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

Volume 144
-
Number 4

Year of Publication: 2016

Authors:

Niroj Kumar Pani, Bikram Keshari Rath, Sarojananda Mishra

10.5120/ijca2016910507
{bibtex}2016910507.bib{/bibtex}

Abstract

Secure routing in wireless ad hoc network has been an active area of research and in recent years, a number of secure routing protocols have been introduced. These solutions may be classified as proactive, reactive, and hybrid based on the routing information update mechanism deployed. Studies reveal that the reactive (on-demand) ones often outperform the others due to their ability to adjust the amount of network overhead created to track the mobility in the network. However, the existing secure on-demand routing protocols have also some limitations. In this paper, the weakness of existing popular secure reactive routing protocols is analyzed on the ground of topology exposure. Then a new topology-hiding secure on-demand routing protocol, called TSOR is proposed based on timestamp approach and asymmetric cryptography. Security analysis of TSOR shows that it efficiently defeats all possible threats imposed by external or internal adversaries. Simulation results demonstrate that our protocol has a better capability of finding reliable and shortest routes in the presence of malicious nodes at the cost of low routing overhead.

References

1. R. Di Pietro, S. Guarino, N.V. Verde, J. Domingo-Ferrer, “Security in wireless ad-hoc networks – A survey”, Elsevier Computer Communications 51, 2014, pp.1–20.
2. Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang, “Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges”, IEEE Communications Surveys & Tutorials 13 (4), 2011, pp.658-672.
3. W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, W. Kellerer, “Castor: scalable secure routing for ad hoc networks”, in: Proc. IEEE Conference on Computer Communications (INFOCOM), 2010, pp. 1-9.
4. Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols”, IEEE Communications Surveys & Tutorials 10 (4), 2008 pp.78-93.
5. Pervaiz, O. Mohammad, Mihaela Cardei, and Jie Wu, "Routing security in ad hoc wireless networks", Springer US Network Security, 2010, pp.117-142.
6. N.M. Chacko, S. Sam, P.G.J. Leelipushpam, "A survey on various privacy and security features adopted in MANETs routing protocol", in: International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013, pp.508-513.
7. S. Kumar, G. Pruthi, A. Yadav, M. Singla, "Security Protocols in MANETs", in: Second International Conference on Advanced Computing & Communication Technologies (ACCT), 2012, pp.530-534.
8. P. Papadimitratos, Z.J. Haas, "Secure data communication in mobile ad hoc networks", J. Select. Areas Commun. 24 (2), 2006, pp.343–356.
9. Y.C. Hu, A. Perrig, D.B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks", in: Proc. ACM International Conference on Mobile Computing and Networking (MOBICOM), Atlanta, 2002, pp.23-28.
10. Jiang, Tingyao, Qinghua Li, and Youlin Ruan, "Secure dynamic source routing protocol", in: Proc. IEEE International Conference on Computer and Information Technology (CIT'04), 2004.
11. M.G. Zapata, "Securing ad hoc routing protocols", in: Proc. ACM workshop on wireless Security, Atlanta, Sep 2002, pp.1-9.
12. K. Sanzgir, B. Dahill, "A secure routing protocol for ad hoc networks", in: Proc. IEEE International Conference on Network Protocols, 2002, pp.1-10.
13. Acs, Gergely, Levente Buttyan, and Istvan Vajda, "Provable security of on-demand distance vector routing in wireless ad hoc networks", Springer Security and Privacy in Ad-hoc and Sensor Networks, 2005, pp.113-127.
14. S. Ghazizadeh, O. Ilghami, E. Sirin, "Security-aware adaptive dynamic source routing protocol", in: Proc. IEEE Conference on Local Computer Networks, 2002.
15. Yujun Zhang, Tan Yan, Jie Tian, Qi Hu, Guiling Wang, Zhongcheng Li, "TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks", Elsevier Ad Hoc Networks 21, 2014, pp.109–122.
16. Yih-Chun Hu, A. Perrig, D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks", in Proc. IEEE Conference on Computer Communications (INFOCOM), 2003, pp.1976-1986.
17. http://www.isi.edu/nsam/ns.
18. J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, J. Jetcheva, "A performance comparison of

multi-hop wireless ad hoc network routing protocols", in: Proc. ACM MOBICOM, Oct. 1998, pp.85–97.

Index Terms

Computer Science Wireless

Keywords

Ad-hoc networks, Security attacks, Secure routing.