Trust: An Approach for Securing Mobile ad hoc Network

Chung Tien NGUYEN and Olivier CAMP

Departement of Computer Science, ESEO
ANGERS, France

Abstract. When functionning in the ad hoc mode, wireless networks do not rely on a predefined infrastructure for achieving the basic network functionalities. Hosts of such networks need to count on one another to keep in contact with the network and carry out services such as routing, security, auto-configuration,... Network services and, in particular, security thus strongly depend on the way the nodes find the correct partners with which they can cooperate efficiently. As consequence, it seems important for ad hoc networks to provide a representation of trust together with a mechanism to evaluate it. In this paper, we present ad hoc networks, and show how trust is fundamental in the existing propositions to improve their security. After identifying the characteristics of existing trust models, we focus on those that should be implemented in a trust model for ad hoc networks.

1 Introduction

Wireless technologies offer, today, new possibilities in the fields of telecommunications. The development of wireless communication allows manipulation of information through mobile calculating units such as laptop computers, personal organisers, mobile phones, sensors,... These units should be capable of accessing the network through a wireless communication interface and are able to roam freely.

Such mobile environments, which are composed of mobile units interconnected by radio links, allow a very flexible way of implementing communicating applications in various fields. In particular, they allow the establishment of networks in sites where it is difficult, or even impossible, for an infrastructure to be installed - eg; construction sites, mobile laboratories, search and rescue operations, battlefields, ...

Wireless mobile networks can be divided into two classes: infrastructured mobile networks (i.e cellular network,...), and mobile ad hoc networks which are self organised and do not need an infrastructure. There are no dedicated routers, servers, access points or cables in these networks and theirs entities can join or leave the networks at any time.

The security provided by ad hoc networks should be equivalent to that expected from traditional infrastructured wired networks. However, due to the lack of infrastructure and entry point, it is difficult to transpose existing solutions to this type of context.

In such a complex environment, it is difficult for an entity to determine which entities are malicious and which are not. This is a very important point since entities in it need to communicate and cooperate in order to achieve basic network services. Several

Tien NGUYEN C. and CAMP O. (2005).
Trust: An Approach for Securing Mobile ad hoc Network.
In *Proceedings of the 4th International Workshop on Wireless Information Systems*, pages 92-103
DOI: 10.5220/0002574000920103
Copyright © SciTePress

techniques can be used to identify entities that are authorized to join the network but such restrictions tend to degrade the network's efficiency. It is necessary for the entities to be able to determine the trust they can have in each other and, based on this trust, determine with which entities they can cooperate. A trust model allowing an entity to determine to what extend it can trust the others seems to be necessary to improve the security of ad hoc network.

Our goal is to develop a fully decentralised trust model, suitable for ad hoc networks, a dynamic and completely distributed environment.

The rest of the paper is structured as follows: in section 2 we present ad hoc networks, existing propositions to provide security to these networks and show that trust is a fundamental issue in most of them. Section 3 does a brief survey of existing trust models and introduces the key notions of reputation, recommendation and reciprocity. In section 4, we go through some important characteristics of existing trust models and identify those that seem important for ad hoc networks. Section 5 concludes the paper and discusses potential directions for future works.

2 Ad hoc networks

A mobile ad hoc network (MANET) is a wireless network made up of autonomous and mobile nodes. It does not need a predefined infrastructure to exist. It is created spontaneously by a temporary association of mobiles, which communicate through radio links. If the diameter of the network exceeds the radio transmission range, nodes have to participate in a routing protocol that considers the dynamic aspects of the network.

This type of network has the following characteristics:

- A dynamic topology that evolves rapidly in time according to the movement of mobiles, their emission power, and the characteristics of the communication channel.
- Unreliable connections with variable flow and limited bandwidth.
- Battery powered nodes that thus have a limited lifetime.
- An open network without any entry point on which administrative services can be installed

Implementation of security solutions in such an environment is a hot and challenging issue.

Firstly, MANETs are open. Since they have no clear entry point, a node can integrate the network by simply entering the transmission zone of another node. There is thus a probability of accepting a potential attacker into the network. Therefore, we should not only consider malicious attacks from outside the network, but also those launched from within the network by compromised nodes.

Moreover, the performances of MANETs do not allow for all security services to be implemented. Wireless connections in a MANET make it quite easy to carry out passive eavesdropping, active impersonation, message replay, and distortion. When within radio range of a node, an attacker can eavesdrop the messages it transmits (violate their confidentiality), delete these messages, and modify them (violate the availability and integrity).

Furthermore, MANETs are dynamic because their topology may change frequently and nodes may often join and leave the network. Security solutions based on a static configuration of the network would thus not be sufficient.

Finally, a MANET can become enormous and contain hundreds or, even thousands, of nodes. Security mechanisms should be scalable to handle such large networks.

Many security solutions have been proposed to implement security in MANETs.

In [1], the authors propose a solution based on group management. The whole network is a hierarchy of special purpose groups and sub-groups defined in accordance to the application context. The hierarchy signifies that a group can comprise several sub-groups and each sub-group can comprise several sub-sub-groups. A management framework is provided for establishing and managing this hierarchy. This framework supports control on group composition and allows for basic operation such as group joins and leaves. A manager administrates each group and sub-group. It is responsible for creating and maintaining group and for receiving and processing group operations sent by users. The manager is selected after a mechanism described in [2], this mechanism allows automatically selecting a manager by taking into account the status of the network and the capacity of the node. Mobile code is used to manages group and to determine if a node can become a manager.

A solution, which is considered as a method to strengthen the security in MANETs, is intrusion detection. Intrusion detection systems (IDS) allow detecting violations against the security policy. In a MANET, it is difficult to analyze network activities globally. Each node only possesses a limited vision of the network's activities. This limit depends on the characteristics of stations and is an important constraint for intrusion detection algorithm. Each station thus needs its own intrusion detection system, and makes it participate in the network's global intrusion detection mechanism.

[3] and [4] propose this kind of IDS. [3] uses independent agents on each station to locally detect intrusions. When a local anomaly is detected or evidence is not clear, the agents participate in a global detection. [4] proposes an architecture for IDS in which information is collected and exchanged using mobile agents. To determine if an intrusion is occurring, a node uses local information and more information gathered from remote nodes by the agents. Information collected remotely will only be usable if it can be trusted, i.e if the nodes it was obtained from are trusted by the gathering agent.

[5] proposes another solution for security: secure routing protocol. The authors add the notion of trust to the routing protocol AODV (Ad-hoc On demand Distance Vector routing). In this protocol, routing information is encrypted so that a malicious node cannot know who the sender is and nodes included in the route are authenticated. Encryption levels are selected in accordance with the trust levels existing between successive nodes and the level of security required by the application, needing the route. However, [5] does not specify how the trust level between nodes is determined.

In [6], Prashant Dewan and Partha Dasgupta make use of the concept of reputation in the routing protocol of MANETs. Reputation of an entity is determined through its past behavior. It is used to calculate probability that transactions between nodes are satisfied. The reputation of an entity is increased when it successfully transfers data packets and decreased when it does not. Each entity keeps information about the

reputation of nodes it knows and transfers this information, in recommendation, to other entities. The mechanism supposes that entities do not falsify their reputation.

Trust and reputation seem to be important factors in the field of security in ad hoc network and research in this field is very active. In a network in which many different kinds of nodes and users coexist, the notions of trust and reputation are necessary but difficult to realize.

3 Trust and reputation

3.1 Definition

Trust is a decisive factor in collective performance, particularly in virtual communities. Literature on this subject is plentiful and definitions are various, for example:

- Trust proceeds from reasoning, the ratio effort-benefit of an individual action within a collective.
- Trust is based on a nomination such as a label, a certificate. For example, we are able to confide our health and our life to an unknown doctor just because he obtained a national diploma, which we do not even care to verify. In electronic commerce, we use credit card numbers to buy merchandises on web sites, which possess well-known digital certificates.
- Trust comes from intuition, from belief, which do not suppose a true deliberation. This trust is emotional, aesthetic and irrational.
- Trust is based on a sort of ”engagement to respect the norm” that comes from a rule of reciprocal duty. This trust is defined as ”an expectation on the motivation of the other to behave in accordance with whatever is predicted in a given situation”. This definition considers individuals as rational and foreseeable actors, and their rationality is strengthened by their correct choices and their acts [7].

The theory of rationality supposes that individual choices rely on utilitarian reasoning:

- If I prefer A to B and B to C, then I prefer A to C
- All decisions are based on cost-benefit ratio, or on a risk analysis.

Certain try to put trust in relation with other concepts such as cooperation, recommendation,

Gambetta, in [8], establishes a connection between trust and cooperation and a certain degree of trust is required to realize cooperation. If trust is unilateral, the cooperative task cannot be realized. Thus, the higher degree of trust, the higher the possibility of realizing cooperation.

Recommendation plays an important role in the field of trust since it is impossible to trust everybody. When someone does not know whether he can put his trust in someone or not, she tends to ask a trusted third person. Suppose that A wants to know how he can place his trust in unknown X: if A can get a recommendation concerning X from a trusted entity B, the trust granted to X is function of this recommendation and of the trust granted to B. If B has no information concerning X, she will ask other entities. In

general, the longer the chain of recommendation, the lower the possibility of granting trust to the concerned person.

Patha Dasgupta gives another view of trust in [9]. According to him, though a measure of trust does not exist, it is possible to calculate the level of trust through intermediary. Dasgupta considers trust as knowledge or information. In his opinion, trust is expectation on activities of an entity when it reacts in a given context. Dasgupta concludes that trust is based on reputation, which is constructed through behaviors in known circumstances.

3.2 Direct trust and recommendation

In [10], Beth, Borcherding and Klein formally present trust relationship. They consider a system consisting of entities, which communicate via links. Some trusted entities, called Authentication Server (AS), play the role of authenticating agents for other entities. That means, when one entity wants to obtain information berfore engaging in a new experiences with others, it needs to ask an AS. If this AS cannot do that, it will ask another AS and become a mediator of the experience. The degree of trust is based on the number of positive end negative experiences.

[10] defines six classes of trust: key generation, identification, secret keeping, non-interference, clock synchronization and performance of algorithmic steps. Each class can have two types of trust: direct trust and recommendation trust. Direct trust is granted directly to the other entity while recommendation trust is based on the recommendation of a third entity.

In [10], direct trust is defined as follows:

$$A\ trust_x^{seq}\ B\ value\ V$$

A direct trust relationship exists if all *A*'s experiences with *B* with regard to trust class *x* are positive. *Seq* is a sequence of entities that mediated the experiences between *A* and *B*. The trust value, *V*, is an estimation of the probability that *B* behaves well. This is base on the number of positive experiences *A* has had with *B*.

Recommendation trust is defined as follows:

$$A\ trust_x^{seq}\ B\ when.path\ S_p\ when.target\ S_t\ value\ V$$

Recommendation trust exists if *A* accepts reports from *B* about experiences with third parties with regard to trust class *x*. The third parties are restricted to the entities in S_{t} (the target constraint set) and the mediators of the experiences are restricted to S_{p} (the path constraint set).

The example of derivation of a trust relationship with a recommendation in figure 1 is given in [10]. With the help of some rules, a new trust relationship can be established from a set of initial relationships.

Based on existing trust relationships, shown in figure 1(a), the new trust relationship between *A* and *C* and between *A* and *D* can be derived. The derivation can be presented by the following equations:

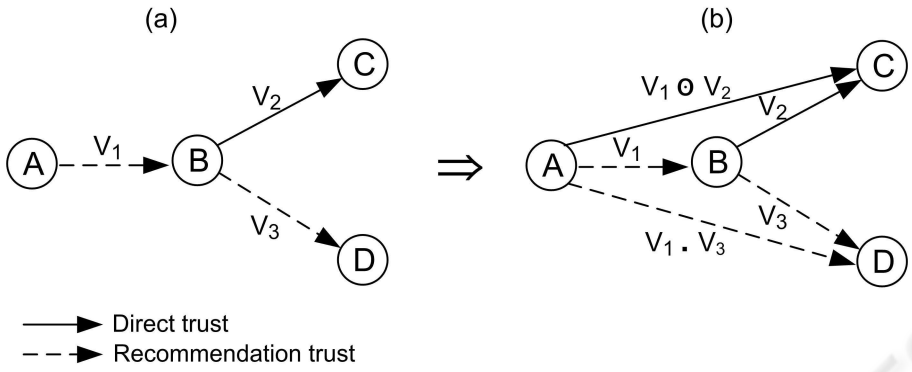

Fig. 1. Derivation of trust

Derived trust between *A* and *C*

$$V_1 \odot V_2 = 1 - (1 - V_2)^{V_1}$$

Recommendation trust between *A* and *D*

$$V_1 \cdot V_3 = simple\, multiplication\, between\, V_1\, and\, V_3$$

This multiplication shows that the value of derived recommendation trust decreases when the recommendation chain grows.

3.3 Relationship between trust, reputation and reciprocity

[11] proposes a model for calculating trust and reputation for E-Business. This model defines three concepts: trust, reputation and reciprocity. Trust is the subjective expectancy of an individual about the future behavior of others, based on their previous relations. The reputation of an entity is the perception of individuals, and created through its activities in the past. Each individual shows her reciprocity if she responds correlatively to what others give to her - i.e; she collaborates with people who collaborate with her and has a negative behavior with those who do not.

With this model, the author expects individuals to trust a person, who has a high reputation and to be cautious with people, who don't. When an individual frequently shows her reciprocity, she can incite others to increase her reputation.

Suppose that an individual a_j wants to estimate the reputation of individual a_i to establish cooperation. The set *A* of *N* individuals, which a_j asks for information about a_i, is called the "*embedded social network*": *A* = $\{a_1, a_2, ..., a_N\}$

Reputation is diffused so that individuals, who cooperate well, are rewarded. The following relations are expected:

– Augmentation of reputation of a_i in *A* increases the trust, which is granted to a_i by *A*.

- Augmentation of trust in a_i increases the possibility that a_j responds positively to actions requested by a_i
- Augmentation of the reciprocity between a_i and other members of *A* increases the reputation of a_i in *A*

However, the activity space of this model is binary: Two nodes either cooperate or they do not.

4 A Trust model for ad hoc mobile networks

MANETs evolve in a completely open environment. Many nodes can join the network for different purposes: researchers want to discus with each others, professors want to exchange their opinions about courses or exams, students want to do exercises together, some people, if possible, just want to know what others are doing. When belonging to a MANET, a node usually goes in communication with a large number of other nodes. However, hosts do not necessarily trust all the others, sometimes simply because they do not know anything about each other. They need to be able to choose good nodes, with which they can cooperate to complete their task. This choice depends on the trust between them; and nodes should be able to evaluate the trust they have in each other.

A model allowing the expression of trust among nodes seem necessary for MANETs.

Existing models are applied in different security domains: PGP (Pretty Good Privacy), Maurer-D and SPKI by public key infrastructures, X509 by certification authorities, Poblano in peer-to-peer environment,... These models possess characteristics specifically adapted to their domain. They can be classified as follows:

- The types of trust represented in the model.
- The representation of trust.
- The possible evolutions of trust.
- The centralization of the model.

4.1 Types of trust

The trust granted to an entity can be:

- *Direct trust*: based on historic relation with the entity
- *Recommendation trust*: based on the recommendation of a third party concerning the entity's behaviors.

Direct trust is essential to a majority of models. Based on its experiences with other entities, an entity can decide to cooperate with them. But direct trust is not sufficient. MANETs are a complex environments and evolve constantly, their members change and the number of member may be large. An entity should therefore be able to place its trust in others through one or several recommendations obtained from third parties. The problem of recommendation trust is more complex than that of direct trust. In the simplest case, trust in an entity can be assumed if there is a recommendation from somebody in whom we have direct trust. In more complex cases, trust can be calculated according to the experiences for which the recommendation holds. That helps in determining more precisely the range of trust in the recommended entity.

4.2 Representation of the trust

In certain trust models, reputation is used to determine trust between entities. Supposing that an entity *A* trusts an entity *B* for achieving a particular service, data transfers, for example. In this case, *A* can say that *B* has a reputation of being reliable in transferring data. Reputation can be deduced from behaviors of an entity in past occasions.

In order to represent reputation or trust, a model can use a binary representation or a degreed representation. The first one allows to represent only two states: complete trust or no trust at all. This representation is simple and avoids ambiguous interpretations. It is used in many implementations: X509, SPKI,... However, it is sometimes too restrictive. Since the trust accorded to an entity may not be complete but sufficient for cooperation.

In degreed trust, there are more than two states of trust. The degrees of trust can be discrete or continuous.

Considering the presentations of trust in Maurer-D [12] or PGP [13], trust is represented by discrete degrees. PGP uses public key cryptography to encrypt electronic mails and uses a graph based approach of trust to certify public keys. Trust in PGP is certainty that a public key belongs to a specific individual. There is no certificate authority that is trusted totally and signs all public keys. Instead, individuals sign public key for others and progressively establish a web of public key, which is interconnected by signatures. An individual *P* trusts the public key of an individual *Q* (*P* does not know *Q*) if it is signed by individuals (introducers) which are trusted by *P*. The level of trust granted to an entity is function of the number of recommendation it has and who we got them from (their introducers). Various degrees of trust can be granted to a public key. They are categorized in PGP as follows:

- *Undefined*: we cannot say whether this public key is valid or not.
- *Marginal*: this public key may be valid be we cannot be too sure.
- *Complete*: we can be wholly confident that this public key is valid.
- *Ultimate*: the public key owners construct locally.

Levels of trust are granted to introducers:

- *Full*: recommendations from this introducer are always trusted.
- *Marginal*: recommendations from this introducer are only trusted partially.
- *Untrustworthy*: recommendations from this introducer are not trusted.
- *Unknown*: this introducer is not known.

Some models adopt a finer representation of trust and represent it by a continuously evolving value. This value represents the probability that the concerned entity collaborates correctly. Trust may be the result of a reasoning based on objective events or subjective beliefs: we talk about subjective logic and objective logic.

In the case of MANETs, a degreed representation seems more suitable. Indeed, cooperation in MANETs is various, it is realized for different purposes and does not necessarily need to use the highest levels of trust at all times. Using a degreed representation, entities have more chances to cooperate and complete their tasks. Furthermore, with this representation, the security policy of MANETs can be specified more precisely by fixing necessary thresholds of trust to carry out different types of cooperation.

4.3 Evolution of trust

Evolution of trust is made up of two main phases:

- The initial trust formation phase: this phase allows initialization of the trust granted to an entity
- The revision phase: this phase updates the trust in others.

The initial trust formation phase In this phase, an entity initializes its trust in others. It can be described by user defined assertion or automatically computed by an algorithm.

PGP is an example of manual description of initial trust. The user specifies the degree of trust he has in an introducer. This trust determines how recommendations from this introducer should be considered.

Concerning the automatic formation, it can be constrained or not.

Without constraints, trust is safely based on recommendation. For example, in [12], an entity places its trust in others when a trust derivation rule is satisfied. The general rule is that, for all $i \geq 1$, *P* trusts *Q* level *i*, if *R*, whom *P* trusts with level $i + 1$, makes a recommendation for *Q*. The formal description is as follows:

$$\forall Q,\, R,\, i \geq 1 \,:\, Aut_{P,R},\, Trust_{P,R,i+1},\, Rec_{R,Q,i} \vdash Trust_{P,Q,i}$$

where *Aut* is the statement for *P*'s belief in the authenticity of *R*'s public key, *Rec* indicate the recommendation, and *Trust* is the statement indicating trust.

With constraints, the deduction allowing to grant trust to an entity is restricted by constraints. For instance, [14] defines the Time-To-Live constraint as the maximum length of the recommendation chain.

In X509, in the case of certification authority system, the constraints are the certificates' extension fields, which allow to limit the number of accepted certificates.

The revision phase Trust in an entity is not constant, it evolves in its life. The variation of the degree of trust depends on many factors: experiences of the entity, the context in which it evolves. Trust evolves when:

- The entity realises that the value of trust it possesses is inaccurate
- Another entity seems to be better than the presently most trusted.

Trust among entities can be function of experiences among them. Reagle Jr. [15] proposes a model to manage reputation between sellers and buyers in an electronic commerce system. The evolution of reputation is based on the most recent experience between agents. It is simply a change from trust to distrust and leads to an interruption of interactions with the suspected agent.

BBK [10] uses positive and negative experiences to make trust evolve. Direct trust exists if there are no negative experiences with the entity in question.

These models use a simple variable to represent the value of trust in order to save memory. This is not sufficient for determining the coherence between the most recent

experience with the entity and its activities in the past. Jøsang [16] proposes an approach based on knowledge to represent more information. This approach needs more resources.

The information used and the way it is represented depend on the application of the trust model and on available resources. In fact, the more effective the model, the more resources it consumes. A balance between these factors needs to be found.

4.4 Centralization of trust model

Recommendations may come from different sources. In some cases, recommendation comes from a central network entity (a user, an organization,...) which all members trust: X509 is an examples. All members trust the Certificate Authorities' (CA) public key and only recommendations originating from the CA are accepted. In such a centralized model, trust in entities depends on a limited number of network entities: the CAs. If the appropriate CAs are not available, trust in some entities can not be calculated. In other cases, network entities can use recommendations from any entities they trust. This is the case in PGP's web of trust. A member in system can trust and choose anyone as a introducer. Since then, he will believe in recommendations of this introducer. That is suitable for activities in evolutionary environment. The lack of central point in ad hoc network leads to the need of such a distributed trust system, in which entities can get recommendation from several sources. A trust model for ad hoc network should thus rely on a totally decentralised model.

Table 1. Characteristics of existing trust models

Model	Type		Representation		Evolution				Centralized
					Logic		Initial formation		
	Direct	Recom.	binary	degree	Subj.	Obj.	no contrs.	with contrs.	
BBK[10]	×	×		×	×		×	×	×
Jøsang [16]	×	×		×	×		×	×	×
Marsh[17]	×	×		×	×			×	×
Maurer-D[12]		×	×		×		×	×	×
PGP[13]	×	×		×	×			×	
SPKI [18]	×	×	×		×		×	×	×
X509 [19]	×	×	×				×	×	×
Sierra [20]	×	×	×				×	×	×
Poblano [21]		×		×		×	×		×
Model proposed	×	×		×	×	×	×	×	

The efficiency and the application context of a trust model depend on its characteristics. In table 1, we summarize the characteristics proposed by existing models and propose a list of characteristics that should, from our point of view, be implemented by a trust model for MANETs.

5 Conclusion and future works

In this paper, we have presented MANETs, and certain aspects concerning their security. We have also shown how trust concept is necessary for improving the security in MANET, which characteristics existing trust models have. Finally, we have identified aspects, which, in our opinion, should be implemented in a trust model wireless for MANETs. This model should have the following characteristics:

- Model both direct trust and recommendation trust.
- Use a degreed representation of trust. A binary representation is insufficient for the complex environment of MANETs.
- The initial trust formation should be automatic and manual. Trust must be evolutionary. This requires knowledge about objective logic and subjective logic.
- Support a distributed system in which entities can get recommendations from different sources.

This work is only the preliminary phase in the establishment of a trust model adapted to the nature of MANETs. One of the factors we will particularly focus on, will be the decentralized nature of the model. In the next step of our work, we plan to fully specify the model and see if it can be adapted to deal with other types of distributed applications such as multi agent systems in which trust is also an important issues.

Acknowledgement

The work of Mr. Chung Tien NGUYEN is supported by a scholarship from *Conceil Général du Maine et Loire, France*.

References

1. Meissner, A., Musunoori, S.B.: Group integrity management support for mobile ad-hoc communities. In: Middleware Workshops. (2003) 53–59
2. Shen, C.C., Jaikaeo, C., Srisathapornphat, C., Huang, Z.: The guerrilla management architecture for ad hoc networks. Proceedings of IEEE MILCOM, Anaheim, California, USA (2002)
3. Zhang, Y., Lee, W.: Intrusion detection in wireless ad-hoc networks. In: Proceedings of the 6th annual international conference on Mobile computing and networking. (2000) 275–283
4. Percher, J.M.: An Intrusion Detection Model for Wireless Ad Hoc Networks (in French). PhD thesis, Universit de Versailles (2004)
5. Nekkanti, R.K., wei Lee, C.: Trust based adaptive on demand ad hoc routing protocol. In: Proceedings of the 42nd annual Southeast regional conference. (2004)
6. Dewan, P., Dasgupta, P.: Trusting routers and relays in ad hoc networks. 2003 International Conference on Parallel Processing Workshops (2003) 351
7. Prax, J.Y.: The role of trust in collective performance. In: Manual of Knowledge Management - A Second Generation Approach. (2003)
8. Gambetta, D.: Can We Trust Trust? In: Trust: Making and Breaking Cooperative Relations. Department of Sociology, University of Oxford (2000) 213–237

9. Dasgupta, P.: Trust as a Commodity. In: Trust: Making and Breaking Cooperative Relations. Department of Sociology, University Oxford (2000) 49–72
10. Beth, T., Borcherding, M., Klein, B.: Valuation of trust in open networks. In: Proc. 3rd European Symposium on Research in Computer Security – ESORICS '94. (1994) 3–18
11. Mui, L., Mohtashemi, M., Halberstadt, A.: A computational model of trust and reputation. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 7. (2002)
12. Maurer, U.: Modelling a public-key infrastructure. In: ESORICS: European Symposium on Research in Computer Security, LNCS, Springer-Verlag (1996)
13. Abdul-Rahman, A.: The pgp trust model. EDI-Forum: the Journal of Electronic Commerce (1997)
14. Joseph, S.: Neurogrid: Semantically routing queries in peer-to-peer networks. In: Revised Papers from the NETWORKING 2002 Workshops on Web Engineering and Peer-to-Peer Computing, Springer-Verlag (2002) 202–214
15. Reagle, J.: Trust in a cryptographic economy and digital security deposits:protocols and policies. Master's thesis, University of Maryland Baltimore County (1996)
16. Jøsang, A.: The right type of trust for distributed systems. In: Proceedings of the 1996 workshop on New security paradigms, ACM Press (1996) 119–131
17. Marsh, S.: Formalising Trust as a Computational Concept. PhD thesis, Department of Mathematics and Computer Science, University of Stirling (1994)
18. Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., Ylonen, T.: Spki certificate theory. RFC 2693 (1999)
19. Housley, R., Ford, W., Polk, W., Solo, D.: Internet x.509 public key infrastructure certificate and crl profile. RFC 2459 (1999)
20. OpenPrivacy: (Sierra: An openprivacy reputation management framework) OpenPrivacy projects.
21. Chen, R., Yeager, W.: Poblano: A distributed trust model for peer-to-peer networks. Sun Microsystems (2001)