Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XXII, Issue 85, January-March 2016
Pages 18-26

On Implementation of Resilient Networks. A Case Study

Luminița Copaci, Angelica Bacivarov
EUROQUALROM, Faculty of Electronics, Telecommunications and Information Technology,
University "Politehnica" of Bucharest, Romania
lcopaci@yahoo.com

Abstract
The cost of failures within communication networks is significant. The communication networks – and the Internet in particular – are still vulnerable to malicious attacks, human mistakes such as misconfigurations, and a range of environmental challenges. In the first part of this paper the concept of resilience is defined and analyzed; its significance in different fields is comparatively analyzed. The main goal of this paper is to quantify via analytical models and simulation experiments the damage that a successful attacker can have on the performance of a communication network In particular, the paper is focused on studying resilience of ad hoc network. Consequently, the DoS attacks are analysed in order to assess the damage that difficult-to-detect attackers can cause. Our methodology is to study DoS resilience via a new and general class of protocol compliant denial-of-service attacks, which we refer to as JellyFish (JF). The JellyFish target closed-loop flows that are responsive to network conditions such as delay and loss. In addition to the JF attack, the Black Hole attack is studied, too.

Keywords: Communication networks, Resilience, Models, Simulation, Malicious attacks, DoS attacks, JellyFish, Black Hole

References:

[1] E. Hollnagel, D.D. Woods, and N Leveson. Reslience Engineering: Concepts and Precepts. Ashgate Publishing, 2006.
[2] S. Bohacek, J. Hespanha, J. Lee, C. Lim, and K. Obraczka. TCP-PR: TCP for persistent packet reordering, Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems, May 2003.
[3] S. A. Begum, Techniques for resilience of Denial of service Attacks in Mobile Ad Hoc Networks, International Journal of Scientific & Engineering Research, Volume 3, Issue 3, March 2012.
[4] P. Smith, D. Hutchinson, M. Scholler, A. Fessi. M.Karaliopoulos, C. Lac, B. Plattner, Network Resilience: A Systematic Approach, IEEE Communications Magazine, pp. 88-97, July 2011.
[5] D.J Smith, Reliability, Maintainability and Risk, 7th ed., Elsevier, 2005.
[6] V. Gupta, S.V. Krishnamurthy, and M. Faloutsos. Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks, Proceedings of MILCOM, 2002.
[7] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks, Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking (MobiCom 2002), September 2002.
[8] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Ad Hoc Networks, 2003.

[9] Alin Copaci, Luminița Copaci, “Ensuring the Resilience against Denial of Service Attacks in Ad-hoc Networks”, Proceedings of the 11th IEEE International Conference in Quality and Dependability, Sinaia, sept 2008, pp. 179-186.
[10] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols, Proceedings ofWiSe 2003, September 2003.
[11] David B. Johnson and D. Maltz. The dynamic source routing protocol for mobile ad hoc networks (DSR), April 2003.
[12] V Kawadia and P. R. Kumar. Power control and clustering in ad hoc networks, Proceedings of IEEE Infocom, 2003.
[13] A. Kuzmanovic and E. Knightly. Low-Rate TCP-Targeted Denial of Service Attacks, Proceedings of ACM SIGCOMM 2003, Karlsruhe, Germany, August 2003.
[14] P. Michiardi and R. Molva. CORE: A Collaborative Reputation Mechanism To Enforce Node Cooperation In Mobile Ad Hoc Networks, Proceedings of The 6th IFIP Communications and Multimedia Security Conference, Portorosz, Slovenia, September 2002.
[15] P. Papadimitratos and Z. Haas. Secure data transmission in mobile ad hoc networks., Proceedings of WiSe, 2003.
[16] https://en.wikipedia.org/wiki/Denial-of-service_attack (accessed 10.01. 2015).
[17] F. Legendre, T. Hossmann, F. Sutton, B. Plattner, 30 Years of Wireless Ad Hoc Networking Research: What about Humanitarian and Disaster Relief Solutions? What are we still missing?, International Conference on Wireless Technologies for Humanitarian Relief (ACWR 11), 2011.
[18] M. Zhang, B. Karp, S. Floyd, and L. Peterson. RR-TCP: A reordering robust TCP with DSACK, Proceedings of IEEEICNP 2003, Atlanta, November 2003.
[19] I. Aad, J.-P. Hubaux and E. Knightly. Impact of Denial of Service Attacks on Ad Hoc Networks, in IEEE Transactions on Networking, 2008 .
[20] https://en.wikipedia.org/wiki/Resilience (accessed 20.04. 2014).