Trust and Reputation Mechanisms for Multi-agent Robotic Systems

Igor A. Zikratov\textsuperscript{1}, Ilya S. Lebedev\textsuperscript{1}, and Andrei V. Gurtov\textsuperscript{2}

\textsuperscript{1} ITMO University, Russia
\textsuperscript{2} Helsinki Institute for Information Technology HIIT and Department of Computer Science and Engineering, Aalto University, Finland

Abstract. In this paper we analyze the functioning of multi-agent robotic systems with decentralized control in conditions of destructive information influences from robots-saboteurs. We considered a type of hidden attacks using interception of messages, formation and transmission of misinformation to a group of robots, and also realizing other actions which have no visible signs of invasion into a group of robots. We analyze existing models of information security of the multi-agent information system based on a measure of trust, calculated in the course of interaction of agents. We suggest a mechanism of information security in which robots-agents produce levels of trust to each other on the basis of the situation analysis developing on a certain step of an iterative algorithm with the use of onboard sensor devices. For improving the metric of likeness of objects relating to one category (“saboteur” or “legitimate agent”) we suggest an algorithm to calculate reputation of agents as a measure of the public opinion created in time about qualities of robots of the category “saboteur” in a group of legitimate robots-agents. It is shown that inter-cluster distance can serve as a metric of quality of trust models in multi-agent systems. We give an example showing the use of the developed mechanism for detection of saboteurs in different situations in using the basic algorithm of distribution of targets in a group of robots.

Keywords: Information security, groups of robots, multi-agent robotic systems, attack, vulnerability, modeling.

1 Introduction

Groups of robots implementing a complex system which consists of many simple devices is a new and actively developing direction of group robotic technology. We assume that desirable group behavior arises from interaction of robots-agents among themselves and their interaction with the environment. The interaction of agents happens in the environment out of a controlled territory that is in conditions where there is a possibility of physical access to robots by the attacker. In such system agents possess several important properties [1]:

S. Balandin et al. (Eds.): NEW2AN/ruSMART 2014, LNCS 8638, pp. 106–120, 2014.
© Springer International Publishing Switzerland 2014
• autonomy: agents are at least partially independent;
• limited view: none of agents have a view of whole system, or the system is so complicated that the knowledge of it has no practical application for the agent;
• decentralization: there are no agents who control all group.

Unique features of a multi-agent robotic system (MRS) complicate the use of existing mechanisms of information security (IS) and give opportunity to attackers to impact on group algorithms (adaptive behavior). The need for research in information security (IS), and also the qualitative description of main threats and features of their implementation in relation to MRS led to appearance of several publications [2, 3]. One of unique threats inherent for MRS as a multi-agent system is the use by attackers of robots-saboteurs who realize harmful actions. We understand robot-saboteur activities as a harmful information influence (attack) directed on implementation of a threat to information security concerning robots-agents $R_j$ ($j = \overline{1, N}$) and realized with the use of information tools and technologies as a result of which the new action selected by agents won’t promote an increase of system functionality in available conditions.

In this article we consider mechanisms of soft security directed on detection and neutralization of hidden attacks which do not have identified signs unlike attacks which are carried out by jamming of communication links, DDoS-attacks, cracking and compromising of ciphers, etc. In case of the hidden attacks, robots, their systems and communication links function in a standard mode. Realizing a hidden attack, robots-saboteurs of a warring party can provide false or misleading information, and traditional mechanisms of security can’t protect users from this type of threats.

For protection against such hidden attacks we can use a method of the protected agent states, methods of mobile cryptography, a method of Ksyudong [6], Buddy Security Model [7, 8], which matches well with the principles of creation of decentralized systems. Besides, for providing of protection of the user from such threats, we use mechanisms of social monitoring, namely trust and reputation systems. These mechanisms are based on calculation of trust of agents to each other, realized in the course of monitoring of actions of an agent in the system [8, 9, 10, 11, 12]. Distinction in ways of computation of the trust level is caused by features of the domain where interaction of participants takes place. It can be the electronic markets, peer-to-peer networks, on-line social networks, etc. As a result, in existing models of trust there are different treatments of the concept of trust and reputation, different subjects and objects of trust are considered.

The goal of this paper is development of a method of protection of MRS from hidden attacks of robots-saboteurs, based on computation of a measure of trust and reputation to robots-agents in a group of robots in case of decentralized control.

The rest of the paper is organized as follows. In Section 2, we provide a brief survey on multi-agent robotic systems. In Section 3, we develop a model of multi-agent decision making using trust and reputation. In Section 4, we describe implementation of the model as well as its simulated functionality. Finally, Section 5 concludes the paper.