Governing the Authenticity and Degree of Autonomy of Agents in Multiagent System

Rashmi Singh
Banasthali University, Banasthali, Rajasthan, India.

Aarti Singh
Maharishi Markandeshwar University, Mullana-Ambala.

Saurabh Mukherjee
Banasthali University, Banasthali, Rajasthan, India.

Abstract – Agent communication is an unavoidable process in a multagent system and in order to control the inter-agent interference, the communication is controlled using interaction protocols. The initial analysis of available agent interaction protocols suggests that not much works governing the authenticity and degree of autonomy of agents are available. Although, measures ensuring the security of data could be seen but the policies controlling the meddling by agents is not available. The paper proposes a three level security policy that is able to control the agent interaction in a positive way i.e. the policies have been designed so as to promote establishment of communication rather than denying the connection.

Index Terms – Multiagent Systems, Degree of Autonomy, Authentication of Agents, Agent Interaction Protocols.

1. INTRODUCTION

Multiagent systems [1] are finding vital applications and are proving to be very useful in solving complex and distributed problems. Since, agents in a multiagent system collaborate and coordinate with each other to execute a common plan, the level to which these are allowed to peep in not guided and is traditionally not defined. For instance, a reliable agent with high degree of trust may be granted higher degree of autonomy in contrast to agents with lower trustworthiness. An agent's trust percentile is computed using CNTEP [2] and RCNTEP [3].

Now, since agents interact and migrate from one system to another, these might turn malicious and a limit on the autonomy is desired. Therefore, policies governing the authenticity as well as the degree of autonomy of agents are desired. Hence, a policy document governing the authenticity and degree of autonomy of agents in multiagent system, securing a multiagent system is being presented in the work. This work considers GIPMAS [4], a clustering based generic interaction protocol for multiagent system as the base protocol which is a highly flexible protocol and offers high degree of autonomy to agents. It allows agents to be interacting with their peers as well as their ancestor agents. However, the authors have considered limiting the autonomy at no place and no mention of securing the interaction is available. Since, the protocol demands high degree of reliability value, agents might turn self-interested to increase their reliability values instead of considering the credibility of entire system. In order to ensure that communication amongst the agents is secure; policies permitting the level of communication amongst agents are highly desired. The aim of this paper is to provide a new three level security policy keeping the underlying architecture of GIPMAS intact.

The rest of the paper is structured as follows: Section 2 provides an overview of GIPMAS, the underlying protocol. Section 3 presents the related work. Section 4 presents the novel policies and section 5 finally concludes.

2. BACKGROUND

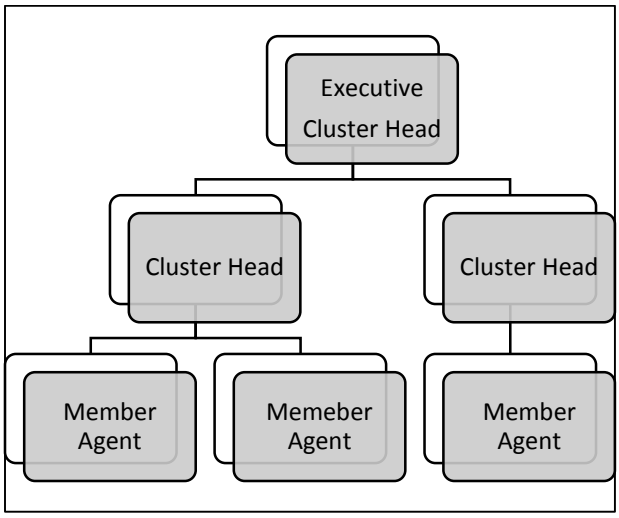

Figure 1: Hierarchy of Agent

GIPMAS is an important agent interaction protocol which initially employs clustering as the basis of grouping agents and

permits agents to interact with their peers as well as agents at higher level. The agents in GIPMAS are classified as Executive Cluster Head (ECH), Cluster Head (CH) and Member Agents (MA). The hierarchy of agents thus formed is shown in figure 1. Agents in GIPMAS work as a coherent unit and are required to cooperate according to the specified interaction rules. GIPMAS allows member agents to interact with their peers as well as respective CH and in turn CH can interact with ECH but not with peer CHs. In the event of relocation of CH, a new agent with highest degree of reliability value, maximum capability set and minimum communication delay is the most probable new CH.

However, the protocol also permits movement of MAs as well as CHs to other clusters, thus provoking the need of security. Further, in order to become CH and ECH, member agents might turn malicious and work towards increasing their own credibility rather than working as part of team and considering the credibility of entire MAS. Further, GIPMAS allows supports sharing of runtime knowledge amongst various agents. Therefore, there is high probability that agents might start misusing their abilities and autonomy thus granted to them. Therefore, this work suggests instead of permitting open interaction, agents should be allowed to communicate according to certain policy. The policy defined should be such that it neither constrains the abilities of agents nor permits open interaction to all agents. Simply speaking, the requirement of having a check on the autonomy of agents is highly desired and thus policies which offer to establish the communication instead of straightforward denying the connection is being explored in the upcoming section.

3. RELATED WORK

The section discusses the work of eminent researchers, who had putting efforts addressing the design challenges pertaining to interaction of agents, in particular [5,6]. Contract Net Protocol (CNP) [7] is a FIPA standardized protocol that offers distributed task allocation to limited number of agents. There are few protocols which emphasis on commitments [8] while distributing the tasks..Agentis [9] allows constructing MAS focusing on services and tasks. GIPMAS supports intelligent clustering of agents heterogeneous agents. Various interaction protocols are available but most of them are silent about considering security of messages as well agents themselves. To the best of our knowledge, no protocol has decided the leveled security policies. Since, GIPMAS is a clustering based protocol, the clusters in large scale distributed MAS are difficult to manage. The simplest solution is to have a centralized control but this not only limits the autonomy of agents but also adversely affects the scalability of a multiagent system. Further centralized solutions offer more complexity when data is widely distributed and perfect clusters are hard to find. Gray et al. [10] focused on authentication to verify the agent's owners, authorization to assign access restrictions and enforcement to ensure that the agent does not violate these restrictions. In another approach, Francisco et al. [11] have dealt with security issues in a project called DEEPSIA (Dynamic online Internet Purchasing System based on Intelligent Agents) that supports companies as purchasers in electronic commerce e-procurement processes. They have focused on extending the well-known KQML agent communication language to incorporate security functions and proposed a new S-KQML (Secure-Knowledge Query Manipulation Language) that includes authentication, integrity and privacy. A similar work offering three layer secure architecture [12] restricts itself to KQML and hence cannot be in general applied to a MAS not using KQML performatives.

The related work reveals that very few researchers have considered of designing governing policies imposing the access restriction on agents. Hence this paper uniquely contributes a three level policy restricting the access to agents but on the other hand it should favor the communication.

4. THE PROPOSED GOVERNING POLICY

In GIPMAS, communication between source and a destination agent is established using as the conventional FIPA standardized performatives. Further, CH is a responsible for grouping of agents according to their attributes and interests. All member agents have access to the preconditions, constraints and common shared ontology. Although agents are grouped in accordance to the final approval of CH but during the clustering process, CH do not ensure the authenticity of agents and also there is no access restriction. Hence, with the passage of time, agents may get more and more intelligent understanding their own interests, hence the boon of high degree of autonomy becomes the curse with respect to agents going off-beam and peeping into unauthorized zone. Hence, a strategy is desired to that allows the agent to operate with full autonomy simultaneously restricting the access if the agent cannot prove its trustworthiness. As shown in figure 2, an agent's reliability and trustworthiness is evaluated three-fold at all three levels i.e. ECH, CH and MA.

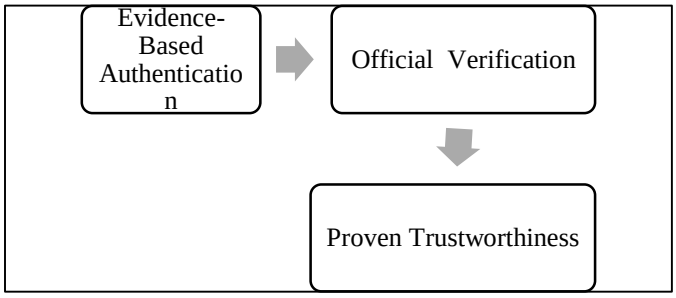

Figure 2: The Proposed Layers of Policies

The Evidence-based authentication is the simplest level of constraint imposed. In this case, peer agents are required to authenticate each other. If a positive feedback is received about

the agent for whom evidence is gathered, the agent is granted high level permissions only to take the task. Here, high level permissions implies that agent is allowed to take up the task at abstract level and is not delegated any confidential tasks or any mission critical tasks. However, it may happen that a group of agents gets malicious start generating false authentication.

Table 1: Evaluation Parameters

Layer	Permission Type	Parameters
Evidence-Based Authentication	High-Level	RequestingAgent Id AuthenticatingAgent Id Authentication_Time Authenticated Unauthenticated
Official Recognition	Middle	Evidence-Based Authentication Security Certificate
Proven Trustworthiness	Low-Level	Officially Recognized Trust Certificate

Official Recognition

This is next layer of identifying an agent. An agent having evidence-based authentication can demand more permissions. In order for more intrinsic permissions, an agent should its official certificate of security issued from certifying agency such as FIPA, IBM etc. On producing this security certificate, agent is officially recognized and is granted deep-down permissions such as checking of official records, personal mails etc.

Proven Trustworthiness

This is the highest layered policy that grants low-level permissions. It is the most lenient policy. However, it demands the most stringent certificate i.e. trust certificate. An agent possessing trust certificate is granted all permissions ranging from abstract access to confidential access. These agents can check emails as well as are authorized to perform financial transactions. In addition to trust certificate, the agent should also have above two levels of permission. The trust certificate is only granted to agents successfully undergoing through RCNTEP.

Table 1 delineates the parameters used for evaluation while granting the policy permission.

Evidence-Based Authentication

Following steps illustrates the execution of the three layered governing policy as shown in figure 3.

Step 1: Apply for Layer 1 Permissions

Permission requesting agent requests for authentication from peer agents (now playing the role of authenticating agents). Authenticating agents if have ever interacted with requesting agent shall send the feedback on the basis of previous interactions. For finding the history, agents can refer to their logs or registry agent. If layer 1 permissions accessible, apply for Official Recognition.

Step 2: Apply for Layer 2 Permissions

An agent applies for layer 2 permissions if and only if it is possessed with layer 1 permission. Along with layer 1 permissions, the agent presents its security certificate to cluster head. If CH accepts the security certificate, it declares the agent as officially recognized and grants permission pertaining to next level of access i.e. proactive modifications and rational decisions are allowed.

Step 3: Apply for Layer 3 Permissions

Alike step 2, an agent requesting for low-level permissions, must have layer 1and layer 2 permissions. The agent is now required to prove its trustworthiness. The agents trust percentile is generated using RCNTEP in GIPMAS. Higher is the trust percentile, higher is the reliability and thus better would be the permissions and vice-verca.

The flow-diagram representing the execution of above policy is depicted in figure 3.

5. CONCLUSION

The paper contributesthree-fold security policy that is able to govern the degree of autonomy and authenticity of agents in a multiagent system. The proposed step by step strategy can incorporate security ranging from strictest level to lenient level rather than denying the communication directly.

REFERENCES

[1] Wooldridge, Michael, and Nicholas R. Jennings. "Intelligent agents: Theory and practice." *Knowledge engineering review* 10.2 (1995): 115-152.

[2] Aarti Singh, Dimple Juneja, and A. K. Sharma. "Introducing Trust Establishment Protocol in Contract Net Protocol." *Advances in Computer Engineering (ACE), 2010 International Conference on*. IEEE, 2010.

[3] Aarti Singh and Dimple Juneja. "An Improved Design of Contract Net Trust Establishment Protocol." *International Journal on Communication* 4.1 (2013): 19.

[4] Dimple Juneja, Rashmi Singh, Aarti Singh, Saurabh Mukherjee,"A Clustering Based Generic Interaction Protocol for Multiagent Systems", Information Systems Design and Intelligent Applications, Volume 434 of the series Advances in Intelligent Systems and Computingpp 563-572

[5] Alberti, Marco, et al. "Specification and verification of agent interaction protocols in a logic-based system." Proceedings of the 2004 ACM symposium on Applied computing. ACM, 2004

[6] Juneja D., Jagga A., Singh A., "A Review of FIPA Standardized Agent Communication Language and Interaction Protocols", Journal of Network Communications and Emerging Technologies, Vol. 5. Special Issue 2 (2015), 179-191.

[7] Hussein, KarimMohie El Din, and FenioskyPe. "Collaborative agent interaction control and synchronization system." U.S. Patent No. 7,007,235. 28 Feb. 2006.
[8] Fornara, Nicoletta, and Marco Colombetti. "Defining interaction protocols using a commitment-based agent communication language." *Proceedings of the second* international joint conference on Autonomous agents and multiagent systems. ACM, 2003.
[9] D'Inverno, Mark, D. Kinney, and Michael Luck. "Interaction protocols in Agentis." Multi Agent Systems, 1998. Proceedings. International Conference on. IEEE, 1998.
[10] Gray, Robert S., et al. "D'Agents: Security in a multiple-language, mobile-agent system." Mobile agents and security. Springer Berlin Heidelberg, 1998. 154-187.
[11] Milagres, Francisco, et al. "Dealing with security within DEEPSIA Project." (2002).
[12] Rabi, Muhammad, et al. Secure knowledge query manipulation language: a security infrastructure for agent communication languages. Technical report, University of Maryland Baltimore County, 1998.

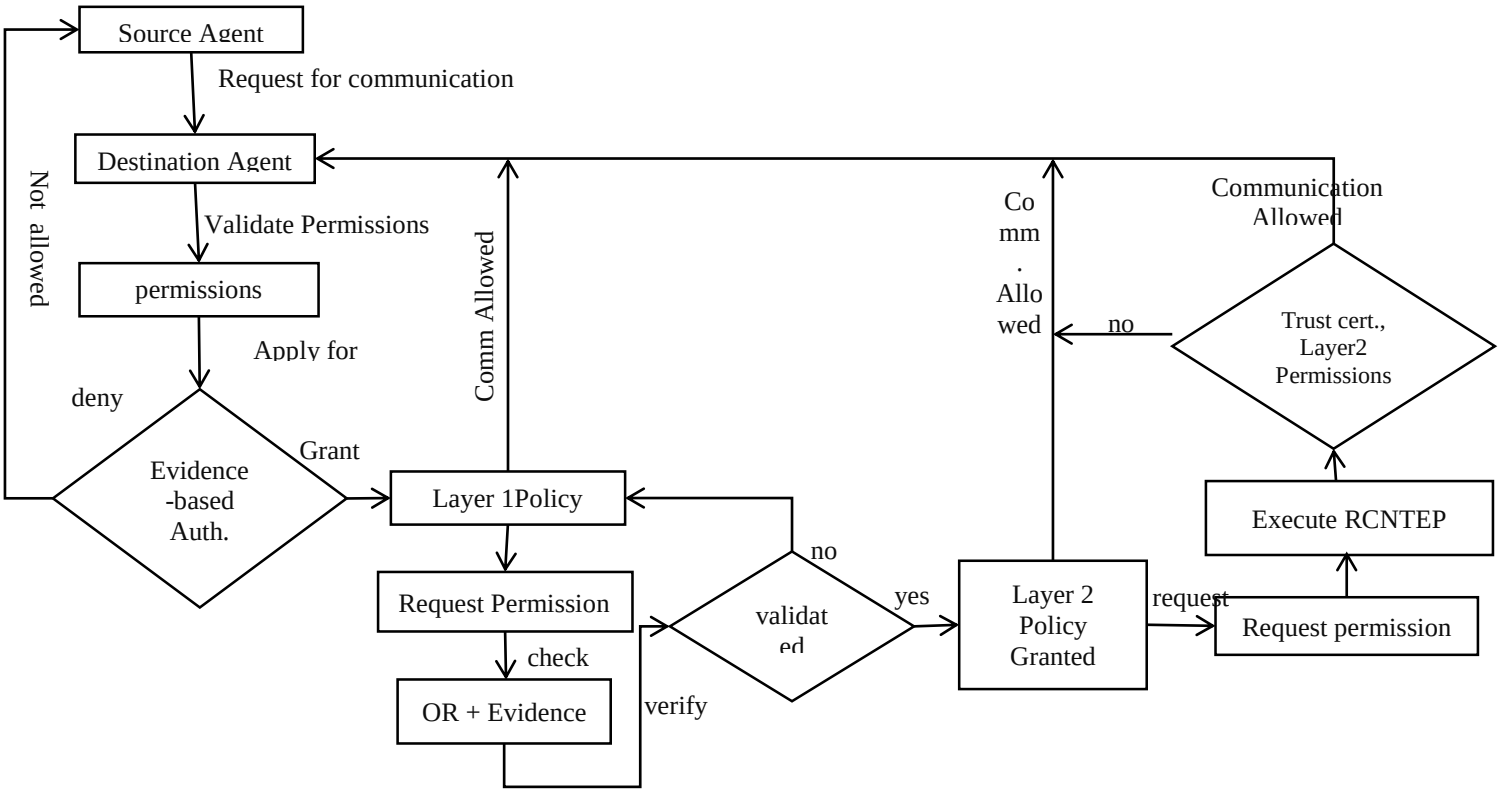

Figure 3: The Flow Diagram of Proposed Strategy