論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Resilient Consensus in Multi-Agent Systems with Limited Resources
著者(和文)	WangYuan
Author(English)	Yuan Wang
出典(和文)	学位:博士(学術), 学位授与機関:東京工業大学, 報告番号:甲第11334号, 授与年月日:2019年9月20日, 学位の種別:課程博士, 審査員:石井 秀明,山村 雅幸,三宅 美博,DEFAGO XAVIER,小野 功
Citation(English)	Degree:Doctor (Academic), Conferring organization: Tokyo Institute of Technology, Report number:甲第11334号, Conferred date:2019/9/20, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	情報工学 系 知能情報 コース	申請学位（専攻分野）： Academic Degree Requested	博 士 （学術） Doctor of Philosophy
学生氏名： Student's Name	Wang Yuan	指導教員（主）： Academic Supervisor(main)	Ishii Hideaki
		指導教員（副）： Academic Supervisor(sub)	

要旨（英文 800 語程度）
Thesis Summary（approx.800 English Words ）

In large-scale multi-agent systems, consensus problems form one of the fundamental problems related to distributed algorithms. There, agents interact locally and exchange their information with each other in order to arrive at the global objective of sharing a common value. In recent years, security problems in multi-agent systems have become a critical issue. Malicious attacks can lead the systems to undesirable operations or even accidents. In an uncertain environment where faults or even adversarial attacks can be present, it is of great importance to defend consensus algorithms by raising their security levels so as to avoid being influenced by such uncertainties in their decision makings.

This thesis studies the problem of resilient consensus in multi-agent systems where attackers may update the adversary agents' value arbitrarily. The objective of adversary agents is to prevent the regular agents from reaching consensus. We focus on solving the resilient consensus problem with emphasis on resource saving. In particular, we study the saving of four resources: (1) Communication resources, (2) memory resources, (3) energy resources, and (4) graph resources. The thesis consists of four parts dealing with these issues as follows:

(1) We consider resilient versions of discrete-time multi-agent consensus in the presence of faulty or even malicious agents in the network. To save communication resources, we develop event-triggered update rules, which can mitigate the influence of the malicious agents and at the same time reduce the communication. Each regular agent updates its state based on a given rule using its neighbors' information. Only when the triggering condition is satisfied, they send their current states to their neighbors. Otherwise, the neighbors will continue to use the state received in the last time. Assuming that a bound on the number of malicious nodes is known, we propose two update rules with event-triggered communication. They follow the so-called mean subsequence reduced (MSR) type algorithms and ignore values received from potentially malicious neighbors. We provide full characterizations for the necessary connectivity in the network for the algorithms to perform correctly, stated in terms of the notion of graph robustness. A numerical example is provided to demonstrate the effectiveness of the approach.

(2) We further extend the event-triggered update scheme for the problem of multi-agent consensus in the presence of faulty and malicious agents within the network. To save memory resources, we focus on the case where the agents take integer (or quantized) values. This quantization approach is moreover combined with the event-based communication protocols for solving the resilient consensus problem. To keep the regular agents from being affected by the behavior of faulty agents, algorithms of the MSR type are employed, where neighbors taking extreme values are ignored in the updates. Different from the real-valued case, the quantized version requires the update rule to be randomized. We characterize the error bound on the achievable level of consensus among the agents as well as the necessary structure for the network in terms of the notion of robust graphs. We verify via a numerical example the effectiveness of the proposed algorithms.

(3) We study the problem of resilient consensus in multi-agent networks with bounded input constraints. To save energy resources, model predictive control schemes are introduced to solve the resilient consensus problem with input constraints under synchronous and asynchronous communications. Each regular agent solves a constrained finite-time optimal problem with the states of its neighbors and updates its state based on a predetermined update rule. Assuming that the maximum number of malicious nodes is known, we derive algorithms which ignore the large and small values from neighbors to avoid the influence of the malicious nodes. It is guaranteed to attain resilient consensus under the topological condition expressed in terms of graph robustness. Simulation examples are provided to demonstrate the effectiveness of the proposed algorithm.

(4) To save graph resources, several modified MSR algorithms are proposed to solve resilient consensus problem for the case of mobile adversary models. We first discuss the three typical mobile malicious models in the area of computer science and apply them to the resilient consensus problem in multi-agent systems. We check that the related results for binary agreement in complete graphs can guarantee approximate resilient consensus. Moreover, we extend the mobile malicious models to non-complete graphs and propose several novel protocols which are guaranteed to work under certain classes of network connectivity conditions. In addition, based on the so-called Garay's mobile malicious model, we improve the update rules for the cured agents to reduce the necessary connections. Numerical examples are provided to check the efficacy of our results.