

## Documents

Khan, B.U.I.<sup>a</sup>, Anwar, F.<sup>b</sup>, Olanrewaju, R.F.<sup>c</sup>, Mat Kiah, M.L.B.<sup>d</sup>, Mir, R.N.<sup>d</sup>

**Game Theory Analysis and Modelling of Sophisticated Multi-Collusion Attack in MANETs**

(2021) *IEEE Access*, .

**DOI:** 10.1109/ACCESS.2021.3073343

<sup>a</sup> Department of ECE, Kulliyah of Engineering, IIUM, Kuala Lumpur, Malaysia.

<sup>b</sup> Department of Computer System &#x0026; Technology, University of Malaya, Kuala Lumpur, Malaysia.

<sup>c</sup> Department of Computer Science and Engineering, National Institute of Technology, Jammu and Kashmir, India.

**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 paper 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 research 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. The simulation outcome of the proposed mathematical model in MATLAB ascertains that it outperforms the game theory's baseline approach. CCBY

**Author Keywords**

Ad hoc networks; Colluder; Computational modeling; Game Theory; Games; Mobile Adhoc Network; Mobile computing; Multi-Collusion Attacker; Multistage game; Routing; Secure Routing; Security; Streaming media

**Index Keywords**

Computation theory, Internet of things, MATLAB, Mobile ad hoc networks, Mobile security, Network security; Analysis and modelling, Auxiliary information, Internet of Things (IoT), Multimedia signals, Optimal strategies, Optimization principle, Real time streaming, Security requirements; Game theory

**Publisher:** Institute of Electrical and Electronics Engineers Inc.

**ISSN:** 21693536

**Language of Original Document:** English

**Abbreviated Source Title:** IEEE Access

2-s2.0-85104256088

**Document Type:** Article  
**Publication Stage:** Article in Press  
**Source:** Scopus

---

**ELSEVIER**

Copyright © 2021 Elsevier B.V. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.

