GAME THEORY ANALYSIS AND MODELLING OF SOPHISTICATED MULTI-COLLUSION ATTACK IN MANETS

ABSTRACT

Mobile Adhoc Network (MANET) has been a core topic of research since the last decade. Currently, this form of networking paradigm is increasingly being construed as an integral part of upcoming urban applications of Internet-of-Things (IoT), consisting of massive connectivity of diverse types of nodes. There is a significant barrier to the applicability of existing routing approaches in conventional MANETs when integrated with IoT. This routing mismatch can lead to security risks for the MANET-based application tied with the IoT platform. This project examines a pragmatic scenario as a test case wherein the mobile nodes must exchange multimedia signals for supporting real-time streaming applications. There exist two essential security requirements viz. i) securing the data packet and ii) understanding the unpredictable behavior of the attacker. The current study considers sophistication on the part of attacker nodes. They are aware of each other's identity and thereby collude to conduct lethal attacks, which is rarely reflected in existing security modeling statistics. This project harnesses the potential modeling aspect of game theory to model the multiple-collusion attacker scenario. It contributes towards i) modeling strategies of regular/malicious nodes and ii) applying optimization principle using novel auxiliary information to formulate the optimal strategies. The model advances each regular node's capability to carry out precise computation about the opponent player's strategy prediction, i.e., malicious node.