίου 2015

Περιεχόμενα

Κατάλογος σχημάτων

Κατάλογος πινάκων

Κεφάλαιο 1

Εισαγωγή

Όταν το 1969 γεννήθηκε το ARPANET η ιδέα που το ώθησε ήταν η κοινή χρήση υπολογιστικών πόρων από απομακρυσμένες περιοχές. Δηλαδή εάν σε κάποιο ερευνητικό κέντρο χρειαζόταν να γίνουν πολλοί υπολογισμοί, να μπορούσαν να γίνουν σε κάποιο εξειδικευμένο υπολογιστικό σύστημα που ήταν γεωγραφικά απομακρυσμένο από το ερευνητικό κέντρο.

Η ιδέα αυτή ποτέ δεν δούλεψε πραγματικά - για αρχή, όλοι οι υπολογιστές είχαν διαφορετικά λειτουργικά συστήματα και προγράμματα, ενώ η χρήση του μηχανήματος κάποιου άλλου ήταν πολύ δύσκολή. Επίσης μέχρι να υλοποιηθεί το ARPANET η τεχνολογία είχε φτάσει στο σημείο να μην το έχει ανάγκη αφού είχαν εμφανιστεί οι πρώτοι προσωπικοί υπολογιστές και ο καταμερισμός χρόνου σε υπολογιστικά συστήματα δεν πρόσφερε ποία τόσα οφέλη.

Έτσι είναι λογικό να πούμε ότι το ARPANET απέτυχε στο σκοπό του, αλλά στη διαδικασία αυτή έκανε μερικές σημαντικές ανακαλύψεις που είχαν ως αποτέλεσμα τη δημιουργία των τεχνολογιών του πρώτου Διαδικτύου. Σε αυτές περιλαμβάνονταν το e-mail, η μεταγωγή πακέτων εφαρμογών, και φυσικά η ανάπτυξη του Transport Control Protocol - Internet Protocol - Internet Protocol ή TCP / IP.

Στην συνέχεια και λόγω της ραγδαίας εξάπλωσης των προσωπικών υπολογιστών το Internet έγινε ή ποίο μεγάλη απόδειξη της ισχύς του νόμου του Metclafe κατά τον οποίο:

> ”Η αξία ενός δικτύου είναι ανάλογη με το τετράγωνο του αριθμού των κόμβων, δηλαδή του αριθμού των χρηστών του δικτύου.”

Σήμερα, το Διαδίκτυο με πάνω από 3 δισεκατομμύρια χρήστες είναι το βασικότερο μέσο εύρεσης και ανταλλαγής δεδομένων της ανθρωπότητας Ένας πολίτης του 21ου αιώνα δεν χρειάζεται να γνωρίζει κάθε μικρή πληροφορία, το μόνο που χρειάζεται να ξέρει είναι σε ποίο σημείο του διαδικτύου μπορεί να την βρει.

Έτσι τώρα, βρισκόμαστε σε μία μεταβατική περίοδο. Το Διαδίκτυο είναι ευρέως αποδεκτό και αναγκαίο, αλλά η έμφυτη ανθρώπινη περιέργεια καθώς και η δημιουργικότητα μας οδηγούν στο επόμενο βήμα. Στο Διαδίκτυο των Πραγμάτων.

Ποία είναι όμως η διάφορα του Διαδικτύου από το Διαδίκτυο των Πραγμάτων;

Τα λεγόμενα του Kevin Ashton, συνιδρυτή και εκτελεστικού διευθυντή του Auto-ID Center στο MIT είναι ξεκάθαρα:

> ”Σήμερα οι υπολογιστές - και, ως εκ τούτου, το Διαδίκτυο - εξαρτώνται σχεδόν εξ ολοκλήρου από τα ανθρώπινα όντα για πληροφορίες. Σχεδόν το σύνολο των περίπου 50 petabytes δεδομένων διαθέσιμων στο Διαδίκτυο, συλλαμβάνεται και δημιουργείται από τον άνθρωπο με την πληκτρολόγηση, το πάτημα ενός κουμπιού εγγραφής, την λήψη μιας ψηφιακής φωτογραφίας ή την σάρωση ενός barcode.
>
> Το πρόβλημα είναι πώς, οι άνθρωποι έχουν περιορισμένο χρόνο, προσοχή και ακρίβεια. Γιαυτό και δεν είναι πολύ καλοί στο καταγραφή των δεδομένων που αφορούν τα πράγματα του γύρω κόσμου. Αν είχαμε υπολογιστές που ήξεραν οτιδήποτε μπορούσαν να ξέρουν για τα πράγματα γύρω τους - με τη χρήση δεδομένων που συνέλεξαν αυτόνομα χωρίς καμία βοήθεια από εμάς - τότε θα ήταν σε θέση να παρακολουθούν και να μετράνε τα πάντα. Έτσι θα μειωνόντουσαν σε μεγάλο βαθμό η σπατάλη αγαθών, οι απώλειες από λάθη και το γενικότερο κόστος. Θα γνωρίζαμε από το πότε τα πράγματα θα χρειάζονται αντικατάσταση ή επισκευή έως και το αν ήταν φρέσκα ή όχι.”

1.1 Κοινωνικό Διαδίκτυο των Πραγμάτων και Προβλήματα Εμπιστοσύνης

Η Διπλωματική αυτή εργασία γεννήθηκε για να αντιμετωπισθούν ανησυχίες σχετικά με τις δράσεις των Εικονικών Οντοτήτων(Virtual Entities), οι οποίες αποτελούν την αναπαράσταση των πραγμάτων στον ψηφιακό κόσμο. Όταν λοιπόν σε αυτές τις Εικονικές Οντότητες προσθέσουμε την δυνατότητα να έχουν κοινωνικούς δεσμούς μέσο φιλίας, μέσο οικογένειας(ανήκουν στον ίδιο χρήστη) ή και μέσο ομοιότητας (έχουν τον ίδιο ρόλο στο σύστημα), τότε βρισκόμαστε στο Κοινωνικό Διαδίκτυο των Πραγμάτων [1]. Ειδικότερα αυτή η εργασία έγινε στα πλαίσια του COSMOS(Cultivate resilient smart Objects for Sustainable city applicatiOn) [2], σκοπός του οποίου είναι η δημιουργία έξυπνων αντικειμένων, προκειμένου να καταστεί δυνατή μια έξυπνη πόλη. Στο COSMOS

- Τα πράγματα θα είναι σε θέση να μάθουν βασιζόμενα σε εμπειρίες άλλον,
- ενώ μέσα από την απόκτηση και την ανάλυση της γνώσης τα πράγματα θα γνωρίζουν τις συνθήκες και τα γεγονότα που συμβαίνουν και ανάλογα θα μεταβάλουν τη συμπεριφορά τους.
- Οι διαχειριστικές αποφάσεις θα λαμβάνονται σε πραγματικό χρόνο για κάθε Εικονική Οντότητα βασιζόμενες στην ασφάλεια των πραγμάτων, την γεωγραφική τους θέση, τις σχέσεις που έχουν με άλλες εικονικές οντότητες καθώς και άλλες ψηφιακές πληροφορίες που θα εξάγονται από
- Complex Event Processing και άλλες τεχνολογίες Κοινωνικών Μέσων ώστε να εντοπίζεται η χρήσιμη πληροφορία μεσα στον τεράστιο αριθμό δεδομένων (Big Data)

[1] www.social-iot.org/
[2] www.iot-cosmos.eu/

Στα πλαίσια λοιπόν του COSMOS υπήρξε η ανάγκη να υπάρχει γνώση για το πόσο έμπιστος μπορεί να θεωρηθεί ένα πάροχος πληροφοριών ή/και υπηρεσιών. Με αυτή τη γνώση θα ήταν δυνατό:

- Να εντοπίζεται γρήγορα η πιο αξιόπιστη πηγή πληροφοριών και να μειώνεται η επικοινωνία με ταυτόχρονη βελτιστοποίηση της απόδοσης
- Να μπορεί μία Εικονική Οντότητα να κρίνει αυτόνομα πόσο πιθανό είναι να ικανοποιηθεί από μία προσφερόμενη υπηρεσία πριν προβεί στην δοσοληψία επειδή
  - μπορεί κάποια υπηρεσία να είναι προϊόν
  - μπορεί να μας δοθεί γνώση που θα ρισκάρει την ασφάλεια του συστήματος ή/και των τελικών χρηστών

1.2 Δομή της Διπλωματική Εργασίας

Η διπλωματική εργασία δομείται ως εξής:

Chapter 2
Σε αυτό το κεφάλαιο γίνεται μία εισαγωγή στη βασικές ιδέες που χαρακτηρίζουν γενικά τα συστήματα εμπιστοσύνης - φήμης. Στην συνέχεια αναλύονται οι βασικές αρχιτεκτονικές τους καθώς και οι διάφοροι τρόποι εξαγωγής των δεικτών φήμης και εμπιστοσύνης. Τέλος παρουσιάζονται βασικά συστήματα φήμης και εμπιστοσύνης που χρησιμοποιούνται σε διάφορους τομείς της υπολογιστικής επιστήμης.

Chapter ??
Vulneralibilities and attack-models We describe the tracing concepts we employed in BlkKin so that we can achieve the needed expressiveness. We so present Zipkin, which is an open-source implementation of these tracing concepts and another BlkKin's building block.

Chapter ??
DESIGN + USE CASE SCENARIOS We describe the BlkKin's design and architecture, the communication protocols used and the tracing information flow.

Chapter ??
IMPLEMENTATION WSN TOOLKIT We analyze the process of creating BlkKin, our contributions to the tracing infrastructure and the means used or created to extract the information needed in order to serve the different roles that BlkKin can play.

Chapter ??
EVALUATION We cite our experience of using BlkKin in Archipelago and RADOS instrumentation and its use as a debugging and an alerting mechanism.

Chapter ??
CONCULSION-FUTURE WORK We provide some concluding remarks and give some future work that could be done to improve and evolve BlkKin.

Κεφάλαιο 2

Θεωρητικό και Τεχνολογικό Υπόβαθρο

2.1 Ορισμοί Εννοιών

Τα συστήματα εμπιστοσύνης και φήμης αποτελούν μία εξέλιξη της τελευταίας δεκαπενταετίας και χρησιμοποιούνται ευρέως σε διαδικτυακές αλληλεπιδράσεις μεταξύ τόσο ανθρώπων (e-bay, amazon) όσων και μηχανών (ευφυών δραστών, peer-to-peer συστημάτων κτλ.). Η ιδέα πάνω στην οποία βασίζονται είναι: η συλλογή κριτικής για έναν δράστη από άλλα μέλη της κοινότητας τα οποία έχουν ήδη αποκτήσει κάποιες εμπειρίες με τον πρώτο. Με αυτόν τον τρόπο υπάρχει η δυνατότητα να γνωρίζει κάποιος για ”το ποιόν” κάποιου άλλου χωρίς να χρειάζεται να τον γνωρίσει, δηλαδή να αλληλεπιδράσει με αυτόν. Αυτή η δυνατότητα με την σειρά της ”εξαναγκάζει” του δράστες ενός συστήματος να συμμορφωθούν με τους κανόνες της δικτυακή κοινότητας της οποίας είναι μέλη.

Όταν η αίτηση για παροχή υπηρεσιών ή για απόκτηση δεδομένων γίνεται online μεταξύ οντοτήτων πρότερα αγνώστων μεταξύ τους τότε μπορούν να προκύψουν 2 βασικά προβλήματα.

1. Το πρώτο πρόβλημα που δεν εξετάζεται στην παρούσα εργασία είναι πώς τα δεδομένα που παρέχονται (και στην περίπτωση του COSMOS η γνώση) μπορεί να χρησιμοποιηθούν από τον παραλήπτη για διαφορετικούς σκοπούς από αυτούς που ισχυρίζεται. Έτσι να τον βοηθήσουμε άθελα μας στου κακόβουλους ή γενικότερα αντίθετους από το καλό της κοινότητας σκοπούς.
2. Αντίθετα αυτή η εργασία εστιάζει στο πρόβλημα του ρίσκου πού παίρνει ένας χρήστης όταν ζητάει μία υπηρεσία, επειδή μπορεί τελικά να μην την λάβει σε ικανοποιητικό βαθμό οπότε να πρέπει να την ξαναζητήσει. Ακόμα είναι δυνατόν να κινδυνέψει η ασφάλεια του (αντί για σωστό αρχείο να σταλεί κάτι που περιέχει ένα Trojan), ενώ στην δική μας περίπτωση μπορεί η γνώση και εν συνεχεία οι δράσεις που προτείνονται να προκαλέσουν προβλήματα ασφαλείας όχι μόνο στον ψηφιακό κόσμο των Εικονικών Οντοτήτων, όσο και στο φυσικό κόσμο των πραγμάτων και των ανθρώπων.

2.1.1 Soft Security

Ως ασφάλεια στην πιο γενική της έννοια μπορούμε να ορίσουμε ”την κατάσταση στην οποία κάποιος ή κάτι βρίσκεται μακριά από οποιονδήποτε κίνδυνο και οποιαδήποτε προσπάθεια αλλοίωσης αυτής της κατάστασης θα αποτύχει” (ή και να πετύχει θα είναι δυνατή η επαναφορά στην αρχική κατάσταση χωρίς κόστος). Αυτός ο ορισμός είναι πολύ γενικός και περιλαμβάνει την ασφάλεια ανθρώπων την ασφάλεια περιουσιών ακόμα και την ασφάλεια υγείας.

Στην επιστήμη των υπολογιστών η βασικότερη κατηγορία ασφάλειας είναι η ασφάλεια που παρέχει ως υπηρεσία τον αποκλεισμό δραστών εξωτερικών του συστήματος από την απόκτηση πρόσβασης σε προστατευόμενες πληροφορίες ή πόρους. Αυτό το είδος ”hard security” παρέχεται μέσα από την πιστοποίηση και τον έλεγχο πρόσβασης(access control) στα υπολογιστικά συστήματα καθώς και μέσα από την κρυπτογραφία στα κανάλια επικοινωνίας κατά την ανταλλαγή εμπιστευτικών πληροφοριών. Όμως το πρόβλημα μπορεί να αντιστραφεί και τότε όλες αυτές οι μέθοδοι είναι αναξιόπιστες. Αυτό θα συμβεί στην περίπτωση που η επίθεση γίνει εντός του συστήματος. Μία τέτοια επίθεση συμβαίνει όταν κάποιος δράστης ή γενικότερα κομμάτι του συστήματος, που έχει δικαίωμα να ενεργεί στο σύστημα, γίνει κακόβουλο ή ελαττωματικό.

Αυτά τα προβλήματα λύνονται μέσα από εφαρμογές του ”Soft Security” το οποίο είναι

Ορισμός 1 (Soft Security) 1: *Η συνεργασία των δραστών ενός συστήματος ώστε να αποκλείσουν μη κοινωνικά αποδεχτές συμπεριφορές.*

Με αυτόν τον τρόπο μπορεί να προστατευθεί η κοινότητα από κακόβουλους δράστες οι οποίοι όμως έχουν κάθε δικαίωμα να ενεργούν. Ουσιαστικά να εφαρμοστεί ένα είδος κοινωνικού αποκλεισμού. Ένας από τους βασικότερους μηχανισμούς για την επίτευξή αυτού του είδους ασφαλείας είναι με την χρήση των εννοιών της εμπιστοσύνης και της φήμης. [1]

2.1.2 Η Έννοια της Εμπιστοσύνης

Στον κόσμο των ανθρώπινων οντοτήτων η ύπαρξη της έννοιας τις εμπιστοσύνης είναι εμφανής στις καθημερινές μας αλληλεπιδράσεις. Θα μιλήσουμε για τα προβλήματα μας και της εμπειρίες μας - δηλαδή θα δώσουμε ευαίσθητες προσωπικές πληροφορίες- στους φίλους μας οι οποίοι περιμένουμε να μας βοηθήσουνε με δικές τους εμπειρίες, καθώς και να βοηθηθούν από τις πληροφορίες μας. Επίσης θα πάμε να αγοράσουμε προϊόντα από μαγαζιά που γνωρίζουμε και έχουμε ξαναπάει επειδή πιστεύουμε πως η ποιότητα ου προϊόντος ή της υπηρεσίας που θα λάβουμε θα είναι ικανοποιητική για εμάς.

Στον κόσμο όμως της υπολογιστικής επιστήμης ο ορισμός και η μοντελοποίηση της εμπιστοσύνης είναι αρκετά δύσκολη. Αυτό συμβαίνει επειδή τις ανθρώπινες σχέσεις τις κυβερνούνε συναισθήματα όπως αγάπη και αφοσίωση που δεν έχουν καμία θέση στον ψηφιακό κόσμο. Στο έργο του Audun Jøsang υπάρχει μία εξαιρετική συγκέντρωση για τους διαφόρους ορισμούς της εμπιστοσύνης και τις φήμης. Εκεί λοιπόν αναφέρεται πώς υπάρχουν δύο βασικοί ορισμοί για την εμπιστοσύνη τους οποίους ονομάζουμε εμπιστοσύνη αξιοπιστίας (reliability trust) και εμπιστοσύνη απόφασης (decision trust)

Όπως προϊδεάζει και το όνομα η εμπιστοσύνη αξιοπιστίας μπορεί να ερμηνευθεί ως η αξιοπιστία κάποιου δράστη ή αντικειμένου, και ο ορισμός του Gambettaπαρέχει ένα παράδειγμα του πώς μπορεί να διατυπωθεί:

Ορισμός 2 (Εμπιστοσύνη Αξιοπιστίας) 1: *Εμπιστοσύνη είναι η υποκειμενική πιθανότητα από την οποία ένα άτομο, A, περιμένει από ένα άλλο άτομο, B, να κάνει μία συγκεκριμένη ενέργεια από την οποία εξαρτάται η ευημερία του.*

Αυτός ορισμός περιεχέι την έννοια της εξάρτησης του A από τον B, και την αξιοπιστία (δηλαδή την πιθανότητα) του B όπως την αντιλαμβάνεται ο A.

[1] Φυσικά και η έννοια της εμπιστοσύνης είναι χρήσιμη και για το ”hard security” (εμπιστοσύνη σε ένα πιστοποιητικό ή μία Certificate Authority που το υπογράφει), αλλά ουσιαστικά αυτό είναι μία εφαρμογή ”Soft Security” της ανθρώπινης κοινωνίας που χρησιμεύει στο hard security της υπολογιστικής επιστήμης.

Όμως η εμπιστοσύνη μπορεί να είναι πολύ πιο σύνθετη από τον παραπάνω ορισμό. Αυτό συμβαίνει επειδή το γεγονός ότι η αξιοπιστία ενός δράστη είναι υψηλή δεν οδηγεί στην τυφλή εμπιστοσύνη του για οποιαδήποτε ενέργεια. Το ρίσκο τις αποτυχίας μίας συγκεκριμένη συναλλαγής μπορεί να είναι πολύ μεγάλο. Δηλαδή με απλά λόγια, ένας δράστης μπορεί να θεωρηθεί αξιόπιστος για μία απλή συναλλαγή, όμως για κάποια πιο κρίσιμη η αξιοπιστία του να μην είναι αρκετά καθησυχαστική. Για να συμπεριλάβουμε λοιπόν την πιο ευρεία έννοια που μπορεί να χαρακτηριστεί ως εμπιστοσύνη, μπορεί να χρησιμοποιηθεί ο ακόλουθος ορισμός των McKnight & Chervany

Ορισμός 3 (Εμπιστοσύνη Απόφασης) 1: *Η εμπιστοσύνη είναι ο βαθμός στον οποίο ένα άτομο είναι πρόθυμο να εξαρτηθεί από κάτι ή κάποιον σε μια δεδομένη κατάσταση με ένα αίσθημα σχετικής ασφάλειας, ακόμη και αν οι αρνητικές συνέπειες είναι δυνατές.*

Ο γενικότερος αυτός ορισμός μας παρέχει μία χρήσιμη ασάφεια αφού περιλαμβάνει πτυχές μίας ευρύτερης έννοιας της εμπιστοσύνης, η οποία περιέχει της έννοιες της εξάρτησης από αυτόν που απολαμβάνει την εμπιστοσύνη, της αξιοπιστίας αυτού καθώς και της ύπαρξης ενός παράγοντα κινδύνου που πρέπει να αποδεχτεί το άτομο που καλείτε να εμπιστευτεί κάποιο άλλο άτομο, ανάλογο με την εκάστοτε συναλλαγή.

2.1.3 Η Έννοια της Φήμης

Γυρίζοντας πίσω στον κόσμο τον ανθρώπων μπορούμε εύκολα να εντοπίσουμε άλλη μία έννοια η οποία χαρακτηρίζει εάν μεγάλο αριθμό ενεργειών και αποφάσεων μας. Αυτή η έννοια είναι η φήμη. Όταν για παράδειγμα θέλει ένα άτομο να αποκτήσει πρόσβαση σε μία υπηρεσία καινούργια (δηλαδή που δεν την έχει ξαναχρησιμοποιήσει), όπως για παράδειγμα να πάει σε ένα φροντιστήριο το παιδί του να μάθει μία ξένη γλώσσα ή να βρει έναν καλό μηχανικό για να του χτίσει το σπίτι του. Τότε ένα από τους βασικούς παράγοντες της επιλογής θα είναι η φήμη. Δηλαδή θα συλλέξει πληροφορίες από τον κοινωνικό του περίγυρο και αφού τις σταθμίσει ανάλογα με την εμπιστοσύνη του στης πηγές προέλευσής τους θα εξάγει την φήμη του πιθανού παρόχου της υπηρεσίας.

Στην Υπολογιστική Επιστήμη μοντελοποιούμε την φήμη με ακριβώς τον ίδιο τρόπο. Έτσι μπορούμε να ορίσουμε την φήμη ως:

Ορισμός 4 (Φήμη) 1: *Φήμη είναι το τι λέγεται ή πιστεύεται δημόσια για το ποιόν ή τον χαρακτήρα κάποιου ατόμου ή αντικειμένου*

Παρ'όλη την στενή συγγένεια των εννοιών της φήμης και της εμπιστοσύνης έχουν μία θεμελιώδη διαφορά. Η φήμη βασίζεται στην εμπειρία του κοινωνικού συνόλου με ένα άτομο ενώ η εμπιστοσύνη είναι προσωπικό ζήτημα και δεν επηρεάζεται από το κοινωνικό σύνολο. Μπορούμε να δούμε ξεκάθαρα την διαφορά τους στης παρακάτω προτάσεις:

1. "Θα εμπιστευτώ τον Χ επειδή έχει καλή Φήμη"
2. "Θα εμπιστευτώ τον Υ παρόλο που έχει κακή φήμη, επειδή μαζί μου είναι καλός"

Οι παραπάνω φράσεις δείχνουν ξεκάθαρα πώς εάν και η υπηρεσία που τα δυο άτομα θέλουν αιτηθούν είναι η ίδια, το άτομο 1, που δεν έχει αλληλεπιδράσει ποτέ με τον Υ, θα προτιμήσει τον Χ εμπιστευόμενος το κοινωνικό σύνολο από όπου εξήγε την καλή φήμη του Χ. Αντίθετα το άτομο 2 ένα και ξέρει πως ο Χ έχει καλύτερη φήμη από τον Υ θα διαλέξει τον Υ επειδή έχει καλή προϊστορία μαζί του, ουσιαστικά επειδή τον εμπιστεύεται. Αυτή η παρατήρηση δείχνει πώς η υποκειμενική γνώμη ενός ατόμου για ένα άλλο έχει μεγαλύτερο βάρος από την γνώμη του κοινωνικού σύνολου και έτσι στο τέλος η εμπιστοσύνη σε ένα άτομο θα υπερισχύσει της φήμης του.

2.2 Αρχιτεκτονικές Δικτύωσης Συστημάτων Εμπιστοσύνης

Όπως αναφέραμε οι κλασσικοί τρόποι που έχει η κοινωνία για την εξαγωγή φήμης και εμπιστοσύνης απουσιάζουν από τα online συστήματα που κατασκευάζουμε. Για αυτό τον λόγο χρειαζόμαστε ηλεκτρονικά υποκατάστατα. Οι βασικότερες ιδιότητες που πρέπει να έχει ένα ένα σύστημα βασιζόμενο στην φήμη είνα:

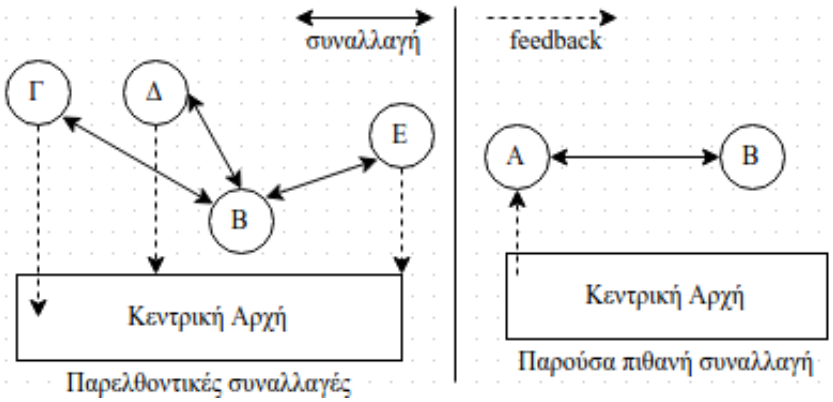
1. Οι οντότητες πρέπει να είναι μακρόβιες έτσι ώστε μετά από μία συναλλαγή να υπάρχει πιθανότητα μία μελλοντικής επαφής με την ίδια οντότητα
2. Οι συναλλαγές να αποτιμώνται και οι βαθμολογίες να διανέμονται σε άλλα μέλη τις κοινότητας
3. Οι αποφάσεις για της συναλλαγές μίας οντότητας να επηρεάζονται από τις βαθμολογίες των παλιών συναλλαγών

Οι τεχνικές αρχές για τα συστήματα φήμης περιγράφονται στο παρών και το ακόλουθο τμήμα. Η αρχιτεκτονική του δικτύου καθορίζει πώς οι αξιολογήσεις των συναλλαγών αξιοποιούνται και διανέμονται ανάμεσα στα μέλη των συστημάτων. Οι δύο κύριοι τύποι είναι οι συγκεντρωτικές και οι κατανεμημένες αρχιτεκτονικές.

2.2.1 Συγκεντρωτικές Αρχιτεκτονικές

Στις συγκεντρωτικές αρχιτεκτονικές, οι πληροφορίες για την επίδοση ενός μέλους συγκεντρώνονται από τις βαθμολογίες των άλλων μελών της κοινότητας οι οποίοι είχαν άμεση εμπειρία με τον πρώτο. Η κεντρική αρχή η οποία συγκεντρώνει τις βαθμολογίες εξάγει τελικά την δείκτη της φήμης του κάθε μέλους της κοινότητας τον οποίο μπορεί να δει όποιος ενδιαφέρεται. Τα άλλα μέλη με την σειρά του χρησιμοποιούν αυτούς τους δείκτες όταν θέλουν να αλληλεπιδράσουν με άγνωστα, για αυτούς, μέλη της κοινότητας και θέλουν να αποφασίσουν εάν θα προβούν σε κάποια συναλλαγή ή όχι. Η ουσία είναι πώς συναλλαγές με άτομα που έχουνε υψηλότερο δείκτη φήμης έχουν πιο πολλές πιθανότητες να είναι επιτυχημένες από συναλλαγές με άτομα χαμηλού δείκτη φήμης.

Στο Σχ.2.1 παρακάτω φαίνεται μία τυπική αρχιτεκτονική με κεντρική αρχή.



Σχήμα 2.1: Συγκεντρωτική Αρχιτεκτονική

Ο Α θέλει να προβεί σε μία συναλλαγή με τον Β, ενώ δεν έχει κάποια παρελθοντική εμπειρία με αυτόν. Για αυτό ρωτάει την κεντρική αρχή, η οποία με την σειρά της γυρίζει τον δείκτη φήμης που έχει υπολογίσει βασιζόμενη σε πληροφορίες από άλλα μέλη τις κοινότητας όταν αυτά αλληλεπίδρασαν με τον Β και κοινοποίησαν στην κεντρική αρχή την εμπειρία τους.

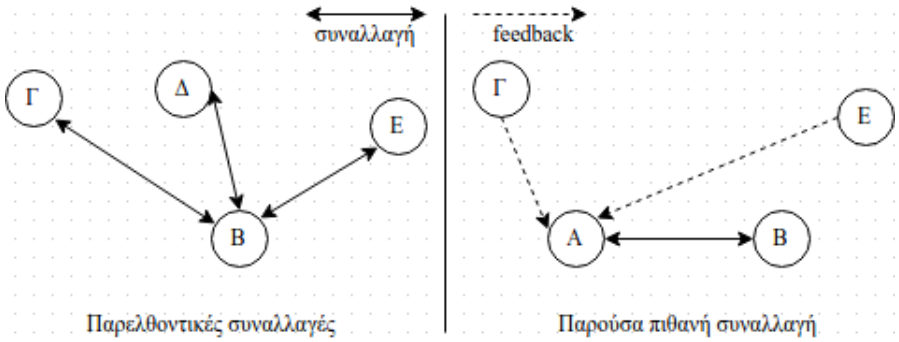
Τα δύο βασικά κομμάτια των συγκεντρωτικών συστημάτων φήμης είναι:

1. Τα συγκεντρωτικά πρωτόκολλα επικοινωνίας που επιτρέπουν στους συμμετέχοντες να παρέχουν αξιολογήσεις για τα μέλη των συναλλαγών στην κεντρική αρχή, καθώς και να αποκτήσουν έναν δείκτη φήμης των πιθανών εταίρων στην συναλλαγή από την κεντρική εξουσία.

2. Έναν τρόπο υπολογισμού φήμης που χρησιμοποιείται από την κεντρική αρχή να εξάγει δείκτες φήμη για κάθε μέλος, με βάση τις αξιολογήσεις που έλαβε, και ενδεχομένως άλλες πληροφορίες όπως θα δούμε στην παράγραφο 2.3 παρακάτω.

2.2.2 Κατανεμημένες Αρχιτεκτονικές

Υπάρχουν περιβάλλοντα όπου ένα κατανεμημένο σύστημα φήμης, δηλαδή χωρίς τις κεντρικές λειτουργίες, είναι καταλληλότερο από ένα συγκεντρωτικό σύστημα. Σε ένα κατανεμημένο σύστημα, δεν υπάρχει κεντρικό σημείο για την υποβολή των αξιολογήσεων ή την απόκτηση δεικτών φήμης των άλλων. Αντ'αυτού, μπορεί να υπάρχουν κατανεμημένα σημεία αποθήκευσης όπου μπορούν να υποβληθούν αξιολογήσεις ή ο κάθε συμμετέχοντας απλά να καταγράφει τη γνώμη του σχετικά με τις εμπειρίες του με άλλα μέλη της κοινότητας, και να παρέχει ο ίδιο τις πληροφορίες αυτές, κατόπιν αιτήματος. Ένας τρίτος συμβαλλόμενος, ο οποίος ενδιαφέρεται να συναλλαχθεί με δεδομένο άλλο μέλος της κοινότητας, πρέπει να βρει τις κατανεμημένες αποθήκες, ή να προσπαθήσει να αποκτήσει βαθμολογίες από όσα μέλη της κοινότητας μπορεί τα οποία είχαν άμεση εμπειρία με το εν λόγω μέλος-στόχο. Αυτό απεικονίζεται στο Σχ.2.2 παρακάτω.



Σχήμα 2.2: Κατανεμημένη Αρχιτεκτονική

Ο τρίτος συμβαλλόμενος (στο Σχ.2.2 ο Α) υπολογίζει μόνος του των δείκτη της φήμης του μέλους στόχου (Β) βασιζόμενος στην μερική ή ολική γνώση που συνέλεξες από ένα τους "γνωστούς" του. (εδώ έχει μερική γνώση επειδή δεν πήρε feedback από τον Δ).

Τα δύο βασικά κομμάτια των κατανεμημένων συστημάτων φήμης είναι:

1. Τα κατανεμημένα πρωτόκολλα επικοινωνίας που επιτρέπουν στους συμμετέχοντες να λάβουν και να στείλουν βαθμολογίες για άλλα μέλη της κοινότητας

2. Έναν τρόπο υπολογισμού φήμης που χρησιμοποιείται από κάθε μέλος της κοινότητας για να εξάγει δείκτες φήμης με βάση τις αξιολογήσεις που έλαβε, και ενδεχομένως άλλες πληροφορίες όπως θα δούμε στην παράγραφο 2.3 παρακάτω.

2.3 Τρόποι υπολογισμοί φήμης και εμπιστοσύνης

2.3.1 Bayesian

Τα Bayesian συστήματα λαμβάνουν δυαδικές αξιολογήσεις ως είσοδο (δηλαδή θετική ή αρνητική τιμή), και βασίζονται στον υπολογισμό των δεικτών με χρήση των *βήτα συναρτήσεων πυκνότητας πιθανότητας* (ΣΠΠ). Ο ενημερωμένος δείκτης υπολογίζεται συνδυάζοντας τις προηγούμενες τιμές των δεικτών φήμης με τη νέα βαθμολόγια.Ο δείκτης της φήμης ή/και της εμπιστοσύνης μπορεί να αναπαρασταθεί είτε με τη μορφή μιας πλειάδας παραμέτρων βήτα μορφής *(α, β)* (όπου *α* και *β* αντιπροσωπεύουν τον αριθμό των θετικών και αρνητικών αξιολογήσεων, αντίστοιχα), είτε με τη μορφή της τιμής της προσδοκία της βήτα ΣΠΠ. Προαιρετικά μπορεί να υπάρχει και ή διακύμανση. Το πλεονέκτημα των Bayesian συστημάτων είναι ότι παρέχουν μία θεωρητικά ορθή βάση για τον υπολογισμό των δεικτών, ενώ το μόνο μειονέκτημα που θα μπορούσε να καταλογιστεί είναι ότι είναι υπερβολικά πολύπλοκα για να τα κατανοήσει ο μέσος άνθρωπος.

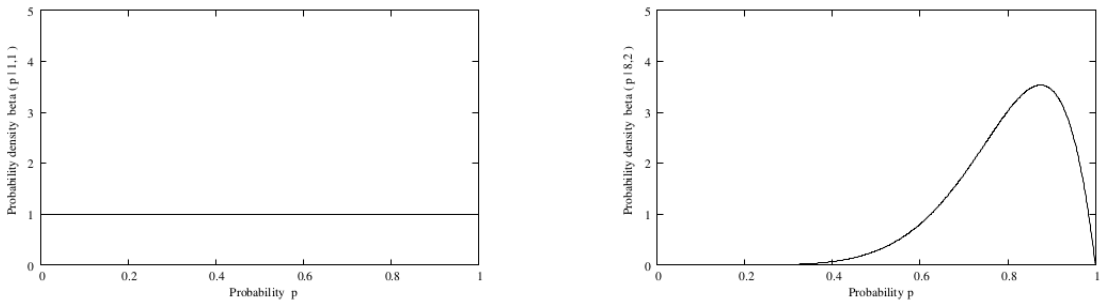
Η βήτα οικογένεια κατανομών είναι μια συνεχής οικογένεια συναρτήσεων κατανομής μεταβαλλόμενη από τις δύο παραμέτρους α και β. Η βήτα ΣΣΠ συμβολίζεται με beta(p | α, β) μπορεί να εκφραστεί χρησιμοποιώντας τη συνάρτηση γάμμα Γ ως εξής:

$$beta(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\,\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \; o\pi ou \;\; 0 \le p \le 1,\; \alpha,\; \beta \;>\; 0 \tag{2.1}$$

με τον περιορισμό ότι η πιθανότητα $p \neq 0 \;\; \alpha\nu\, \alpha \;<\; 1$, και $p \neq 1 \;\; \alpha\nu\, \beta \;<\; 1$. Η τιμή της προσδοκίας της κατανομής beta δίνεται από:

$$E(p) = \frac{\alpha}{(\alpha+\beta)} \tag{2.2}$$

Στην αρχική κατάσταση όπου δεν είναι τίποτα γνωστό η εκ των προτέρων ΣΠΠ είναι η ομοιόμορφη κατανομή βήτα κατανομή όπου $\alpha = 1,\; \beta = 1$ η οποία φαίνεται στο σχήμα 2.3 παρακάτω. Στην συνέχεια αφού παρατηρηθούν ν θετικές και μ αρνητικές βαθμολογίες η εξαγόμενη κατανομή είναι η βήτα κατανομή(α,β) όπου α=ν+1 και β=μ+1. Για παράδειγμα εάν παρατηρηθούν 7 θετικές και 1 αρνητική βαθμολογίες τότε η ΣΠΠ φαίνεται στο σχήμα 2.3 .



(a) Uniform PDF beta$(p \mid 1, 1)$ (b) PDF beta$(p \mid 8, 2)$

Σχήμα 2.3: Βήτα Συναρτήσεις Πυκνότητας Πιθανότητας

Μία ΣΠΠ αυτού του τύπου εκφράζει την αβέβαιη πιθανότητα ότι οι μελλοντικές αλληλεπιδράσεις θα είναι θετικές. Το πιο φυσικό είναι να καθοριστεί ο δείκτης φήμης ως συνάρτηση της τιμής της προσδοκίας. Η τιμή αυτή (της πιθανότητας προσδοκίας) σύμφωνα με την Εξ. 2.2 είναι E(p) = 0,8. Αυτό μπορεί να ερμηνευθεί λέγοντας ότι η σχετική συχνότητα μιας θετικής έκβασης στο μέλλον είναι αβέβαιη, και ότι ή πιθανότερη τιμή της (της συχνότητας) είναι 0,8.

2.3.2 Διακριτών Καταστάσεων

2.3.3 Ασαφούς Λογικής

2.3.4 Άθροιση ή εξαγωγή Μέσου Όρου

2.4 Γνωστά Συστήματα φήμης κ εμπιστοσύνης σε διαφόρους τομείς

2.4.1 Business

2.4.2 Mobile-ad-hoc Networks

2.4.3 Vehicular Networks

2.4.4 Peer-to-Peer Systems

2.4.5 Internet of Things