IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 6, June 2024

Impact Factor: 5.731

Automatic Method to Predict and Classify Cyber Hacking Breaches using Machine Learning

Vishnu Shankara M A[1] and Dr. H. Jayamangala[2]

PG Student, Department of Computer Applications[1]

Assistant Professor, Department of Computer Applications[2]

Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

22304257@vistas.ac.in and jayamangala.scs@velsuniv.ac.in

Abstract: *The fast propagation of computer networks has changed the viewpoint of network security. Easy accessibility conditions cause computer networks to be susceptible against several threats from hackers. Threats to networks are numerous and potentially devastating. Up to the moment, researchers have developed Malware Detection Systems (MDS) capable of detecting attacks in several available environments. A boundlessness of methods for misuse detection as well as anomaly detection has been applied. Many of the technologies proposed are complementary to each other, since for different kinds of environments some approaches perform better than others. This project presents a new Malware detection system that is then used to survey and classify them. The taxonomy consists of the detection principle, and second of certain operational aspects of the Malware detection system. In our project we have used algorithms like Random Forest (RF) as existing and Support Vector Machine (SVM) as proposed systems. From the results it is proved that the proposed SVM will work better than existing RF. All are measured in terms of accuracy*

Keywords: Cyber hacking, network threats, malware detection, Random Forest, Support Vector Machine

I. INTRODUCTION

Sensor networks are intricate systems composed of interconnected sensor nodes that communicate with each other either through wired or wireless means, facilitating the exchange of sensed data. A sensor node, a fundamental component of these networks, comprises sensors for data collection, optional actuators for effecting changes based on collected data, and capabilities for processing data and networking. These nodes, typically numerous and distributed spatially, collaborate to gather information about objects and oversee associated processes. Each sensor node is equipped with essential components including a sensing element (sensor), a microprocessor (microcontroller) for signal processing, a transceiver for communication, and an energy source for powering operations.

In the context of a Wireless Sensor Network (WSN) depicted in the provided illustration, twelve sensor nodes and a network sink, serving as a gateway, form the network. Each sensor node is an autonomous device featuring a transceiver, a microcontroller, and a sensing element. These nodes measure various physical conditions such as temperature, humidity, pressure, and vibration, converting them into digital data. Moreover, they possess the capability to process and store measured data before transmission.

The network sink, which also functions as a sensor node, plays a crucial role in aggregating valuable data from other sensor nodes. Typically powered by a stationary source, the network sink is often connected to a server responsible for processing data received from the WSN. This connection can be established directly if the server and WSN are situated on the same object. However, if remote access to the WSN is required, the network sink serves as a gateway, facilitating interaction through global networks like the Internet.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

II. LITERATURE SURVEY

1. Secure Knowledge and Cluster-Based Malware Detection Mechanism for Smart Wireless Sensor Networks Amjad Mehmood, Akbar Khanan, Muhammad Muneer Umar, Salwani Abdulla, Khairul Akram Zainol Ariffin, Houbing Song IEEE 2023.

Wireless sensor networks, due to their nature, are more prone to security threats than other networks. Developments in WSNs have led to the introduction of many protocols specially developed for security purposes. Most of these protocols are not efficient in terms of putting an excessive computational and energy consumption burden on small nodes in WSNs. This paper proposes a knowledge-based context-aware approach for handling the Malwares generated by malicious nodes. The system operates on a knowledge base, located at the base station, which is used to store the events generated by the nodes inside the network. The events are categorized and the cluster heads (CHs) are acknowledged to block maliciously repeated activities generated. The CHs can also get informational records about the maliciousness of intruder nodes by using their inference engines. The mechanism of events logging and analysis by the base station greatly affects the performance of nodes in the network by reducing the extra security related load on them.

2. Threshold Tuning-Based Wearable Sensor Fault Detection for Reliable Medical Monitoring Using Bayesian Network Model Haibin Zhang, Jiajia Liu, Nei Kato IEEE 2023.

As the medical body sensor network (BSN) is usually resource limited and vulnerable to environmental effects and malicious attacks, faulty sensor data arise inevitably which may result in false alarms, faulty medical diagnosis, and even serious misjudgment. Thus, faulty sensory data should be detected and removed as much as possible before being utilized for medical diagnosis-making. Most available works directly employed fault detection schemes developed in traditional wireless sensor networks (WSN) for body sensor fault detection. However, BSNs adopt a very limited number of sensors for vital information collection, lacking the information redundancy provided by densely deployed sensor nodes in traditional WSNs. In light of this, a Bayesian network model based sensor fault detection scheme is proposed in this paper, which relies on historical training data for establishing the conditional probability distribution of body sensor readings, rather than the redundant information collected from a large number of sensors. Furthermore, the Bayesian network-based scheme enables us to minimize the inaccuracy rate by optimally tuning the threshold for fault detection. Extensive online dataset has been adopted to evaluate the performance of our fault detection scheme, which shows that our scheme possesses a good fault detection accuracy and a low false alarm rate.

3. A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation Cong Pu, Sunho Lim IEEE 2023.

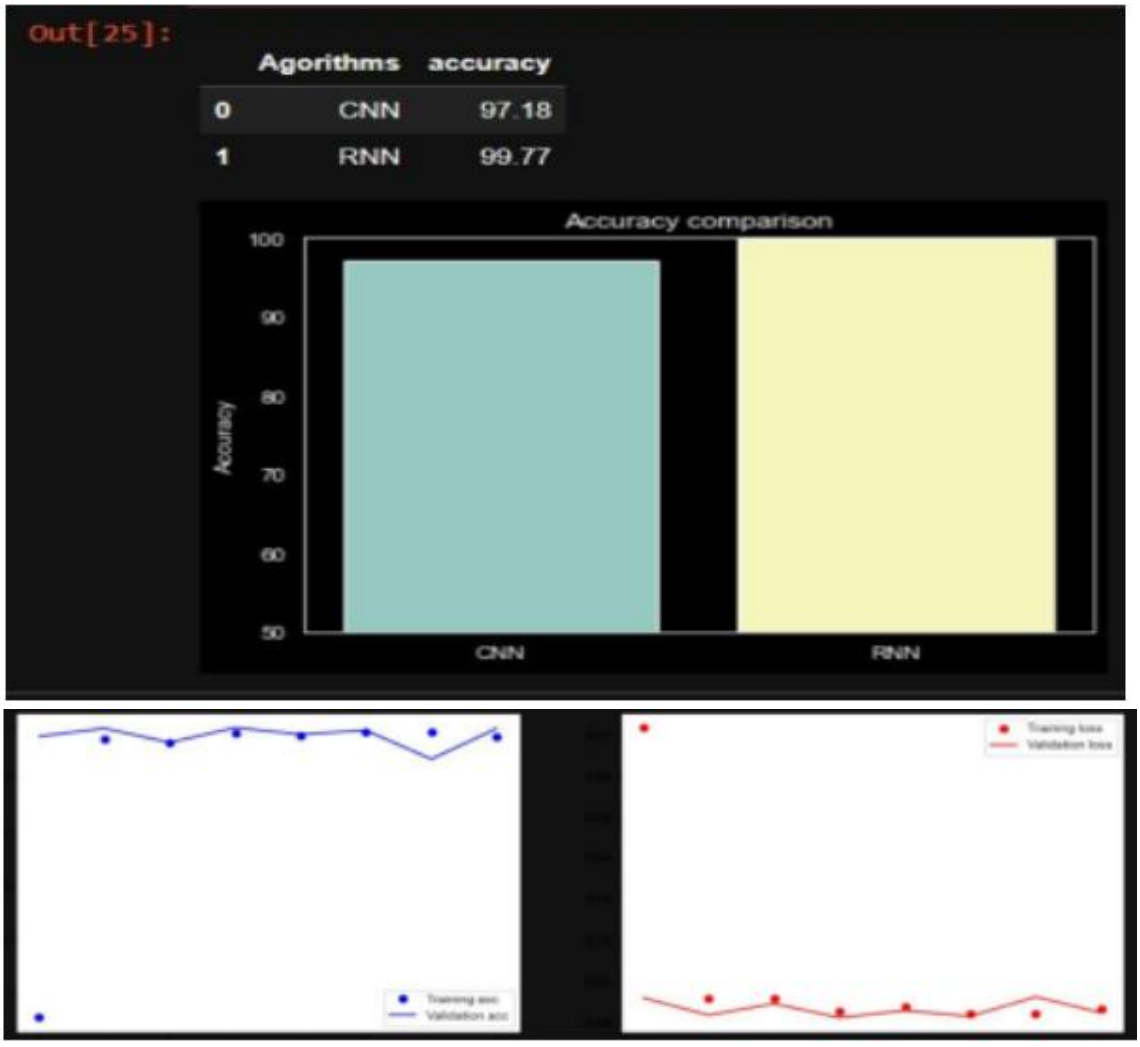
Due to the lack of centralized coordination, physical protection, and security requirements of inherent network protocols, wireless sensor networks (WSNs) are vulnerable to diverse denial-of-service (DoS) attacks that primarily target service availability by disrupting network routing protocols or interfering with on-going communications. In this paper, we propose a light-weight countermeasure to a selective forwarding attack, called SCAD, where a randomly selected single checkpoint node is deployed to detect the forwarding misbehavior of a malicious node. The proposed countermeasure is integrated with timeout and hop-by-hop retransmission techniques to quickly recover unexpected packet losses due to the forwarding misbehavior or bad channel quality. We also present a simple analytical model and its numerical result in terms of false detection rate. We conduct extensive simulation experiments for performance evaluation and comparison with the existing SCHEMAS and CAD schemes. The simulation results show that the proposed countermeasure can improve the detection rate and packet delivery ratio (PDR) as well as reduce the energy consumption, false detection rate, and successful drop rate.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

III. METHODOLOGY SECTION

Organizations have increasingly turned to Malware Detection Systems (MDS) to gather and analyze a range of attacks occurring within their host systems or networks. These systems serve to identify and analyze potential threats, encompassing both external attacks, commonly known as Malwares, and internal breaches referred to as misuses. This paper proposes an integrated model that combines Malware Detection (MD) and Malware Prevention (MP), drawing upon established techniques such as Intruder Detection (ID). This approach diverges from previous studies that typically focus solely on either detection or prevention, often relying on either Intruder Detection or Signature-based detection. While some efforts have explored hybrid methods, such as employing Signature-based Intruder Detection, they often lack prevention capabilities. In contrast, our proposed Integrated Detection and Prevention System (IDPS) not only identifies attacks but also actively prevents them, leveraging prevention mechanisms. This novel approach enables our system to outperform hybrid systems by preemptively blocking malicious events and incorporating them into a database of known signatures, facilitating earlier detection by Signature-Based Malware Detection systems. Deploying such an integrated model in wireless environments offers enhanced risk mitigation compared to traditional systems or those solely reliant on Malware Detection methods.

V. OUTPUT SCREENS



VI. CONCLUSION

The realm of malware detection has garnered significant attention from both academia and industry. Presently, there exists a comprehensive background on the state-of-the-art of Malware Detection Systems (MDS), delineated through a proposed taxonomy that encompasses examples from past and ongoing projects. This taxonomy not only sheds light on recent advancements but also comprehensively captures the evolution of these systems over time. Each technique within this taxonomy boasts its own set of advantages and drawbacks. It is evident that there is no singular criterion capable of providing absolute defense against computer network malware. Indeed, no one-size-fits-all solution exists that can serve as a standard defense against all potential attacks. Constructing and maintaining computer systems and networks impervious to attacks pose both technical challenges and economic burdens. The selection of a detection technique hinges upon various factors, including the specific anomalies the system is expected to encounter, the nature and behavior of the data, the operational environment, cost considerations, computational constraints, and the requisite security level.

REFERENCES

[1] I. F. Akyildiz et al., "Wireless Sensor Networks: A Survey, "Elsevier Comp. Networks, vol. 3, no. 2, 2019, pp. 393–422

[2] G.Li, J.He, Y. Fu. "Group-based Malware detection system in wireless sensor networks" Computer Communications, Volume 31, Issue 18 (December 2019)

[3] Michael Brownfield, "Wireless Sensor Network Denial of Sleep Attack", Proceedings of the 2019 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY.

[4] FarooqAnjum, DhanantSubhadrabandhu, Rahul Shetty, "On Optimal Placement of Malware Detection Modules in Sensor Networks", Proceedings of the First International Conference on Broadband Networks (BROADNETS19).

[5] Parveen Sadotra et al, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.9, September- 2019, pg. 23-28

[6] K. Akkayaand M. Younis, ―A Survey of Routing Protocols in Wireless Sensor Networks, ‖ in the Elsevier Ad Hoc Network Journal, Vol. 3/3 pp. 325-349, 2019.

[7] A. Abduvaliyev, S. Lee, Y.K Lee, "Energy Efficient Hybrid Malware Detection System for Wireless Sensor Networks", IEEE International Conference on Electronics and Information Engineering, Vol.2, pp. 25-29, August 2019.

[8] Parveen Sadotra and Chandrakant Sharma. A Survey: Intelligent Malware Detection System in Computer Security. International Journal of Computer Applications 151(3):18-22, October 2019.

[9] A. Araujo, J. Blesa, E. Romero, D. Villanueva, "Security in cognitive wireless sensor networks. Challenges and open problems", EURASIP Journal on Wireless Communications and Networking, February 2019.

[10] A. Becher, Z. Benenson, and M. Dorsey, \Tampering with motes: Real-world physical attacks on wireless sensor networks." in SPC (J. A. Clark, R. F. Paige, F. Polack, and P. J.Brooke, eds.), vol. 3934 of Lecture Notes in Computer Science, pp. 104{118, Springer, 2019.

[11] I. Krontiris and T. Dimitriou, \A practical authentication scheme for in-network programming in wireless sensor networks," in ACM Workshop on Real- World Wireless Sensor Networks, 2019.

[12] M. Ali Aydın *, A. HalimZaim, K. GokhanCeylan "A hybrid Malware detection system design for computer network security" Computers and Electrical Engineering 35 (2019) 517–526