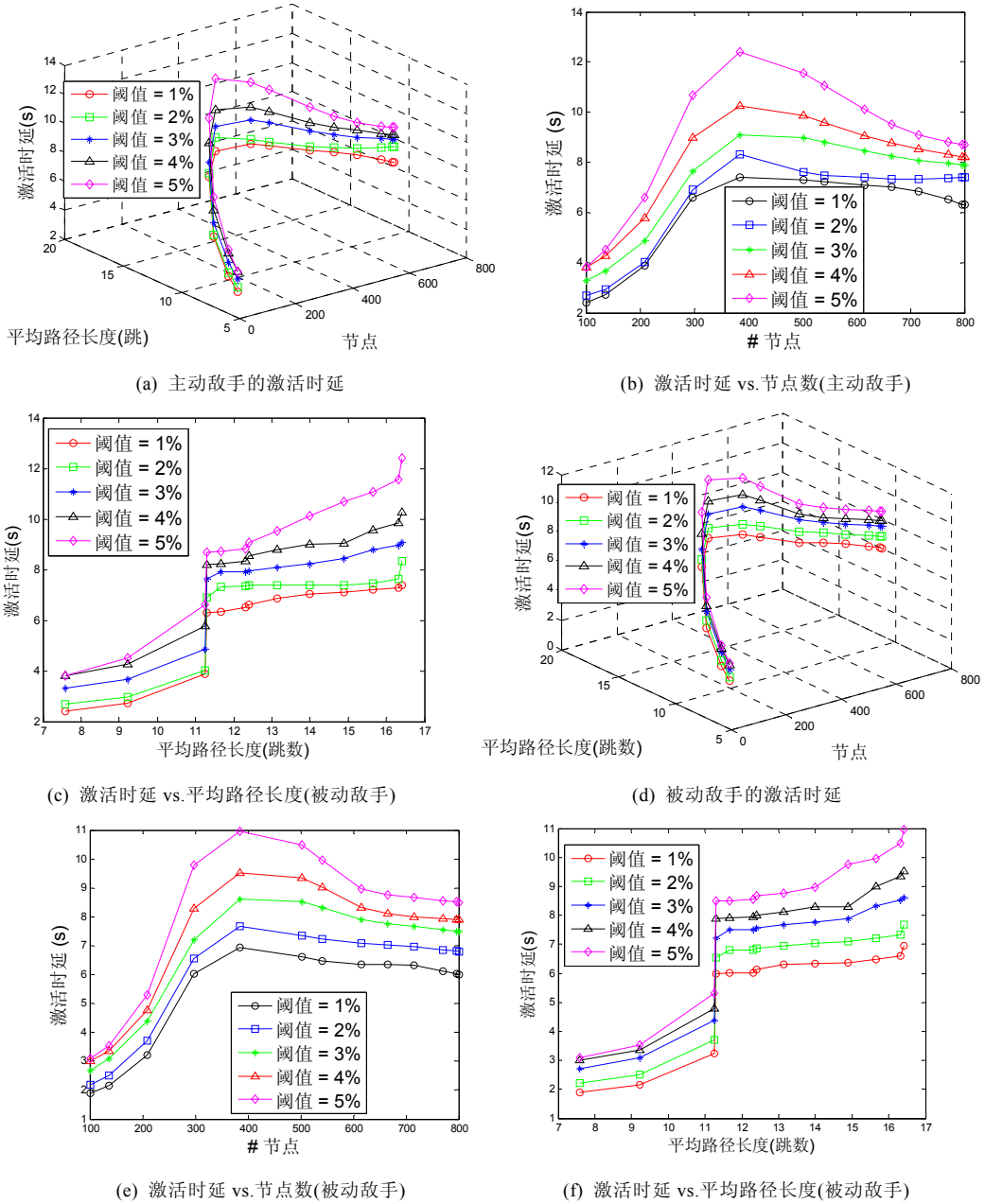
的原因是:节点数量增多时,网络总流量提高并且网络的路径变化增大,这些变化容易被 Sink 节点发现.另外,阈值和网络规模相同时,对于主动敌手的探测漏报率比探测被动敌手的漏报率更低.这是因为主动敌手采取了反探测策略,如随机转发或篡改数据包,反而让 Sink 能更容易判断攻击发生.

图 10 展示了 Pworm 在不同阈值和敌手模型下的激活时延.



(a) 主动敌手的激活时延

(b) 激活时延 vs.节点数(主动敌手)

(c) 激活时延 vs.平均路径长度(被动敌手)

(d) 被动敌手的激活时延

(e) 激活时延 vs.节点数(被动敌手)

(f) 激活时延 vs.平均路径长度(被动敌手)

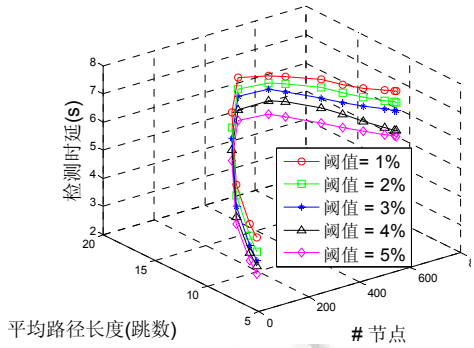
Fig.10 Activation latency shown for active and Passive adversaries

图 10 主动敌手和被动敌手的激活延迟变化

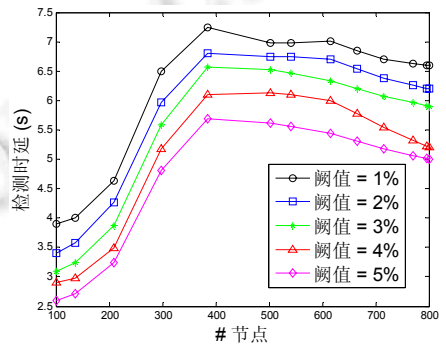
从图 10 中可以看出,激活时延变化趋势为:激活时延先随着网络规模的增大而增长;当网络规模达到 300 个~400 个节点时,激活时延的值最大;之后,激活时延的值逐渐缩短.原因主要来自两方面:首先,当网络规模较少

时,网络路径较短,此时,Sink 节点能很快地收集网络拓扑信息,这时,激活时延也较短;其次,当节点数量大于 300 个节点时,随着节点数量增大,网络中节点更加密集,每个节点几乎都能找到一条更短的路径到达 Sink 节点,使得网络平均路径长度反而变短,此时,激活时延减少.图 10(c)为激活时延随网络平均路径长度的变化关系,可以看出:网络规模小时,激活时延较短.图 10(d)~图 10(f)所示被动敌手模型中,激活时延的变化情况类似于图 10(b),但阈值相同时,被动敌手中激活时延的值比主动敌手中更少.

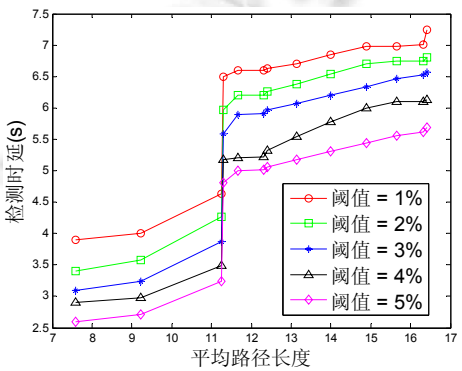
图 11 为不同阈值和敌手模型下的检测时延.检测时延的变化非常类似于激活时延的变化情况,只是检测时延的值略高.



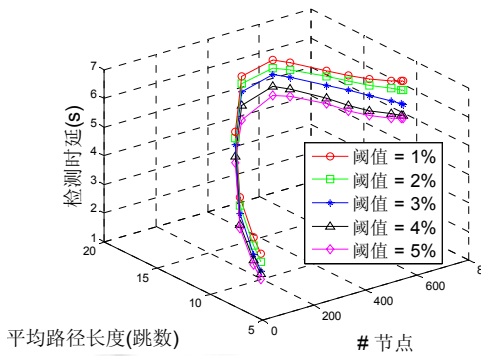
(a) 主动敌手的检测时延



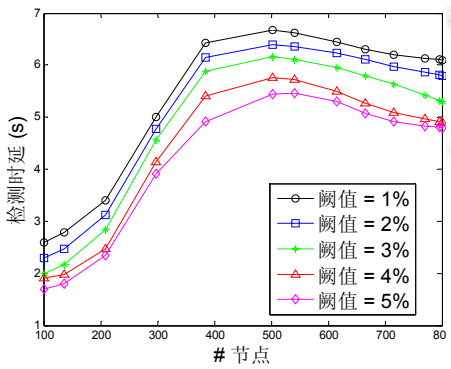
(b) 检测时延 vs.节点数(主动敌手)



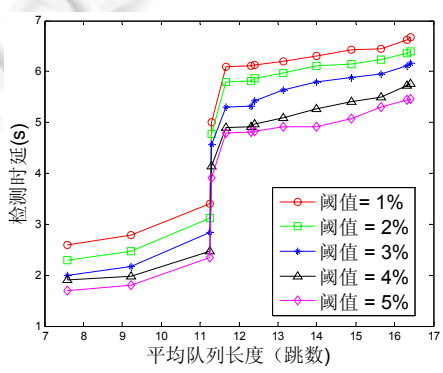
(c) 检测时延 vs.平均路径长度(被动敌手)



(d) 被动敌手的检测时延



(e) 被动敌手的检测时延



(f) 检测时延 vs.平均路径长度(被动敌手)

Fig.11 Detection latency shown for active and passive adversaries

图 11 主动敌手和被动敌手的激活检测变化

我们可以看出:网络中节点数量越多时,网络的总流量和路径的长度越大.此时,Sink 节点收集网络路径所需时间也变长,使得检测时延增大.

总之,由图 10 和图 11 可见:阈值较大时,激活时延和检测时延均增长.这是因为阈值较大时,Sink 节点需要较长时间来观测变化路径的比例.不同阈值时,检测时延和激活时延的变化规律一致,均为网络规模较小时,时延以较快的速度提升到一个最大值;之后,随着网络越来越密集而降低.图 10(c)、图 10(f)以及图 11(c)、图 11(f)中,网络平均路径长度的变化也遵循先增大后减小的趋势.路径长度短时,两种时延的值均较小;反之,网络规模的增大,引起延迟和平均路径长度均增大.

6 结 论

对于无线传感器网络和无线自组织网络而言,虫洞攻击是最严重的威胁之一.现有的虫洞探测方法或者需要较强的网络拓扑假设,或需要额外硬件等,这些问题限制了现有方法在传感器网络中的应用.本文基于虫洞节点对网络流量和拓扑影响的观察,提出了一个轻量级、被动式、实时的虫洞攻击探测方案 Pworm.通过安全包标记,我们将检测过程融入正常的数据包转发过程中,再利用虫洞攻击的两个特征——路径变化和路径长度缩短对虫洞进行实时检测.因此,Pworm 不仅能探测主动和被动虫洞敌手,还能定位虫洞的位置.实验结果表明:我们的方案误报率为 0,漏报率低于 5%,整体时延不超过 14s,能实时、准确的检测虫洞节点.

References:

[1] Capkun D, Buttyán L, Hubaux JP. Sector: Secure tracking of node encounters in multi-hop wireless networks. In: Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks. 2003. 21−32. [doi: 10.1145/986858.986862]

[2] Dong DZ, Li M, Liu Y, Li XY. Topological detection on wormholes in wireless ad hoc and sensor networks. In: Proc. of the IEEE ICNC. 2009. 314−323. [doi: 10.1109/ICNP.2009.5339673]

[3] Ban XM, Rik S, Cao J. Local connectivity tests to identify wormholes in wireless networks. In: Proc. of the ACM MobiHoc. 2011. 13−24. [doi: 10.1145/2107502.2107519]

[4] Khalil I, Bagchi S, Shroff NB. Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks. In: Proc. of the IEEE Securecomm and Workshops. 2006. 1−12. [doi: 10.1109/SECCOMW.2006.359564]

[5] Hu L, Evans D. Using directional antennas to prevent wormhole attacks. In: Proc. of the NDSS. 2004. 1−9.

[6] Ho JW, Wright M, Das SK. Distributed detection of mobile malicious node attacks in wireless sensor networks. Ad Hoc Networks, 2012,10(3):512−523. [doi: 10.1016/j.adhoc.2011.09.006]

[7] Lu XP, Dong DZ, Liao XK. MDS-Based wormhole detection using local topology in wireless sensor networks. Int'l Journal of Distributed Sensor Networks, 2012,2012:1−9. [doi: 10.1155/2012/145702]

[8] Hu YC, Perrig A, Johnson DB. Packet leashes: A defense against wormhole attacks in wireless networks. In: Proc. of the IEEE INFOCOM. 2003. 1976−1986. [doi: 10.1109/INFCOM.2003.1209219]

[9] Wang X, Wong J. An end-to-end detection of wormhole attack in wireless ad-hoc networks. In: Proc. of the Computer Software and Applications. 2007. 39−48. [doi: 10.1109/COMPSAC.2007.63]

[10] Lazos L, Poovendran R. Serloc: Secure range-independent localization for wireless sensor networks. In: Proc. of the ACM Workshop on Wireless Security. 2004. 1−8. [doi: 10.1145/1023646.1023650]

[11] Wu JF, Chen HL, Lou W, Wang ZB, Wang Z. Label-Based DV-hop localization against wormhole attacks in wireless sensor networks. In: Proc. of the IEEE Networking, Architecture and Storage. 2010. 79−88. [doi: 10.1109/NAS.2010.41]

[12] Chen HL, Chen WD, Wang ZB, Wang Z, Li YJ. Mobile beacon based wormhole attackers detection and positioning in wireless sensor networks. Int'l Journal of Distributed Sensor Networks, 2014, 2014. 1−10. [doi: 10.1155/2014/910242]

[13] Chen HL, Lou W, Wang Z. Secure localization against wormhole attacks using conflicting sets. In: Proc. of the 29th IEEE Int'l Performance Computing and Communications (IPCCC 2010). 2010. 25−33. [doi: 10.1109/PCCC.2010.5682340]

[14] Wang W, Bhargava B. Visualization of wormholes in sensor networks. In: Proc. of the ACM Workshop on Wireless Security. 2004. 51−60. [doi: 10.1145/1023646.1023657]

[15] Xu Y, Ouyang Y, Le Z, Ford J, Makedon F. Analysis of range-free anchor-free localization in a WSN under wormhole attack. In: Proc. of the ACM MSWiM. 2007. 344−351. [doi: 10.1145/1298126.1298185]

[16] Song SJ, Wu HJ, Choi BY. Statistical wormhole detection for mobile sensor networks. In: Proc. of the IEEE ICUFN. 2012. 322−327. [doi: 10.1109/ICUFN.2012.6261721]

[17] Chan KS, Alam MR. Topology comparison-based wormhole detection for MANET. Int'l Journal of Comunication Systems, 2014, 27(7):1051−1068. [doi: 10.1002/dac.2397]

[18] Maheshwari R, Gao J, Das SR. Detecting wormhole attacks in wireless networks using connectivity information. In: Proc. of the INFOCOM. 2007. 107−115. [doi: 10.1109/INFCOM.2007.21]

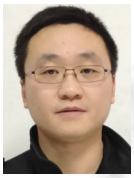
[19] Song N, Qian L, Li X. Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach. In: Proc. of the IEEE IPDSP. 2005. 8−15. [doi: 10.1109/IPDPS.2005.471]

[20] Zhao Z, Bo W, Dong X, Yao L, Gao F. Detecting wormhole attacks in wireless sensor networks with statistical analysis. In: Proc. of the IEEE ICIE. 2010. 251−254. [doi: 10.1109/ICIE.2010.66]

[21] Buttyán L, Dóra L, Vajda I. Statistical wormhole detection in sensor networks. Security and Privacy in Ad-hoc and Sensor Networks, 2005,3813:128−141. [doi: 10.1007/11601494_11]

[22] Chen HL, Lou W, Wang Z, Wu JF, Wang ZB, Xia AH. Securing DV-hop localization against wormhole attacks in wireless sensor networks. Pervasive and Mobile Computing, 2015,16:22−35. [doi: 10.1016/j.pmcj.2014.01.007]

[23] Ji SY, Chen TT, Zhong S. Wormhole attack detection algorithms in wireless network coding systems. IEEE Trans. on Mobile Computing, 2015,14(3):660−674. [doi: 10.1109/TMC.2014.2324572]



鲁力(1978－),男,贵州铜仁人,博士,副教授,博士生导师,CCF 会员,主要研究领域为无线系统安全.

Muhammad Jawad HUSSAIN (1982－),男,博士生,主要研究领域为无线系统安全.

朱金奇(1981－),女,博士,副教授,主要研究领域为无线网络及安全.