A Survey Article on Wormhole Attack Detection and Security in Wireless Sensor Networks

International Journal of Computer Applications Foundation of Computer Science (FCS), NY, USA

Volume 177
Number 2

Year of Publication: 2017

Authors:
Harpal, Gaurav Tejpal, Sonal Sharma

10.5120/ijca2017915666

Abstract

For the duration of multihop portable methods, including ad-hoc and also indicator / probe sites, the prerequisite for co-operation amongst nodes in order to trade one another's offers shows the crooks to numerous security attacks. A particularly damaging attack is called your wormhole attack, where the harmful node documents command and also data traffic at 1 place and also routes that to the colluding node, which replays that locally. This could have a damaging result about Class Company by simply defending against nodes through obtaining tracks which will are far more than 2 trips away. During this paper, we active a light countermeasure for the wormhole attack, known as LITEWORP, which does not involve specific hardware. LITEWORP is quite suitable for resource-constrained multihop portable sites, including indicator / probe networks. Our own selection permits finding of one's wormhole, with rural location of one's harmful nodes. Simulators ultimate effects demonstrate that pretty much every wormhole is available and also remote in very a quick time period greater than a huge selection of scenarios. The final effects also demonstrate your portion with offers missing consequently of wormhole as soon as LITEWORP is used is negligible than the reduction encountered as soon as the tactic is
just not applied.

References

16. Arora, Mani, Rama Krishna Challa, and Divya Bansal. "Performance evaluation of routing protocols based on wormhole attack in wireless mesh networks." Computer and

Index Terms

Computer Science  Security

Keywords