World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:9, No:06, 2015

Minimum Vertices Dominating Set Algorithm for Secret Sharing Scheme

Authors : N. M. G. Al-Saidi, K. A. Kadhim, N. A. Rajab

Abstract : Over the past decades, computer networks and data communication system has been developing fast, so, the necessity to protect a transmitted data is a challenging issue, and data security becomes a serious problem nowadays. A secret sharing scheme is a method which allows a master key to be distributed among a finite set of participants, in such a way that only certain authorized subsets of participants to reconstruct the original master key. To create a secret sharing scheme, many mathematical structures have been used; the most widely used structure is the one that is based on graph theory (graph access structure). Subsequently, many researchers tried to find efficient schemes based on graph access structures. In this paper, we propose a novel efficient construction of a perfect secret sharing scheme for uniform access structure. The dominating set of vertices in a regular graph is used for this construction in the following way; each vertex represents a participant and each minimum independent dominating subset represents a minimal qualified subset. Some relations between dominating set, graph order and regularity are achieved, and can be used to demonstrate the possibility of using dominating set to construct a secret sharing scheme. The information rate that is used as a measure for the efficiency of such systems is calculated to show that the proposed method has some improved values.

Keywords : secret sharing scheme, dominating set, information rate, access structure, rank
Conference Title : ICMCMSE 2015 : International Conference on Mathematical and Computational Methods in Science and Engineering
Conference Location : Paris, France
Conference Dates : June 25-26, 2015