Received 8 May 2008
Revised 20 September 2008
Accepted 20 October 2008

A review of trust modeling in *ad hoc* networks

Marcela Mejia and Néstor Peña
University of the Andes, Bogotá, Colombia, and
José L. Muñoz and Oscar Esparza
Technical University of Catalonia, Barcelona, Spain

Abstract

Purpose – Mobile *ad hoc* networks rely on cooperation to perform essential network mechanisms such as routing. Therefore, network performance depends to a great extent on giving participating nodes an incentive for cooperation. The level of trust among nodes is the most frequently used parameter for promoting cooperation in distributed systems. There are different models for representing trust, each of which is suited to a particular context and leads to different procedures for computing and propagating trust. The goal of this study is to analyze the most representative approaches for mobile *ad hoc* networks. It aims to obtain a qualitative comparison of the modeling approaches, according to the three basic components of a trust model: information gathering, information scoring and ranking, and action execution.

Design/methodology/approach – The paper identifies the different tasks required by a trust system and compares the way they are implemented when the system model itself is based on information theory, social networks, cluster concept, graph theory and game theory. It also provides a common nomenclature for the models. The study concentrates exclusively on the trust models themselves, without taking into account other aspects of the original articles that are beyond the scope of this analysis.

Findings – The study identifies the main components that a trust model must provide, and compares the way they are implemented. It finds that the lack of unity in the different proposed approaches makes it difficult to conduct an objective comparison. Finally, it also notices that most of the models do not properly manage node reintegration.

Originality/value – The best of our knowledge, the study is the first that uses information scoring and ranking as classification key. According to this key, approaches can be classified as based on information theory, clusters and social network theory, and cooperative and non-cooperative game theory. It also provides a common nomenclature for all of them. Finally, the main contribution of the paper is to provide an analysis of the most representative approaches and present a novel qualitative comparison.

Keywords Trust, Information modelling, Cluster analysis, Social groups, Networking, Game theory

Paper type Literature review

The authors would like to thank the anonymous reviewers' valuable comments and suggestions on the improvement of this article.

This work was partly supported by the Colombian Institute for Science and Technology Development, Colciencias, Universidad Nueva Granada and Universidad de los Andes, in Colombia, as well as the Spanish Government through projects CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", TSI2007-65393-C02-02 "ITACA" and TSI2005-07293-C02-01 "SECONNET", and by the Government of Catalonia under grant 2005 SGR 01015 to consolidated research groups.

Internet Research
Vol. 19 No. 1, 2009
pp. 88-104

1066-2243
DOI 10.1108/10662240910927849

I. Introduction

Mobile *ad hoc* networks (MANETs) allow wireless nodes to establish *ad hoc* communications. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multi-hop topologies. Therefore, network performance depends to a great extent on node cooperation. In fact, due to the lack of infrastructure, each single device within the network is required to be operational and efficient. Besides using the network resources, each node also contributes to the network's operation, so that the greater the cooperation, the better the performance. For example, a recent study shows how cooperation in *ad hoc* networks could affect performance across the TCP/IP protocol stack (Conti *et al.*, 2004). Thus, it is important to encourage node participation in essential network functions such as routing, distributed information storage and processing, distributed authentication, intrusion detection, and selfish node identification.

This article is focused specifically on trust models for promoting cooperation in *ad hoc* networks and it analyzes the most recent research in this area. Other reviews about cooperation in MANETs analyze general aspects of cooperation in different systems. For instance, Marias *et al.* (2006) classify cooperation enforcement schemes in two groups: reputation-based, such as CONFIDANT (Buchegger and Le, 2002), CORE (Michiardi and Molva, 2002), SORI (He *et al.*, 2004) and OCEAN (Bansal and Baker, 2003); and credit-based, such as SPRITE (Zhong *et al.*, 2003), TOKEN (Yang *et al.*, 2002) and VCG (Anderegg and Eidenbenz, 2003). The authors compare these schemes, taking into account six aspects, namely:

(1) class (reputation or credit);

(2) robustness against misleading nodes;

(3) robustness against collusion;

(4) first-hand and second-hand observations;

(5) cryptographic authentication; and

(6) promiscuous observation mechanism.

Laniepce *et al.* (2006) surveys reputation mechanisms that use a monitoring system to overhear the next hop node, as a way to watch behavior inside the neighborhood. The authors identify and analyze four unsolved problems in this type of system, and suggest that a better network-monitoring mechanism is needed to design better reputation systems.

In this article, we identify the main tasks required by a trust model and study how different proposals implement these tasks. Consequently, our study concentrates exclusively on the trust models themselves, without taking into account other aspects of the original articles that are beyond the scope of this article. Our study differs from others in that we propose a model-oriented classification, that is to say, our study is the first that classifies the proposed trust models according to the mechanism they use to calculate the level of trustworthiness. Finally, we identify the different tasks required by a trust system and compare the way they are implemented when the system model itself is based on information theory, social networks, cluster concept, graph theory and game theory. We also provide a common nomenclature for the models. Marias *et al.* (2006) concluded that trust models should be evaluated under a common scenario and Laniepce *et al.* (2006) pointed out that a common simulation setup needs to be defined

to make a quantitative comparison. We conclude that the lack of unity in the different proposed approaches, especially in their assumptions and configuration parameters, makes it difficult to conduct an objective comparison. This seems to lead to a definite research path for future work.

The rest of the article is organized as follows. Section II defines what a trust model is and describes its components. Section III classifies the different approaches. Section IV analyzes the main trust models by means of comparison tables and shows how each approach implements the trust model components. Finally, Section V concludes the article. In order to facilitate the understanding of this document, we have unified the nomenclature and adopted that used by Sun *et al.* (2006).

II. Trust model

In a trust model, an entity called the subject (S) commends the execution of an action (a) to another entity called the agent (A), in which case we say that $T\{S: A, a\}$ is the trust level that S has for A with respect to the execution of action a (Sun *et al.*, 2006). This trust level varies as the entities interact with each other; i.e. if agent A responds satisfactorily to subject S, S can increase the trust level $T\{S: A, a\}$. However, if the subject is disappointed by the agent, the corresponding trust level could decrease by a certain amount or even become the state of no trust at all.

A trust model refers to the conceptual abstraction on which to build mechanisms for assigning, updating and using trust levels between the entities in a distributed system; i.e. the trust model provides the basis for implementing the distributed tools that allow a trust relationship to be established with some degree of credibility among two or more entities for a given action. In this sense, a trust model is a tool for helping the subject of a distributed system to select a reliable agent with which to make transactions, from several agents offering a service.

To make this selection, the trust model should provide the mechanisms needed for each entity to collect information about the behavior of each other entity, then qualify and rank the other entities according to the trust placed in them, and finally execute an action according to the results obtained (Marti and Garcia-Molina, 2005). We analyze these three mechanisms in detail below:

(1) Gathering information on the behavior of each agent. This is the first component in any trust model. The information collected here is subsequently used to determine the degree of confidence that each subject can have in each agent. Within this task, three important aspects should be considered:

- *Sources of information*. These are the different ways in which a subject can obtain knowledge about the behavior of the agents. In the case of an *ad hoc* network, we divide these sources into three types:
  - Personal experience: each node can monitor other nodes within its reception range and, thus, learn about their behavior with regard to the different actions executed in the network.
  - One-hop trusted peers: if the agent is out of the reception range of the subject, the latter asks all its trusted nodes within one hop about their level of trust in this agent, if any.
  - Multiple-hop trusted peers: a trust chain is established, in which the subject asks its trusted peers whether they know the agent and their

trust level in this agent. These nodes can propagate the question until one, some or all the nodes that know the agent have given their references.

- *Validity of the opinions*. All the information collected should be weighted according to its source. Thus, information received from a fully trusted source will have greater validity than that received from a non-reliable node. The weight given to the collected information will be uniform, if all the sources are assumed to be equally reliable.
- *Strangers management*. Nodes are constantly entering and leaving an *ad hoc* network. Some of these nodes may be completely unknown to the network, i.e. they have not had prior interaction with any other node in the network and thus they do not have any history record. Therefore, a mechanism is needed to establish policies for dealing with these unknown nodes. Such policies are very important. If a pessimistic policy is adopted, unknown nodes will be ignored and will never be given the opportunity to initiate a history record. In contrast, if an optimistic policy is adopted, any newcomer can become part of the network, facilitating the entrance of malicious nodes. In addition, it is very important to have a persistent identifier system in order to associate a history of behavior with a particular agent, in such a way that the network mitigates attacks like spoofing or whitewashing (Marti and Garcia-Molina, 2003, 2005).

(2) Reputation scoring and ranking based on the degree of trust, as determined by the policies established for the system. In this phase, a qualification should be computed for each node, according to the assigned weights during the opinion validation in the previous phase. If several peers within the allowed qualification threshold all offer the same service, they should be sorted from greater to lower degree of trust to facilitate the subject's selection process. The qualification can be computed in different ways, as shown below in the description of the selected models.

(3) Taking the intended action according to the results obtained in the two previous steps. In this phase, the interacting peer is chosen and incentives are offered to encourage cooperation within the network. For example, while the best network resources can be allocated to nodes that fully contribute, non-cooperative nodes can be punished. Punishment can range from a warning notice to total isolation from the network.

III. Selected trust models

As explained in the previous section, a trust model has three basic components: information gathering, information scoring and ranking, and action execution (Marti and Garcia-Molina, 2005). In the literature, several trust models have been proposed to improve the performance and security of *ad hoc* networks. Proposed models have different mechanisms to obtain information scoring and ranking, that is to say, different ways of computing the trust level. A wide range of computation mechanisms not only lead to differences in simplicity, sensitivity, and numerical interpretability of trust values, but they also make the comparison among different approaches difficult.

Taking into account the previous discussion, we analyze and classify the diverse approaches in the literature.

For the sake of clarity, we have chosen a sample approach of each type to obtain a qualitative comparison of the different modeling approaches. We have selected samples that define the three basic components (we did not consider partial works). Among them, we chose the ones that provide the most complete and clear information about the trust model.

Below, we provide the classification of the related work regarding information scoring and ranking:

- Information theory – the selected sample work is Sun *et al.* (2006), but there are other works of this kind (Sun *et al.*, 2005; Liu *et al.*, 2008; Hongjun *et al.*, 2008).
- Social networks theory – the selected sample work is Ngai and Lyu (2006), but there are other works of this kind (Balakrishnan *et al.*, 2007; Haghpanah *et al.*, 2007; Li *et al.*, 2004; Pai *et al.*, 2007; Pirzada and McDonald, 2004; Repantis and Kalogeraki, 2006; Zouridaki *et al.*, 2005).
- Clustering – the selected sample work is Buchegger and Le (2002), but there are other works of this kind (Elhdhili *et al.*, 2008; Liu *et al.*, 2004; Meng *et al.*, 2008).
- Graph theory – the selected sample work is Sherwood *et al.* (2005), but there are other works of this kind (Theodorakopoulos and Baras, 2004, 2006).
- Non-cooperative game theory – the selected sample work is Seredynski *et al.* (2007), but there are other works of this kind (Jaramillo and Srikant, 2007; Komathy and Narayanasamy, 2007; Michiardi and Molva, 2003; Wrona and Mähönen, 2004; Yan and Hailes, 2008).
- Cooperative game theory – the selected sample work is Baras and Jiang (2006), but there are other works of this kind (Michiardi and Molva, 2003; Zhong and Wu, 2007).
- Computational intelligence (Hang *et al.*, 2008; Jiang and Baras, 2004; Kane and Browne, 2006; Sabater and Mir, 2003).

As we mentioned in the previous sections, there are other classifications in the literature. But to the best of our knowledge, our study is the first that uses information scoring and ranking as classification key. In the rest of this section we describe the selected models. They are then qualitatively compared in section IV.

A. Trust model based on information theory

Sun *et al.* (2006) proposed a trust model that uses information theory to obtain a quantitative measurement of trust and its propagation through the *ad hoc* network. The model works as follows.

Let us assume that subject A wants to send a packet that must be securely routed through the network, and agent B is able to participate in the routing process, since the routing protocol discovers it as part of a possible route. In the proposed scheme, for secure routing, a trust relationship should be established between A and B. To achieve this, each node (subject) of the *ad hoc* network should build, maintain and update a trust table, a recommendation buffer and an observation buffer. The trust table registers the subject's confidence that the agent will route the packets adequately. This level is computed as a function of the entropy of the probability with which the subject

believes the agent will perform the routing action. The observation buffer registers the information obtained through the subject's personal experience of the behavior of nodes within its reception range. The recommendation buffer maintains the information received from nodes at multiple hops that have had direct interaction with the agent and have trust values above a given threshold. Nodes whose confidence level is below a specific threshold will be marked as malicious nodes and kept in a list that will enable them to be isolated from the network. This model involves four axioms that must be satisfied during the computation of trust as it propagates over the network:

(1) uncertainty is a measure of trust, i.e. the concept of trust describes the certainty of whether the agent will perform an action, in the subject's opinion;

(2) concatenation propagation of trust does not increase trust, i.e. when the subject establishes a trust relationship with the agent through recommendation from a third party, the trust value between the subject and the agent should not be more than the trust value between the subject and the recommender as well as the trust value between the recommender and the agent;

(3) multipath propagation of trust does not reduce trust, i.e. if the subject receives the same recommendations for an agent from multiple sources, the trust value should be no less than when the subject receives less recommendations; and

(4) trust based on multiple recommendations from a single source should not be higher than that from independent sources, i.e. when the trust relationship is established jointly through concatenation and multipath trust propagation in such a way as to have multiple recommendations from a single source, the trust built on these correlated recommendations should not be higher than the trust built upon recommendations from independent sources.

Based on these axioms, the authors also present a distributed system for building, maintaining and updating the trust tables associated with the observed behavior and the recommendations originating from other nodes.

B. Trust model based on social networks

Buchegger and Le (2002) proposed a trust system based on social networks, namely CONFIDANT (cooperation of nodes: fairness in dynamic *ad hoc* networks). The CONFIDANT protocol works as an extension of a reactive source-routing protocol for mobile *ad hoc* networks. It improves network performance by making misbehavior unattractive, as it detects and isolates badly-behaved nodes and gives incentives to well-behaved nodes for correct forwarding. CONFIDANT consists of four components that are present in each node:

(1) the monitor to allow each node to watch the behavior of surrounding nodes, in order to detect unusual actions;

(2) the reputation system to evaluate nodes' routing and forwarding behavior by rating their performance;

(3) the path manager to take the best decision for the whole network, by avoiding paths that include malicious nodes; and

(4) the trust manager to control the incoming and outgoing alarm messages that warn against malicious behavior from any node.

These four elements interact as follows: the monitor system is used for each node to watch behavior in its neighborhood. If suspicious activity is detected, the reputation system is informed, in order to update and analyze the aggressor's node history. If the aggressor's bad behavior exceeds a threshold, its rating is updated and this information is passed to the trust manager and the path manager. The trust manager warns other nodes by sending an alarm message and the path manager removes all routes containing the aggressor node. This whole process is performed when the report generating node is fully trusted or when several nodes report the same situation.

C. Trust model based on clusters

Ngai and Lyu (2006) proposed a distributed public key authentication service using both a network model and a trust model that stop nodes from receiving false public keys from malicious nodes.

The network model divides the nodes into symmetrical clusters by means of a modified Max-Min D-cluster algorithm (Amis *et al.*, 2000), in such a way that the nodes can directly monitor their neighbors' behavior inside the cluster. For the trust model, each node maintains a table with quantitative values that represent the trust level of each node. The table can be updated by either direct monitoring of cluster neighbors, or by recommendations received for out-of-cluster nodes. For these recommendations, every node can certify any other node based on its trust table.

In this scheme, authentication is carried out through certificates signed by a group of trusted nodes, called introducers. If a node s requires the public key of another node t, s must request the public key certificate, signed by n introducers who are selected by having the greatest trust level in node s' table, as in a threshold cryptography scheme. These nodes will respond to s with t's public key certificate and with the trust level they have in t. This value will be used to compute the trust level of s in t. Node s can detect the malicious behavior of one of the introducers if its certificate does not agree with the certificate sent by the other n-1 selected introducers. After having filtered suspicious introducers, s can compute the trust value in t by means of a probabilistic relation among the recommendation values and its own trust in the introducers (Beth *et al.*, 1994). The value thus calculated is then placed in the trust table of s. If this value is higher than all the entries in the table, or if it is among the highest ones, t becomes an introducer. During an initialization phase, a special entity, called the dealer, appoints the first introducers before disconnecting itself from the network.

D. Trust model based on graph theory

Sherwood *et al.* (2005) describe a trust inference algorithm in terms of a directed and weighted graph T, called the Trust Graph. The vertexes of T correspond to the users in the system. The edge from vertex i to vertex j represents the confidence that node i has in node j, for which a quantitative value between 0 and 1 is assigned. Each new transaction can add a new directed edge to the trust graph or update the label of an existing edge with its new trust value. The subject gives this trust value to the agent from the qualification given to the transaction. This value is certified by a subject and handed to the agent after each transaction. This scheme was developed for a peer-to-peer network running cooperative applications, i.e. applications in which part of the node's resources are used by other nodes during the application operation time.

In the trust graph approach there are two ways for a node A to infer the qualification of a node B.

If A has had interactions with B, it simply looks at the corresponding edge label value between A and B in T. If there has not been any previous interaction between A and B, A should follow a path in T that goes from A to B in order to obtain the edge values and infer from these values the trust value in B. This can be achieved in two different ways: by using the strongest path or by averaging the weights among several of the disjoint strongest paths. In the first case, the trust value from A to B will be the lowest value among the edges of the strongest path. For example, in Figure 1 the strongest path is AEFB and the lowest value along the path is 0.8, so the trust from A to B is 0.8. In the second case, the two strongest disjoint paths are AEFB (0.8) and ACDB (0.6), which are weighted with the values of their first vertexes, $0.9/(0.9 + 0.6)$ and $0.6/(0.9 + 0.6)$ respectively, so the trust from A to B will be $(3/5)*0.8 + (2/5)*0.6 = 0.72$.

E. Trust model based on non-cooperative game theory

Seredynski *et al.* (2007) present a trust model based on node behavior and applied to the routing service in *ad hoc* networks. In this model, node behavior is based on game theory and the interactions among the nodes are represented as the prisoner dilemma. Each node uses a time-varying strategy that defines whether it should route or discard the packets. This strategy is based on the past behavior of the network (which is summarized in the current value of payoff) and in the trust level in the node that generated the packet to be routed.

The trust model is comprised of four elements: a trust evaluation mechanism, a network model based on game theory, a strategy and a genetic algorithm to evolve the strategy.

In the trust evaluation mechanism, each node maintains a trust table based on the observed behavior of its neighbors. Thus, for example, if node B is observing node A, which is within its transmission range, it can know the number of packets that have been sent to A to be routed, pcs_A, and the number of packets that A has effectively sent, pcf_A. Therefore, B can compute the rate of delivery $f_r(B, A) = \text{pcf}_A/\text{pcs}_A$. With this rate, B can determine the trust level that B should have in A, as shown in Table I.

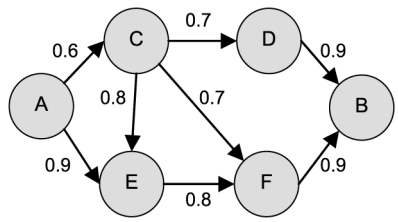

Figure 1.
Trust graph to compute $T\{A{:}B\}$

$f_r(B,A)$	$T\{B:A\}$	
1-0.9	3	Highest trust level
0.9-0.6	2	
0.6-0.3	1	
0.3-0	0	Lowest trust level

Table I.
Relation between delivery rate and trust level

In the network model based on game theory, each intermediate node that receives a packet should decide whether to route it or to discard it, according to its strategy. This strategy evolves through a genetic algorithm that aims to maximize the mean payoff. Once the game has finished, each participant receives a payoff according to the decision they took and to the source trust level they had. In this model, two types of nodes are defined: source nodes and intermediate nodes. Therefore, two types of payoff tables should be maintained, as shown in Tables II and III.

This scheme defines non-cooperative games, according to the way the authors model the network, as a set of independent nodes that takes decisions following their own strategy and without affecting the other nodes' decisions. The scheme encourages cooperation among all the nodes in the routing process through the incentives they receive (the higher the cooperation in routing, the greater the payoff; the greater the payoff, the higher the trust level; the higher the trust level, the better the assigned routes for its packets). Therefore, nodes seek to maximize their payoff in order to get better resources from the network when they need them.

F. Trust model based on cooperative game theory

Baras and Jiang (2006) model an *ad hoc* network as a group of nodes that interacts in order to offer and demand packet routing services. Since the routing service will be more efficient if every node cooperates, a system that encourages the nodes to cooperate should be implemented. The authors propose a scheme based on cooperative games, in which the nodes can form coalitions in order to maximize their payoff, in such a way as to obtain the best network performance, i.e. the best utilization of its resources. In the proposed model, each node i has a self-defined game strategy γ_i; a trust value t_i, which depends on the opinion expressed by the other nodes; and a payoff value x_i, obtained after each run. Figure 2 shows the interaction among the different elements of node i and their neighbors. The strategies are updated depending on the payoff: each node tends to select the strategy that maximizes its payoff. However, these strategies are negotiated among all the nodes that make up the coalition (the nodes with higher trust levels). Therefore, the model proposes the utilization of cooperative game theory, in which all nodes are allowed to negotiate and to use the agreed strategy. The received payoff depends on the contribution to the coalition (i.e. on whether node i opted or not for the agreed strategy) and on the trust level.

Table II.
Payoff table – source node

Transmission state	Payoff
Successful	5
Failed	0

Table III.
Payoff table – intermediate node

	Trust level			
Decision	$T = 3$	$T = 2$	$T = 1$	$T = 0$
Route	3	2	1	0.5
Discard	0.5	1	2	3

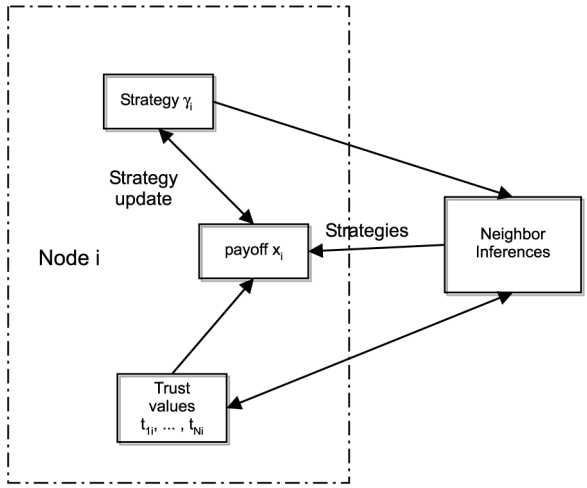

Figure 2.
Block diagram on the interactions between a node *i* and its neighbors

This model uses a feedback relation among the strategy, the payoff and the trust level, in such a way that a change in one of these elements affects directly the value of the other two elements. This encourages the contribution of nodes to the routing process, as each node will want to collaborate mostly with those nodes that have a high trust level, and the trust level will depend on how the neighbors perceive a node's behavior and its corresponding payoff. The proposed scheme is modeled as a discrete time system, in which the parameters' values depend on each other and on the behavior in the previous time.

IV. Comparison

This section includes a comparative analysis of the above models, emphasizing the methods utilized by each model to carry out the three tasks described in Section II, where the purpose is to help the subject to select the most appropriate agent with which to interact.

Table IV shows a comparison of the data collection task for each trust model. Each approach uses experience as the main data source, taking advantage of a characteristic of wireless networks, whereby all nodes can listen to the information transmitted within their reception range. However, four of these approaches also use references of neighbor nodes as an additional data source and, although each approach has a particular way of collecting and validating recommendations, the purpose is the same in every model.

With respect to the treatment given to new nodes entering the network, all approaches show a common factor in their policies. All of them determine some minimum trust level assigned to the new node and allow this value to change according to behavior. Thus, the new node can become part of the network, creating its own history record and collaborating with the distributed functions, or it can be isolated by its malicious or selfish behavior.

Table V shows the data qualification and sorting process for each model. In this particular task, we can appreciate a clear difference among the studied approaches. Each one uses different mathematical tools to quantify the trust level that a subject can have in a network agent for carrying out an interaction. The lack of unity becomes

Trust model approach	Gathering information		
	Information source	Opinion validity	Foreign management
1. Information theory	Personal experience, based on direct observations Recommendations are requested from trusted nodes at multiple hops that have had direct interaction with the agent	Recommendations are only requested from highly trusted nodes. The trust level is used to weight the recommendation in the qualification	In the range [−1, 1], a new node is assigned a value of 0. This value is updated according to its behavior
2. Social networks	Personal experience within the cluster. Recommendations are requested from introducers among clusters	This approach utilizes certificates, which are validated by the introducers through voting	A new node enters the cluster with the minimum trust level. This value is updated according to the mode's behavior
3. Graph theory	Personal experience Recommendations are requested from trusted nodes that have had direct interaction with the agent	In direct transactions, a credential containing the trust level is received. Otherwise, trust is inferred from edge values within the graph	New nodes have a default trust level, according to the applications Reference credentials are presented
4. Non-cooperative game theory	Personal experience based on direct observations	There are no recommendations. Trust is inferred from direct observations only	In the range [0, 3], a new node is assigned a value of 1. This value is updated according to the mode's behavior
5. Cooperative game theory	Personal experience (does the agent cooperate within the coalition?) Recommendations from K trusted neighbor nodes	Opinions are collected from k nodes and the trust level is adopted by majority of votes	Every node is assumed to be trusted. The mode's behavior can lead to its trust level being reduced

Table IV.
Gathering information

evident when trust in agents of a distributed system has to be determined and interpreted. Although each author presents his proposal as an efficient solution in the context of *ad hoc* networks, we are not aware of any quantitative comparative study that determines the relative advantages and disadvantages of each model, or the contexts in which some of them can perform better than others.

Finally, Table VI shows the action that is carried out in each trust model once the trust information has been qualified and sorted. The execution of an action is the last task within a trust model. The comparative table allows us to conclude that all the studied approaches have two aims when executing this action:

(1) to update the data tables in order to maintain a trust level that accurately reflects the behavior of the agents within the network; and

(2) to detect and isolate the nodes that negatively affect network performance.

Although all the approaches seek the same objectives, they differ in the method they use.

Trust model approach	Reputation scoring and ranking
1. Information theory	Trust is defined as a measure of uncertainty, for which its value is given either as a probability or as a function of the entropy of that probability. Trust propagation computation satisfies four basic axioms
2. Social networks	The trust level is computed by relating recommendations with direct observations
3. Graph theory	The value of an edge from node i to node j represents the trust level node i has on node j. Under direct interaction, the edge label is the trust level. Otherwise, a new graph is constructed with the interested nodes, and the trust level is computed as a function of the presented credentials (graph edges) and the requested references to trusted nodes that have had prior interaction with the agent
4. Non-cooperative game theory	Every node is initially assigned a trust value 1. A node receives a payoff every time it routes a packet. Trust level changes according to a feedback relationship among the strategy, the payoff and the trust level, in such a way that change in one of these elements directly affects the value of the other
5. Cooperative game theory	Every node is initially assigned a trust value 1. This value can be reduced to 0 or remain at 1, according to how much the node cooperates with the network. There is a feedback relationship among the strategy, the payoff and the trust level, in such a way that change in one of these elements directly affects the value of the other over time

Table V.
Reputation scoring and ranking

Trust model approach	Taking action
1. Information theory	Tables are updated according to direct observations and recommendations Nodes work only with those nodes within the trust threshold Malicious nodes are isolated
2. Social networks	Trust level is also reduced for nodes that sent erroneous recommendations Nodes below the threshold level are isolated
3. Graph theory	Trust tables are updated Credentials are generated Nodes with negative credentials are isolated
4. Non-cooperative game theory	Non-cooperative nodes are isolated Nodes receive incentives: the greater the cooperation, the better the routes Strategies are updated
5. Cooperative game theory	Non-cooperative nodes are isolated Strategies are updated Trust levels are updated according to the previous iterations, based on behavior rules

Table VI.
Taking action

V. Remarks and further work

After identifying the three basic components that should be provided by a trust model and obtaining a qualitative comparison of a representative set of proposals, it became evident the lack of unity in the different approaches in the literature; especially in their assumptions and configuration parameters, which makes an objective comparison difficult to conduct.

On the other hand, it is important to highlight the deficiency of some schemes in the management of node reintegration. Aspects such as energy level, monitoring misdetection or low link quality should be taken into account before isolating a node due to lack of cooperation. In this sense, nodes should be allowed to have transitory misbehaviors without compromising their willingness to cooperate. Thus, it is necessary to include mechanisms to allow nodes to return to the network after mitigating conditions. Some approaches use a threshold scheme so that when misbehavior exceeds the threshold, the related node is definitively revoked. If the threshold is not exceeded; the node is only penalized for the misbehavior. We should also consider other aspects apart from trust, such as resources availability, not to overwhelm trusted nodes when assigning distributed jobs among peer nodes. All these aspects show the lack of a common view in these systems and they also make difficult a quantitative comparison of the different approaches.

Regarding research activities for each analyzed approach, we have noticed some deficiencies that have to be overcome. For instance, the models based on information theory provide a promising theoretic framework but they are not directly implementable. The models based on clusters and social network require a dealer, but it is impractical to designate a dealer in such a highly distributed environment. The models based on non-cooperative game theory require a centralized evolution of the optimal strategies. This raises important concerns about who is going to compute the evolution and how long it will take to evolve an acceptable set of strategies. The models based on cooperative game theory use much bandwidth and computation resources for building and maintaining the coalitions. Finally, the models based on graph theory must efficiently manage computational complexity of graph analysis.

In our opinion, results for non-cooperative game theory models are promising. The goal is to achieve a distributed trust model adaptable to the highly dynamic conditions of MANET. However, this is only possible if optimal strategies can be found at nearly real-time by means of a distributed algorithm. To achieve this, we are currently working on a distributed genetic algorithm based on bacterial genetic mutation.

VI. Conclusions

In this article, we have identified three basic components that should be provided by a trust model:

(1) information gathering;

(2) information scoring and ranking; and

(3) action execution.

Then, we analyzed the most representative approaches for mobile *ad hoc* networks and we obtained a qualitative comparison of the modeling approaches according to the

basic components. Approaches can be classified as based on information theory, clusters and social network theory, and cooperative and non-cooperative game theory. The main contribution of our analysis is presented in Tables IV-VI. As conclusions from the analysis we can observe that all the approaches take advantage of promiscuous monitoring in the wireless network, which allows the node to use experience as its main data source. Some approaches also use experience of neighbor nodes as an additional data source. With respect to the treatment given to new nodes, a minimum trust level is assigned and then this value is increased or decreased according to the node's behavior. It is in the data qualification and sorting where clear differences between approaches can be appreciated since each approach uses different mathematical tools to quantify the trust level. Finally, the approaches in the literature have two purposes regarding the action that is carried out once the information has been qualified and sorted:

(1) updating the data tables in order to maintain a trust level that accurately reflects the behavior of the agents within the network; and

(2) detecting and isolating the nodes that negatively affect the network performance.

However, approaches differ in the method they use to carry out these actions. To conclude it is worth mentioning that we used and unified nomenclature for all the models and that we focused on the main drawbacks and potential advantages of each approach.

References

Amis, A., Prakash, R., Vuong, T. and Huynh, D. (2000), "Maxmin D-cluster formation in wireless *ad hoc* network", *Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings*, Vol. 1, IEEE, New York, NY, pp. 32-41.

Anderegg, L. and Eidenbenz, S. (2003), "*Ad hoc*-VCG: a truthful and cost-efficient routing protocol for mobile *ad hoc* networks with selfish agents", *Proceedings of 9th Annual International Conference on Mobile Computing and Networking*, pp. 245-59.

Balakrishnan, V., Varadharajan, V., Tupakula, U. and Lucs, P. (2007), "TEAM: trust enhanced security architecture for mobile *ad hoc* networks", *15th IEEE International Conference on Networks, ICON*, pp. 182-7.

Bansal, S. and Baker, M. (2003), *Observation-based Cooperation Enforcement in* Ad Hoc *Networks*, Technical Report, Stanford University, Stanford, CA.

Baras, J. and Jiang, T. (2006), "Cooperation, trust and games in wireless networks", in Boston, B. (Ed.), *Advances in Control, Communication Networks, and Transportation Systems*, SpringerLink, New York, NY, pp. 183-202.

Beth, T., Borcherding, M. and Klein, B. (1994), "Valuation of trust in open networks", *Proceedings of the Conference on Computer Security*, Springer Verlag, Berlin, pp. 3-18.

Buchegger, S. and Le, J. (2002), "Performance analysis of CONFIDANT protocol", *Proceedings of the 3rd ACM International Symposium on Mobile* Ad Hoc *Networking and Computing*, pp. 226-36.

Conti, M., Gregori, E. and Masselli, G. (2004), "Cooperation issues in mobile *ad hoc* networks", *Proceedings of 24th International Conference on Distributed Computing Systems Workshops*, IEEE, New York, NY, pp. 803-8.

Elhdhili, M., Azzouz, L. and Kamoun, F. (2008), "CASAN: clustering algorithm for security in *ad hoc* networks", *Computer Communications*, Vol. 31 No. 13, pp. 2972-80.

Haghpanah, N., Akhoondi, M. and Kargar, M. (2007), "Trusted secure routing for *ad hoc* networks", *Proceedings of the 5th ACM International Workshop on Mobility Management and Wireless Access*, pp. 176-9.

Hang, C., Wang, Y. and Singh, M. (2008), "An adaptive probabilistic trust model and its evaluation", *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems*, Vol. 3, pp. 1485-8.

He, Q., Wu, D. and Khosla, P. (2004), "SORI: a secure and objective reputation-based incentive scheme for *ad hoc* networks", *Proceedings of IEEE Wireless Communications and Networking Conference*, Vol. 2, pp. 825-30.

Hongjun, D., Zhiping, J. and Xiaona, D. (2008), "An entropy-based trust modeling and evaluation for wireless sensor networks", *International Conference on Embedded Software and Systems, ICESS*, pp. 27-34.

Jaramillo, J. and Srikant, R. (2007), "DARWIN: distributed and adaptive reputation mechanism for wireless *ad hoc* networks", *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking*, pp. 87-98.

Jiang, T. and Baras, J. (2004), "Ant-based adaptive trust evidence distribution in MANET", *Proceeding of the 24th International Conference on Distributed Computing Systems Workshops*, IEEE, New York, NY, pp. 588-93.

Kane, K. and Browne, J.C. (2006), "Using uncertainty in reputation methods to enforce cooperation in *ad hoc* networks", *Proceedings of the 5th ACM Workshop on Wireless Security*, pp. 105-13.

Komathy, K. and Narayanasamy, P. (2007), "Best neighbor strategy to enforce cooperation among selfish nodes in wireless *ad hoc* network", *Computer Communications*, Vol. 30 No. 18, pp. 3721-35.

Laniepce, S., Demerjian, J. and Mokhtari, A. (2006), "Cooperation monitoring issues in *ad hoc* networks", *Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing*, pp. 695-700.

Li, X., Lyu, M. and Liu, J. (2004), "A trust model based routing protocol for secure *ad hoc* networks", *Proceedings of IEEE Aerospace Conference (IEEEAC)*, pp. 1286-95.

Liu, Z., Joy, A. and Thompson, R. (2004), "A dynamic trust model for mobile *ad hoc* networks", *Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04)*, pp. 80-5.

Liu, Z., Yau, S., Peng, D. and Yin, Y. (2008), "A flexible trust model for distributed service infrastructure", *11th IEEE Symposium on Object-oriented Real-time Distributed Computing (ISORC)*, pp. 108-15.

Marias, G., Georgiadis, P., Flitzanis, D. and Mandals, K. (2006), "Cooperation enforcements schemes for MANETs: a survey", *Wireless Communication and Mobile Computing*, Vol. 6 No. 3, pp. 319-32.

Marti, S. and Garcia-Molina, H. (2003), "Identity crisis: anonymity vs reputation in P2P systems", *Third International Conference on Peer-to-Peer Computing*, pp. 134-41.

Marti, S. and Garcia-Molina, H. (2005), "Taxonomy of trust: categorizing P2P reputation system", *Computer Networks Science Direct*, Vol. 50 No. 4, pp. 472-84.

Meng, X., Zhang, G., Kang, J., Li, H. and Li, D. (2008), "A new subjective trust model based on cloud model", *IEEE International Conference on Networking, Sensing and Control, ICNSC*, pp. 1125-30.

Michiardi, P. and Molva, R. (2002), "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile *ad hoc* networks", *Proceedings of 6th IFIP Communication and Multimedia Security Conference*, Vol. 228, pp. 107-21.

Michiardi, P. and Molva, R. (2003), "A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile *ad hoc* networks", *Proceeding of the Workshop on Modelling and Optimization in Mobile,* Ad Hoc *and Wireless Networks*, pp. 3-5.

Ngai, E. and Lyu, M. (2006), "An authentication service based on trust and clustering in wireless *ad hoc* networks: description and security evaluation", *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Vol. 1, pp. 94-103.

Pai, S., Roosta, T., Wicker, S. and Sastry, S. (2007), "Using social network theory towards development of wireless *ad hoc* network trust", *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, pp. 443-50.

Pirzada, A. and McDonald, C. (2004), "Establishing trust in pure *ad hoc* networks", *Proceedings of the 27th Australasian Conference on Computer Science*, Vol. 26, pp. 47-54.

Repantis, T. and Kalogeraki, V. (2006), "Decentralized trust management for *ad hoc* peer-to-peer networks", *Proceedings of the 4th International Workshop on Middleware for Pervasive and* Ad Hoc *Computing*.

Sabater, J. and Mir, I. (2003), *Trust and Reputation for Agent Societies*, Monografies de l'Institut d'Investigació en Intelligencia Artificial, Bellaterra.

Seredynski, M., Bouvry, P. and Klopotek, M. (2007), "Modelling the evolution of cooperative behavior in *ad hoc* networks using a game based model", *IEEE Symposium on Computational Intelligence and Games*, pp. 96-103.

Sherwood, R., Lee, S. and Bhattacharjee, B. (2005), "Cooperative peer groups in NICE", *Computer Networks Science Direct*, Vol. 50 No. 4, pp. 523-44.

Sun, Y., Yu, W., Han, Z. and Liu, R. (2005), "Trust modeling and evaluation in *ad hoc* networks", *Global Telecommunications Conference GLOBECOM '05*, Vol. 3, IEEE, New York, NY.

Sun, Y., Yu, W., Han, Z. and Liu, R. (2006), "Information theoretic framework of trust modeling and evaluation for *ad hoc* networks", *IEEE Journal on Selected Areas in Communications*, Vol. 24 No. 2, pp. 305-17.

Theodorakopoulos, G. and Baras, J. (2004), "Trust evaluation in *ad hoc* networks", *Proceedings of the 3rd ACM Workshop on Wireless Security*, pp. 1-10.

Theodorakopoulos, G. and Baras, J. (2006), "On trust models and trust evaluation metrics for *ad hoc* networks", *IEEE Journal on Selected Areas in Communications*, Vol. 24 No. 2, pp. 318-28.

Wrona, K. and Mähönen, P. (2004), "Analytical model of cooperation in *ad hoc* networks", *Telecommunication Systems*, Vol. 27 Nos 2-4, pp. 347-69.

Yan, L. and Hailes, S. (2008), "Cooperative packet relaying model for wireless *ad hoc* networks", *Proceeding of the 1st ACM International Workshop on Foundations of Wireless* Ad Hoc *and Sensor Networking and Computing*, pp. 93-100.

Yang, H., Meng, X. and Lu, S. (2002), "Self-organized network-layer security in mobile *ad hoc* networks", *Proceedings of the 1st ACM Workshop on Wireless Security*, pp. 11-20.

Zhong, S. and Wu, F. (2007), "On designing collusion-resistant routing schemes for non-cooperative wireless *ad hoc* networks", *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking*, pp. 278-89.

Zhong, S., Chen, J. and Yang, R. (2003), "Sprite: a simple, cheat-proof, credit-based system for mobile *ad hoc* networks", *Proceedings of IEEE INFOCOM2003*, pp. 1987-97.

Zouridaki, C., Mark, B., Hejmo, M. and Thomas, R. (2005), "A quantitative trust establishment framework for reliable data packet delivery in MANETs", *Proceedings of the 3rd ACM Workshop on Security of* Ad Hoc *and Sensor Networks*, pp. 1-10.

Corresponding author
Marcela Mejia can be contacted at: am.mejia75@uniandes.edu.co