

{tag}____
Journal
Number 1 - Article 5

{/tag}

MANETs

© 2010 by IJCA____

Year of Publication: 2010

Authors:

Farhan Abdel-Fattah

Zulkhairi Md. Dahalin

Shaidah Jusoh

10.5120/1011-48

{bibtex}spe48t.bib{/bibtex}

Abstract

Mobile Ad hoc networks (MANETs) are susceptible to several types of attacks due to their open medium, lack of centralized monitoring and management point, dynamic topology and other features. Many of the intrusion detection techniques developed on wired networks cannot be directly applied to MANET due to special characteristics of the networks. However, all such intrusion detection techniques suffer from performance penalties and high false alarm rates. In this paper, we propose a novel intrusion detection method by combining two anomaly methods Conformal Predictor k-nearest neighbor and Distance-based Outlier Detection (CPDOD) algorithm. A series of experimental results demonstrate that the proposed method can effectively detect anomalies with low false positive rate, high detection rate and achieve higher detection accuracy.

Reference

- Detecting outliers using transduction and statistical testing. In KDD '06: Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, pages 55_64, New York, NY, USA, 2006. ACM.
- Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. *ACM Comput. Surv.*, 41(3):1_58, 2009.
- Hongmei Deng, Roger Xu, Jason Li, Frank Zhang, Renato Levy, and Wenke Lee. Agent-based cooperative anomaly detection for wireless ad hoc networks. In ICPADS '06: Proceedings of the 12th International Conference on Parallel and Distributed Systems, pages 613_620, Washington, DC, USA, 2006.
- Yingfang Fu, Jingsha He, and Guorui Li. A distributed intrusion detection scheme for mobile ad hoc networks. *Computer Software and Applications Conference, Annual International*, 2:75_80, 2007.
- Alex Gammerman and Volodya Vovk. Prediction algorithms and confidence measures based on algorithmic randomness theory. *Theor. Comput. Sci.*, 287(1):209_217, 2002.
- Alexander Gammerman and Vladimir Vovk. Hedging predictions in machine learning. *Comput. J.*, 50(2):151_163, 2007.
- GloMoSim. Glomosim website, June 2007.
- Yi-an Huang, Wei Fan, Wenke Lee, and Philip S. Yu. Cross-feature analysis for detecting ad-hoc routing anomalies. In *ICDCS '03: Proceedings of the 23rd International Conference on Distributed Computing Systems*, page 478, Washington, DC, USA, 2003. IEEE Computer Society.
- A. Karygiannis, E. Antonakakis, and A. Apostolopoulos. Host-based network monitoring tools for manets. In *PE-WASUN '06: Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks*, pages 153_157, New York, NY, USA, 2006. ACM.
- Yang Li, Binxing Fang, Li Guo, and You Chen. Network anomaly detection based on tcm-knn algorithm. In *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pages 13_19, New York, NY, USA, 2007. ACM.
- Yang Li and Li Guo. An active learning based tcm-knn algorithm for supervised network intrusion detection. *Computers & Security*, 26(7-8):459_467, 2007.
- Yihua Liao and V. Rao Vemuri. Use of k-nearest neighbor classifier for intrusion detection, 2002.
- Tom M. Mitchell. *Machine Learning*. McGraw-Hill, New York, 1997.
- C. Siva Ram Murthy and B.S. Manoj. *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2004
- Hadi Otrok, Joey Paquet, Mourad Debbabi, and Prabir Bhattacharya. Testing intrusion detection systems in manet: A comprehensive study. *Communication Networks and Services Research, Annual Conference on*, 0:364_371, 2007.
- Animesh Patcha and Jung-Min Park. Network anomaly detection with incomplete audit data. *Comput. Netw.*, 51(13):3935_3955, 2007.
- Charles Perkins and Elizabeth Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90_100, 1997.
- Glenn Shafer and Vladimir Vovk. A tutorial on conformal prediction. *J. Mach. Learn. Res.*, 9:371_421, 2008.
- W J Ulivla. Evaluation of intrusion detection system. *J. J. Res. Natl. Inst. Stand. Technol.*,

108(6):453_473, 2003.

- Liwei vivian Kuang. Dnids: A dependable network intrusion detection system using the csi-knn algorithm, 2007
- Fu Xiao and Xie Li. Using outlier detection to reduce false positives in intrusion detection. In NPC '08: Proceedings of the 2008 IFIP International Conference on Network and Parallel Computing, pages 26_33, Washington, DC, USA, 2008. IEEE Computer Society.
- Ke Zhang, Marcus Hutter, and Huidong Jin. A new local distancebased outlier detection approach for scattered real-world data. CoRR, abs/0903.3257, 2009.
- Yongguang Zhang, Wenke Lee, and Yi-An Huang. Intrusion detection techniques for mobile wireless networks. Wirel. Netw., 9(5):545_556, 2003.

Index Terms

Computer Science

Wireless Networks

Key words

CPDOD

MANET Intrusion detection

CP-KNN

Dynamic intrusion detection

Conformal Prediction