International Journal of Innovative Research in Engineering
Volume 3, Issue 4 (July-August 2022), PP: 149-151.
www.theijire.com
ISSN No: 2582-8746

Detection of Eavesdropper in Sybil Attack using DV-HOP Algorithm

Dr. A.S. Shanthi[1], G. Mona Jacqueline[2], P. Nethaji[3], M. Dhanish[4], S. Gowtham[5], B. Gnanamani[6]
[1,2,3,4,5,6]Department of Computer Science and Engineering, Tamilnadu College of Engineering, Tamilnadu, India.

How to cite this paper Dr. A.S. Shanthi[1], G. Mona Jacqueline[2], P. Nethaji[3], M. Dhanish[4], S. Gowtham[5], B. Gnanamani[6], "Detection of Eavesdropper in Sybil Attack using DV-HOP Algorithm", IJIRE-V3I04-149-151.

Abstract: *We analyze PHY-layer authentication in wireless networks, which employs radio channel information (such as received signal strength indicators) to detect spoofing attacks. A zero-sum authentication game is often used to represent the interactions between a legit receiver and spoofers. The receiver picks the hypothesis test threshold to maximize its utility based on the Bayesian risk in spoofing detection, while the spoofers choose their attack patterns to lower the receiver's utility. The static authentication game's Nash equilibrium is derived, and its uniqueness is explored. In a dynamic radio environment, we also study a recurrent PHY-layer authentication game. As tough as it is, to retrieve the correct channel parameters in the radio nodes. We suggest spoofing in advance. A CPS is a mixture of sophisticated control, awareness, computing, and communication systems. The variety and complexity of CPs have revealed potential security and resilience problems. The integration of bulk physical layer components makes it more difficult to protect against physical vulnerabilities. Cyber-integration, on the other hand, which relies on network connectivity and internet of things(IoT) based devices, necessitates significant investments in security designs and upgrade to protect against unanticipated cyber-threats.*

Key Word: *PHY-layer authentication; Spoofers; CPS; Cyber-integration.*

I. INTRODUCTION

Smart systems that incorporate engineered dynamic networks of physical and computational components are characterized as cyber-physical systems(CPSs). The completely interconnected and integrated systems add new functionalities to vital infrastructures including electric power systems, water networks, transportation, home automation, and health care, allowing for technological development. A CPS is a mixture of advanced control, awareness, computing, and communication systems. The complex nature of CPSs have shown potential hazards to system security and resilience. The interconnectedness of bulk physical layer components makes it very difficult to protect against physical vulnerabilities. Cyber-Integration, on the other hand, which relies on network connectivity and internet of things(IoT) based devices, necessitates large investments in security designs and upgrades to protect against unanticipated cyber-attacks.

II. RELATED WORK

Mohammadreza F.M. Arani et al., described while addressing environmental concerns, the smart grid paradigm promises dramatic improvements in power system dependability, robustness, and efficiency. However, becausethese smart power systems heavily rely on communication and informationtechnologies, the cyber-attacks surface has grown, exposing a new class of vulnerabilities that could disrupt power system performance. They examine the aurora attack class of attacks in this research, concentrating on a microgrid point of common coupling (PCC). In contrast to the aurora assault on synchronous generator breakers, it is proven that the micro grid load level, storage, and distributed generation characteristics all play a role in the success of the attack. Furthermore, a distributed ownership mitigation mechanism is proposed and investigated. Based on the OPAL-RT real-time power system simulator and the OPNET communication protocol, a co-simulation platform has been developed.

Later Rui Tan et al, The latest information and communication technologies used in smart grids are under cybersecurity threats. This white paper examines the impact of integrity attacks on real-time pricing (RTP). This is an important feature of smart grids that use these technologies to improve system efficiency. Recent studies show that RTP creates a closed loop of interdependent real-time price signals and price demand. Such a control loop can be exploited by an attacker who aims to destabilise the pricing system. In particular, small malicious changes to the price signal can be repeatedly amplified by the closed loop, which can cause serious failures such as inefficiencies and power outages. This white paper uses a control-theoretic approach to derive the basic conditions for RTP stability under two broad classes of integrity attacks: scaling attacks and delayed attacks. When an attacker could compromise the price signal sent to a smart meter by lowering the price with a scaling attack or by offering an older price to more than half of all consumers whose attacks are delayed. only. Indicates that there is a risk of instability in the RTP system. The results provide useful guidelines for analyzing the impact of various attack parameters on system stability, allowing system operators to take appropriate steps to protect their RTP system.

And, Yousif Dafalla et al.,Nanogrid is a customer's facility that can generate electricity and supply it to power. Communication network. These supplies are based on the renewable energy source behind the meter and are marked as follows: A "prosumer setup" that enables customers not only to consume electricity but also to produce electricity. The private nanogrid consists of the physical layer, which is a home-scale power system, and the cyber layer, which is used by manufacturers and grid operators to remotely monitor and control the nanogrid. As renewable energy sources become more widespread, nanogrids are at the forefront of a paradigm shift in the operating environment, and their proper operation is important for power grids. This white paper conducts a cybersecurity assessment of state-of-the-art residential Nanogrid deployments.

To this end, we have developed an actual experimental nanogrid setup based on photovoltaic (PV) generation. They analyzed the security and restoring force of this system at both cyber and physical levels. We've noticed that Nanogrid's current cybersecurity measures have improved compared to previous generations, but there are still major concerns. According to our experiments, these concerns range from abuse of well-known protocols such as Secure Shell (SSH) and Domain Name Service (DNS) to leaks of sensitive information and major flaws in software update mechanisms. While multiple nanogrid breaches can adversely affect the entire power grid, the analysis focused on individual homes and determined the economic loss of the breached deployment through Simulink-based simulations.

III.METHODOLOGY

The distance vector hop (DV-Hop) localization algorithm raises errors and suggests a new DV-Hop localization algorithm based on a half-dimensional weighted center of gravity to show the accumulation of errors in wireless sensor networks (WSNs). This algorithm followed a two-dimensional location distribution, designed the smallest communication radius, and first formed a valid network connection. The algorithm then modifies the distance between the beacon node and its neighbors to form a more accurate hop distance so that the shortest path can be optimized. Finally, the proposed localization algorithm was theorized and validated in simulation experiments involving the same communication radius, different communication radii, and different node radii within the same communication radius, and the proposed algorithm and DV hop localization algorithm. Experimental results show that the proposed localization algorithm reduced average localization errors and improved localization accuracy.

Dynamic watermarking is a way to watermark an image, giving the user full control over the watermark long after the image is published online. This is an evolution of traditional watermarks, embedded in the image itself and more constrained when compared. Dynamic watermarks that are better than traditional watermarks. If you have an image, can remove the traditional watermark from theimage.

Most of the images uploaded online are not protected from download. This provides limited protection, even if they are watermarked. Traditional watermarks always appear in the same proportions as the rest of the image. No matter where you look. This means that it is not easy to see on mobile devices and can hinder your ability to stop thieves. Depending on your settings, image-based dynamic watermarks can be responsive. In other words, it can be adjusted automatically according to how the image is displayed.

It exhibits several different behaviors and interacts in context-sensitive ways. CPS includes an interdisciplinary approach that integrates cybernetics, mechatronics, design, and process science theories. Systems Cyber Physical Security. The Cyber Physical System Security (CPSSEC) project addresses security concerns for cyber physical systems (CPS) and Internet of Things (IoT) devices. CPS and IoT are playing an increasingly important role in critical infrastructure, government, and everyday life. Cars, medical devices, building management and smart grids are examples of CPS. Closely related areas of the IoT continue to evolve and grow as costs fall and sensors and platforms merge.

First, define the MTD using a simple but common notation. Capture important aspects of such defense. Thenclassify this defense as follows: Different subclassesdepending on what you move, when you move it, and how they move it they move. To answer the latter question, I'll show you how to use the domain Knowledge and modelling of game theory to help defenders come up with an effective and efficient exercise strategy. Second, understand the practicality Learn how different MTDs are implemented among these defenses also, software defined networking and Virtualization of network functions serves as a key element in their implementation.

IV.RESULTS AND DISCUSSION

A server is anything that has some resource that can be shared. There are computer servers, which provide computing power, print servers, which manage a collection of printers, disk servers which provide networked disk space and web servers which store web pages. A client is simply any other entity that wants to gain access to a particular server. It processes to a port until a client connects to it.A server is allowed to accept multiple clients connected to the same port number, although each session is unique.When the cluster member sends a message, the message can be viewed in the cluster head form. As many number of cluster member can sends a message all of them will be observed in the cluster head SN organize a group of clusters where the base station node and the CH are trustworthy and not compromised by any attack.The second module consists of a sensor node where the number of cluster heads and the number of cluster members can be created in cluster member. The member information will be displayed where the member is identified in which cluster at the number of member id, the position of member id and the energy all of them can be connected with the base station.

V.CONCLUSION

In view of the disadvantages in the practical application of the DV-Hop algorithm in WSNs, such as the uneven distribution of nodes, holes, and large errors in the average hop distance, a novel localization algorithm, combining the DV-Hop algorithm with a half-measure weighted centroid, was proposed. Beacon nodes realize their localization by using the centroid algorithm and then use the localized accuracy as the weight for localizing unknown nodes. Through theoretical reasoning and simulation experiments, it was found that the improved localization algorithm reduced the localization errors and improved the localization accuracy of unknown nodes compared with the DV-Hop algorithm whether used in the same networks or not. Compared with the DV-Hop algorithm, whose localization accuracy increases from 0.6 to 0.7, other DV-HOP is about 0.3; and new DV-Hop shows a localization accuracy fluctuating stably within 0.1. It was worth noting that the study was performed in an ideal network simulation environment, so there remains the need to research the application of the improved algorithm under realistic network environments in the future.

References

[1]. M.F. Arani, A.A. Jahromi, D. Kundur and M. Kassouf, "Modelling and simulation of the aurora attack on micro grid point of common coupling,"in 2019 7th workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES). IEEE, 2019, pp. 1-6.

[2]. R. Tan, V. Badrinath Krishna, D.K. Yau and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," 2013, pp. 439-450.

[3]. Y. Dafalla, B. Liu, A.A Hahn, H.Wu, R. Ahmadi and A.G. Bardas, "Prosumer nanogrids: A cybersecurity assessment," IEEE Access, vol. 8, pp. 131 150 – 131 164, 2020, event IEEE Access.

[4]. B. Liu and H. Wu, "Optimal d-facts placement in moving target defense against false data injection attacks," IEEE Transactions on Smart Grid, pp. 1-1, 2020, event: IEEE Transactions on smart grid.

[5]. Z. Zhang, R. Deng, D.K Yau, P. Cheng and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," IEEE Transactions on Information Forensics and Security, vol. 15, pp.2320 – 2335, 2019.

[6]. S. Lakshminarayana and D.K. Yau, "Cost-benefit analysis of moving target defense in power grids," IEEE Transactions on Power Systems, 2020.

[7]. J. Tian, R. Tan, X. Guan and T. Liu, "Enhanced hidden moving target defense in smart grids," IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 2208 – 2223, 3 2019 44.

[8]. X. Niu, J. Li , J. Sun and K. Tomsovic "Dynamic detection of false data injection attack in smart grid using deep learning," in 2019 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2019, pp. 1-6.

[9]. Y. Li, Y. Wang and S. Hu, "Online generative adversary network based measurement recovery in false data injection attacks: A cyber-physical approach," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2031-2043, 2020.

[10]. G. Ding, Q. Wu, Y.D. Yao, J. Wang and Y.Chen, "Kernel-based learning for statistical signal processing in cognitive radio networks: Theoretical foundations, example applications, and future directions," IEEE Signal Processing Magazine, vol. 30, no. 4, pp. 126-136, 2019.