Abstract

The exponential growth in wireless network faults, vulnerabilities, and attacks make the WLAN security management a challenging research area [29]. Data mining applied to intrusion detection is an active area of research. The main reason for using data mining techniques for intrusion detection systems is due to the enormous volume of existing and newly appearing network data that require processing. Data mining follows anomaly based intrusion detection. The drawback of the anomaly based intrusion detection in a wireless network is the high rate of false positive. This can be solved by designing a hybrid intrusion detection system by connecting a misuse detection module to the anomaly detection module. In this paper, we propose to develop a hybrid intrusion detection system for wireless local area networks, based on Fuzzy logic. In this Hybrid Intrusion Detection system, anomaly detection is performed using the Bayesian network technique and misuse detection is performed using the Support Vector Machine (SVM) technique. The overall decision of system is performed by the fuzzy logic. For anomaly detection using Bayesian network, each node has a monitoring agent and a classifier within it for its detection and a mobile agent for information collection. The anomaly is measured based on the naïve Bayesian technique. For misuse detection using SVM, all the data that lie within the hyper plane are considered to be normal whereas the data that lie outside the hyper plane are considered to be intrusive. The outputs of both anomaly detection
and misuse detection modules are applied by the fuzzy decision rules to perform the final decision making. Hybrid detection system improves the detection performance by combining the advantages of the misuse and anomaly detection [33].

References

- Shu Yun Lim and Andy Jones, "An Anomaly-based Intrusion Detection Architecture to Secure Wireless Networks".
- Harley Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", September 11, 2003 Independent Study
A Hybrid Data Mining based Intrusion Detection System for Wireless Local Area Networks

- Susan M. Bridges and Rayford B. Vaughn, &quot;Intrusion Detection Via Fuzzy Data Mining&quot;, Accepted for Presentation at The Twelfth Annual Canadian Information Technology Security Symposium June 19-23, 2000, The Ottawa Congress Centre.
- Jaydip Sen &quot;An Agent-Based Intrusion Detection System for Local Area Networks.&quot; in International Journal of Communication Networks and Information Security (IJCNIS) Vol. 2, No. 2, 2010
- Torres. L. M at el., &quot;An anomaly-based intrusion detection system for IEEE 802.11 networks&quot;, 2010, pages: 1-6
- S. Tamilarasan, Aramudan, &quot;A Performance and Analysis of Misbehaving node in MANET using Intrusion Detection System&quot;, IJCSNS (2011), Vol. 11 No. 5 pp. 258-264
- Haddadi. F, Sarram M. A, &apos;Wireless intrusion detection system using lightweight agent&apos;, ICCNT (2010), pp. 84-87
- Kok Chin Khor et al., &quot;Comparing Single and Multiple Bayesian Classifiers Approaches for Network Intrusion Detection&quot;, ICCEA (2010), pages: 325-329
- Guan Xiao Qing et al., &quot;Network intrusion detection method based on Agent and SVM&quot;, ICIME (2010), china, pp. 399-402.
- Yu-Xin Meng et al., &quot;The practice on using machine learning for network anomaly intrusion detection&quot;, ICMLC (2011), Volume-2, pp. 576-581
- Chetan. R et al., &quot;Data mining based network intrusion detection system: A database centric approach&quot;, ICCCI (2012), pp. 1-6
- Noreen Kausar et al., &quot;Communications in Computer and Information
index terms

computer science

networks

keywords

intrusion detection system (ids) wireless local area network (wlan) support vector machine (svm)

bayesian network

monitoring agent