Trust-based Dynamic Service Composition in Tactical Networks

Jin-Hee Cho, Jemin George
U.S. Army Research Laboratory
Adelphi, Maryland, U.S.A.
{jinhee.cho, jemin.george}@us.army.mil

Abstract — This short paper proposes a trust-based dynamic service composition scheme for heterogeneous tactical networks where resources are restricted and the network operations deployed under time-critical conditions demand fast cadence. Unlike the existing approaches, this work employs composite trust metric so that a user may consider multiple dimensions of trust towards service provider selection aiming to maximize the service satisfaction on the received services. Leveraging the idea of matching required qualifications of service request with the trustworthiness of the service providers, the proposed scheme maximizes the user service satisfaction based on the tradeoff between trust and risk.

Index Terms—trust, risk, service composition, tactical networks

I. INTRODUCTION

In the domain of web services, research on service composition has been substantially explored to maximize quality-of-service (QoS) that is provided to users. The definition of service composition derives from the business logic that a client needs multiple services. We call the process of developing a composite service “service composition” [1]. However, in the web services domain, the main research focuses on increasing QoS based on a user’s request but without any resource constraints.

Recently, Geyik et al. [2] studied a service composition mechanism in sensor networks where resources (i.e., battery) are severely restricted. In [2], the authors proposed a heuristic approaches to identify a service graph that generates minimum communication and computation cost. In [8], the authors proposed to use switch options that enable adjusting composition in response to changing conditions of the networks.

In this work, we introduce a soft decision making strategy based on the concept of trust for service composition, which can be incorporated into the framework of [2], [8] as a part of metadata. Trust-based service composition and selection also have been studied in the web services domain [3],[4]. However, these works only considered a single dimension of trust although trust is complex and multidimensional [6].

Unlike the literature, we propose a trust-based service composition using a composite trust metric in heterogeneous tactical military networks (e.g., consisting of entities including sensors, manned vehicles, unmanned vehicles, and soldiers carrying devices). We may want to consider the following scenario. An entity in military network environments may be a soldier or a commander that may request a series of services to execute a given mission. The commander may want to receive a series of information about a target entity or situation for a certain decision making. Each service in one service composition package may be independently provided while it may be required to be sequentially provided upon the completion of a prior work. A service request (SR) should include specific information on required service characteristics including nature (e.g., high functional capability or many connections with other entities), importance (e.g., impact on overall service), spatial (e.g., physical location) or temporal information (e.g., timeline for start/end, observation window for sensors). In this work, we introduce a composite trust considering multiple dimensions of trust that can be described by users for their service request to maximize their satisfaction in terms of QoS. In addition, the composite trust can be also used to evaluate service providers (SPs) to identify an optimal set of SPs in the service composition package requested by the users. This work aims to propose a trust-based approach that identifies optimal service composition and selection in order to maximize mission performance in heterogeneous tactical networks where resources are restricted but high temporal/spatial net-centric operations are required. Compared to [2], our work also considers misbehaving entities (e.g., selfish or malicious) and both mobile and stationary entities. Further, different from [3], [4], our proposed trust-based service composition considers multiple dimensions of trust to optimally match the service request and trust of SPs.

II. TRUST-BASED SERVICE COMPOSITION

In this section, we briefly describe the composite nature of trust and outline how trust metric can be modeled. In addition, we show a brief overview of the proposed trust-based service dynamic composition scheme.

A. Composite Trust

The concept of trust originally derives from social sciences with numerous definitions. However, we can find a very common definition of trust in many disciplines: trust is the willingness to take a risk [7]. Trust is an act to accept risk even if a negative consequence may occur. In this work, we employ the tradeoff analysis between trust and risk in the
The process of selecting SPs in order to maximize a user’s satisfaction, ultimately resulting in high mission performance in military tactical networks. Numerous dimensions of trust are defined in the literature. As an example of composite trust, Cho et al. [6] used a composite trust concept which encompasses the social trust and the QoS trust. While social trust is mainly related to capability for “sociable” purposes, QoS trust is closely associated with task performance capability. Chang et al. [5] used a metric to measure a composite trust based on both direct and indirect evidence. The generic form of the trust metric that entity i assigns to entity j is shown by:

$$T_{ij}(t) = \alpha T_{ij}^{D-X}(t) + (1 - \alpha)T_{ij}^{I-D-X}(t)$$

where $0 < \alpha < 1$

X can be any dimension of trust and each trust value can be scaled in [0, 1] with weights ($\alpha$ and 1-$\alpha$) to consider direct evidence and indirect evidence.

B. Trust-based Dynamic Service Selection

This section shortly describes the proposed trust-based service selection scheme. Fig. 1 shows an overview of the trust-based service graph that selects a SP based on SR consisting of multiple services $s_i$. This example scenario requires the sequential completion of services. That is, only when a prior service is completed successfully, then the next service can be provided.

![Fig. 1: Trust-based Service Graph](image)

Each service $s_i$ is a vertex in graph $G = (V, E)$ where the edge $E = (s_i, s_j)$ can be established between two entities i and j when entity j meets trust-based criteria of SR. A user encloses the description of required qualification towards potential SPs in the SR. Each service composition package may consist of a series of services and a SP for each service should meet a given criteria. Similar to task modeling in [5], the required criteria may include the timeline for start/end or observation window, importance (I: impact on the overall service), urgency (U: strict/flexible deadline), difficulty (D: workload), and required trust level per trust property X ($TH_{trust}$).

Although the user encloses all trust-based criteria as the required qualifications of SPs in the SR, trust evaluation of entity i towards entity j may be subjective due to its inherent limitation such as spatial/temporal situation or given capability. When a current SP selects a next SP, it should assess trust-risk tradeoff analysis that provides information on “how much a given SP reveals risk in terms of required trust thresholds on trust property X.” Depending on the allowed level of an acceptable risk, a service graph solution for a given SR can be found. That is, if the allowed acceptable risk level is too stringent (low), even the service graph solution cannot be found. However, if the acceptable risk level is too loose (high), the service graph solution generated may not result in a successful completion due to untrustworthy SPs selected.

Fig. 1 also shows a dynamic nature of the proposed scheme. When the current SP initially found a qualified next SP but found it failed to provide an expected service, the previous SP may detect the failure and can look for another next SP for high resilience against service provision failure.

III. CONCLUSION AND FUTURE WORK

This work proposed a trust-based service composition that uses a trust-based soft decision making approach, with the goal to increase performance of service composition and its successful service provision with high user satisfaction.

This work guides the future work as follows: (1) developing a composite trust metric based on key dimensions of trust considered upon different types of service requests; (2) investigating the tradeoff between trust and risk upon network dynamics changes (e.g., connectivity or hostility); and (3) implementing the proposed schemes to show its performance, compared to baseline counterparts.

REFERENCES