Trust and Security in Mission-Critical P2P through Information Flow Approach

Vijay Kumar
University of Missouri-Kansas City

1. Introduction

We propose a new type of P2P infrastructure which we refer to as Mission-Critical P2P (MC-P2P) system. It is *a set of fully functional peer nodes some of which are highly specialized in their functionality. MC-P2P = {P_1, Pp_2,…, P_∞)*; *where P_i's* are *fully connected peer nodes some of which could be highly specialized*. The information exchange between P_i and P_j ($i = j$ or $i \neq j$) is free from temporal and spatial constraints and can take place through wired and wireless medium without the mediation of any central or distributed servers [you93]. Each peer is associated with a peer-profile (P-profile) that, in addition to other useful information, defines the capability of the peer (specialized or general). We define *a capability set C_s* of a *MC-P2P system C_s = {C_1, C_2, …, C_m} where C_i is a capability of a peer Pi.* We also define *a minimum capability set of MC-P_2P as $C_{s\text{-}min}$ = minimum capability set which must be satisfied by a peer to be in the network. Thus for Pi and Pj to be peers $C_{Pi} \cap C_{Pj} \geq C_{s\text{-}min}$*. Since in *MC-P2P* a task may have special requirements (strict deadlines, location-dependent constraints, temporal constraints, etc.), the set of Specialized Peers (SP) controls the functions of the entire *MC-P2P* network. SPs work in collaboration with general purpose peers to complete the mission on time. We refer to these common peers as Dedicated Peers (DP) in this project. Thus, *MC-P2P* is a set of SPs and DPs where SPs play the role or Brokers or Super-peers. We define TDA (AFRL) surveillance system where a number of UAVs are networked together to monitor terrorist movement and take timely action and QED-2 (AFRL) as *MC-P2P*. Some monitoring components (UAVs, video cameras, etc.) are positioned permanently at fixed locations because of their location-dependent capability. We define *SP = {L/L, C_{SP}} where L/L represents geographical location in terms of Long and Lat and C_{SP} is the special capability of a SP.*

Unlike conventional P2P system, *MC-P2P* is not so ad-hoc because a subset of peers may not be allowed to power off or randomly leave and enter the network but others are free to behave in an ad-hoc manner. Because of the nature of the task, *MC-P2P* will have relatively more stringent trust and security requirements compared to conventional P2P network.

We define (a) global and (b) local trust categories where *Local trust $\subset$ Global trust*. Global trust must satisfy spatial and temporal properties. Local trust is associated with a peer and if the peer is mobile then it may have spatial trust or temporal trust or both. Spatial trust indicates location-dependent trust. For example, a surface vehicle cannot be trusted when it is in water. Similarly, in the case of temporal trust a peer can be trusted within a time frame. We define a basic trust which must be present in every peer: *Local trust $\cap$ Spatial trust = Basic trust*. A similar categorization has been presented in the work of [mar94] where it was stated that no-trust and distrust are different. There are a large number of reports on this issue; however, most of them relate to computer systems in general [bla94] and for P2P systems [ass03, bha02, wan03, zho03]. The case of no-trust does not exist in *MC-P2P*.

2. Our Objectives

Our goal here is to provide a trust infrastructure for MC-P2P systems. Such systems require extending trust past the user reputation that has been the primary focus to date. Our aim is to develop a trust establishment scheme that identifies if a peer wishing to join MC-P2P is trustworthy in performing its task including security. We will experiment with a few trust establishment schemes, such as Sanjay Madria's game playing approach that plays games specific to mission-critical tasks.

3. Universal Trust Set

Our aim is to develop a general trust model where we emphasize local sufficiency. We address the following issues.

- Identification and creation of UTS to include all parameters to define the capability of a peer.
- Identification and creation of an ontology of trust levels.
- Identification of trust levels that can be generated mutually and local trust.
- Reliable scheme for storing trust data and a scheme for verifying trust values of peers.
- Scheme for dissemination of trust values to other peers.
- Scheme for creation of a localized trust group.

We define a *Universal Trust Set* (*UTS*) = $\{e_1, e_2, \ldots, e_n\}$; where e_i is a trust parameter. A parameter is a characteristic of a peer. For example RAM size of a peer may be one of its e_i's. Our first task, therefore, is the identification of members of UTS, which will suffice for all P2P systems. Since a P2P could be highly heterogeneous, each peer would have its own subset drawn from UTS. Thus, the status (responsibility, contents, etc.) of a peer will be fixed or identified by the values of a subset of parameters drawn from UTS.

Development of Universal Trust Set: UTS is a finite set of relevant parameters for building trust on a peer [bea04]. The quality of UTS will depend on its member selection scheme. We propose to include different categories of parameters such as the geographical location of the peer, the user group of the peer, in case of a mobile peer its geographical movement domain, its past and present activity history, and so on. The UTS will select parameters from all possible real battle-front environments where a *MC-P2P* can exist. We argue that it would be useful to define an upper limit of UTS cardinality using some semantic analysis of UTS parameters. Thus, our algorithm will use a set of association rules to identify parameters that are (a) complementary, (b) related, and (c) dependent. We define a "Measure of Satisfaction (MoS)" which will help to identify the maximum cardinality of UTS sufficient for evaluating highest level of trust for a peer.

Development of Local Trust Set: We define a Local Trust Set (LTS) $\subset$ UTS for any new peer that joins the network. This approach takes care of the inclusion of any new node to P2P network. When a new node arrives, it presents its credentials and parameters values to the system. The system matches this set with UTS, creates a LTS for this node and computes its trust level. The creation of LTS will determine its inclusion into the network. Note that if an LTS for a new peer cannot be created, then it is obvious that it cannot be included in the P2P network.

We use LTSs of a pair of peers for establishing trust link. If $LTS\ (p_i) \cap LTS\ (p_j) = \varnothing$, then p_i and p_j may not create a trust link because p_i and p_j have nothing in common. We map a peer trust to the tree using its LTS for identifying its trust level. This mapping will also help to establish one sided or mutual trust link. If a pair of peers maps to the same level and to the same node of the tree, then they may be candidates for one sided or mutual trust link. A complete mapping (mapping of all nodes to the tree) will provide us a good sense of the state of all nodes and the state of P2P network. It is possible that the tree may shrink or expand, in which case the trust mappings will also change.

References

[asso3] Assedin, F., and Mahewsaran, M., 2003, Trust modeling for peer-to-peer based computing systems, Proc. Intl. Parallel and Distributed Processing Symposium.

[mar94] Marsh, S. 1994, Formalising Trust as a Computational Concept, PhD Dissertation, University of Stirling.

[bha03] Bhargava, B., and Zhong, Y., 2002, Authorization Based Evidence and Trust, in Proceedings of International Conference on Data Warehousing and Knowledge Discovery (DAWAK'2002), LNCS, Vol. 2454, France.

[wan03] Wang, Y., and Vassileva, J., 2003, Trust and reputation in peer-to-peer networks, Proc Third Intl Conference on Peer-to-Peer Computing (P2P'03), Linköping, Sweden.