An Overview of Reputation and Trust in Multi Agent System in Disparate Environments

Surya Pavan Kumar.Gudla¹, N. Preeti²
¹,²Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh, India

Abstract— Trust management is emerging as a promising technology to facilitate collaboration among entities in collective environment. It is hard to say what trust exactly is because it is a multidimensional, multidisciplinary and multifaceted concept. We can find various definitions of trust in the literature. Today most of the systems evaluating trust, based on reputation and security where considered as interchangeably, though they are not same. The difference between security, reputation and trust is explained, highlighting that reputation partially affects trust. A survey of trust and reputation systems in various domains is conducted, with more details given to models in Agent based system (ABS) and Multi agent system (MAS) as they are closely related to each other. This paper summarizes with the types of attributes to which trust refers to and factors to be contributed evaluating trust and some examples of the systems of various domains in which these factors have been implemented are stated.

Keywords — Trust, Reputation, security, Agent, Multi Agent System, Trust Models

I. INTRODUCTION

An agent (adaptive or intelligent agents and multi-agent systems) constitute one of the most prominent and attractive technologies in Computer Science at the beginning of this new century. Agent can be a person, a machine, a piece of software, or a variety of other things. Agents are attractive delivery channels for increasing reach and driving down cost of delivering services. Though many definitions abound, we minimally define an agent to be a program that performs a task on behalf of some other entity (like a person or larger program) [18]. Expanding on this definition, agents may have a number of characteristics.

The agents in a multi-agent system have several important characteristics

A. Autonomy

The agents are at least partially independent, self-aware and autonomous.

B. Local views

No agent has a full global view of the system, or the system is too complex for an agent to make practical use of such knowledge.

C. Decentralization

There is no designated controlling agent (or the system is effectively reduced to a monolithic system)

Agents can be divided into different types like passive agents agent without goals and Active agents with simple goals. Agents can be formed into different environments like Virtual Environment, Discrete environment and Continuous Environment.

Agent environments can be organized according to various properties like Accessibility (depending on if it is possible to gather complete information about the environment), Determinism (if an action performed in the environment causes a definite effect), Dynamics (how many entities influence the environment in the moment), Discreteness (whether the number of possible actions in the environment is finite), Episodicity (whether agent actions in certain time periods influence other periods), and Dimensionality (whether spatial characteristics are important factors of the environment and the agent considers space in its decision making).

Agents may execute various behaviors appropriate for the system they represent— for example, producing, consuming, or selling. In addition, agents may be capable of evolving, allowing unanticipated behaviors to emerge. Figure-I below shows canonical view of agent system.

Figure I Canonical view of Agent System

In this paper the sections are organized as follows: section 2 deals with Literature Survey, specifying relation between Agent Based System and Multi Agent System, and problems encountered and its applications.
Section 3 discusses the Notion of trust, Trust Metric and parameters of Trust and Establishing Trust Metric. Section 4 describes the contrast between Security, Reputation and Trust and achieving security in Multi Agent system. Section 5 describes trust in various domains and Section 6 summarizes this work.

II. RELATED WORK

In this section we look into some of the issues, applications and rapport between Agent Based System (ABS) and Multi Agent System (MAS).

A. Relation between Agent Based system and Multi Agent system

Agent-based System (ABS) is a system modeled as a collection of autonomous decision-making entities called agents. Each agent individually assesses its situation and makes decisions on the basis of a set of rules. Agent-based models consist of dynamically interacting rule-based agents. The systems within which they interact can create real-world-like complexity. In some cases, though not always, the agents may be considered as intelligent and purposeful [20]. The modeling process used for agent based system is best described as Inductive Reasoning. Inductive Reasoning is reasoning in which the premises (is an assumption that something is true) seek to supply strong evidence for (not absolute proof of) the truth of the conclusion.

Agent-based models can explain the emergence of higher-order patterns—network structures of terrorist organizations and the Internet, power-law distribution in the sizes of traffic jams, wars, and stock-market crashes. Rather than focusing on stable states, many models consider a system's robustness—the ways that complex systems adapt to internal and external pressures so as to maintain their functionalities. The task of harnessing that complexity requires consideration of the agents themselves—their diversity, connectedness, and level of interactions.

Some application domains where agent technologies plays crucial role includes are listed below.

- Ambient Intelligence, the seamless delivery of ubiquitous computing, continuous communications and intelligent user interfaces to consumer and industrial devices;
- Grid Computing, where multi-agent system approaches will enable efficient use of the resources of high-performance computing infrastructure in science, engineering, medical and commercial applications;
- Electronic Business, where agent-based approaches are already supporting the automation and semi-automation of information-gathering activities and purchase transactions over the Internet;
- Semantic Web, where agents are needed both to provide services, and to make best use of the resources available, often in cooperation with others;
- Bioinformatics and Computational Biology, where intelligent agents may support the coherent exploration of data revolution occurring in biology.

B. Multi Agent System

A Multi Agent System (MAS) is a computerized system composed of multiple interacting intelligent agents within an environment [19]. Multi-agent systems can be used to solve problems that are difficult or impossible for an individual agent or a monolithic system to solve [5].

Individual agents are capable of autonomous action to a certain extent (they don’t need to be told exactly what to do)

C. Foundational problems of Multi Agent Systems (MAS)

The agent design problem is how should agents act to carry out their tasks?

The society design problem is how should agents interact to carry out their tasks? These are known as the micro and macro perspective of MAS.
MAS as a dynamic system is where the agents may be unintentionally affect the environment in unpredictable ways.

Now-a-days security and privacy issues have become critically important with the fast expansion of multi-agent systems. Most network applications such as grid computing and p2p n/w’s can be viewed as MAS which are open, anonymous, and dynamic in nature. Such characteristics of MAS introduce vulnerabilities and threats to providing secured communication when malicious agents appear. One feasible way to minimize the threats is to evaluate the trust and reputation of the interacting agents. Trust is a crucial aspect for any form of interaction. In brief, trust is the reputation of entity where reputation is opinion about others. Trust is a belief that ensures entity as secure and reliable.

D. Applications of Multi Agent System

Multi-agent systems are applied in the real world to graphical applications such as computer games. They are also used for coordinated defense systems. Other applications include Transportation, Logistics, Graphics, and GIS [19].

It is widely being advocated for use in networking and mobile technologies, to achieve automatic and dynamic load balancing, high scalability, and self-healing networks.

III. Notion Of Trust

Trust is a crucial aspect for any form of interaction. With modern day systems becoming more and more distributed, dynamic and open at the same time, solution approaches involving multi-agent systems, due to its ability to act autonomously and rationally have gained larger interest. The popularity of online trading businesses, virtual organizations over the Internet, the Grid etc, are in the form of widespread use by the users support the fact above. In Open and Dynamic Multi Agent Systems (MASs), agents often need to rely on resources or services provided by other agents to accomplish their goals [4]. During this process, agents are exposed to the risk of being exploited by others. For example agents may eavesdrop on message exchanges between two other agents; they may masquerade as some other agent. Thus trust models should provide mechanism that their agents can use to defend themselves against attacks of other agents and humans and able to differentiate trust worthy from untrustworthy agent in the network.

By performing trust, increases the network lifetime, throughput and resilience of agents in the network.

A. Trust Metric

Trust metric is a measurement of the degree to which one social actor (an individual or a group) trusts another social actor. Trust metrics enable trust modeling and reasoning about trust [6]. They are closely related to reputation systems. The first commercial forms of trust metrics in computer software were in applications like eBay’s Feedback Rating.

B. Parameters that contribute towards trust metric

Agent Reputation is an agent’s own version of its reputation acquired by accumulating the positive ratings offered to it by other agents in the past

Average reputation is the ratio of total number of positive rating score to total number of transactions.

Aggregated Rating While considering interaction with unknown agents the subject agent would enquire trust worthiness of the other agent in the agent society to produce an aggregate rating.

Agent’s Community Guarantee is an agent might be a member of certain reputed and trustworthy community. Hence, it might sometime also be desirable that the agents own version of its reputation be given a greater weight.

C. Establishing the trust metric

Let X be an agent whose trust value is being measured in any ith instance of time t. Let R(X) denote the total reputation possessed by the agent X, which is a direct correlation to the number of successful transactions of X in past, and R(Xi) give the reputation of X at sometime t=i, due to the positive ratings of other agents. Similarly, n(TRx) gives the total number of transaction (successful as well as unsuccessful) that the agent X has had with all other agents for which it was reputed by them. Let, AGR(X) stand for the aggregate rating of the agent X by all member agents with whom it has interacted in the past. Also, let CGF(X) represent the community guarantee factor for the agent X. The function CGF (X) represents the contribution of all the communities of which the agent X is a member of.

We assume here that an agent if it is not a member of at least one established community is not reliable enough for believing what it says of itself. In other words, in case where CGF(X) has a zero value, the total computation of trust relies on the aggregated rating obtained by the agent from other agents. For simplicity, here we will consider only two states of community guarantee, either an agent is backed up by established community (CGF(X) = 1), or it is not (CGF(X) = 0).
With these, the trust of agent X, T(X) can be defined as:

\[ T(x) = \sum_{i=1}^{n} W_G \cdot CFG(x) \cdot R(x_i) + W_B \cdot AGR(x) \]

Where, W_G, and W_B are the weight factors associated with each of the components of the agent X’s trust measurement.

**IV. CONTRAST BETWEEN SECURITY, REPUTATION AND TRUST**

Today most of the systems considering security, reputation and trust interrelated to each other even though not. Security fully varies from reputation to trust and from context to context. Security defines provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Security involves the authorization of access to data in a network, which is controlled by the network administrator.

**A. Security Breach**

Security Breach is occurred for various reasons. A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter. A security breach is also known as a security violation.

1) **Types of Security Breach**

**Physical Security Breach** is one form of breach is a physical security breach, wherein the intruder steals physical data, such as files or equipment that contains the data. Intruders could steal computers, particularly laptops, for this purpose. Businesses should monitor access to their property to cut down on such incidents and require employees to lock away their laptops when not in use.

**Electronic Security Breach** is another form of breach is an electronic security breach, wherein the intruder gets into a business’ systems to access sensitive data. The intruder gains such access by taking advantage of any weaknesses in the systems, such as inadequate firewall protection.

This could also happen if the organization does not have adequate password protection for sensitive data. This sort of security breach is one reason businesses should perform constant security updates.

**Data Capture Security Breach** is Data capture, or skimming, is a practice whereby the intruder captures and records the data on a magnetic card stripe, such as on a credit card. This form of security breach helps the intruder produce copies of credit and debit cards. The intruder could either be an employee of a merchant who handles the customer’s card, or it could be an external intruder. An external intruder could attach a device to card readers or ATM machines to skim information.

**B. Security in MAS**

In MAS communication is manifold. Confidentiality of communication between agents, services, hosts, etc. must be guaranteed. Threats can be external or internal. Eavesdroppers may want to listen to agents private information may disrupt agent platform and may want to impersonate other agents or service, etc. when agents are used in open environments such as the Internet, security is major concern protecting an agent’s code and the data it has acquired while traversing a network. Hosts on which an agent resides may be malicious, and often infeasible to determine the trustworthiness of hosts in advance in open environments.

In principle, protecting agents from malicious hosts requires, Protecting the integrity of the migration path of an agent, Protecting the integrity of the agent’s data and (binary) code, Ensuring confidentiality of the agent’s data and Ensuring integrity of the agent’s control flow.

**C. Reputation and Trust**

Trust has been the focus of researchers for a long time from the social sciences, where trust between humans has been studied to the effects of trust in economic transactions. In brief, trust is the reputation of entity where reputation is opinion about others. Trust is a belief that ensures entity as secure and reliable. Although intuitively easy to comprehend, the notion of trust has not been formally defined. Reputation is not to be confused with trust: the former only partially affects the latter. Reputation is the opinion of one person about the other. Trust is a derivation of the reputation of an entity [8]. Based on the reputation, a level of trust is bestowed upon an entity.

Reputation based trust models are basically divided into two category based on the way information is aggregated from an evaluator’s perspective [7].
They are Direct/Local experience model” and “Indirect/Global reputation model” where direct experience is derived from direct encounters or observations (firsthand experience) and indirect reputation is derived from inferences based on information gathered indirectly (secondhand evidence such as by word-of-mouth).

D. Types of Attributes to which trust refers to

Not only do trust definitions vary significantly in terms of type of construct, but they also vary in terms of the attributes of the person trusted[13][14][15][16][17]—the belief or expectancy referent. To research something multi-effectively, one must first understand all its dimensions. Otherwise, one study may unintentionally overlap another.

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Attribute Type refers to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competence</td>
<td>Ability, capability and judgment</td>
</tr>
<tr>
<td>Predictability</td>
<td>Includes consistency</td>
</tr>
<tr>
<td>Goodness</td>
<td>Faith in moral integrity</td>
</tr>
<tr>
<td>Goodwill</td>
<td>Based on confidence</td>
</tr>
<tr>
<td>Benevolent</td>
<td>Being kind and fair</td>
</tr>
<tr>
<td>Honesty</td>
<td>Includes integrity and sincerity</td>
</tr>
<tr>
<td>Credibility</td>
<td>Believing and trusting</td>
</tr>
<tr>
<td>Reliability</td>
<td>Trusted to work well and to behave in the way required</td>
</tr>
<tr>
<td>Safe</td>
<td>Includes keeping confidence</td>
</tr>
<tr>
<td>Shared understanding</td>
<td>Includes Synchronization</td>
</tr>
</tbody>
</table>

V. TRUST IN VARIOUS DOMAINS

Understanding the notion of trust is the key to model trust properly in a various discipline. Trust has been using in every daily life interactions like buying, selling, communicating, cooperating and decision making etc.

A. Trust in E-commerce

Today Trust has become very importance in e-commerce applications like performing electronic transactions, being encountered with high risk factors like impersonation, fraud, privacy, dishonest people, page-jacking, and parallel webs. 76 percent of Internet users are concerned about “identity theft” if their personal information were leaked to unauthorized individuals.
Without Trust E-commerce will not be success [12]. To determine trust in E-commerce trust mechanism is matched with interaction between participants and also various behaviors (attributes) are also taken into consideration like interaction, user identity, user environment and valid information [3].

Models used to obtain trust are Direct/Indirect Trust, Beta Reputation Trust and ReGret Trust.

Factors contributed are Recommendations (word-of-mouth mechanism), Past Experiences (beliefs about the truth of the statements) and Rating experiences (direct experience, witness reputation and analysis of social network) to evaluate Trust in systems.

B. Trust in Distributed Systems

The migration of processing of computational jobs from centralized systems to open distributed systems have resulted in many communication channels and transactions, to span a range of domains and organizations, not all of which can be trusted to the same extent. Some of the distributed systems are P2P and Grid Computing is encountered with selfish routing and misbehavior of nodes [1][2]. Hence trust relationship highlighted with trust management system which can navigate these issues. As Grid environment encompass with various characteristics like Dynamics, instability and uncertainty, generating trust queries in the system is very complex. Though many research scientists recognize its importance but there is no consensus in what trust is and on what constitutes a trust management [9]. However trust between two entities may not be symmetric. So trust refers to the subjective probability by which an individual A expects that another individual B performs a given action on which its welfare depends.

Various Trust models are derived to evaluate trust in open distributed systems like Reputation Based Management system, Secure Trust Model, Distributed Trust Model and Bayesian Network model etc.

Factors to be contributed are Reputation (past Transaction, and Trust score) Trustworthiness (indicator of the quality of entity service), Feedback Score (score on secure service) and Trust Relationship (Score of service provider and service requester).

C. Trust in Adhoc Networks

An Ad-hoc network of wireless nodes is a temporarily formed network, created, operated and managed by the nodes themselves. It is also often termed an infrastructure-less, self-organized, or spontaneous network [1][2].

The survival of adhoc network is solely dependent upon the cooperative and trusting nature of nodes. At the time of collaboration among the nodes services are not fully utilized due to the fear of not being trusted and the potential risk with such collaboration. Hence various trust models were proposed, provides a dynamic measure of reliability and trustworthiness in an ad hoc network. There is no a priori trusted subset of nodes to support the network functionality. Trust may only be developed over time, while trust relationships among nodes also change. The absence of fixed trust infrastructure, limited resources, ephemeral connectivity and availability, shared wireless medium and physical vulnerability, make trust establishment in adhoc networks.

Trust models adopted to adhoc networks are CONFIDANT (based on direct observations and on second-hand information from other nodes and is updated according to a Bayesian estimation) and CORE(reputation calculated from direct observations’ using a weighted mean of the observations rating factors, giving more relevance to the past observations). A trust model that is based on experience alone may not be secluded from attacks in an ad-hoc network but it can identify routes with a certain measure of confidence.

Factors to be contributed to evaluate trust in adhoc networks are battery consumption, packets forwarded or dropped or any other such parameter topology changes, node mobility, node failure, propagation channel conditions) that helps to establish a mutual trust level.

VI. Conclusion

Trust as an essential attribute in building a relationship between entities has been studied for a long time by researchers from discrete scientific fields. Every field has examined modeling and calculating trust using different techniques, and one of the most prominent and promising techniques is the use of statistics, mainly probabilities to solve the problem, especially in dynamic networks, where the topology is changing rapidly. This paper has briefly introduced a precise definition of Security, Reputation and Trust in view of Agent Based system and Multi Agent System. A concise and closely related survey of trust models used to formulate trust in different domains, like E-commerce, Open Distributed Networks and Ad-hoc networks has been presented, and also the way in which the trust updating process is achieved and factors contributed to evaluate trust has also been discussed and summarized.
REFERENCES


BIOGRAPHIES

Mr. Surya Pavan Kumar Gudla received his MCA and MTech in CSE Engg from Aditya Institute of Technology and Management, Tekkali. He is currently working as Asst.Prof. in Department of Computer Science & Engineering, in Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh, India. He has 4 years of experience in teaching MCA and Computer Science and Engineering related subjects. His Interested areas are Computer Networks, Mobile Computing and Data Mining.

Mrs. N.Preeti received the MCA from Maharaja Post Graduate College, Vizianagram and MTech in CSE Engg from the Department of Computer Science and Engineering in Aditya Institute of Technology and Management, Tekkali. She is currently working as Asst.Prof. in Department of Computer Science & Engineering, in Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh, India. She has 7 years of experience in teaching MCA and Computer Science and Engineering related subjects. Her Interested areas are Computer Networks, Mobile Computing and Distributed & parallel computing.