

Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs-errata

RUTVIJ H. JHAVERI¹
SANKITA J. PATEL²
DEVESH C. JINWALA³

¹Shri Sád Vidya Mandal Institute of Technology, Bharuch, India
^{2, 3}Sardar Vallabhbhai National Institute of Technology, Surat, India
¹rutusoft@yahoo.com
²sjp@coed.svnit.ac.in
³dcj@svnit.ac.in

Abstract. This errata is published to clarify the differences between the paper and our previously published related work.

Keywords: R-AODV.

(Received First version received January 10th, 2012 / Accepted March 4th, 2012)

1 Clarification

In [2], we proposed a modification of AODV that explains functionality in the form of flow-charts; the PEAK value is calculated by RREP sequence number, routing table sequence number and number of replies that gives lower detection rate for malicious nodes, while in [1] PEAK value is calculated by number of sent out RREQs, number of received RREPs and routing table sequence number giving higher detection rate for malicious nodes. Thus, the key part of algorithm is completely different from the one discussed in [2]. Moreover, in [2] the proposal is discussed without any theoretical analysis and simulation results, while in [1], we thoroughly describe the background with various simulation results along with their analysis for different network parameters.

In [3], R-AODV protocol to protect MANET against Grayhole attack is tested in ideal conditions while the work in [1] extends the work by considering practical scenarios under different network conditions; in [3], simulations are done in ideal conditions assuming nearly 100 per cent PDR while in [1] simulations are carried out assuming real world scenarios. The paper [1] discusses the R-AODV protocol in detail and de-

picts that the approach can be equally applied to Blackhole attack; moreover, it includes results for Blackhole attack which was not tested in [3]. In [3], simulations are carried out with only one network parameter which is Network Size, while the paper [1] contains simulation results with five different parameters such as Network Size, Pause Time, Mobility, Traffic Load and Multiple Attackers; we analyze our approach with more results and more graphs. Thus, the R-AODV protocol is exhaustively tested with various network conditions under Blackhole and Grayhole attacks.

References

- [1] Jhaveri, R. H., Patel, S. J., and Jinwala, D. C. Improving route discovery for aodv to prevent blackhole and grayhole attacks in manets. *INFOCOMP Journal of Computer Science*, 11(1):1–12, 2012.
- [2] Jhaveri, R. H., Patel, S. J., and Jinwala, D. C. A novel approach for grayhole and blackhole attacks in mobile ad-hoc networks. In *Proceeding of Second International Conference on Advanced Computing & Communication Technologies*, pages 556–560, 2012.

- [3] Jhaveri, R. H., Patel, S. J., and Jinwala, D. C. A novel solution for grayhole attack in aodv based manets. In *Proceeding of International Conference on Advances in Communication, Network and Computing*, pages 60–67, 2012.