

Advanced Techniques of Attacks Detection in Wireless Networks

Supervisor: prof. Mgr. Jašek Roman, Ph.D., DBA

Consultant: Ing. Malaník David, Ph.D., ---

Department: Department of Informatics and Artificial Intelligence

Programme: Information Technologies

Abstract:

Wireless technologies are increasingly being used for critical business and industrial applications. At the same time, the more and more popular and desirable freedom the wireless network brings. However, wireless security and security is becoming a very important issue. There are new other threats that need to be defended. These include, for example, attacks targeting to the wireless network integrity, administrator's configuration errors, user violations, and attempts to acquire intellectual property. As a result, the service may be denied or downgraded, bypassing company security mechanisms, such as corporate firewalls, DLPs, antiviruses, or antispam. The topic of the thesis deals with the problem of Intelligent Network involvement to detect intruders in wireless networks. It examines the capabilities of integrating intelligent honeypots to detect and eliminate the intruder and solves both intrusion detection and DOS / DDOS detection against total infrastructure. The research goal is to find and verify the real possibilities of using intelligent networks in the field of data security support on wireless networks and mobile technologies.

Literature:

- [1] GUIZANI, Mohesen, Hsiao-Hwa CHEN a Chonggang WANG. The future of wireless networks: architectures, protocols, and services. Boca Raton: CRC Press, an imprint of the Taylor and Francis Group, and informa business, [2016]. Wireless networks and mobile communications series. ISBN 9781482220940.
- [2] COLEMAN, David D. CWSP: certified wireless security professional official study guide. Indianapolis, Ind.: Wiley Pub., c2010. Serious skills. ISBN 0470438916.
- [3] SINGH, Abhishek, Baibhav SINGH a Hirosh JOSEPH. Vulnerability analysis and defense for the Internet. New York: Springer, c2008. Advances in information security, 37. ISBN 0387743901.
- [4] RAMACHANDRAN, Vivek. Kali linux wireless penetration testing beginner's guide - third edition. PACKT Publishing Limited, [2018]. ISBN: 9781788831925.
- [5] ORIYANO, Sean. Kali linux wireless penetration testing cookbook. PACKT Publishing Limited,[2017]. ISBN: 9781783554089.
- [6] FASYUSHIN,Vyacheslav. Building a pentesting lab for wireless networks. Packt Publishing Limited,[2016].ISBN: 9781785283154.
- [7] ALOTAIBI, Majid. Security to wireless sensor networks against malicious attacks using Hamming residue method. EURASIP Journal on Wireless Communications and Networking [online]. 2019, 2019(1) [cit. 2019-02-07]. DOI: 10.1186/s13638-018-1337-5. ISSN 1687-1499. source: <https://jwcn-urasipjournals.springeropen.com/articles/10.1186/s13638-018-1337-5>.

[8] FANG, Dongfeng, Yi QIAN a Rose Qingyang HU. Security analysis for interference management in heterogeneous networks. *Ad Hoc Networks* [online]. 2019, 84, 1-8 [cit. 2019-02-07]. DOI: 10.1016/j.adhoc.2018.07.028. ISSN 15708705.
Source:<https://linkinghub.elsevier.com/retrieve/pii/S1570870518305341>