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

Volume 135
-
Number 12

Year of Publication: 2016

Authors:

Manish Kumar Suman, Sini Shibu

10.5120/ijca2016908488
{bibtex}2016908488.bib{/bibtex}

Abstract

Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. An ad-hoc wireless network is a collection of nodes that come together to dynamically create a network, with no fixed infrastructure or centralized administration. In mobile ad-hoc networks, data transmission is performed within an untrusted wireless environment. The lack of centralized infrastructure in ad-hoc network makes it vulnerable to various attacks. Sybil attack is one of the serious attacks, which form a serious threat in the networks, especially against many ad hoc wireless routing protocols, and location based wireless security system.

In the Sybil attack incorporates a malicious device with the ability to illegitimately take on several identities in the same network. The forged identity from a malicious device is called a Sybil node. A malicious device can obtain an identity for a Sybil node in two different ways; (a) generating a new identity; or (b) taking the identity from an existing node (with the cooperation of the node or by developing a spoofing attack). We identify two types of Sybil attacks. In the

first type, malicious nodes do not take part in finding routes, meaning that, legitimate nodes do not know their existence. In the second type, malicious nodes do create route advertisements and legitimate nodes are aware of the existence of malicious nodes, just do not know they are malicious. Some of the researchers have proposed many solutions for Sybil attack.

In this paper, an efficient method to detect a Sybil attack called modified Sybil detection AODV protocol has been proposed. Detection of Sybil attack is performed using number of hops in different paths from source to destination and delay of each node in different paths from source to destination. The destination is able to detect both kinds of Sybil attacks. The performance of modified Sybil detection AODV protocol is justified by simulations.

References

1. Christian Lochert, Bj¨ornScheuermann, and Martin Mauve, A survey on congestion control for mobile ad hoc networks, Wireless Communications & Mobile Computing, Vol. 7, pp.655 – 676, June.2007
2. TiranuchAnantvalee and Jie Wu, A Survey on Intrusion Detection in Mobile Ad Hoc Networks, Wireless Mobile Network Security, pp.170-196, 2003.
3. Yongguang Zhang AndWenke Lee, Intrusion Detection in Wireless Ad-Hoc Networks, MOBICOM, 2000, pp. 275-283
4. Andr´eWeimerskirch and Gilles Thonet, Distributed Light-Weight Authentication Model for Ad-hoc Networks, Lecture Notes In Computer Science; Vol. 2288, pp. 341 354, 2001
5. I. Chlamtac, M. Conti, and J. Liu, Mobile Ad Hoc Networking: Imperatives and Challenges, Ad Hoc Networks, vol. 1, pp. 13-64, no. 1, 2003.
6. L. Buttyan, J.P. Hubaux, Report on a working session on security in wireless ad hoc networks, Mobile Computing and Communications Review 6 (4), 2002.
7. Ejaz Ahmed, KashanSamad, WaqarMahmood, Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks, AusCERT2006 R&D Stream Program, Information Technology Security Conference, May 2006, Australia.
8. J.P. Hubaux, L. Buttyan, S. Capkun, The quest for security in mobile ad hoc networks, in: Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), October, 2001
9. Shuyao Yu, Youkun Zhang, Chuck Song and Kai Chen, A security architecture for Mobile Ad Hoc Networks, Available:http://blrc.edu.cn/blrcweb/publication/kc2.pdf.
10. J. Lundberg, Routing Security in Ad Hoc Networks, 2000.Availabe: http://citeseer.nj.nec.com/400961.html.
11. HAO YANG, HAIYUN LUO, FAN YE, SONGWU LU andAND LIXIA ZHANG, Security in mobile ad hoc networks: Challenges and solutions, IEEE Wireless Communications, vol. 11, pp. 38-47, Feb., 2004.
12. IoannaStamouli, “Real-time Intrusion Detection for Ad hoc Networks”, M. Sci. dissertation, University of Dublin, 2003
13. F. Stajano, and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks,” Proc. 7th Int’l. Workshop on Security Protocols, Cambridge, UK, April 1999, pp. 172-194.
14. J.-F. Raymond, “Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems,” Proc. Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA,

July 2000, pp. 7-26.

15. Bo Sun, Kui Wu, Udo W. Pooch. Alert aggregation in mobile ad hoc networks.Proc. ACM workshop on Wireless security, 2003.

16. M. Drozda, H. Szczerbicka. Artificial Immune Systems: Survey and Applications in Ad Hoc Wireless Networks.Proc. 2006 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'06), pp. 485-492, Calgary, Canada, 2006.

17. P. Papadimitratos, and Z.J. Haas, “Securing the Internet Routing Infrastructure,” IEEE Communications, vol. 10, no.40, October 2002, pp. 60-68.

18. Y.-C. Hu, A. Perrig, and D.B. Johnson, “Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Networks,” Proc. 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom’03), San Francisco, CA, April 2003

19. Yih-Chun Hu, Adrian Perrig, and Dave Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols."In Proceedings of the ACM Workshop on Wireless Security (WiSe), San Diego, California, September 2003.

20. Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks,” Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.

21. L. Zhou, and Z.J. Haas, “Securing Ad hoc Networks,” IEEE Network Magazine, vol. 6, no. 13, November/December 1999, pp. 24-30.

22. D.B. Johnson, D.A. Maltz, Y.-C.Hu, and J.G. Jetcheva, The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR), Internet Draft, draft-ietf-manet-dsr-07.txt, February 2002.

23. C.E Perkins, E.M. Royer, and S. Das, “Ad hoc On-demand Distance Vector (AODV),” RFC 3561, July. 2003.

24. C.E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Proc. SIGCOMM ’94 Conf. Communications Architectures, Protocols and Applications, ACM Press, 1994, pp. 234–244.

25. Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks."In Wireless Networks Journal, 11(1), 2005.

26. A. Perrig, R. Canetti, D. Song and J.D. Tygar, Efficient and secure source authentication for multicast, in: Proceedings of the Network and Distributed System Security Symposium, NDSS’01 (February 2001) pp. 35–46.

27. P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation (CNDS), January 2002.

28. P. Papadimitratos and Z.J. Haas, “Secure Message Transmission in Mobile Ad Hoc Networks,” Elsevier Ad Hoc Networks J., Elsevier, vol. 1, no. 1, 2003, pp. 193–209.

29. KimayaSanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding-Royer, “Authenticated Routing for Ad Hoc Networks”, Proceedings of IEEE journal on selected areas in communications, Volume 23, No. 3, March 2005

30. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, “A Secure Routing Protocol for Ad hoc Networks”, Proc. 10th IEEE Int’l. Conf. Network Protocols (ICNP’02), IEEE Press, 2002, pp. 78-87.

31. M.G. Zapata, N. Asokan, Securing ad hoc routing protocols, in: Proceedings of ACM Workshop on Wireless Security (WiSe), Atlanta, September 2002.

32. P. Papadimitratos, and Z.J. Haas, “Secure Link State Routing for Mobile Ad hoc Networks,” Proc. IEEE Workshop on Security and Assurance in Ad hoc Networks, IEEE Press, 2003, pp. 27-31.

Index Terms

Computer Science Wireless

Keywords

Ad-hoc networks, Security, Sybil attack, Attacked path, Wireless.