INTRUSION DETECTION IN MOBILE AD HOC NETWORKS USING TRANSDUCTIVE MACHINE LEARNING TECHNIQUES

FARHAN ABDEL-FATTAH AHMAD FARHAN

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2011

INTRUSION DETECTION IN MOBILE AD HOC NETWORKS USING TRANSDUCTIVE MACHINE LEARNING TECHNIQUES

Thesis Submitted to the College of Arts and Sciences, Universiti Utara Malaysia, in full fulfillment of the requirement for the degree of Doctor of Philosophy

By

Farhan Abdel-Fattah Ahmad Farhan

Kolej Sastera dan Sains
(UUM College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA TESIS / DISERTASI
(Certification of thesis / dissertation)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

FARHAN ABDL FATTAH

calon untuk Ijazah PhD
(candidate for the degree of)

telah mengemukakan tesis / disertasi yang bertajuk:
(has presented his/her thesis / dissertation of the following title):

INTRUSION DETECTION IN MOBILE AD HOC NETWORKS USING TRANSDUCTIVE MACHINE LEARNING TECHNIQUES

seperti yang tercatat di muka surat tajuk dan kulit tesis / disertasi.
(as it appears on the title page and front cover of the thesis / dissertation).

Bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada : ***02 Mac 2011.***
That the said thesis/dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on:
March 02, 2011.

Pengerusi Viva: *(Chairman for Viva)* **Prof. Dr. Che Su Mustaffa** Tandatangan *(Signature)*

Pemeriksa Luar: *(External Examiner)* **Assoc. Prof. Dr. R. Badlishah Ahmad** Tandatangan *(Signature)*

Pemeriksa *Dalam*: *(Internal Examiner)* **Dr. Massudi Mahmuddin** Tandatangan *(Signature)*

Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)* **Prof. Dr. Zulkhairi Md. Dahalin** Tandatangan *(Signature)*

Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)* **Dr. Shaidah Jusoh** Tandatangan *(Signature)*

Tarikh:
(Date) ***March 02, 2011***

PERMISSION TO USE

In presenting this thesis in fulfillment of the requirements for a postgraduate degree from University Utara Malaysia, I agree that University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisors or, in her absence, by the Dean of Postgraduate Studies and Research. It is understood that any copying or publication or use of this thesis or part there of for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and University Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Postgraduate Studies and Research
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

ABSTRAK

Tesis ini mengemukakan satu kajian di mana objektifnya adalah untuk merekabentuk model pengesanan pencerobohan untuk Mobile Ad Hoc Network (MANET). MANET merupakan satu sistem berotonomi yang mengandungi sekumpulan nod bergerak tanpa infrastruktur. Persekitaran MANET sangat mudah terjejas disebabkan kriteria MANET itu sendiri seperti medium yang terbuka, topologi dinamik, kerjasama teragih dan keupayaan terbatas. Malangnya, mekanisma terdahulu yang direkabentuk untuk melindungi rangkaian tidak sesuai digunakan untuk MANET tanpa sebarang pengubahsuaian. Pada masa lalu, kaedah pembelajaran mesin telah berjaya digunakan di dalam beberapa kaedah pengesanan pencerobohan kerana keupayaannya untuk mendapati dan mengesan serangan baru. Kajian ini, menyiasat penggunaan kaedah pembelajaran mesin untuk merekabentuk pengesanan pencerobohan yang paling sesuai bagi jenis rangkaian yang mencabar ini. Algoritma yang dicadangkan ini, menggunakan kombinasi model yang menggunakan dua perbezaan pengukuran (metrik ukuran ketidaksesuaian dan metrik "*Local Distance-based Outlier Factor*" (LDOF)) bagi memperbaiki keupayaan pengesanan. Tambahan pula, algoritma tersebut berupaya memberi keyakinan bergred yang memberi indikiasi kebolehpercayaan klasifikasi tersebut. Di dalam pembelajaran mesin, pemilihan ciri faktor yang paling berkaitan adalah satu keperluan yang mustahak, terutama di dalam MANET di mana topologi rangkaiannya adalah dinamik. Ciri pemilihan digunakan untuk untuk pemilihan berkaitan ciri-ciri subset bagi membina model ramalan dan memperbaiki prestasi pengesanan pencerobohan dengan mengeluarkan ciri-ciri yang tidak berkaitan. Ramalan *"transductive conformal"* dan pengesanan unsur luaran telah digunakan untuk ciri pemilihan algoritma. Teknik pengesanan pencerobohan yang terdahulu mempunyai masalah berkaitan dengan persekitaran yang dinamik. Secara khususnya, isu seperti pengumpulan serangan masa nyata berkaitan audit data dan pengesanan kerjasama global. Justeru itu, ia memberi motivasi kepada penyelidik untuk merekabentuk senibina baru pengesanan pencerobohan yang melibatkan teknik pengesanan yang lebih efisyen bagi mengesan keganjilan di dalam MANET. Model cadangan tersebut mempunyai senibina hirarki kerjasama dan teragih, di mana nod berkomunikasi dengan region gateway nod untuk membuat keputusan. Bagi pengesahan penyelidikan ini, penyelidik mempersembahkan kajian kes menggunakan perisian simulasi GLOMOSIM dengan menggunakan protokol penghalaan AODV. Pelbagai serangan aktif telah diimplementasikan. Beberapa siri hasil daripada eksperimen ini menunjukkan bahawa model pengesanan pencerobohan yang dicadangkan mampu mengenalpasti secara efektif kelainan dengan kadar positif kepalsuan yang rendah, kadar pengesanan yang tinggi dan mencapai kadar ketepatan pengesanan yang tinggi.

ABSTRACT

This thesis presents a research whose objective is to design an intrusion detection model for Mobile Ad hoc NETworks (MANET). MANET is an autonomous system consisting of a group of mobile nodes with no infrastructure support. The MANET environment is particularly vulnerable because of the characteristics of mobile ad hoc networks such as open medium, dynamic topology, distributed cooperation, and constrained capability. Unfortunately, the traditional mechanisms designed for protecting networks are not directly applicable to MANETs without modifications. In the past decades, machine learning methods have been successfully used in several intrusion detection methods because of their ability to discover and detect novel attacks. This research investigates the use of a promising technique from machine learning to designing the most suitable intrusion detection for this challenging network type. The proposed algorithm employs a combined model that uses two different measures (nonconformity metric measures and Local Distance-based Outlier Factor (LDOF)) to improve its detection ability. Moreover, the algorithm can provide a graded confidence that indicates the reliability of the classification. In machine learning algorithm, choosing the most relevant features for each attack is a very important requirement, especially in mobile ad hoc networks where the network topology dynamically changes. Feature selection is undertaken to select the relevant subsets of features to build an efficient prediction model and improve intrusion detection performance by removing irrelevant features. The transductive conformal prediction and outlier detection have been employed for feature selection algorithm. Traditional intrusion detection techniques have had trouble dealing with dynamic environments. In particular, issues such as collects real time attack related audit data and cooperative global detection. Therefore, the researcher is motivated to design a new intrusion detection architecture which involves new detection technique to efficiently detect the abnormalities in the ad hoc networks. The proposed model has distributed and cooperative hierarchical architecture, where nodes communicate with their region gateway node to make decisions. To validate the research, the researcher presents case study using GLOMOSIM simulation platform with AODV ad hoc routing protocols. Various active attacks are implemented. A series of experimental results demonstrate that the proposed intrusion detection model can effectively detect anomalies with low false positive rate, high detection rate and achieve high detection accuracy.

PUBLICATIONS FROM THIS RESEARCH

The following journals and conference papers have been produced from the research reported in this thesis:

- Farhan Abdel-Fattah, Zulkhairi Md. Dahalin, and Shaidah Jusoh. Distributed and cooperative hierarchical intrusion detection on MANET. International Journal of Computer Applications, 12(5):32–40, December 2010. Published By Foundation of Computer Science, USA.
- Farhan Abdel-Fattah, Zulkhairi Md. Dahalin, and Shaidah Jusoh. Dynamic intrusion detection method for mobile ad hoc network using CPDOD algorithm. IJCA Special Issue on MANETs, (1):22–29, 2010. Published by Foundation of Computer Science, USA. (This paper was selected as Best Paper).
- Farhan Abdel-Fattah, Zulkhairi Md. Dahalin, and M.T. Hatim. Mobile agent intrusion detection system for mobile ad hoc networks: A non-overlapping zone approach. In ICI 2008 : 4th IEEE/IFIP International Conference in Central Asia on Internet, pages 1 –5, 2008.
- Farhan Abdel-Fattah, Zulkhairi Md. Dahalin, and Shaidah Jusoh. Wrapper Feature-Selection Method for Intrusion Detection in Ad Hoc Network. (in review)

ACKNOWLEDGEMENTS

All thanks and praises are due to Allah, Whom we thank and seek for help and forgiveness. Whomsoever Allah guides, will never be misled and whomsoever He misguides, will never find someone to guide them. I testify that none has the right to be worshipped, except Allah, Alone without partners, and that Muhammad is Allah's slave and Messenger.

In completing this thesis, I owe a debt of gratitude and thanks to many persons have supported me throughout this difficult yet challenging journey. While being thankful to all of them, I must register my gratitude to some in particular. First and foremost, I would like to express my deepest appreciation to my supervisor Prof. Dr. Zulkhairi Md. Dahalin for his guidance and consistent support. His knowledgeable, wise and inspiring discussions has guided me throughout my whole PhD. I would like to also thank my second supervisor Dr. Shaidah Jusoh; she taught me the methodology, theoretical framework of study during my PhD journey. I would like to thank Prof. Hatim Mohamad Tahir, for introducing me to Intrusion Detection Systems and for all the things he taught to me during all these years.

I would like to thank my parents for their never-ending support and encouragement throughout my education. My father Abdel Fattah Farhan has been a great and wise teacher in my life and my lovely mother for her infinite patience especially during my absence. I would like to thank my dear brothers Mr. Mohammad, Mr. Jalal, Mr. Rashad, Mr. Jamil, Dr. Khalid and Mr. Wadea, and dear sisters Zeinab and Halimah. I would like to extend my gratitude to my wife, who has been very patient while pursuing my graduate studies and research. To my dear sons, Maryam, Sarah, Mohammad, Salma and Bushra.

I would like express my appreciation to my close friends; Mohammad Shuaib, Ghassan Najjar, Khuzairi Mohd Zaini.

I would like to also thank all academic and administrative staff in College of Arts and Sciences, my sincere gratitude goes to you. Finally, the author would like to express thanks to his colleagues, friends and relatives for their love, patience and understanding while pursuing his graduate studies and research.

TABLE OF CONTENTS

List of Algorithms

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AODV	Ad Hoc On Demand Distance Vector Routing Protocol
ANN	Artificial Neural Network
AUC	Area Under the Curve
BHAT	Black Hole Attack
CF	Confidence Factor
CP	Conformal Predictor
CP-kNN	Conformal Predictor K-Nearest Neighbor
CSI-KNN	Combined Strangeness and Isolation measure K-Nearest Neighbor
CV	Cross validation
DARPA	Defence Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DOD	Distance-based Outlier Detection
DoS	Denial of Service
DRAT	Dropping Routing Traffic Attack
DT	Decision Tree
FN	False Negative
FNR	False Negative Rate

FP	False Positive
FPR	False Positive Rate
FS	Feature Selection
IG	Information Gain
IDS	Intrusion Detection System
GA	Genetic Algorithm
LDOF	Local Distance-based Outlier Factor
MANET	Mobile Ad hoc Network
ML	Machine Learning
MLA	Machine Learning Algorithm
RCAT	Resource Consumption Attack
ROC	Receiver Operating Characteristic
SVM	Support Vector Machine
TPR	True Positive Rate

CHAPTER 1

INTRODUCTION

1.1 Research Background

Mobile Ad hoc Network (MANET) consists of nodes which are built up from mobile devices such as mobile computers, Personal Digital Assistant (PDA) and wireless phones. The nodes communicate with each other using wireless links and forming a temporary network without the aid of an established infrastructure or a centralized administration. The absence of a centralized administration and node mobility makes all MANETs nodes behave as both hosts and routers. In general, the cooperation of all nodes in MANET ensures reliable routing services. On the other hand, dependency and decentralization of MANET allows an adversary to exploit new type of attacks that are de-

Bibliography

[1] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, MobiCom '00, (New York, NY, USA), pp. 275–283, ACM, 2000.

[2] O. Kachirski and R. Guha, "Intrusion detection using mobile agents in wireless ad hoc networks," in *Proceedings of the IEEE Workshop on Knowledge Media Networking*, (Washington, DC, USA), pp. 153–158, IEEE Computer Society, 2002.

[3] G. Shafer and V. Vovk, "A tutorial on conformal prediction," *Journal of Machine Learning Research*, vol. 9, pp. 371–421, 2008.

[4] H. Liu and L. Yu, "Toward integrating feature selection algorithms for classification and clustering," *IEEE Transaction on Knowledge and Data Engineering*, vol. 17, no. 4, pp. 491–502, 2005.

[5] H. Otrok, J. Paquet, M. Debbabi, and P. Bhattacharya, "Testing intrusion detection systems in manet: A comprehensive study," *Fifth Annual Conference on Communication Networks and Services Research (CNSR'07)*, pp. 364–371, 2007.

[6] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Communications*, vol. 11, pp. 48 – 60, Feb. 2004.

[7] B. Sun, K. Wu, and U. W. Pooch, "Alert aggregation in mobile ad hoc networks," in *Proceedings of the 2nd ACM Workshop on Wireless Security*, WiSe '03, (New York, NY, USA), pp. 69–78, ACM, 2003.

[8] Y. Xiao, X. Shen, T. Anantvalee, and J. Wu, *A Survey on Intrusion Detection in Mobile Ad Hoc Networks, Wireless/Mobile Network Security*. Springer-Verlag New York, Inc., 2006.

[9] Y. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security and Privacy*, vol. 2, pp. 28–39, May 2004.

[10] H. Deng, R. Xu, J. Li, F. Zhang, R. Levy, and W. Lee, "Agent-based cooperative anomaly detection for wireless ad hoc networks," in *Proceedings of the 12th International Conference on Parallel and Distributed Systems*, (Washington, DC, USA), pp. 613–620, IEEE Computer Society, 2006.

[11] Y. Li and J. Wei, "Guidelines on selecting intrusion detection methods in manet," in *Proceedings of ISECON 2004, v 21. ISSN: 1542-7382*, 2004.

[12] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C. Y. Tseng, T. Bowen, K. Levitt, and J. Rowe, "A general cooperative intrusion detection architecture for manets," in *Proceedings of the Third IEEE International Workshop on Information Assurance (IWIA05)*, pp. 57–70, IEEE Computer Society, 2005.

[13] J. H. Cho, I. R. Chen, and P. G. Feng, "Performance analysis of dynamic group communication systems with intrusion detection integrated with batch rekeying in mobile ad hoc networks," in *Proceedings of the 22nd International Conference on Advanced Information Networking and Applications*, (Washington, DC, USA), pp. 644–649, IEEE Computer Society, 2008.

[14] Y. Xiao, X. Shen, and D. Z. Du, *Wireless Network Security (Signals and Communication Technology)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[15] T. Chen and V. Venkataramanan, "Dempster-shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Computing*, vol. 9, no. 6, pp. 35 – 41, 2005.

[16] J. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," in *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, MobiHoc '01, (New York, NY, USA), pp. 146–155, ACM, 2001.

[17] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," in *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*, SAINT-W '03, (Washington, DC, USA), pp. 368–373, IEEE Computer Society, 2003.

[18] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, pp. 21–38, January 2005.

[19] Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '03, (New York, NY, USA), pp. 135–147, ACM, 2003.

[20] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A dynamic anomaly detection scheme for aodv-based mobile ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 58, pp. 2471 –2481, June 2009.

[21] H. Otrok, M. Debbabi, C. Assi, and P. Bhattacharya, "A cooperative approach for analyzing intrusions in mobile ad hoc networks," in *Proceedings of the 27th International Conference on Distributed Computing Systems Workshops*, (Washington, DC, USA), pp. 86–93, IEEE Computer Society, 2007.

[22] C. S. R. Murthy and B. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2004.

[23] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 56 –63, 2007.

[24] A. Hijazi and N. Nasser, "Using mobile agents for intrusion detection in wireless ad hoc networks," in *Second IFIP International Conference on Wireless and Optical Communications Networks*, pp. 362 – 366, 2005.

[25] Y. Huang, W. Fan, W. Lee, and P. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in *Proceedings of the 23rd International Conference on Distributed Computing Systems*, pp. 478 – 487, May 2003.

[26] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," *Wireless Network*, vol. 9, pp. 545–556, September 2003.

[27] S. Şen and J. A. Clark, "A grammatical evolution approach to intrusion detection on mobile ad hoc networks," in *Proceedings of the Second ACM Conference on Wireless Network Security*, WiSec '09, (New York, NY, USA), pp. 95–102, ACM, 2009.

[28] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, pp. 15:1–15:58, July 2009.

[29] R. Khanna and H. Liu, "Control theoretic approach to intrusion detection using a distributed hidden markov model," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 24 –33, 2008.

[30] A. Mitrokotsa, N. Komninos, and C. Douligeris, "Intrusion detection with neural networks and watermarking techniques for manet," in *IEEE International Conference on Pervasive Services*, pp. 118 –127, 2007.

[31] B. Sun, K. Wu, Y. Xiao, and R. Wang, "Integration of mobility and intrusion detection for wireless ad hoc networks: Research articles," *International Journal of Communication Systems*, vol. 20, pp. 695–721, June 2007.

[32] T. M. Mitchell, *Machine Learning*. New York: McGraw-Hill, 1997.

[33] Q. Song and N. Kasabov, "Nfi: a neuro-fuzzy inference method for transductive reasoning," *IEEE Transactions on Fuzzy Systems*, vol. 13, no. 6, pp. 799 – 808, 2005.

[34] S. Pang and N. Kasabov, "Inductive vs transductive inference, global vs local models: Svm, tsvm, and svmt for gene expression classification problems," in *Proceedings of the 2004 IEEE International Conference on Neural Networks*, vol. 2, pp. 1197 – 1202 vol.2, 2004.

[35] F. Yang, H. Z. Wang, H. Mi, C. Lin, and W. W. Cai, "Using random forest for reliable classification and cost-sensitive learning for medical diagnosis," *BMC Bioinformatics*, vol. 10, no. S-1, 2009.

[36] Y. Wang, Y. Qiu, Y. Miao, G. Dai, and G. Li, "Current perception threshold measurement via single channel electroencephalogram based on confidence algorithm," in *7th International Symposium on Neural Networks, Shanghai, China*, pp. 58–62, 2010.

[37] H. Papadopoulos, V. Vovk, and A. Gammermam, "Conformal prediction with neural networks," in *Proceedings of the 19th IEEE International Conference on Tools with Artificial Intelligence - Volume 02*, ICTAI '07, (Washington, DC, USA), pp. 388–395, IEEE Computer Society, 2007.

[38] Z. Zhu, Y.-S. Ong, and M. Dash, "Wrapper-filter feature selection algorithm using a memetic framework," *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 37, no. 1, pp. 70–76, 2007.

[39] K. El-Khatib, "Impact of feature reduction on the efficiency of wireless intrusion detection systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 8, pp. 1143 –1149, 2010.

[40] Q. Yang and F. Li, "Support vector machine for intrusion detection based on lsi feature selection," in *The Sixth World Congress on Intelligent Control and Automation, WCICA.*, vol. 1, pp. 4113 –4117, 2006.

[41] W. Wong and C. Lai, "Identifying important features for intrusion detection using discriminant analysis and support vector machine," in *2006 International Conference on Machine Learning and Cybernetics*, pp. 3563 –3567, 2006.

[42] Z. Zhu, S. Jia, and Z. Ji, "Towards a memetic feature selection paradigm," *Computational Intelligence Magazine*, vol. 5, pp. 41–53, May 2010.

[43] I. H. Witten and E. Frank, *Data Mining: Practical Machine Learning Tools and Techniques*. Morgan Kaufmann, 2 ed., 2005.

[44] N. Aboudagga, M. T. Refaei, M. Eltoweissy, L. A. DaSilva, and J.-J. Quisquater, "Authentication protocols for ad hoc networks: taxonomy and research issues," in *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*, Q2SWinet '05, (New York, NY, USA), pp. 96–104, ACM, 2005.

[45] H. M. Deng, W. L, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 40, pp. 70 – 75, Oct. 2002.

[46] C. E. Perkins and E. M. Royer, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computer," in *Proceedings of the 1994 ACM Special Interest Group on Data Communication*, pp. 234–244, ACM, 1994.

[47] A. Iwata, C. Chiang, G. Pei, M. Gerla, and T. Chen, "Scalable routing strategies for ad hoc wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, pp. 1369 –1379, Aug. 1999.

[48] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," *in Proceedings of the IEEE International In Multi Topic Conference (INMIC)*, vol. 17, pp. 62–68, Aug. 2002.

[49] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," in *IETF Internet Draft, MANET Working Group*, (United States), RFC Editor, 2003.

[50] D. B. Johnson, D. A. Maltz, and J. Broch, "Ad hoc networking," ch. DSR: the dynamic source routing protocol for multihop wireless ad hoc networks, pp. 139–172, Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2001.

[51] Z. J. Haas and M. R. Pearlman, "The performance of query control schemes for the zone routing protocol," *IEEE/ACM Transactions on Networking*, vol. 9, pp. 427–438, August 2001.

[52] R. Heady, G. Lugar, M. Servilla, and A. Maccabe, "The architecture of a network level intrusion detection system," tech. rep., University of New Mexico, Albuquerque, NM, August 1990.

[53] I. Kim, Y. Kim, and K. Kim, "Zone-based clustering for intrusion detection architecture in ad-hoc networks," in *Management of Convergence Networks and Services* (Y. T. Kim and M. Takano, eds.), vol. 4238 of *Lecture Notes in Computer Science*, pp. 253–262, Springer Berlin / Heidelberg, 2006.

[54] X. Cheng and S. Wen, "A real-time hybrid intrusion detection system based on principle component analysis and self organizing maps," in *2010 Sixth International Conference on Natural Computation (ICNC)*, vol. 3, pp. 1182 –1185, 2010.

[55] S. Northcutt and J. Novak, *Network Intrusion Detection: An Analyst's Handbook*. Thousand Oaks, CA, USA: New Riders Publishing, 3rd ed., 2002.

[56] M. A. Maloof, *Machine Learning and Data Mining for Computer Security: Methods and Applications (Advanced Information and Knowledge Processing)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005.

[57] C. Manikopoulos and S. Papavassiliou, "Network intrusion and fault detection: a statistical anomaly approach," *IEEE Communications Magazine*, vol. 40, pp. 76 – 82, Oct. 2002.

[58] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security* (Y. Xiao, X. S. Shen, and D. Z. Du, eds.), Signals and Communication Technology, pp. 103–135, Springer US, 2007.

[59] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications*, vol. 14, pp. 85–91, December 2007.

[60] P. Yi, Y. Jiang, Y. Zhong, and S. Zhang, "Distributed intrusion detection for mobile ad hoc networks," in *SAINT Workshops*, pp. 94–97, 2005.

[61] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems.," *Computer Networks*, pp. 805–822, 1999.

[62] A. K. Ghosh and A. Schwartzbard, "A study in using neural networks for anomaly and misuse detection," in *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, (Berkeley, CA, USA), pp. 12–20, USENIX Association, 1999.

[63] V. S. H. Rao and V. R. Vemuri, *Enhancing Computer Security With Smart Technology*. Boca Raton, FL, USA: CRC Press, Inc., 2005.

[64] S. Axelsson, "The base-rate fallacy and its implications for the difficulty of intrusion detection," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, CCS '99, (New York, NY, USA), pp. 1–7, ACM, 1999.

[65] A. Patcha and J.-M. Park, "Network anomaly detection with incomplete audit data," *Computer Network*, vol. 51, no. 13, pp. 3935–3955, 2007.

[66] P. Mohapatra and S. Krishnamurthy, *Ad Hoc Networks: Technologies and Protocols*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2004.

[67] N. Milanovic, M. Malek, A. Davidson, and V. Milutinovic, "Routing and security in mobile ad hoc networks," *IEEE Computer*, vol. 37, pp. 61–65, February 2004.

[68] Y. an Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in *Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID04)*, pp. 125–145, 2004.

[69] J.-H. Cho, I.-R. Chen, and P.-G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," *IEEE Transactions on Reliability*, vol. 59, no. 1, pp. 231 – 241, 2010.

[70] P. Papadimitratos and Z. J. Haas, "Secure data transmission in mobile ad hoc networks," in *Proceedings of the 2nd ACM Workshop on Wireless Security*, WiSe '03, (New York, NY, USA), pp. 41–50, ACM, 2003.

[71] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 1st ACM Workshop on Wireless Security*, WiSE '02, (New York, NY, USA), pp. 1–10, ACM, 2002.

[72] M. Guerrero Zapata, "Secure ad hoc on-demand distance vector (saodv) routing," Sept. 2006. INTERNET-DRAFT Draft-guerrero-manet-saodv-06.txt.

[73] Y. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications*, WMCSA '02, (Washington, DC, USA), pp. 3–13, IEEE Computer Society, 2002.

[74] P. Albers, O. Camp, J. marc Percher, B. Jouga, and R. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," in *Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002)*, pp. 1–12, 2002.

[75] Y. Fu, J. He, and G. Li, "A distributed intrusion detection scheme for mobile ad hoc networks," in *Proceedings of the 31st Annual International Computer Software and Applications Conference - Volume 02*, COMPSAC '07, (Washington, DC, USA), pp. 75–80, IEEE Computer Society, 2007.

[76] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for aodv," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '03, (New York, NY, USA), pp. 125–134, ACM, 2003.

[77] R. S. Puttini, J.-M. Percher, L. Mé, O. Camp, R. De Sousa, C. J. B. Abbas, and L. J. García-Villalba, "A modular architecture for distributed ids in manet," in *Proceedings of the 2003 International Conference on Computational Science and Its Applications: Part III*, ICCSA'03, (Berlin, Heidelberg), pp. 91–113, Springer-Verlag, 2003.

[78] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 56 –63, 2007.

[79] S. R. Michalski, G. J. Carbonell, and M. T. Mitchell, eds., *Machine learning an artificial intelligence approach volume II*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1983.

[80] Y. Li, B. Fang, L. Guo, and Y. Chen, "Network anomaly detection based on tcm-knn algorithm," in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*, (New York, NY, USA), pp. 13–19, ACM, 2007.

[81] L. Kuang and M. Zulkernine, "An anomaly intrusion detection method using the csi-knn algorithm," in *Proceedings of the 2008 ACM Symposium on Applied Computing*, SAC '08, (New York, NY, USA), pp. 921–926, ACM, 2008.

[82] S. Amershi and C. Conati, "Unsupervised and supervised machine learning in user modeling for intelligent learning environments," in *Proceedings of the 12th International Conference on Intelligent User Interfaces*, IUI '07, (New York, NY, USA), pp. 72–81, ACM, 2007.

[83] S. Siersdorfer and S. Sizov, "Meta methods for model sharing in personal information systems," *ACM Transaction on Information Systems*, vol. 26, pp. 22:1–22:35, October 2008.

[84] P. Garcua-Teodoro, J. Duaz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers and Security*, vol. 28, no. 1-2, pp. 18–28, 2009.

[85] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, pp. 273–297, 1995.

[86] H. Deng, Q. A. Zeng, and D. Agrawal, "Svm-based intrusion detection system for wireless ad hoc networks," in *2003 IEEE 58th Vehicular Technology Conference, VTC 2003-Fall*, vol. 3, pp. 2147 – 2151 Vol.3, 2003.

[87] V. N. Vapnik, *The nature of statistical learning theory*. New York, NY, USA: Springer-Verlag New York, Inc., 1999.

[88] A. Gammerman and V. Vovk, "Prediction algorithms and confidence measures based on algorithmic randomness theory," *Theoretical Computer Science*, vol. 287, no. 1, pp. 209–217, 2002.

[89] R. Laxhammar and G. Falkman, "Conformal prediction for distribution-independent anomaly detection in streaming vessel data," in *Proceedings of the First International Workshop on Novel Data Stream Pattern Mining Techniques*, StreamKDD '10, (New York, NY, USA), pp. 47–55, ACM, 2010.

[90] T. Cover and P. Hart, "Nearest neighbor pattern classification," *IEEE Transactions on Information Theory*, vol. 13, pp. 21–27, January 1967.

[91] D. Aha and D. Kibler, "Instance-based learning algorithms," *Machine Learning*, vol. 6, pp. 37–66, 1991.

[92] M. Esmaili, B. Balachandran, R. Safavi-Naini, and J. Pieprzyk, "Case-based reasoning for intrusion detection," in *Proceedings of the 12th Annual Computer Security Applications Conference*, ACSAC '96, (Washington, DC, USA), pp. 214–223, IEEE Computer Society, 1996.

[93] T. Lane and C. E. Brodley, "Temporal sequence learning and data reduction for anomaly detection," *ACM Transaction on Information Systems Security*, vol. 2, pp. 295–331, August 1999.

[94] Y. Liao and V. R. Vemuri, "Use of k-nearest neighbor classifier for intrusion detection," Computers and Security, vol. 21, pp. 439– 448, 2002.

[95] E. Alpaydin, *Introduction to Machine Learning Second Edition*. New York: MIT Press, 2010.

[96] F. Xiao and X. Li, "Using outlier detection to reduce false positives in intrusion detection," in *Proceedings of the 2008 IFIP International Conference on Network and Parallel Computing*, (Washington, DC, USA), pp. 26–33, IEEE Computer Society, 2008.

[97] A. H. Sung and S. Mukkamala, "The feature selection and intrusion detection problems," in *Lecture Notes in Computer Science*, pp. 468–482, Springer-Verlag, 2004.

[98] A. L. Blum and P. Langley, "Selection of relevant features and examples in machine learning," *Artificial Intelligence*, vol. 97, pp. 245–271, 1997.

[99] M. Dash and H. Liu, "Feature selection for classification," *Intelligent Data Analysis*, vol. 1, pp. 131–156, 1997.

[100] I. Guyon and A. Elisseeff, "An introduction to variable and feature selection," *Journal of Machine Learning Research*, vol. 3, pp. 1157–1182, March 2003.

[101] E. Alpaydin, *Introduction to Machine Learning*. New York: MIT Press, October 2004.

[102] I. Guyon, S. Gunn, M. Nikravesh, and L. Zadeh, eds., *Feature Extraction, Foundations and Applications*. Springer, 2006.

[103] W. Punch, E. Goodman, M. Pei, L. Chia-Shun, P. Hovland, and R. Enbody, "Further research on feature selection and classification using genetic algorithms," in *Proceeding of Fifth International Conference on Genetic Algorithms and their Applications (ICGA 93)*, pp. 557–564, 1993.

[104] F. Pernkopf and P. O'Leary, "Feature selection for classification using genetic algorithms with a novel encoding," in *Proceedings of the 9th International Conference on Computer Analysis of Images and Patterns*, CAIP '01, (London, UK), pp. 161–168, Springer-Verlag, 2001.

[105] M. Guennoun, A. Lbekkouri, and K. El-Khatib, "Optimizing the feature set of wireless intrusion detection systems," *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, pp. 32–40, October 2008.

[106] K. A. Chrysostomou, *The Role of Classifiers in Feature election: Number vs Nature*. PhD thesis, 2008.

[107] J. H. Holland, *Adaptation in Natural and Artificial Systems*. University of Michigan Press, 1975.

[108] L. Buttyán and J. Hubaux, "Report on a working session on security in wireless ad hoc networks," *Mobile Computing and Communications Review*, vol. 6, pp. 74–94, January 2003.

[109] M. I. Petrovskiy, "Outlier detection algorithms in data mining systems," *Programming and Computer Software*, vol. 29, pp. 228–237, July 2003.

[110] K. Zhang, M. Hutter, and H. Jin, "A new local distance-based outlier detection approach for scattered real-world data," *In Proceedings of the13th Pacific-Asia Conference on Knowledge Discovery and Data Mining*, vol. 5467, pp. 813–822, 2009.

[111] K. Prakobphol and J. Zhan, "A novel outlier detection scheme for network intrusion detection systems," in *Proceedings of the 2008 International Conference on Information Security and Assurance (ISA 2008)*, (Washington, DC, USA), pp. 555–560, IEEE Computer Society, 2008.

[112] D. Barbará, C. Domeniconi, and J. P. Rogers, "Detecting outliers using transduction and statistical testing," in *Proceedings of the 12th Annual SIGKDD International Conference on Knowledge Discovery and Data Mining*, (New York, NY, USA), pp. 55–64, ACM, 2006.

[113] M. Dash, H. Liu, and J. Yao, "Dimensionality reduction for unsupervised data," in *Ninth IEEE International Conference on Tools with AI, ICTAI'97*, pp. 532–539, 1997.

[114] J. Yang and V. G. Honavar, "Feature subset selection using a genetic algorithm," *IEEE Intelligent Systems*, vol. 13, pp. 44–49, March 1998.

[115] G. Forman, I. Guyon, and A. Elisseeff, "An extensive empirical study of feature selection metrics for text classification," *Journal of Machine Learning Research*, vol. 3, pp. 1289–1305, 2003.

[116] J. Olajec, R. Jarina, and M. Kuba, "Ga-based feature extraction for clapping sound detection," in *Neural Network Applications in Electrical Engineering, 2006. NEUREL 2006. 8th Seminar on*, pp. 21 –25, 2006.

[117] C. H. Lee, J. W. Chung, and S. W. Shin, "Network intrusion detection through genetic feature selection," in *Proceedings of the Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel / Distributed Computing*, (Washington, DC, USA), pp. 109–114, IEEE Computer Society, 2006.

[118] T. Shon, Y. Kim, C. Lee, and J. Moon, "A machine learning framework for network anomaly detection using svm and ga," in *Information Assurance Workshop, IAW '05*, pp. 176 – 183, 2005.

[119] G. Stein, B. Chen, A. S. Wu, and K. A. Hua, "Decision tree classifier for network intrusion detection with ga-based feature selection," in *Proceedings of the 43rd Annual Southeast Regional Conference - Volume 2*, ACM-SE 43, (New York, NY, USA), pp. 136–141, ACM, 2005.

[120] K. Shazzad and J. S. Park, "Optimization of intrusion detection through fast hybrid feature selection," in *Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT 2005.*, pp. 264 – 267, 2005.

[121] J. Cucurull, M. Asplund, and S. Nadjm-Tehrani, "Anomaly detection and mitigation for disaster area networks," in *Proceedings of the 13th International Conference on Recent Advances in Intrusion Detection*, RAID'10, (Berlin, Heidelberg), pp. 339–359, Springer-Verlag, 2010.

[122] E. Jonsson and T. Olovsson, "A quantitative model of the security intrusion process based on attacker behavior," *IEEE Transactions on Software Engineering*, vol. 23, pp. 235–245, April 1997.

[123] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos, "Host-based network monitoring tools for manets," in *Proceedings of the 3rd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks*, (New York, NY, USA), pp. 153–157, ACM, 2006.

[124] GloMoSim, "Glomosim website," http://pcl.cs.ucla.edu/projects/glomosim/, jun, 2007.

[125] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, 1997.

[126] Y. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in *Proceedings of the 23rd International Conference on Distributed Computing Systems*, (Washington, DC, USA), p. 478, IEEE Computer Society, 2003.

[127] W. J. Ulivla, "Evaluation of intrusion detection system," *Journal of Research of National Institute and Standards and Technology*, vol. 108, no. 6, pp. 453–473, 2003.

[128] A. Slaby, "Roc analysis with matlab," in *Proceedings of the ITI 2007 29th International Conference on Information Technology Interfaces*, pp. 191 –196, 2007.

[129] F. Provost and P. Domingos, "Tree induction for probability-based ranking," *Machine Learning*, vol. 52, pp. 199–215, September 2003.

[130] I. Hendrickx, *Local Classification and Global Estimation Explorations of the k-nearest neighbor algorithm.* PhD thesis, Universiteit Van Tilburg, 2005.

[131] X. Wu, V. Kumar, J. Ross Quinlan, J. Ghosh, Q. Yang, H. Motoda, G. J. McLachlan, A. Ng, B. Liu, P. S. Yu, Z.-H. Zhou, M. Steinbach, D. J. Hand, and D. Steinberg, "Top 10 algorithms in data mining," *Knowledge and Information Systems*, vol. 14, pp. 1–37, December 2007.

[132] I. H. Witten, E. Frank, L. Trigg, M. Hall, G. Holmes, and S. J. Cunningham, "Weka: Practical machine learning tools and techniques with java implementations," in *Proceedings ICONIP / ANZIIS / ANNES99 Future*

Directions for Intelligent Systems and Information Sciences, pp. 192–196, Dunedin, New Zealand, November 1999.