{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 151
-
Number 4

Year of Publication: 2016

Authors:

Ratnakumari Challa, Devaraju Isuru, Kanusu Srinivasa Rao

10.5120/ijca2016911721

{bibtex}2016911721.bib{/bibtex}

Abstract

In the network several problems are caused due to the presence of malicious nodes. It is very important to find the malicious nodes in the network in order to eliminate the problems caused by those nodes. This paper proposes a model where Reed-Muller codes are used to find the locations of the malicious nodes and calculate the probability that a node is malicious. Based on the probability of each malicious node, the system localizes or discards the nodes which have higher error probability. Sometimes removal of a malicious node causes breakage of network into parts i.e. if it is an articulation point. It leads to the reconstruction of the network. This reconstruction process is very complex and expensive. In this case, such nodes cannot be discarded. To avoid the reconstruction of the network an algorithm is proposed to handle the malicious activity caused by an articulation point. Message tampering is the frequently occurred malicious activity in most of the networks when the communication takes place between source and destination. To handle message tampering at articulation points, this system performs error correction using Reed-Muller decoding algorithm.

References

1. Aho AV, Hopcroft JE. The design and analysis of computer algorithms. Pearson Education India; 1974 Sep 1.
2. Kacewicz A, Wicker S. Application of Reed-Muller codes for localization of malicious nodes. In Communications (ICC), 2010 IEEE International Conference on 2010 May 23 (pp. 1-7). IEEE.
3. Cooke B. Reed-Muller error correcting codes. MII Undergraduate J. Math. 1999; 1:21-7.
4. Wicker SB. Error control systems for digital communication and storage. Englewood Cliffs: Prentice hall; 1995 Jan 15.
5. Saini R, Khari M. Defining malicious behavior of a node and its defensive methods in Ad Hoc network. International Journal of Computer Applications. 2011 Apr; 20(4):18-21.
6. Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS). 1982 Jul 1; 4(3):382-401.
7. Ho T, Leong B, Koetter R, Médard M, Effros M, Karger DR. Byzantine modification detection in multicast networks using randomized network coding.
8. Padmanabhan VN, Simon DR. Secure traceroute to detect faulty or malicious routing. ACM SIGCOMM Computer Communication Review. 2003 Jan 1; 33(1):77-82.
9. Todd K. Moon, Lecture 9 Reed Muller Codes, ECE 7670", 1 April 2006 (2006-04-01), pages1-8, XP55004016.
10. Reed IS. A CLASS OF MIJLTIPLE-ERROR-CORRECTING CODES AND THE DECODING SCHEFE.
11. Rubin FR. enumerating all simple paths in a graph. IEEE Transactions on Circuits and Systems. 1978 Aug; 25(8):641-2.

Index Terms

Computer Science Information Sciences

Keywords

Coding Theory, Error Control Codes, Malicious Behaviour, Reed-Muller Codes.