



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
Επικ. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2015

.....
Ελευθέριος Κόκορης - Κόγιας

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

Copyright © Ελευθέριος Κόκορης - Κόγιας, 2015.

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

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 πιο 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 στις 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, προτείνεται το σύστημα RTIoT (Reputation & Trust for the Internet of Things). Στην συνέχεια προστίθενται χαρακτηριστικά, όπως η ικανότητα μίας κακόβουλης Εικονικής Οντότητας (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 παρουσιάζουμε τα αποτελέσματα μέσα από μία προσομοίωση στο TRMSIM-WSN και τα συγκρίνουμε με άλλα συστήματα Εμπιστοσύνης/Φήμης.

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 propose the RTIoT(Reputation & Trust for the Internet of Things) system. then 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 demonstrate the results of a simulation using the TRMSIM-WSN simulator and compare them with other reputation systems.

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

Περίληψη	5
Abstract	7
Ευχαριστίες	9
Περιεχόμενα	11
Κατάλογος σχημάτων	13
Κατάλογος πινάκων	15
1. Εισαγωγή	17
1.1 Κοινωνικό Διαδίκτυο των Πραγμάτων και Προβλήματα Εμπιστοσύνης	18
1.2 Δομή της Διπλωματικής Εργασίας	19
2. Θεωρητικό και Τεχνολογικό Υπόβαθρο	21
2.1 Ορισμοί Εννοιών	21
2.1.1 Soft Security	22
2.1.2 Η Έννοια της Εμπιστοσύνης	22
2.1.3 Η Έννοια της Φήμης	23
2.2 Αρχιτεκτονικές Δικτύωσης Συστημάτων Εμπιστοσύνης	24
2.2.1 Συγκεντρωτικές Αρχιτεκτονικές	25
2.2.2 Κατανεμημένες Αρχιτεκτονικές	26
2.3 Τρόποι υπολογισμοί φήμης και εμπιστοσύνης	27
2.3.1 Bayesian	27
2.3.2 Διακριτών Καταστάσεων	28
2.3.3 Ασαφούς Λογικής	28
2.3.4 Ροής Εμπιστοσύνης	29
2.3.5 Άθροιση ή εξαγωγή Μέσου Όρου	29
2.4 Γνωστά Συστήματα φήμης κ εμπιστοσύνης σε διαφόρους τομείς	30
2.4.1 Business	30
2.4.2 Mobile-ad-hoc Networks	30
2.4.3 Peer-to-Peer Systems	30
2.4.4 Internet of Things	30
3. Τύποι επιθέσεων - Αντιμετώπιση με RT-IOT	31
3.1 Επιθέσεις στο Διαδίκτυο των πραγμάτων	31
3.1.1 Μεμονωμένες κακόβουλες Εικονικές Οντότητες	31
3.1.2 Συνεργαζόμενες κακόβουλες Εικονικές Οντότητες	32
3.1.3 Μερικώς κακόβουλες Εικονικές Οντότητες	33

3.1.4	Κακόβουλοι κατάσκοποι	34
3.1.5	Sybil attack	35
3.1.6	Ψευδής δήλωση στοιχείων	35
3.2	RT-IOT	37
3.3	Βασικά Σενάρια Χρήσης	38

Κατάλογος σχημάτων

2.1	Συγκεντρωτική Αρχιτεκτονική	25
2.2	Κατανεμημένη Αρχιτεκτονική	26
2.3	Βήτα Συναρτήσεις Πυκνότητας Πιθανότητας	27
3.1	Μεμονωμένες κακόβουλες Εικονικές Οντότητες	31
3.2	Συνεργαζόμενες κακόβουλες Εικονικές Οντότητες	32
3.3	Μερικώς κακόβουλες Εικονικές Οντότητες	34
3.4	Κακόβουλοι κατάσκοποι	35
3.5	Sybil attack	36

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 δύσκολη. 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 μέσω φιλίας, μέσω οικογένειας (ανήκουν στον ίδιο χρήστη) ή και μέσω ομοιότητας (έχουν τον ίδιο ρόλο στο σύστημα), τότε βρισκόμαστε στο Κοινωνικό Διαδίκτυο των Πραγμάτων¹. 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 άλλων,
- 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 μέσα στον τεράστιο αριθμό δεδομένων (Big Data)

¹ www.social-iot.org/

² www.ios-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 3

DESIGN + USE CASE SCENARIOS + attack-models 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 ??

CONCLUSION-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 (ευφών 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 προϊόν" 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 του.
2. Αντίθετα αυτή η εργασία εστιάζει στο πρόβλημα του ρίσκου που 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 της εμπιστοσύνης είναι εμφανής στις καθημερινές μας αλληλεπιδράσεις. Θα μιλήσουμε για τα προβλήματα μας και της εμπειρίας μας -δηλαδή θα δώσουμε ευαίσθητες προσωπικές πληροφορίες- στους φίλους μας οι οποίοι περιμένουμε να μας βοηθήσουν 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 κυβερνούν συναισθήματα όπως αγάπη και αφοσίωση που δεν έχουν καμία θέση στον ψηφιακό κόσμο. Στο έργο του Audun Jøsang υπάρχει μία εξαιρετική συγκέντρωση για τους διάφορους ορισμούς της εμπιστοσύνης και της φήμης. Εκεί λοιπόν αναφέρεται πώς υπάρχουν δύο βασικοί

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.

ορισμοί για την εμπιστοσύνη τους οποίους ονομάζουμε εμπιστοσύνη αξιοπιστίας (reliability trust) και εμπιστοσύνη απόφασης (decision trust)

Όπως προϋποθέτει και το όνομα η εμπιστοσύνη αξιοπιστίας μπορεί να ερμηνευθεί ως η αξιοπιστία κάποιου δράστη ή αντικειμένου, και ο ορισμός του Gambetta παρέχει 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 περιεχέει την έννοια της εξάρτησης του *A* από τον *B*, και την αξιοπιστία (δηλαδή την πιθανότητα) του *B* όπως την αντιλαμβάνεται ο *A*.

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 των 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 στις 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 στις παρακάτω προτάσεις:

1. "Θα εμπιστευτώ τον X επειδή έχει καλή φήμη"
2. "Θα εμπιστευτώ τον Y παρόλο που έχει κακή φήμη, επειδή μαζί μου είναι καλός"

Οι παραπάνω φράσεις δείχνουν ξεκάθαρα πώς παρόλο που η υπηρεσία που τα δυο άτομα θέλουν αιτηθούν είναι η ίδια, το άτομο 1, που δεν έχει αλληλεπιδράσει ποτέ με τον Y, θα προτιμήσει τον X εμπιστευόμενος το κοινωνικό σύνολο από όπου εξήγε την καλή φήμη του X. Αντίθετα το άτομο 2 ένα και ξέρει πως ο X έχει καλύτερη φήμη από τον Y θα διαλέξει τον Y επειδή έχει καλή προϋστορία 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 συνόλου 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 είναι:

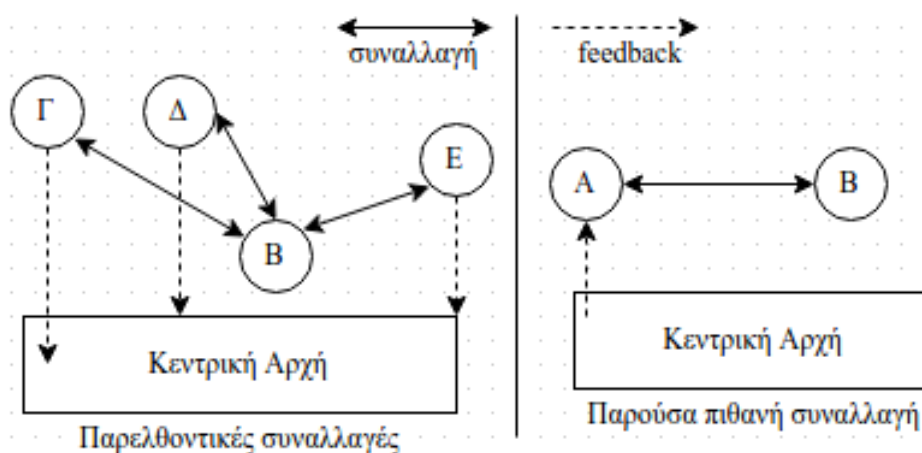
1. Οι οντότητες πρέπει να είναι μακρόβιες έτσι ώστε μετά από μία συναλλαγή να υπάρχει πιθανότητα μία μελλοντικής επαφής με την ίδια οντότητα
2. Οι συναλλαγές να αποτιμώνται και οι βαθμολογίες να διανέμονται σε άλλα μέλη της κοινότητας
3. Οι αποφάσεις για της συναλλαγές μίας οντότητας να επηρεάζονται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

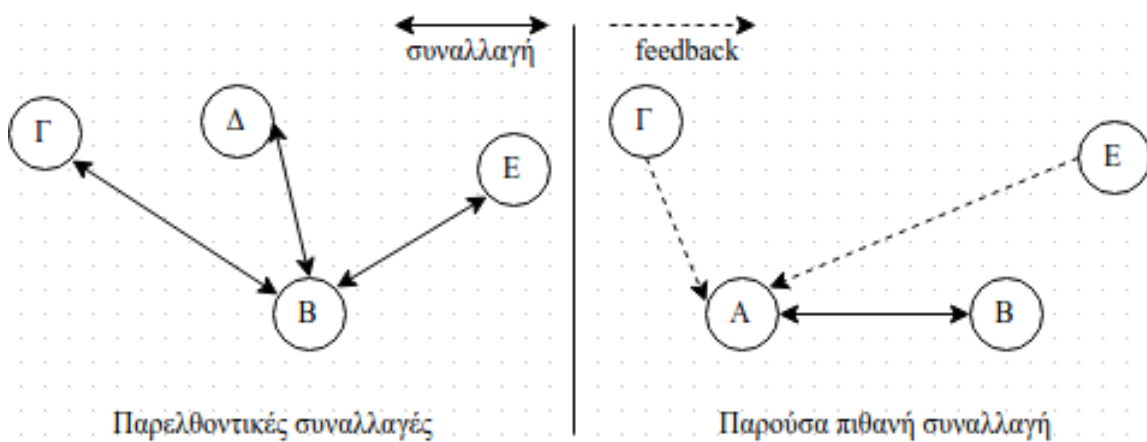
Ο Α θέλει να προβεί σε μία συναλλαγή με τον Β, ενώ δεν έχει κάποια παρελθοντική εμπειρία με αυτόν. Για αυτό ρωτάει την κεντρική αρχή, η οποία με την σειρά της γυρίζει τον δείκτη φήμης που έχει υπολογίσει βασιζόμενη σε πληροφορίες από άλλα μέλη της κοινότητας όταν αυτά αλληλεπιδράσαν με τον Β και κοινοποίησαν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

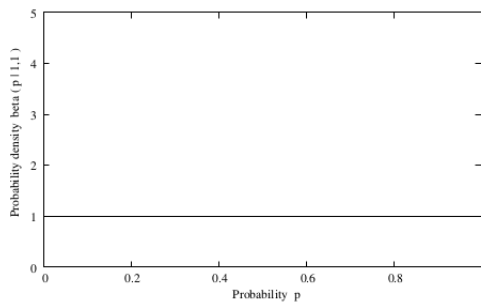
Η βήτα οικογένεια κατανομών είναι μια συνεχής οικογένεια συναρτήσεων κατανομής μεταβαλλόμενη από τις δύο παραμέτρους α και β . Η βήτα ΣΠΠ συμβολίζεται με $\text{beta}(p | \alpha, \beta)$ μπορεί να εκφραστεί χρησιμοποιώντας τη συνάρτηση γάμμα Γ ως εξής:

$$\text{beta}(p|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1} (1-p)^{\beta-1} \text{ όπου } 0 \leq p \leq 1, \alpha, \beta > 0 \quad (2.1)$$

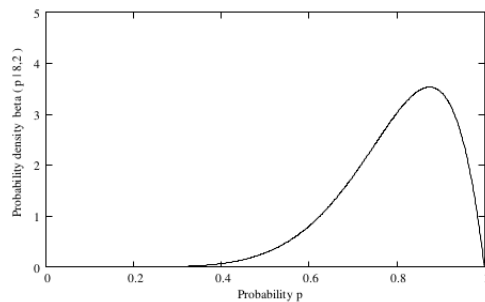
με τον περιορισμό ότι η πιθανότητα $p \neq 0$ αν $\alpha < 1$, και $p \neq 1$ αν $\beta < 1$. Η τιμή της προσδοκίας της κατανομής beta δίνεται από:

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

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 n θετικές και m αρνητικές βαθμολογίες η εξαγόμενη κατανομή είναι η βήτα κατανομή(α, β) όπου $\alpha = n+1$ και $\beta = m+1$. Για παράδειγμα εάν παρατηρηθούν 7 θετικές και 1 αρνητική βαθμολογίες τότε η ΣΠΠ φαίνεται στο σχήμα 2.3.



(a) Uniform PDF $\text{beta}(p | 1, 1)$



(b) PDF $\text{beta}(p | 8, 2)$

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 η πιθανότερη τιμή της (της συχνότητας) είναι 0,8.

2.3.2 Διακριτών Καταστάσεων

Οι άνθρωποι μπορούν συχνά να αξιολογήσουν καλύτερα την απόδοση συστημάτων όταν οι τιμές έχουν διακριτή λεκτική μορφή, σε σχέση με όταν είναι συνεχείς μετρήσεις. Αυτό ισχύει επίσης και για τον καθορισμό των δεικτών εμπιστοσύνης. Ορισμένοι συγγραφείς, συμπεριλαμβανομένων έχουν προτείνει διακριτά μοντέλα εμπιστοσύνης. Για παράδειγμα, στο μοντέλο του Αμπντούλ Ραχμάν & Hales (2000) , η αξιοπιστία ενός παράγοντα X μπορεί να έχει τιμές: Πολύ Αξιοπιστα, Αξιοπιστα, Αναξιοπιστα, Πολύ Αναξιοπιστα. Το μέλος της κοινότητας (Y) που θέλει να βρει την αξιοπιστία κάποιου μπορεί να συνδυάσει τη δική του άποψη για την αξιοπιστία του X με την φήμη που εξάγει από την κοινότητα.

Look-up πίνακες, με εγγραφές για την υποβάθμιση / αναβάθμιση της εμπιστοσύνης που έχει ο Y στον X , χρησιμοποιούνται για να καθορίσουν την εξαγόμενη εμπιστοσύνη στο X . Κάθε φορά που ο Y είχε προσωπική εμπειρία με το X , αυτό μπορεί να χρησιμοποιηθεί για τον προσδιορισμό της αξιοπιστίας του. Η υπόθεση είναι ότι η προσωπική εμπειρία αντικατοπτρίζει την πραγματική αξιοπιστία του X και ότι η φήμη που λαμβάνει για τον X , η οποία διαφέρει από την προσωπική εμπειρία, δείχνει αν ο Y υποτιμά ή υπερτιμά τον X . Παρατηρήσεις από "φίλους" που υπερεκτιμούν των Y θα υποβαθμιστεί πριν ληφθούν υπόψιν, και το αντίστροφο.

Το μειονέκτημα των διακριτών τιμών είναι ότι δεν είναι εύκολο να εφαρμοστούν σε αυτά κλασσικοί υπολογισμοί. Αντ' αυτού, πρέπει να χρησιμοποιηθούν ευριστικοί μηχανισμοί όπως look-up πίνακες.

2.3.3 Ασαφούς Λογικής

Η εμπιστοσύνη και η φήμη μπορούν να παρασταθούν ως γλωσσικά ασαφείς έννοιες, όπου συναρτήσεις συμμετοχής περιγράφουν σε ποιο βαθμό ένας παράγοντας μπορεί να περιγραφεί ως π.χ. αξιοπιστος ή αναξιοπιστες. Η ασαφής λογική προβλέπει κανόνες για το συλλογισμό με ασαφείς μετρικές αυτού του είδους. Το σύστημα που προτείνει Manchala (1988, καθώς και η εξαγωγή της φήμης στο σύστημα REGRET που προτείνουν οι Sabater & Sierra (2001,2002) εμπίπτουν σε αυτή την κατηγορία. Στο σύστημα των Sabater & Sierra, αυτό που αποκαλούν ατομική φήμη προέρχεται από ιδιωτικές πληροφορίες σχετικά με ένα συγκεκριμένο δράστη ενώ αυτό που ονομάζουν κοινωνική φήμη προέρχεται από την ενημέρωση του κοινού σχετικά με αυτόν τον δράστη, τέλος αυτό που αποκαλούν context dependent φήμη εξάγεται από τις συμφοραζόμενες πληροφορίες.

2.3.4 Ροής Εμπιστοσύνης

Τα συστήματα που υπολογίζουν την εμπιστοσύνη ή τη φήμη με επανάληψη μέσω βρόχου ή με αυθαίρετα μεγάλες αλυσίδες μπορούν να ονομαστούν μοντέλα ροής.

Ορισμένα μοντέλα ροής έχουν σταθερή τιμή ολικής εμπιστοσύνης / φήμης για το σύνολο του συστήματος και η τιμή αυτή μπορεί να κατανεμηθεί μεταξύ των μελών της κοινότητας. Οι συμμετέχοντες μπορούν να αυξήσουν την εμπιστοσύνη / φήμη τους μόνο σε βάρος των άλλων. Ο PageRank της Google [52] ανήκει σε αυτή την κατηγορία. Σε γενικές γραμμές, η φήμη ενός συμμετέχοντος αυξάνει ως συνάρτηση της εισερχόμενης ροής, και μειώνεται ως συνάρτηση της εξερχόμενης ροής. Στην περίπτωση της Google, πολλοί υπερσύνδεσμοι εισερχόμενοι (που δείχνουν σε αυτή) σε μια ιστοσελίδα συμβάλλουν στην αύξηση του δείκτη PageRank ενώ πολλοί υπερσύνδεσμοι εξερχόμενοι (που υπάρχουν μέσα) από μια ιστοσελίδα οδηγούν στη μείωση του δείκτη PageRank για την εν λόγω ιστοσελίδα.

Τα μοντέλα ροής δεν απαιτούν πάντα το άθροισμα των βαθμολογιών φήμης / εμπιστοσύνης να είναι σταθερό. Ένα τέτοιο παράδειγμα είναι το σύστημα EigenTrust [35], το οποίο υπολογίζει δείκτες εμπιστοσύνη σε δίκτυα P2P μέσω επαναλαμβανόμενου πολλαπλασιασμού και ομαδοποίησης των βαθμολογιών εμπιστοσύνης έως ότου οι δείκτες εμπιστοσύνης για όλα τα μέλη της P2P κοινότητας συγκλίνουν σε σταθερές τιμές.

2.3.5 Άθροιση ή εξαγωγή Μέσου Όρου

Η συνηθέστερη μορφή υπολογισμού φήμης / εμπιστοσύνης είναι να υπολογίζεται το συνολικό αριθμό των θετικών αξιολογήσεων και το συνολικό αριθμό των αρνητικών αξιολογήσεων ξεχωριστά, και να εξαχτεί μια συνολική βαθμολογία ως το θετικό άθροισμα μείον το αρνητικό. Αυτή είναι η αρχή που χρησιμοποιείται στο φόρουμ του eBay η οποία περιγράφεται λεπτομερώς στο [55]. Το πλεονέκτημα είναι ότι ο καθένας μπορεί να καταλάβει την αρχή πίσω τον υπολογισμό της φήμης, το μειονέκτημα είναι ότι ο υπολογισμός είναι πρωτόγονος και, ως εκ τούτου ο δείκτης της φήμης δίνει μιας φτωχής εικόνα αν και αυτό οφείλεται επίσης στον τρόπο που παρέχεται αξιολόγηση.

Ένα ελαφρώς πιο προχωρημένο σύστημα που προτείνεται στο π.χ. [63] είναι να υπολογιστεί ο δείκτης της φήμης ως ο μέσος όρος όλων των αξιολογήσεων. Η αρχή αυτή χρησιμοποιείται στα συστήματα φήμης πολλών εμπορικές ιστοσελίδων, όπως της Amazon περιγράφεται στο [2.4](#)

Προηγμένα μοντέλα σε αυτή την κατηγορία υπολογίζουν ένα σταθμισμένο μέσο όρο όλων των αξιολογήσεων, όπου το βάρος της αξιολόγησης μπορεί να καθορίζεται από παράγοντες όπως ο εκτιμητής της αξιοπιστίας / φήμης, τη ηλικία της αξιολόγησης, η σχέση μεταξύ αξιολογητή και αξιολογούμενου κ.λ.π. Το σύστημα που παρουσιάζεται στην υπόλοιπη εργασία εμπίπτει σε αυτήν την κατηγορία.

2.4 Γνωστά Συστήματα φήμης κ εμπιστοσύνης σε διάφορους τομείς

Τα συστήματα φήμης και εμπιστοσύνης είναι ευρέως διαδεδομένα σε πολλούς τομείς όπου χρησιμοποιούνται πληροφοριακά συστήματα. Ο βασικός λόγος που εφαρμόζεται ένα σύστημα φήμης-εμπιστοσύνης είναι για να αντιμετωπίσει κακόβουλους συμμετέχοντες σε μία κοινότητα οντοτήτων και έτσι να βελτιωθεί τόσο η ασφάλεια όσο και η ποιότητα των υπηρεσιών.

2.4.1 Business

E-bay

Amazon

PageRank

2.4.2 Mobile-ad-hoc Networks

Le Boudec

hubeaux

stanford

2.4.3 Peer-to-Peer Systems

EingenTrust

PeerTrust

PowerTrust

2.4.4 Internet of Things

Atzori

Κεφάλαιο 3

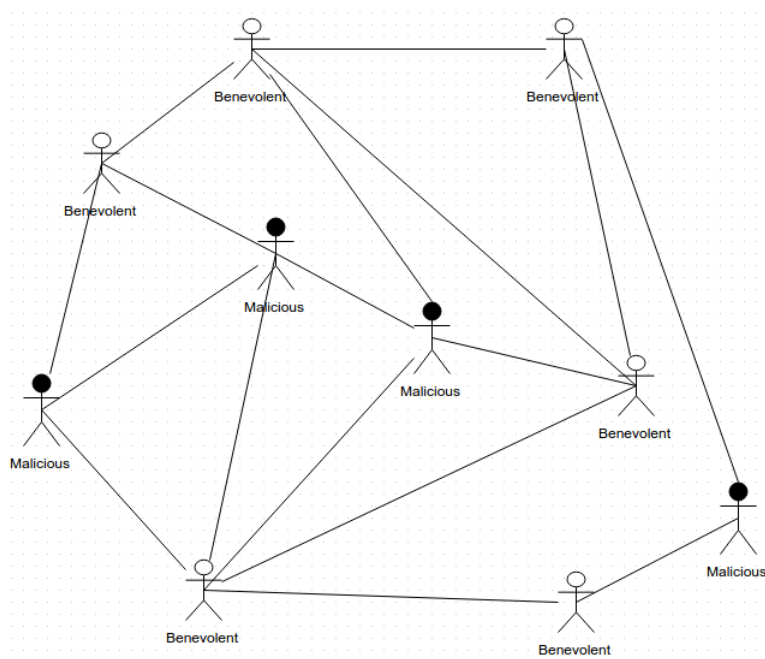
Τύποι επιθέσεων - Αντιμετώπιση με RT-IOT

3.1 Επιθέσεις στο Διαδίκτυο των πραγμάτων

Όπως αναφέρθηκε στο Κεφάλαιο 2 ένας από τους κινδύνους παραβίασης της ασφάλειας του Κοινωνικού Διαδικτύου των Πραγμάτων πηγάζει από επιθέσεις κακόβουλων οντοτήτων οι οποίες όμως νομίμως δρουν εντός της κοινωνίας των πραγμάτων. Σε αυτό το κομμάτι του κεφαλαίου θα αναλύσουμε τις βασικότερες επιθέσεις που μπορούν να συμβούν.

3.1.1 Μεμονωμένες κακόβουλες Εικονικές Οντότητες

Οι μεμονωμένες κακόβουλες Εικονικές Οντότητες Σχ.3.1 είναι ο απλούστερος και ο βασικότερος τύπος επίθεσης. Σε αυτήν την περίπτωση ένα ποσοστό των μελών της κοινότητας έχοντας κακόβουλους σκοπούς προσπαθούν να εκμεταλλευτούν την εμπιστοσύνη των υπόλοιπων και όταν τους ζητηθεί κάποια υπηρεσία ή γνώση αντί να τους εξυπηρετήσουν σωστά στέλνουν δεδομένα που θα οδηγήσουν στο να εκτεθεί ο παραλήπτης σε κίνδυνο ή να οδηγηθεί σε δυσλειτουργία.



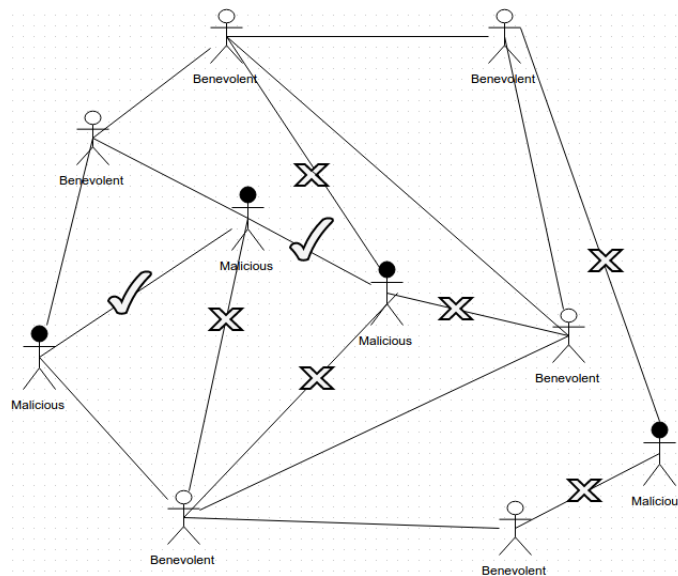
Σχήμα 3.1: Μεμονωμένες κακόβουλες Εικονικές Οντότητες

Η ύπαρξη κακόβουλων Εικονικών Οντοτήτων αποτελεί την βάση όλων των επιθέσεων και ο εντοπισμός τους είναι ο κύριος στόχος του RT-IOT. Για να βρεθούν χρειάζεται η συλλογική συμφωνία του συστήματος στο ποιες ακριβώς είναι.

Αλλά ακόμα και αν δεν τους εντοπίσει το σύστημα ώστε να σταματήσει να τους προτείνει ως πιθανούς φίλους με καλή φήμη, τα μέλη μπορούν αυτόνομα να προστατευθούν. Έτσι μετά από έναν αριθμό αλληλεπιδράσεων μία Εικονική Οντότητα θα χάσει την όποια εμπιστοσύνη τους στον κακόβουλο δράστη και θα τον απορρίψει από τον κοινωνικό του περίγυρο. Το θέμα είναι πόσο γρήγορα θα το κάνει ώστε να περιορίσει του κινδύνους.

3.1.2 Συνεργαζόμενες κακόβουλες Εικονικές Οντότητες

Σε αυτού του είδους της επίθεσης Σχ. 3.2 υπάρχει ένας αριθμός κακόβουλων Εικονικών Οντοτήτων όπως περιγράφηκε στην παράγραφο 3.1.1 οι οποίες όμως τώρα έχουν γνώση (μερική ή ολική) για την ύπαρξη και άλλων κακόβουλων Εικονικών Οντοτήτων. Με αυτή λοιπόν την γνώση συνεργάζονται μεταξύ τους και όταν στέλνουν, είτε στην κεντρική αρχή είτε σε άλλα μέλη της κοινότητας, πληροφορίες για να εξαχθεί ο δείκτης φήμης παραποιούν τα δεδομένα τους και να παρουσιάζουν τους κακόβουλους συνεργάτες τους ως φερέγγυους.



Σχήμα 3.2: Συνεργαζόμενες κακόβουλες Εικονικές Οντότητες

Αυτού του είδους η επίθεση είναι πολύ πιο επικίνδυνη από την προηγούμενη. Αυτό συμβαίνει επειδή δεν είναι δυνατόν να βασιστούν οι Εικονικές Οντότητες στην καλή θέληση των μελών της κοινωνίας για να εξαχθεί η φήμη αφού υπάρχει μεγάλη πιθανότητα να ψεύδονται για τις εμπειρίες τους. Για την αντιμετώπιση του πρέπει:

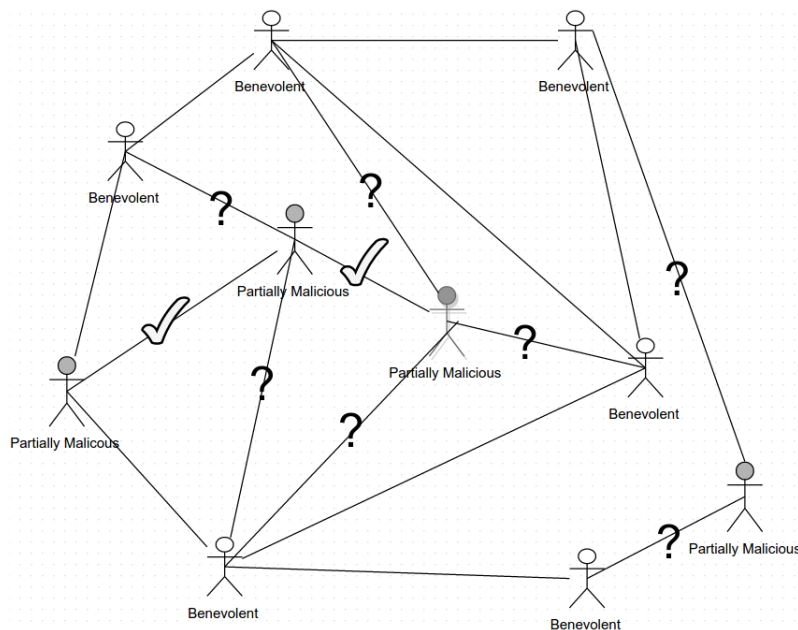
- Στην περίπτωση της κεντρικής αρχής να εντοπιστεί όλη η κοινότητα των κακόβουλων δραστών και να σταματήσει να λαμβάνεται υπόψιν η γνώμη τους κατά την εξαγωγή φήμης.
- Στην περίπτωση συστημάτων χωρίς κεντρική αρχή πρέπει η κάθε Εικονική Οντότητα να εντοπίσει κάποιου έμπιστου φίλου των οποίων η πιθανότητα να ψεύδονται για τις εμπειρίες τους θα είναι μειωμένη σε σχέση με το σύνολο.

Μια εξελιγμένη μορφή αυτής της επίθεσης είναι η κακόβουλες Εικονικές Οντότητες να προσπαθούν να εντοπίσουν μέσω τις φήμης ανταγωνιστικές προς τις υπηρεσίες που εκμεταλλεύονται Εικονικές Οντότητες και να προσπαθήσουν να χαμηλώσουν την φήμη τους με περαιτέρω ψευδής δηλώσεις για την εμπειρία τους με αυτές.

3.1.3 Μερικώς κακόβουλες Εικονικές Οντότητες

Σε αυτού του είδους της επίθεσης Σχ. 3.3 υπάρχουν κακόβουλες συνεργασίες όπως αναφέρθηκαν στην παράγραφο 3.1.2. Η διαφορά τώρα όμως είναι πώς αυτές οι οντότητες προσπαθούν να νικήσουν το σύστημα φήμης αλλάζοντας την συμπεριφορά τους. Αυτό μπορεί αν συμβεί με 2 τρόπους:

1. Αρχικά μπορούν να παρέχουν κακές υπηρεσίες μόνος p % των περιπτώσεων ώστε να μην καταποντίζεται η φήμη τους. Δηλαδή μόλις δουν ότι υπάρχει μία κίνηση αποκλεισμού τους, να γίνονται καλές ώστε να παραμείνουν ενσωματωμένες. Σε αυτή την περίπτωση πρέπει το σύστημα που υπολογίζει την φήμη να έχει μνήμη ώστε να βλέπει καχύποπτα τέτοιου είδους συμπεριφορές και να εφαρμόζει αποκλεισμό με το που ξαναγίνουν κακόβουλες. Παρόλα αυτά αυτή η επίθεση δεν είναι τόσο επικίνδυνη επειδή η κακή συμπεριφορά της Εικονικής Οντότητας είναι φραγμένη από το p
2. Ένας άλλος τρόπος να ξεγελάσουν το σύστημα είναι να προσθέσουν στο ενεργητικό τους και άλλες υπηρεσίες. Έτσι θα είναι πιο εύκολο να εκμεταλλεύονται μία υπηρεσία για τους κακόβουλους σκοπούς τους αλλά να παραμένουν στο απυρόβλητο από το σύστημα φήμης επειδή παρέχουν άλλες καλά. Για να αντιμετωπιστεί αυτού του είδους η επίθεση πρέπει να υπάρχει διαφοροποίηση των δεικτών φήμης ανά υπηρεσία. Αλλά για να μπορέσει παραμείνει κλιμακώσιμο πρέπει να γίνει ομαδοποίηση σε παρόμοιες υπηρεσίες ώστε να περιοριστεί το εύρος που μπορεί να εκμεταλλευτεί μία κακόβουλη Εικονική Οντότητα.

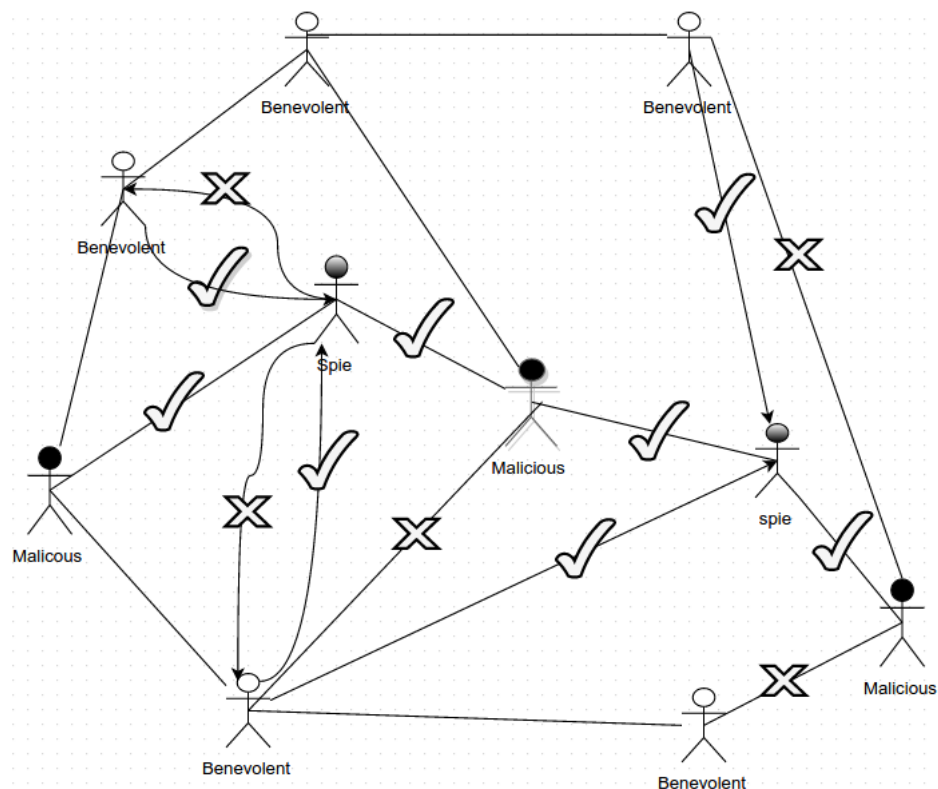


Σχήμα 3.3: Μερικώς κακόβουλες Εικονικές Οντότητες

3.1.4 Κακόβουλοι κατάσκοποι

Αυτού του είδους η επίθεση Σχ. 3.4 είναι βοηθητική στις 3.1.2 και 3.1.3. Οι Εικονικές Οντότητες - κατάσκοποι. Ονομάστηκαν έτσι επειδή στα μάτια του μεγαλύτερου μέρους των μελών του συστήματος παρουσιάζονται ως αξιόπιστες. Αυτό το καταφέρνουν παρέχοντας πάντα μία υπηρεσία καλά. Έτσι αυξάνουν την φήμη τους και την εμπιστοσύνη μεμονωμένων Εικονικών Οντοτήτων προς αυτές. Αυτό όμως που τις κάνει κακόβουλες είναι η συμπεριφορά τους όταν τους ζητηθεί αξιολόγηση ή να προτείνουν κάποιον άλλον πάροχο διαφορετικής υπηρεσίας. Τότε συνεργαζόμενοι με τις κακόβουλες κοινότητες του συστήματος ψεύδονται για τις εμπειρίες τους και προτείνουν κακόβουλες οντότητες για φίλους.

Ένα σύστημα που αντιμετωπίζει όλες τις παραπάνω επιθέσεις δεν μπορεί να αντιμετωπίσει και αυτήν. Για να γίνει αυτό πρέπει να υπάρξει αποσύνδεση της εμπιστοσύνης σε κάποιον ως πάροχο υπηρεσίας, από την εμπιστοσύνη ως πάροχο πληροφοριών. Με αυτόν τον τρόπο θα κρατάμε τους κατασκόπους για να μας παρέχουν σωστές υπηρεσίες αλλά η φήμη της ως παρόχους πληροφοριών θα είναι χαμηλή και άρα δεν θα λαμβάνετε υπόψιν.

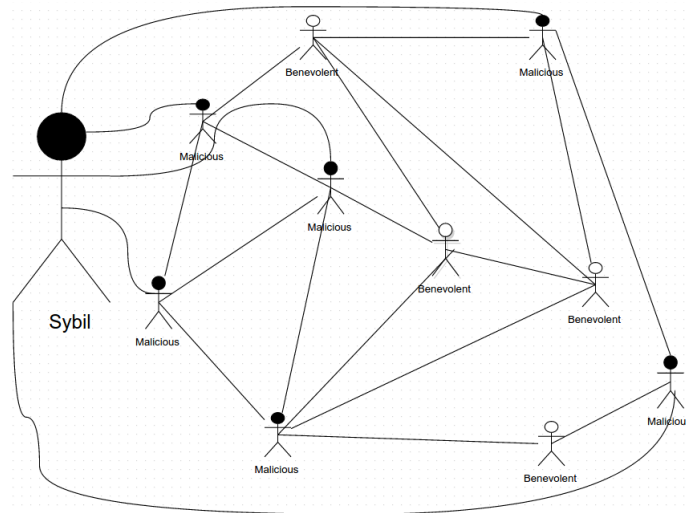


Σχήμα 3.4: Κακόβουλοι κατάσκοποι

3.1.5 Sybil attack

Σε αυτήν την επίθεση Σχ. 3.5 κάποιος καταφέρνει να δημιουργήσει ένα τεράστιο αριθμό εικονικών οντοτήτων και να τις χρησιμοποιήσει για τους κακόβουλους σκοπούς τους. Μόλις μειωθεί η φήμη τους τις διαγράφει και κάνει νέες. Για την αντιμετώπισή του πρέπει:

1. Αρχικά να μην υπάρχει πλεονέκτημα σε μία νέα οντότητα σε σχέση με κάποια με χαμηλή φήμη. Αυτό επιτυγχάνετε με την απουσία αρνητικής βαθμολογίας. Έτσι μία νέα οντότητα αντιμετωπίζεται με καχυποψία και θα πρέπει να αποδείξει την αξία της για να ενσωματωθεί
2. Ακόμα πρέπει να υπάρχει ένα ελάχιστο κόστος για την δημιουργία νέων εικονικών οντοτήτων. Στο σύστημα μας προτείνετε να πρέπει ο χρήστης να συνδέσει την οντότητα του με κάποιο user-id. Το οποίο να μην γίνεται αυτόματα (π.χ χρήση Captcha)



Σχήμα 3.5: Sybil attack

3.1.6 Ψευδής δήλωση στοιχείων

Στον Ατζορι έχει προταθεί ο πολλαπλασιασμός της εμπιστοσύνης σε κάποιον με ένα βάρος για το πόσο εύκολο είναι για αυτόν να συμπεριφερθεί κακόβουλα. Έτσι αναφέρεται ότι θα εμπιστευτεί μία οντότητα πιο εύκολα εάν έχει χαμηλή υπολογιστική ισχύ π.χ. RFID από μία ισχυρή όπως ένα smartphone. Αλλά είναι δυνατόν κάποιος είτε να ισχυριστεί πως είναι οντότητα διαφορετικού τύπου από την πραγματικότητα¹, είτε να έχει τον έλεγχο πραγματικών οντοτήτων τύπου RFID που θα είναι εύκολο να γίνουν έμπιστες και θα τις εκμεταλλεύεται.

Για αυτό εμείς αντιπροτείνουμε το βάρος να είναι ανάλογο με το πόσο επικίνδυνο θα ήταν για μία Εικονική Οντότητα να παραπλανηθεί για μία συγκεκριμένη υπηρεσία. Έτσι υπηρεσίες που θα μπορούσε να δώσει ένα RFID που πιθανώς να ήταν ήσσονος σημασίας θα ζητούνται ακόμα και από Οντότητες μέτριας εμπιστοσύνης, ενώ κρίσιμες υπηρεσίες θα ζητούνται από έμπιστους παρόχους. Το πώς μοντελοποιήθηκε αυτό το βάρος φαίνεται στο ΡΕΦ παρακάτω.

¹ το οποίο ίσως να μπορούσε να ελεγχθεί μέσα από προσπάθεια εντοπισμού των ενεργειών της οντότητας, το οποίο είναι δύσκολο χωρίς κεντρική αρχή που βλέπει όλες τις συναλλαγές

3.2 RT-IOT

3.3 Βασικά Σενάρια Χρήσης