80%左右,说明 TOR 算法采用的信任机制对自私行为具有较好的抑制作用.TOR 算法平均转发延时升高是因为当自私节点增多时,正常节点需要花费更长的时间才能遇到下一跳可信的转发节点.而 Epidemic 算法和 Prophet 算法由于对自私行为没有抑制,很多消息在转发过程中生存时间超时被丢弃,成功转发的消息数量减少,致使两种算法在自私节点数超过 10 时,传递成功率和平均转发延时降低比较明显.SAW 算法由于采用两跳转发策略直接将消息传递给目的节点,使得在转发延迟方面受自私行为影响较小.

由图 8(c)和图 8(d)看出,TOR 算法在网络交付代价和平均跳数方面有优势.这是因为 TOR 算法采用基于信任梯度递增的消息传递策略,只有遇到信任度更高的转发节点时才传递消息,所以不受自私行为影响.Epidemic 和 Prophet 算法随着自私节点规模的增大,其网络交付代价和平均跳数呈下降趋势,这是由于自私节点不参与消息转发,使得网络中消息副本总数减少所致.而 SAW 算法性能表现最优,是因为该算法产生的消息副本数最少的缘故.

5 结束语

提出了一种基于信任机制的机会网络安全路由决策算法 TOR,该算法根据目的节点采集到的信任证据链和消息延时时间计算转发节点的信任度,存储在信任向量表中.信任证据采集利用层状硬币模型和数字签名机制,在传递过程中将节点转发证据动态捆绑到消息包上,由消息携带到目的节点.该方法具有较好的及时性和安全性,付出的额外代价较小.节点周期性地将具有签名和最新的信任向量表利用泛洪方式反馈到网络中,在各个节点迭代形成由多维行向量集组成的只读可信路由表 TRT,作为下一跳转发节点选择和消息副本数分割的决策依据,利用签名和时间戳机制防止信任向量表在反馈过程中被恶意节点篡改,有效保证了路由表的安全性和可靠性.消息沿着信任梯度递增的方向传递,不仅有效抑制恶意行为,而且大大提高了消息投递的成功率,降低了消息投递延时.

References:

[1] Xiong YP, Sun LM, Niu JW, Liu Y. Opportunistic networks. Ruan Jian Xue Bao/Journal of Software, 2009,20(1):124−137 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3467.htm

[2] Su JS, Hu QL, Zhao BK, Peng W. Routing techniques on delay/disruption tolerant networks. Ruan Jian Xue Bao/Journal of Software, 2010,21(1):119−132 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3689.htm [doi: doi: 10.3724/SP.J.1001.2010.03689]

[3] Wu Y, Li JH, Lin C. Survey of security and trust in opportunistic networks. Journal of Computer Research & Development, 2013, 50(2):278−290 (in Chinese with English abstract).

[4] Zhu H, Du S, Gao Z, Dong M, Cao Z. A probabilistic misbehavior detection scheme toward efficient trust establishment in delay tolerant networks. IEEE Trans. on Parallel & Distributed Systems, 2014,25(1):22−32.

[5] Li Y, Yu JH, You XH. An incentive protocol for opportunistic networks with resources constraint. Chinese Journal of Computers, 2013,36(5):947−956 (in Chinese with English abstract).

[6] Lu R, Lin X, Zhu H, Shen X, Preiss B. Pi: A practical incentive protocol for delay tolerant networks. IEEE Trans. on Wireless Communications, 2010,9(4):1483−1493.

[7] Ayday E, Fekri F. An iterative algorithm for trust management and adversary detection for delay-tolerant networks. IEEE Trans. on Mobile Computing, 2012,11(9):1514−1531.

[8] Nelson SC, Bakht M, Kravets R. Encounter-Based routing in DTNs. In: Proc. of the 28th Int'l Conf. on Computer Communications (INFOCOM 2009). Piscataway: IEEE, 2009. 846−854. [doi: 10.1109/INFCOM.2009.5061994]

[9] Chen IR, Bao F, Chang MJ, Cho JH. Dynamic trust management for delay tolerant networks and its application to secure routing. IEEE Trans. on Parallel & Distributed Systems, 2014,25(5):1200−1210.

[10] Li Q, Cao G. Mitigating routing misbehavior in disruption tolerant networks. IEEE Trans. on Information Forensics & Security, 2012,7(2):664−675.

[11] Li F, Wu J, Srinivasan A. Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets. In: Proc. of the 28th Int'l Conf. on Computer Communications (INFOCOM 2009). Piscataway: IEEE, 2009. 2428−2436. [doi: 10.1109/INFCOM.2009.5062170]

[12] Chen BB, Chan MC. MobiCent: A credit-based incentive system for disruption tolerant network. In: Proc. of the 29th Int'l Conf. on Computer Communications (INFOCOM 2010). Piscataway: IEEE, 2010. 1−9. [doi: 10.1109/INFCOM.2010.5462136]

[13] Burgess J, Bissias GD, Corner MD, Levine BN. Surviving attacks on disruption-tolerant networks without authentication. In: Proc. of the 8th ACM Int'l Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc 2007). New York: ACM Press, 2007. 61−70. [doi: 10.1145/1288107.1288116]

[14] Zhao H, Yang X, Li X. cTrust: Trust management in cyclic mobile ad hoc networks. IEEE Trans. on Vehicular Technology, 2013, 62(6):2792−2806.

[15] Wang B, Chen XX. Opportunistic routing algorithm based on trust model for ad hoc network ad hoc. Journal on Communications, 2013,34(9):92−104 (in Chinese with English abstract).

[16] Zhang SF, Huang D, Chen Z, Wu GX. Optimal stopping decision method for routing of opportunistic networks. Ruan Jian Xue Bao/Journal of Software, 2014,25(6):1291−1300 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4434.htm [doi: 10.13328/j.cnki.jos.004434]

附中文参考文献:

[1] 熊永平,孙利民,牛建伟,刘燕.机会网络.软件学报,2009,20(1):124−137. http://www.jos.org.cn/1000-9825/3467.htm

[2] 苏金树,胡乔林,赵宝康,彭伟.容延容断网络路由技术.软件学报,2010,21(1):119−132. http://www.jos.org.cn/1000-9825/3689.htm [doi: doi: 10.3724/SP.J.1001.2010.03689]

[3] 吴越,李建华,林闯.机会网络中的安全与信任技术研究进展.计算机研究与发展,2013,50(2):278−290.

[5] 李云,季弘,尤肖虎.资源受限的机会网络节点激励策略研究.计算机学报,2013,36(5):947−956.

[15] 王博,陈训逊.Ad Hoc 网络中一种基于信任模型的机会路由算法.通信学报,2013,34(9):92−104.

[16] 张三峰,黄迪,陈州,吴国新.一种面向机会网络路由的最优停止决策方法.软件学报,2014,25(6):1291−1300. http://www.jos.org.cn/1000-9825/4434.htm [doi: 10.13328/j.cnki.jos.004434]

李峰(1978－),男,山东德州人,博士,讲师,CCF 专业会员,主要研究领域为机会网络,信任管理.

司亚利(1981－),女,副教授,CCF 学生会员,主要研究领域为移动推荐,信任管理.

陈真(1987－),男,博士,CCF 学生会员,主要研究领域为信任管理,服务计算.

鲁宁(1984－),男,博士,讲师,主要研究领域为网络安全.

申利民(1962－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为柔性软件,协同计算.