

TEAM in AE: Trust Establishment and Assessment Mechanisms in Autonomic Environments

Symeon Papavassiliou, Vassilis Karyotis, Vassiliki Pouli and Vassilis Merikoulias

Institute of Communications and Computer Systems (ICCS)

Network Management & Optimal Design Lab (NETMODE)

9 Iroon Polytechniou str., Zografou 15780, Athens, Greece

Tel: +30 210 772-2550 Fax: +30 210 772-1452 E-mail: papavass@mail.ntua.gr

1. Introduction

The proliferation and integration of communication networks in social life has increased the need for trusted systems of advanced and intelligent capabilities. Autonomic networks, which among others include mobile ad hoc networks (MANETs), mesh networks (essentially MANETs over 802.11), WLANs and peer-to-peer (P2P) systems, exhibit characteristics and properties like distributed operation, self-organization, self-optimizing, self-protection, self-healing, etc. Such systems are self-adaptable, in the sense that they can change themselves beneficially with no or limited human intervention. All network entities participate in network control through individual interactions. However, even if autonomic nodes are modeled as selfish, they are able to gain from collaboration or need to cooperate in order to implement basic networking operations (like packet multihop routing).

Irrespective of the specific scope of a network type (autonomic, wireless, core network, etc.) several mechanisms and operations require that nodes establish some type of communication among them, either for realizing collaboration or for implementing fundamental operations. At the same time, significant concerns have been raised for both cooperative and non-cooperative networks with respect to the security of such networks. Malicious nodes may exploit lack of cooperation to intelligently attack legitimate nodes individually, or they may exploit cooperation capabilities in order to fake identities and create various types of exploitations. Packet exchanges may no longer be as safe as they used to be in the past. Such issues may be exacerbated in networks that distributed operation and autonomic behavior is required, such as ad hoc, P2P, mesh and social networks. Environmental parameters might also perplex the situation, as it is the case in wireless networks (variable channel conditions, fast-fading, etc.).

The modern non-secure and dynamic networking environments call for separate mechanisms that can be used to ensure proper network access and validate the privileges of legitimate nodes. *More specifically, it is necessary to establish a framework under which legitimate nodes of a network will be able to negotiate and trust each other. According to the designated negotiation and trust mechanisms, legitimate behavior will be possible to be evaluated and permitted, while malicious operation will be realized and prevented.*

Based on the definition of trust as well as potential distributed cooperation among nodes in autonomic networks, the concept of roles can be developed - where nodes acquire permissions through their roles - and therefore we can create and define Dynamic Trusted Autonomic Networks (DTANs) based on several negotiated relations and parameters (such as security relations, charging, auditing, etc.).

Trust in autonomic networking cover both inter node - element as well as intra - node elements within a single node, and therefore trust involves both social "behavior" as well as cognitive abilities of networks elements and nodes. Such a consideration reveals that autonomic networks are closely related to the presentation of a social-like environment to the end user, and therefore a trust mechanism that allows for a broader acceptance of the overall autonomic networking framework and operations by the end users, is more a requirement rather than a desire.

The focus of this paper is on the relevant issues regarding the modeling, building and assessment of trust among nodes in autonomic networks. In the following, we first adopt, and then adapt when required, a properly defined framework that is able to accurately describe trust within the area of autonomic systems. In the sequel we outline several mechanisms for building and establishing trust in a distributed fashion, and describe trust assessment methods and potential applications in which such assessment methods could be realized. Finally, the issue of autonomic network and autonomic node trust by the end users is considered.

2. Trust Establishment Framework-Model

In general, trust management includes the collection, analysis and presentation of trust-related data, in order to make assessments and decisions regarding the trust relationships among various entities of a population. Especially for autonomic systems, the aforementioned procedures need to be distributed and oftentimes asynchronous in order to efficiently and transparently assess the evolution of the trustworthiness of the network. *Furthermore, autonomic behavior cannot be deterministically predicted (it depends on individual node behavior, the behavior of the rest of the population and in wireless systems on the environment as well), statistical approaches need to be taken into account in order to define a meaningful and accurate trust handling framework. Thus, trust management must be considered in a distributed and statistical manner.*

Trust can be interpreted as a set of relations among entities participating in network activities. In traditional wired (Internet) paradigms, trust is resolved in a centralized and hierarchical manner, where strategically-selected/placed trusted entities (trusted third parties) exist and users consult them directly or indirectly in order to obtain the required information about other users. On the contrary, nodes in autonomic networks are all peers, meaning that they all bear the same potential trust information. Operations have to be locally constrained to restrict the overhead, but at the same time they need to effectively and accurately reflect the trustworthiness of the network. *A coherent, mathematical, self-contained framework for trust is required to quantify all the aforementioned and allow the accurate design and analysis of trusted systems.*

An autonomous network can be modeled as a directed weighted graph $G(V,E)$, where nodes are the system entities and the edges represent direct trust relations between two peers. The weight of a link represents the degree of confidence from the one entity to the other (the latter being the one pointed by the directed link). Assuming a simple binary trust model, link weights may be -1 if a node does not trust another, 1 if a node trusts a neighbor and 0 denoting uncertainty, also depicted by the absence of a link. G may be coined as the trust graph, in order to be distinguished from the physical communication graph. This approach assumes that nodes have obtained through an appropriate method the values of trust for their neighbors. It is the work of trust building/assessment methods to specify such values. Here we focus on how local trust values are fused to obtain the trustworthiness of the network. Assuming $T=[t_1, t_2, \dots, t_N]$ is the actual trust vector, i.e. the vector with the actual trust values of the N network nodes, and $S=[s_1, s_2, \dots, s_N]$ the estimated trust vector, trust evaluation is the estimation of s_i by each node I , by aggregating the received trust information of neighbors. Due to communication and environmental constraints, the link weights c_{ij} become random variables. The evolution of S over time indicates the overall network trustworthiness and represents an accurate analytical model for the trust of the system.

3. Trust Building Mechanisms

In this section we touch upon the mechanisms that can be used for establishing trust in an autonomic network. Initially, we adopt and present a simple but powerful approach that is able to yield important results, followed by specific guidelines for designing trust-building mechanisms specifically for autonomic networks. Finally, we visit the area of reputation systems that is closely connected with trust and autonomic networks.

3.1 Trust Evaluation Mechanisms

In the following we assume that nodes are able to obtain information on trust about their neighbors and focus on how to fuse such information in a distributed and asynchronous manner. We are interested in methods leading to consensus on the trustworthiness of a network.

In autonomic networks all nodes are considered peers. Therefore, trust evaluation should take all available local information into account, by adopting a local aggregation rule, i.e. a simple local voting rule by using a linear weighted sum. Conflicting opinions about neighboring nodes can be resolved by using effective votes, namely the sum of the link confidences of a pair of nodes about each other. **Trust evaluation becomes a dynamic iterative process that evolves as the local interactions iterate throughout the network.** The result of each iteration is considered binary, in which a neighbor node is decided as trusted or not trusted. By employing a stochastic threshold rule for deciding each iteration, the trust evaluation mechanism becomes a stochastic voting rule that can be cast as a (reversible) Markov chain, the latter having a unique stationary distribution (Markov Random Field, MRF). The states of the chain are the possible configurations of S . Using the MRF's stationary distribution it becomes viable to analyze trust at the steady state. By that analysis, it was found that network topology greatly affects the performance of the system, especially as shortcuts and neighbors are added (on the average). The transition from regular lattices,

to random graphs through small-world structures improves the performance of the trust evaluation rule. Furthermore, emergence of phase transition phenomena in the trust evaluation rule calls for extensive analysis before applying distributed algorithms. In such systems with numerous local interactions, critical parameters need to be identified and properly handled.

In general, noting that the main steps of a generic trust building mechanism in autonomic environments are Monitoring, Interpretation, Computation, Decision-making, effective and usable rules may be realized and implemented among others via the concept of control loops, as described in the sequel.

3.2 Nodes/Networks Autonomy

Nodes/Networks autonomy is about implementing self-* functions for self-optimization and self-adaptation to context or situation driven behavior changes in the networking environment, services or applications. The fundamental concept of an autonomic system is a control loop(s). Inputs to the control loop consist of various status signals, information and views continuously exposed from the system, component(s) or resource(s) being controlled (e.g. protocols, nodes, functionalities, etc.), along with (usually policy-driven) management rules that orchestrate the behavior of the system or component.

Most of these features can be considered part of the term context, which refers to the environmental, and situational details surrounding the nodes involved in trust relationships. *Until now the interdependencies between the context and trust have not been sufficiently addressed, but as various threats are related to context awareness, the context information whenever available can offer opportunities to establish and manage the trust relationships more efficiently.* For example, the location or the role of a user can determine his degree of trust and the services he is authorized to access. One issue here is that context information has a personal character thus actions should be taken to securely protect the individual rights and privacy. Due to the fact that the context information can be used to improve the decision-making and trust-evaluation processes it should become input to the control-loops while outputs will be commands to the system or component(s) to adjust its operation, along with status to other autonomic systems or components.

3.3. Reputation (Trust within a set of nodes)

In contrast to trustworthiness, the reputation of a node is always defined among a set of nodes. It equally reflects the subjective views of a set of nodes. That is, although some nodes do not trust a specific node, it still can have a good reputation among a bigger set of nodes. In fact this could be the objective of a malicious node, and realizing such cases in actual scenarios is very critical for building secure and robust networks. *The problem here is how to aggregate the trust a set of nodes has in a trustee to derive the reputation. Reputation can especially be helpful if a node does not have enough experiences with another potential interaction partner to build its own trust estimate.* In these cases, the node can rely on the reputation value the potential partner has among the community.

Usually, reputation systems consist of two distinct mechanisms. The first one quantifies node trusts, producing essentially opinions about node neighbors and the second is the specific opinion aggregations mechanism. The most frequent approaches adopted for the second mechanism are voting schemes (majority or ranking voting), however several other alternatives, in which nodes cast opinions ballots for groups of nodes, have been proposed as well.

4. Trust Assessment Procedures

In an autonomic network where nodes, usually representing agents, are assigned a trust value we need to devise methods to quickly assess the establishment of trust so that one can quickly respond to the question of whether the correct trust values have been assigned to the correct nodes.

Considering a specific system model comprising of a network - with potentially good and bad nodes - we can study the properties of general evaluation rules and create evaluation rules feasible and realizable under different scenarios. We can then study these evaluation rules (e.g. local voting, statistical voting, statistical threshold decision making) in various network topologies and investigate what kind of network topologies have the best performance in terms of trust evaluation. Moreover, we can have different kinds of adversaries (bad nodes) and try to examine if the proposed strategies evaluate correctly the trust value of good and bad nodes.

Another intriguing method is the one where the trust evaluation is based on the combination of opinions from a specific group of nodes (usually neighbors) assumed to be pre-trusted. Such cases are already reality in contemporary

network services, such as the trusted third parties and the certificate authorities. Furthermore, some interesting methods for trust assessment are those that link a node's trustworthiness with the quality of the evidence the node provides based on local interactions, statistics from previous experiences, its neighbors' opinions, intrusion detection results and data values.

If the trust evaluation is associated with public key certificates then trust management systems should be developed (like PGP) that will check the validity of a public key and its trust level by checking for example how many keys have signed it. Due to the fact that there is no central trusted third party to store, sign and publish trust credentials, some issues arise, like where to find the appropriate credentials, where and how to store them safely while making their searching afterwards efficient and their distribution secure.

Realizing the above methods in real implementations such as random wireless networks or P2P systems can contribute significantly to the overall study of the trust mechanisms and demonstrate their applicability in specific application scenarios.

5. Dynamic Trusted Autonomic Networks (DTAN)

Based on the above trust establishment mechanisms a (trusted) security-based network structure for autonomic networks can be derived. ***Based on the combination of the concepts of trust and roles, where nodes are assumed to acquire permissions through their roles, nodes dynamically will create and/or belong to different communities, where certain levels of security will be assumed and certain actions will be permitted.*** Such an approach and respective trust model (framework) will enable a virtual security structure based on communities that are deployed by one or more users belonging to one trust-related category. ***In this structure, a secure relation amongst nodes is built on mutual trust between those, although, the trust level may vary, depending on their role.***

One conventional process that can be completely redefined based on this notion is the routing function, towards a multiple level secure routing mechanism. A different paradigm may include trust and distributed data sharing. In this case, data is distributed in multiple nodes exploiting redundancy, i.e. more than one nodes may have available the same piece of a larger file. Nodes wishing to access whole parts of information (data files) have to consider both the size as well as the integrity of the chunks they need to collect in order to obtain the correct information. A natural tradeoff arises in which nodes either get the larger parts on the cost that some of them might be corrupted (and thus a lot of resources were wasted for their receipt) or collect smaller but less wasteful chunks. Trust may be used to elevate this procedure to the level that trust values are assigned to the data chunks and once trust is established in the way it was described previously, nodes recover only the trusted ones, conserving valuable resources.

6. Social-based and End-User Trust in Autonomic Networks/Nodes

Dynamic autonomic network systems span multiple domains and many times include end user devices. In such systems no single entity can be expected to have full control and knowledge over the network. Such a network is expected to be ruled by a reduced trust between nodes and users. In order for this kind of networks to be usable and deliver a predicted quality of service to the users, trust and trust management mechanisms must be designed towards increasing trust among users and network elements. ***Therefore, trust is necessary not only for the operation of an autonomic networking environment, but for the adoption of such environment by the end users. The autonomic networking elements should be equipped with good reasons to trust the other elements (both inter and intra node) which they discover and interoperate with, and at the same time the end users of such elements and nodes should be able to trust the system as one entity and be assured that it will serve their purposes.*** Towards this direction the following issues should be considered:

A) How paradigms and solutions already applied in social networking, either web based social networks like facebook, goodread or application based P2P overlay networks, can be utilized into a pure autonomic environment?

B) Could trust models already developed by social science be infused into autonomic networking bringing such networks and infrastructures closer to the end user?

C) Could user interfaces techniques regarding human machine interaction developed and largely adopted by web users be utilized by autonomic networking in order to make these systems more trusted by the end users?