DESCRIPTION

This book deals with malware detection in terms of Artificial Immune System (AIS), and presents a number of AIS models and immune-based feature extraction approaches as well as their applications in computer security.

- Covers all of the current achievements in computer security based on immune principles, which were obtained by the Computational Intelligence Laboratory of Peking University, China.
- Includes state-of-the-art information on designing and developing artificial immune systems (AIS) and AIS-based solutions to computer security issues.
- Presents new concepts such as immune danger theory, immune concentration, and class-wise information gain (CIG).

ABOUT THE AUTHOR

Ying Tan, PhD, is a Professor of Peking University, China. Dr. Tan is also the director of CIL@PKU. He serves as the editor-in-chief of International Journal of Computational Intelligence and Pattern Recognition, associate editor of IEEE Transactions on Cybernetics, IEEE Transactions on Neural Networks and Learning Systems, and International Journal of Swarm Intelligence Research, and also as an Editor of Springer’s Lecture Notes on Computer Science (LNCS). He is the founder and chair of the ICSI International Conference series. Dr. Tan is a senior member of the IEEE, ACM, and CIE. He has published over two-hundred
papers in refereed journals and conferences in areas such as computational intelligence, swarm intelligence, data mining, and pattern recognition for information security.

For additional product details, please visit https://www.wiley.com/en-sg