

# Establishing Agreements in Dynamic Virtual Organizations

Tatyana Ryutov, Clifford Neuman, Li Zhou, Noria Foukia

Information Sciences Institute  
University of Southern California  
{tryutov, bcn, zhou, foukia}@isi.edu

## Abstract

*We present a framework that introduces key concepts relevant to agreement negotiation in Virtual Organizations (VO). The framework serves as a foundation for implementing an automated system that facilitates the establishment of VO agreements, considerably reduces the effort for setting up a VO and consequently reduces the VO's time for operation. The framework captures the relationship between the initial participants' behaviors, expectations, obligations and agreements, making sure that in implementing a system, one does not overlook the important aspects of the agreement structure and negotiation. The framework can be used to validate a negotiation, ensure validity of the achieved agreement and form strategies for future negotiations.*

*A novel aspect of the initial trust establishment described in this paper is the consideration of the effects of the participants' behaviors during the negotiation process on mutual trust.*

*We use the concepts to describe our work-in-progress for specification and negotiation of the agreements that govern the behavior of VO entities.*

## 1. Introduction

On-demand created and self-managed dynamic Virtual Organizations (VO) are becoming increasingly popular for achieving short-term objectives such as joint Distributed Denial of Service (DDoS) attack mitigation, and exploiting fast-changing market opportunities, such as collaborative product assembly [7]. A Virtual Organization is a temporary alliance of autonomous, diverse, and geographically dispersed organizations, where the participants pool resources, information and knowledge in order to meet common objectives.

In general, there are three stages of a VO lifecycle: [5][17] establishment, execution and dissolution. In this paper we are interested in the first stage that is characterized by setting up agreements on key aspects of the joint activity. We present a framework that introduces key concepts relevant to this stage.

Setting up a legally binding agreement under time constraints with insufficient information about other VO participants poses a significant obstacle to the establishment of VOs. There is a pressing need to develop an automated system that facilitates VO creation [12][17].

VO interactions involve significant social organizational issues, such as notions of trust, goal directed behaviors of VO entities, and unpredictable and dynamically evolving VO structures. Another concern is the need to understand and support the competitive or even adversarial interactions that are characteristic to e-business and inter-organizational interactions in general.

Only when these issues are better understood will it be possible to specify effective and well-formed rules of engagement and enforcement necessary to support the creation of a VO. To capture an expression of the social concepts, rules must have representation of normative and non-complying behaviors, member entitlements, obligations, and levels of trust that exist between members. Once such aspects are specified, it is easier to implement an appropriate infrastructure that guarantees a close conformance to the expected and desired behaviors.

We believe that the framework presented in this paper can be used to reason about these issues, making sure that in implementing a system, one is not overlooking the important aspects of agreement structure and negotiation. The framework serves as a foundation for

implementing an automated system that facilitates the establishment of VO agreements, considerably reduces the effort for setting up a VO and consequently reduces the VO's time for operation.

Traditional trust management solutions [2] do not adequately address dynamic aspects of trust. The pre-configured, coarse and static specification of trust in conventional systems is not consistent with human intuitions of trust [11], an individual's opinion of another entity that can evolve based on available evidence. Thus, trust relationships evolve over time and require monitoring and reevaluation. The dynamic and temporal nature of VOs present additional trust management challenges:

- temporary, as opposed to long lived, relationships present a major obstacle for trust development, since short term relationships promote "take and run" behavior;
- parties may not have pre-existing knowledge about one another, or any prior interactions with one another.

It is difficult to give an exact definition of trust due to its complex subjective nature. However, we believe that trust in VOs can be explicitly modeled using four concepts: expectations, obligations, agreements and suspicion levels.

Trust reflects beliefs (or *expectations*) an entity *a* has about entity *b*, that *b* will act in a certain way, based on information about *b*'s attributes (such as competence, technical capabilities, and skills) and/or recommendations from trusted entities [11]. Trust is inheritably linked to risk: trusting entity *a* is vulnerable if *b* does not fulfill *a*'s expectations.

*Obligations* represent the participant's commitment to provide a service under certain terms and conditions to other participant.

The concept of an *agreement* is used to make an explicit declaration of the expected behavior defined in the participants' obligations, and sanctions in the case of non-conformance to the obligations. Agreement monitoring and enforcement mechanisms that register the fulfillment of transactions and apply specified non-conformance sanctions during the VO execution stage are essential to insure the effectiveness of the agreements. Existence of the agreements and enforcement mechanisms allows parties to accept a potentially vulnerable position.

Distrust (or *suspicion level*) specifies a means of revoking previously agreed trust (declared in the agreements). The suspicion level depends on history (past transactional experiences with the party) and is determined by monitoring the following aspects of the participants' behaviors:

1. "lack of goodwill" that appears as signs of non-cooperation and the partner's proactively opportunistic behaviors during the agreement negotiation process;
2. non-compliance represents the belief that a participant is not acting reliably according to the established agreement, possibly exploiting individual objectives and not obeying the agreed policies.

Since the focus of this paper is on the agreement negotiations stage of a VO lifecycle, we mainly consider the first component of distrust – the **lack of goodwill**, that has to do with the participant's behaviors before the agreements are established and actual agreement controlled activities begin.

The notions of trust and agreements/contracts for normative behavior enforcement have been considered by many researchers [1][5][9][10][13][15]. However, to our best knowledge, the trust/contract negotiations in VO environments and the effects of the participants' behaviors during the negotiation process on mutual trust have not been studied at an adequate level. A novel aspect of the initial trust establishment considered in this paper is monitoring the participant's behaviors during the agreement negotiation process and adjusting trust values based on the perceived behaviors. By modeling the agreement negotiation in this way, the relationship between the initial participants' behaviors, expectations, obligations and agreements become more readily apparent for future VO work.

## 2 Agreement Negotiations in VO

The problem of managing agreements in computer systems is complicated in federated environments in the following ways:

- Partners may participate in a task without previous knowledge of the other participants in the collaboration. Trust has to be established in real time on a peer-to-peer basis.
- When negotiating an agreement, each participant may try to get a better QoS, lower rates, higher profit

distribution, etc. We have to support fair resource/service allocation in the presence of competitive VO participants by employing the appropriate agreement rules and monitoring and enforcing the agreements.

- The problem of “free riders”- a participant may try to utilize as much of the VO’s resources as possible without “repaying” the VO (providing access for other members to resources the participant controls).
- Negotiation of agreements may involve sensitive participant’s information. For example, participants may require that certain attributes (e.g., participant’s identity, participating vendors) be hidden during negotiations to ensure fairness and equal opportunity. In this case, attributes might only be revealed at the end of the negotiation or when required level of trust is established.
- Information regarding collaborators may itself be sensitive, and disclosure of a list of acceptable members of a federation may not be releasable to members of the federation.

**In this paper we consider initial negotiation that involves two participants wishing to establish a VO. During the negotiations, parties exchange offers (agreement proposals) and counter-offers until the agreement is reached or failure is reported.** While the agreement enforcement is a vital part of the VO infrastructure, the discussion of the monitoring and enforcing mechanisms is outside of the focus of this paper.

### 3 Key Components

Focusing on the agreement establishing phase between two entities  $a$  and  $b$ , we consider the following structures:

- participants  $a$  and  $b$  that wish to create a VO;
- suspicion levels  $sl_a$  and  $sl_b$  attributed to the participants  $a$  and  $b$ ;
- negotiation history  $H_{a,b}$  maintained locally by the participants  $a$  and  $b$ ;
- agreement  $A$  between  $a$  and  $b$ .

The next sections briefly describe each structure.

### 3.1 Agreement Negotiation Participants

We think of participants as consisting of resources  $R$ , attributes  $\mathcal{S}$ , actions  $X$ , and local policies  $I$ :

$$a = \langle R_a, \mathcal{S}_a, X_a, I_a \rangle, \quad b = \langle R_b, \mathcal{S}_b, X_b, I_b \rangle$$

Set  $R$ :  $R = \{r_{ij}\}$  represents humans, physical resources, services, information, products that a member contributes to VO according to a negotiated agreement.

Set  $\mathcal{S}$ :  $\mathcal{S} = \{s_{ij}\}$  represents requested attributes that a participant must prove. Set  $\mathcal{S}$ :  $\mathcal{S} = \{s_k\}$  represents **verified** (proved) attributes, such as identity, competence, technical knowledge, skills, that a participant must prove to the other party. In the implementation, these attributes are supported by digital certificates issued by trusted authorities that prove the possession of the attributes.

Set  $X$ :  $I = \{x_{ij}\}$  denotes actions that must be performed on the resources (e.g., ship product parts before a deadline). The actions can be conditioned on time, location or other context.

Set  $I$ :  $I = \{i_m\}$  denotes the participant’s local policies that express the participant’s interests and set of private goals. The policies can, for example, represent the workload acceptance levels (together with their agreed prices), include both a minimum desired production output (under which a partner’s participation may not be profitable anymore) and a maximum committed contribution to the VO. Revealing this information to a participating party can speed up the agreement negotiation process. However this “eager” strategy poses certain risks since certain parts of the information may be sensitive and must not be revealed to the other party. Nevertheless, the private goals in some cases can be implicitly inferred during the negotiation process by observing the flow of offers and counter offers.

A VO member can be a service provider as well as a service consumer. A participant must agree not only with what it expects from the other party, but also with what it is obliged to do and with sanctions that will be carried out in case of non-performance. The latter assumes that agreement monitoring and enforcing mechanisms are in place.

$E$  represents expectations - a wish list comprising of a set of obligations that the other entity should undertake as part of the agreement.

$O$  represents obligations an entity would be willing to enter into under an agreement with another participant. A member commits itself to provide a service under certain terms and conditions to another member. An obligation may represent demanded workload for each participant, resources to be contributed, required prices for each participant's contribution, profit distribution, etc.

Set  $W$ :  $W = \{w_m\}$  denotes sanctions. Deviation from prescribed behaviors may be admitted and properly addressed through sanctions that are enforced by the agreement enforcement mechanisms. Obligations include at least one sanction in case of non-performance; otherwise, the obligations might be ineffective.

Obligations and expectations are expressed as a set of Boolean formulas over declarative statements making explicit the expected pattern of the participants' interactions.

Each statement describes whether the statement imposes an **action** that must be taken by another member in the federation and a set of sanctions  $w_i$  ( $w_i$  is in  $W$ ) that will be carried out in case of non-performance, or whether the statement is a **predicate** that must be met, and exception activity taken if it is not met. The statements are described in terms of:

- resources/services (set  $R$ ) that are expected from the other party or must be contributed to the party;
- attributes (set  $S$ ) that the participant or other VO members must prove;
- specific actions (set  $X$ ) which a member has to perform on its own or other members' resources.

Statements may include the following requirements:

- *Privacy* – the requested/guaranteed privacy of data provided to the partner, as well as the participant's identity and privacy of the results produced.
- *Endorsements and accreditation* – a list of certifications that must be held by the partner. These may apply not only to the partner as an organization, but also to the partner's computing environment.

- *Reliability* – the reliability of the partner. This is not so much an information dissemination constraint, but it will affect one's confidence in obtaining results.
- *Reputation* - what others have said about the partner, based on endorsements and other reputation mechanisms.

Each statement is marked as sensitive or non-sensitive. If non-sensitive, the statement can be freely placed in the agreement proposal, otherwise the statement is a subject to a release policy. The policy may require presenting some credentials (e.g., good credit rating or appropriate expertise level) in order to release the statement.

A participant  $a$  enters a negotiation with a participant  $b$  with an agreement proposal  $P_{a,b}$ :

$$P_{a,b} = \langle E_{a,b}, O_{a,b}, \{s^a_{kj}\}, \{s^b_{ij}\} \rangle$$

The agreement proposal consists of the following:

1. Expectations  $E_{a,b}$  expressed as a set of Boolean formulas;
2. A possibly empty set of obligations  $O_{a,b}$  expressed as a set of Boolean formulas ;
3. A possibly empty set of verified attributes  $\{s^a_{kj}\}$ ;
4. A possibly empty set of attributes  $\{s^b_{ij}\}$  requested by  $a$  from  $b$ .

Set  $I$  represents policies that control the agreement negotiation process and release of sensitive information. These policies are conditioned on suspicion levels. The local policies  $I$  of a participant include the following rule sets<sup>1</sup>:

$$\mathit{fulfill}(O_{a,b}, E_{a,b}, O_{b,a}, E_{b,a}) \rightarrow \mathit{true} \text{ or } \mathit{false}$$

In the simplest case  $O_{a,b}$  and  $E_{a,b}$  *fulfill*  $O_{b,a}$  and  $E_{b,a}$  if they are equal. That is:  $O_{a,b} = E_{b,a}$  and  $E_{a,b} = O_{b,a}$ .

In general, the obligations that *fulfill* expectations can be defined as a "superset" of the expectations. For example, consider a user expectation "computational resources must be available no less than 4 hours in any 24 hour period". Then any obligation that guarantees

<sup>1</sup> In this paper we define the rules from the point of view of  $a$ . We omitted the similar set of rules defined from the point of view of  $b$  for brevity.

resource availability over 4 hours per day fulfills the expectation.

$$\text{attribute\_release}(sl_b, P_{b,a}) \rightarrow \{s^a_{ij}\} \text{ or } \{s^b_{nj}\}$$

This rule takes the suspicion level  $sl_b$  attributed to the member  $b$ , a proposal  $P_{b,a}$  that contains a set of verified attributes  $\{s^b_{kj}\}$  presented by  $b$ , a set of attributes  $\{s^a_{ij}\}$  requested by  $b$  from  $a$  and either returns the set of requested verified attributes  $\{s^a_{ij}\}$  or (if attributes presented by  $b$  do not satisfy the attribute release policy) a set of additional attributes  $\{s^b_{nj}\}$  that  $b$  must send in order for  $a$  to present  $\{s^a_{ij}\}$ . The number and types of requested attributes depend on the suspicion level  $sl_b$ : the higher the level, the more attributes may be requested.

$$\text{counter\_offer}(sl_b, P_{b,a}) \rightarrow P_{a,b}$$

This rule takes the suspicion level  $sl_b$  attributed to  $b$ , and the agreement proposal  $P_{b,a}$  sent by  $b$  as input and returns a counter offer  $P_{a,b}$ .

The offer is created with proposed changes to the expectations and obligations specified in  $P_{b,a}$ .

The changes depend on  $sl_b$ . If the suspicion level reaches some threshold,  $a$  may chose to end the negotiation based on the lack of trust in  $b$ .

$$\text{update\_sl}(sl_b, H_{a,b}, I_a) \rightarrow sl_b'$$

This rule takes the suspicion level  $sl_b$  attributed to the member  $b$ , a set of negotiation sessions between  $a$  and  $b$ ,  $H_{a,b}$ , and  $a$ 's local policies  $I_a$  as input and returns a new suspicion level  $sl_b'$ .

Even though the participating parties may have no prior knowledge of one another, some characteristics (e.g., geographic location, communications mechanisms, etc) relevant to the type of the agreement being negotiated contribute to the trust in the participant. These characteristics are specified in local policies  $I$  and are used for calculating the suspicion level. For example, when negotiating the QoS guarantees with a remote participant behind a slow connection, we might be more suspicious about unrealistically high QoS guarantees proposed by the participant, than when negotiating with a participant behind a high speed connection.

During the negotiation process, each participant observes the flow of offers and counter-offers and

according to the rules expressed in local policies  $I$ , adjusts the suspicion level for the negotiating party if a suspicious behavior is detected.

### 3.2 Suspicion Levels

In this framework, initial trust is expressed as conformance of participants to normative negotiation behaviors described in the participants' policy  $I$ . Suspicion levels indicate perceived deviation from the expected behavior. The values are derived from interaction histories  $H$ , allowing the estimation of likely future behaviors. Each suspicion level  $sl_a$  is attributed to a particular member  $a$  and is represented by a vector:

$$sl_a = \langle sl_a^i \rangle, sl_{min} \leq sl_a^i \leq sl_{max}$$

Each component  $sl_a^i$  is attributed to a particular type of suspicion. For example,  $sl_a^1$  may represent a probability of sensitive information leaks (e.g., probing for the participant's maximum offered profit share),  $sl_a^2$  may indicate a probability of DoS on behalf of the participant  $a$ .  $sl_{min}$  represents strong belief that the participant  $a$  is acting in accordance to the normative behavior,  $sl_{max}$  represents strong belief that the participant  $a$  is acting in contrary to the expected or desired behavior.

The Suspicion Level (SL) increases with the occurring times of the suspicious event and decreases when a "positive" event happens (e.g., successful negotiation rounds). The value by which the SL is increased (or decreased) depends on the confidence level that the repeated event indicates malicious (or positive) activity.

### 3.3 Negotiation History

Each participant maintains a history  $H$  of interactions with the negotiating party that consists of a set of negotiation rounds  $Rd^t$  ordered by the time of occurrence  $t$ :

$$H_{a,b} = \{ Rd^t_{a,b} \}$$

Each round  $Rd^t$  includes a proposal and a counter proposal received during that round.

$$Rd^t_{a,b} = \{ P_{a,b}, P_{b,a} \} \text{ where:}$$

$P_{a,b}^t$  is the proposal sent by member  $a$  to member  $b$  in the negotiation round  $Rd_{a,b}^t$ ;

$P_{b,a}^t$  is the proposal sent by member  $b$  to member  $a$  in the negotiation round  $Rd_{a,b}^t$ .

### 3. 4 Agreements

$A$  represents the established agreement that explicitly specifies legitimate interactions between VO members. Agreements are created during the agreement negotiation process where participants iteratively exchange agreement proposals. The process is guided by the participants' private interests expressed in local policies  $I$ .

The agreement  $A$  is next converted (through use of digital signatures and possibly a third trusted party) to a binding document that can have different forms, ranging from temporary contract between machines (if the legal framework allows that) to legally binding contracts between organizations.

$A = \langle O_{a,b}, O_{b,a} \rangle$  represents an agreement between members  $a$  and  $b$ . The sanctions are part of the agreement, since they are included within the obligations. The agreement is reached when:

$$\begin{aligned} \text{fulfill}(O_{a,b}, E_{a,b}, O_{b,a}, E_{b,a}) &\rightarrow \text{true} \quad \text{and} \\ \text{fulfill}(O_{b,a}, E_{b,a}, O_{a,b}, E_{a,b}) &\rightarrow \text{true} \end{aligned}$$

## 4. Agreement Negotiation Example

The following example illustrates an agreement negotiation between two enterprises  $a$  and  $b$  wishing to establish a VO for a commercial collaboration, such as computer assembly.  $a$  produces desktops,  $b$  manufactures monitors. Both parties are interested in maximizing their share of the profits on the end product sales. Each participant defines the minimum profit share it is willing to accept in its local policies  $I$ . This information is secret and is not revealed to the other party.

### Round1

Assume that  $a$  initiates a negotiation by sending a message to  $b$  that contains the first version of an agreement proposal:

$$P_{a,b}^1 = \langle E_{a,b}^1, O_{a,b}^1, \emptyset, s_b \rangle$$

The proposal contains:

- $a$ 's expectation  $E_{a,b}^1 = (x_{ship}, r_{monitor}, w_{fine})$  for  $b$  to ship a monitor and a sanction - specified fine  $w_{fine}$  in the case of non-performance;
- $a$ 's obligation  $O_{a,b}^1 = (x_{share}, r_{profits} 20\%)$  to give  $b$  20% of the profit;
- the quality assurance requirement  $s_b$  that  $b$  needs to prove to  $a$  in order to satisfy the compatibility and quality requirements posed by  $a$  on  $b$ 's product.

The proposal contains an empty set of  $a$ 's verified credentials.

When  $b$  receives  $a$ 's proposal, it first calculates the suspicion level  $sl_a$  attributed to  $a$ . Since there was no prior interaction between  $a$  and  $b$ , the  $sl_a$  is set to a default value  $sl_a^{default}$ . The  $b$ 's local policies  $I_b$  are employed when calculating the suspicion level. For example, the policies may assign a higher suspicion level to foreign partners.

Next,  $b$  generates its expectations  $E_{b,a}$  and obligations  $O_{b,a}$  according to the local policies  $I_b$  that indicate, for example, the minimum profit of 60%.

Next,  $b$  checks whether the proposed obligations and expectations fulfill its own requirements. Since  $a$  proposed lower profit share than  $b$  expects, the **fulfill** function returns **false**. Assume that  $b$  accepts the requested sanction  $w_{fine}$ .

Since there is a requested attribute  $s_b$  that  $b$  has to present to  $a$ ,  $b$  first checks whether the attribute is sensitive. Assume that the attribute is not sensitive and can be freely released.

Next  $b$  generates a counter-proposal  $P_{b,a}^1$ . The proposal indicates that:

- $b$  is willing to supply the monitor if  $a$  commits to the profit share of 60%;
- $b$  agrees to pay fine  $w_{fine}$  if  $b$  does not perform on time;
- $a$  will be a subject to a legal dispute  $w_{dispute}$  if  $a$  does not provide the agreed profit share.

Next  $b$  sends the counter-offer and its certification  $s^b$  to  $a$ .

$update\_sl(\emptyset, \emptyset, I_b) \rightarrow sl_a^{default}$

$fulfill(O_{a,b}^1, E_{a,b}^1, O_{b,a}, E_{b,a}) \rightarrow false$ , where

$O_{b,a} = (x_{share}, r_{profit}, 60\%, w_{fine})$ ,

$E_{b,a} = (x_{ship}, r_{monitor}, w_{dispute})$

$attribute\_release(sl_a^{default}, P_{a,b}^1) \rightarrow s^b$

$counter\_offer(sl_a^{default}, P_{a,b}^1) \rightarrow P_{b,a}^1$

$P_{b,a}^1 = \langle E_{b,a}^1, O_{b,a}^1, s^b, \emptyset \rangle$ , where

$E_{b,a}^1 = (x_{ship}, r_{monitor}, w_{dispute})$ ,

$O_{b,a}^1 = (x_{share}, r_{profit}, 60\%, w_{fine})$

## Rounds 2 to N

When  $a$  receives  $b$ 's counter-offer,  $a$  notices that  $b$ 's profit expectation is higher than the minimum profit specified in  $a$ 's local policies  $I_a$  (which indicates the minimum profit of 50%), and makes a counter offer setting  $b$ 's profit to a lower value. The negotiation proceeds in a similar fashion until the agreement is reached.

If  $b$  is acting suspiciously, for example, constantly exhibiting opportunistic behaviors by not lowering its profit expectation (or even rising the profit expectation each new round),  $a$  will increase the suspicion level  $sl_b$ . This behavior is not necessarily malicious, it is natural for one to wish for a higher profit. However,  $a$  can infer that  $b$  is likely trying to probe the maximum profit share that  $a$  can offer, which is a sign of "lack of good will". Such behavior may indicate potential future problems in the collaboration with  $b$ .

When  $sl_b$  reaches certain threshold (defined in the policies  $I_a$ ),  $a$  may decide not to establish the agreement with  $b$  (by sending a negotiation failure message to  $b$ ) and find a more cooperative partner for the collaboration.

Other types of anomalous behavior include negotiations with the intent of collecting or inferring sensitive information instead of establishing an agreement. An attacker might send requests that require the other party to reveal sensitive attributes that may be unrelated to the nature of agreement (e.g., asking for company's list of clients or internal organizational structure when negotiating a profit share). This technique is a variant of common

"phishing" attacks that could easily exploit agreement negotiation systems.

Malicious participants' behaviors may come in the form of denial of service (DoS) attacks against the implementation of the agreement negotiation system in order to disable a competitor using its underlying protocols. DoS attacks can result from initiating a large number of agreement negotiation sessions, disclosing many credentials to the server that are invalid or irrelevant to the negotiation. The net result of such attacks is that the server expends an excessive amount of computational resources on illegitimate requests and is hampered in its ability to serve requests from legitimate clients.

Investigating the behavioral aspects to be monitored and policies that guide the SL adjustment are the areas for further research.

## 5. Implementation Considerations

In this section we briefly describe infrastructures supporting the framework. In previous work, we developed an *Adaptive Trust Negotiation and Access Control (ATNAC)* framework [19] to address issues of access control in open systems. We are applying these techniques to negotiation of agreement proposals, rather than using them solely to negotiate proofs of security attributes.

The ATNAC framework is based on two well-established systems GAA-API [20][21] and TrustBuilder [23]. The GAA-API provides adaptive access control that captures dynamically changing system security requirements. The TrustBuilder system regulates when and how sensitive information is disclosed to other parties. The Analyzer maintains a separate SL for each requester based on the IP address and certificate-based identity (if available), and stores the information in a Suspicion Database. Analyzer dynamically calculates the SLs based on the information reported by the GAA-API and TrustBuilder.

This combination extends the capabilities of each system. In particular, the framework allows us to detect and thwart certain attacks on electronic transactions, to adapt information disclosure and resource access policies according to a level of suspicion.

We are extending the ATNAC to support the functions defined in Section 3. In particular, we are using the GAA-API to implement the *fulfill()* function that takes proposed and local expectations and obligations, and returns a decision whether the input fulfils the local requirements.

The TrustBuilder modules serve as a basis for implementing the *attribute\_release()* and *counter\_offer()* functions that control the sensitive attribute disclosure, building counter offers, and controlling the negotiation process according to the strategies expressed in the local policies. One of the challenges is mapping the local policies *I*, obligations, and expectations to the policy formats supported by the GAA-API (uses EACL format) and TrustBuilder (employs X.509v3 digital certificates and TPL policies).

The Analyzer module implements the *update\_sl()* that monitors the interactions between members during the agreement negotiation, updates suspicion levels and detects suspicious behaviors and violations as they occur according to the policies *I*. Proper evidence is collected on both the actions and the lack of actions of the agents by observing the negotiation history *H*.

In the implementation, the SL may consist of several components that are related to different aspects of observed behavior. For example, a participant repeatedly presents forged credentials or irrelevant credentials that were not requested by the other party, or a participant persistently tries to get the better shared profit by engaging in lengthy negotiations with little or no progress toward a mutually satisfactory outcome. In our current implementation, the SL is comprised of three components:

$$sl = \langle sl_{DoS}, sl_{IL}, sl_o \rangle$$

*sl<sub>DoS</sub>* indicates a probability of DoS attack on behalf of the requester. *sl<sub>IL</sub>* is attributed to sensitive information leakage attempts. Finally, *sl<sub>o</sub>* indicates other suspicious behaviors (e.g., misuses of a user's identity or impersonation attempts). All three values range from 0.0 to 1.0.

The Analyzer (local to the participant) increases the SL with the occurring times of the suspicious event and decreases the SL when a “positive” event happens (e.g., successful agreement negotiation and/or successfully completed business transaction). The

value by which the SL is increased depends on the confidence level that the repeated events indicate malicious activity. For example, the Analyzer may increase a particular component of SL by 0.25, 0.25, 0.5 on the first, second and third consecutive errors.

We will extend the SL with additional components (and will design and implement the corresponding *update\_sl()* functions) attributed to the “lack of good will” and other suspicious behaviors observed during the agreement negotiation process.

## 6. Related Work

Quirchmayr et al [17] describe an approach to modeling contract establishment in Virtual Enterprises based on the first order predicate logic formalism. VO's main concern is supporting enforceable contracts. This means that it is possible to determine whether the actions of parties are in accordance with the contract in effect. They do not consider notion of trust, negotiation techniques and policies. Damianou et al [6] developed annotation and tools for specifying, analyzing and enforcing obligation and authorization policies for managing large scale distributed systems. PeerTrust [14] is a trust management system that uses a simple and expressive policy language based on distributed logic programs. PeerTrust agents perform automated trust negotiation to obtain access to sensitive resources. Bonatti and Samarati [3] proposed a framework based on policy language and an interaction model for regulating access to network services. This trust establishment framework uses logical rules for accessing services and avoiding unnecessary disclosure of sensitive information.

## 7 Conclusions and Future Work

We presented a framework (still under development) supporting on-demand creation of trust relationships (or agreements) within the context of cross-institutional virtual organizations VO. The organizations are dynamically created in order to achieve a common objective by securely sharing resources, services and information.

Our goal is to create generic, reusable representations of agreements that can be applied across a variety of organizations. In this paper we have shown how the framework can support the agreement negotiations

leading to the establishment of a VO. This framework can serve as a basis for the agreement consistency and compliance checks as well as for the development of implementation rules.

The future work includes specifying the exact structure of local policies *I*, statements and sanctions (that comprise expectations and obligations); extending the framework to support multi-party negotiations; and investigating whether the local policies *I* need to be updated dynamically to accommodate new user requirements and obligations imposed by expectations of the new members. Ultimately we intend to build a tool that allows two parties to negotiate an agreement in real time. Most of the interactions will be done automatically. An input from a user will be required only to resolve any conflicts.

## Acknowledgements

We would like to thank the reviewers whose comments were invaluable in improving the quality of the paper.

This research was supported by funding the National Science Foundation under grants no. CCR-0325951 and ACI-0325409. The views and conclusions contained herein are those of the authors and should not be interpreted as representing the official policies or endorsement of the funding agencies. Figures and descriptions were provided by the authors and are used with permission

## References

[1] F. Almenárez, A. Marín, C. Campo, C. García. A Pervasive Trust Management Model for dynamic Open Environments. First Workshop on Pervasive Security and Trust at MobiQuitous 2004.

[2] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In Proceedings of the IEEE Symposium on Research in Security and Privacy, 96-17, 1996.

[3] P. Bonatti and P. Samarati. A Unified Framework for Regulating Access and Information Release on the Web. In Journal of Computer Security, pages 241-271, Vol. 10, Issue 3, 2002.

[4] V. Cahill, E. Gray, J. M. Seigneur, C. D. Jensen, Y. Chen, et al. Using Trust for Secure Collaboration in

Uncertain Environments. Published by the IEEE CS and IEEE Com Soc, 2003.

[5] H. L. Cardoso and E. Oliveira. Virtual Enterprise Normative Framework within Electronic Institutions. In ESAW'04 - 5th Int. Workshop on Engineering Societies in the Agents World, Toulouse, 2004.

[6] N. Damianou, N. Dulay, E. Lupu, M. Sloman. The Ponder Policy Specification Language. In proceedings of Workshop on Policies for Distributed Systems and Networks (POLICY 2001). Springer-Verlag, LNCS 1995, Bristol, UK, 2001.

[7] H. Davulcu, M. Kifer, L. R. Pokorny, C. R. Ramakrishnan, I. V. Ramakrishnan, and S. Dawson. Modeling and Analysis of Interactions in Virtual Enterprises. In Proceedings of the Workshop on Research Issues in Data Engineering – Information Technology for Virtual Enterprises (RIDE-VE'99), Australia, March 1999.

[8] C. Dellarocas, M. Klein, J. A. Rodriguez-Aguilar. An exception handling architecture for open electronic marketplaces of contract net software agents. In Proceedings of the 2nd ACM Conference on Electronic Commerce, pp.225-232, 2002.

[9] P. Grefen, K. Aberer, Y. Hoffner, and H. Ludwig. Crossflow: cross-organizational workflow management in dynamic virtual enterprises. In Computer Systems Science and Engineering, vol. 15 no 5, pp.277-290, 2000.

[10] F. Griffel. Electronic Contracting with COSMOS – How to establish, negotiate and execute electronic contracts on the internet. In Proceedings of the Second International Enterprise Distributed Object Computation Workshop, 1998.

[11] A. Josang. The right type of trust for distributed systems. In New Security Paradigms'96 Workshop, 1996.

[12] L. M. Macarena-Matos, H. Afsarmanesh, R. Rabelo. Infrastructure developments for agile virtual enterprises. International Journal of Computer Integrated Manufacturing, ISSN 0951-192X, Vol. 16, N. 4-5, 2003.

[13] N. Mezzetti. Towards a Model for Trust Relationships in Virtual Enterprises. 14th International Workshop on Database and Expert Systems Applications (DEXA'03), 2003.

[14] W. Nejdl, D. Olmedilla, and M. Winslett. PeerTrust: Automated Trust Negotiation for Peers on the Semantic Web. In Proceedings of the Workshop on

Secure Data Management in a Connected World (SDM'04) in conjunction with 30th International Conference on Very Large Data Bases, 2004.

[15] M. Nielsen and K. Krukow. On the Formal Modeling of Trust in Reputation-Based Systems. LNCS, Springer –Verlag, ISSN: 0302-9743 , Volume 3113, 2004.

[16] P. Periorellis, S. Parastatidis. Task-Based Access Control for Virtual Organizations. Lecture Notes in Computer Science, Volume 3409, Pages 38 – 47, 2005.

[17] G. Quirchmayr, Z. Milosevic, R. Tagg, J. Cole, and S. Kulkarni. Establishment of Virtual Enterprise Contracts. In Proceedings of DEXA'02 conference, September 2-6, 2002.

[18] A. P. Rocha and E. Oliveira. Electronic Institutions as a Framework for Agents' Negotiation and Mutual Commitment. Lecture Notes In Computer Science; Vol. 2258, ISBN:3-540-43030-X , 232 – 245, 2001.

[19] T. Ryutov, L. Zhou, C. Neuman, T. Leithead, and K. Seamons. Adaptive Trust Negotiation and Access Control. In Proceedings of SACMAT, 2005.

[20] T. Ryutov and C. Neuman. The Specification and Enforcement of Advanced Security Policies. In Proceedings of the Conference on Policies for Distributed Systems and Networks (POLICY 2002), Monterey, California, June 5-7, 2002.

[21] T. Ryutov, C. Neuman, D. Kim and L. Zhou. Integrated Access Control and Intrusion Detection for Web Servers. In IEEE Transactions on Parallel and Distributed Systems, pages 841-850, Vol. 14, No. 9, 2003.

[22] R. Tagg, G. Quirchmayr. Towards an Interconnection Model for Evolution of Shared Workflows in a Virtual Enterprise. In Proceedings of Third Int. Conference on Information Integration and Web-Based Applications and Services, Austria, 2001.

[23] M. Winslett, T. Yu, K. E. Seamons, A. Hess, J. Jacobson, R. Jarvis, B. Smith, and L. Yu. Negotiating Trust on the Web. IEEE Internet Computing, vol. 6, no. 6, 2002.