# Securing A Small Office Home Office Network: Integrating A Supervised Neural Network Algorithm.

Sylvia Worlali Azumah, University of Cincinnati, United States

## ABSTRACT

Small office home office networks have become a target for many threat actors, hackers and cyber attackers and hence there is an urgent need to secure the network from such attackers. Most small office home office network users do not see the need to provide enough security to their networks because they assume no one is going to hack them forgetting that the biggest threat of our small home networks today comes from the outside. The challenge of misconfiguration of routers, firewalls and default configurations in our small home networks renders the network vulnerable to attacks such as DDos , phishing attacks , virus and other network attacks hence the need to implement a detection algorithm to help identify flaws in the pattern of the small office network. It turns out that about 75% of existing approaches focused on intrusion detection in 802.11 wireless networks of a SOHO and not the entire network. These approaches do not efficiently secure the network entirely leaving the rest prone to attacks can occur with or without the internet. This paper proposes to add another layer of security to the other preventive measures in a SOHO network by designing, implementing and testing a supervised neural network algorithm to identify attacks on the small home network and also to send a notification to users to keep them informed of the activities on their network. The supervised neural network algorithm will have dataset representing both attacks and non-attacks which will be used in the training phase. The system should be able to detect and identify the various attacks and anomaly when they occur on the network and help keep the users informed.

Additional Key Words and Phrases: Anomaly detection, cyber-attacks, SOHO, Machine learning.

ACM Reference Format: Sylvia Worlali Azumah. 2020. Title of Manuscript: Securing Small Office Home Office: Integrating A Supervised Neural Network Algorithm. In *IT Research Symposium '20: School of Information Technology IT Research Symposium, April 14, 2020, Cincinnati, OH*, USA.

## INTRODUCTION

Small office home office (SOHO) is a term used to differentiate small businesses from large businesses and midsize businesses. SOHO business normally includes 2 to 50 workers for offices and 2 to 5 users or workers for homes [1]. These businesses utilize the internet in communication storing purchases and other daily and financial tasks.

Building office networks require a lot of devices and accessories such as network cables for example RJ45s and UTP media converters, network adapters and network Operating Systems such as Windows 95, Artisoft LANtastic, and NetWare Lit to monitor and control the flow of information between interconnected devices [3]. The 2 most important devices utilized are Switches and routers. Switches are responsible for connecting multiple servers, computers, printers or any ethernet accessible device, in a building or a room over ethernet. Switches enable devices with ethernet ports to talk to each other [2].

Routers are also very essential in a network the main tasks routers carry out connecting devices to the internet. Routers determine the best "route" or path to dispatch information from one device to

another other interesting add ons are basic security protocols and setting priority to the information being carried [2].
A more generic approach to setting up a network in a SOHO office will use most or all these devices and accessories. The figure 1 below depicts how a SOHO network should be set up. As seen in figure 1 the devices and accessories are all connected to each other to form a network. The next task is to configure all devices in the network to communicate seamlessly with each other [5].
First the router is turned on and connected to an ethernet port then the router's interface is accessed and locked down by changing the adapter settings for the router on an operating system.
Configuring the security and IP addressing is the next step normally setting router name, password and IP addresses are the elements that affect the network security positively on a basic level. All this step does not annul the fact that a small network is impervious to attacks.

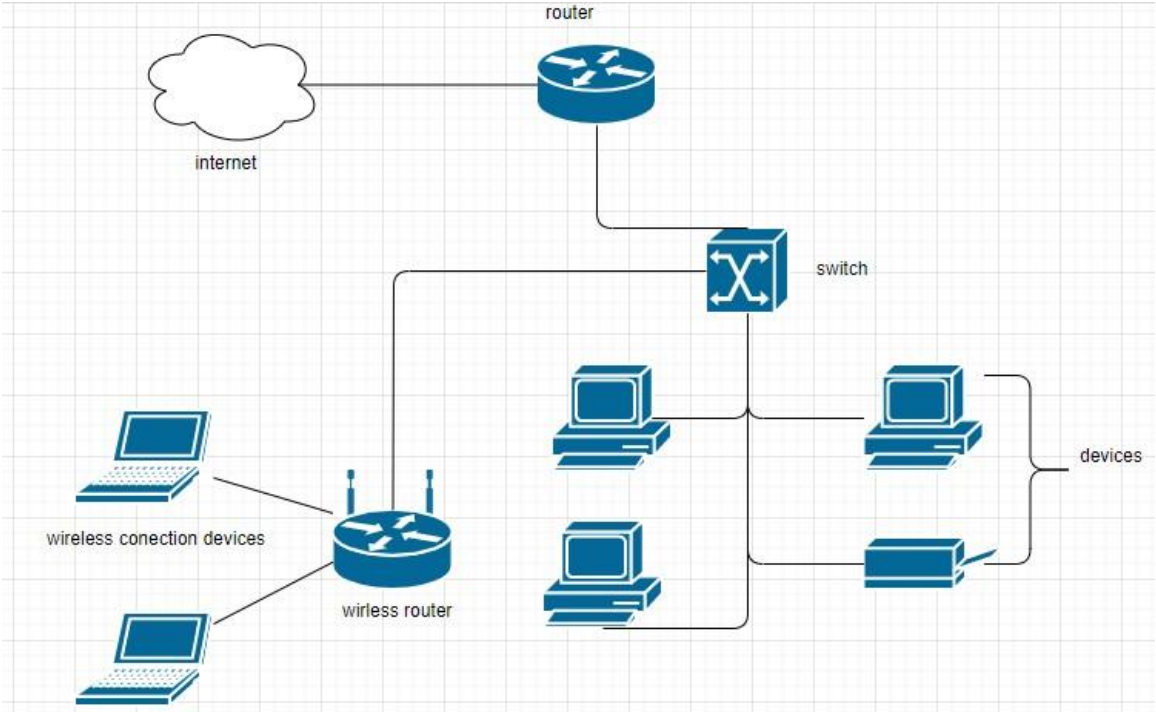


**Figure 1 Sample of small office home office**

Some advanced extra steps include setting DHCP reservations, set up sharing and control and Set up user accounts.
These extra steps ensure robust network for a small setting such as a SOHO business. Cyber Attacks pertaining to home networks can be categorized into 2 kinds, inbound and outbound
Inbound attacks if the home network is breached to target connected devices like desktop computers, tablets, smart TVs, and game consoles via the internet (from internet to home network) [4].
Outbound attacks, on the other hand, refer to instances when hackers access a home device through an inbound attack and then use the device to remotely execute malware, either to obtain sensitive information or intercept communications, or to launch attacks against other external targets (from home network to internet) [4]. Some of these attacks are displayed as well as their number of events in table 1 and 2.

## Table 1 Top 5 Inbound attacks [4]

| Inbound attacks | Number of Events |
|---|---|
| MS17-010 SMB-related | 2,441,996 |
| Brute Force Login via RDP | 1,464,012 |
| Suspicious HTML Iframe Tag | 926,065 |
| Microsoft SQL SA Password Brute Force | 431,630 |

**Table 2 top 5 outbound attacks**

| Outbound attacks | Number of Events |
|---|---|
| MS17-010 SMB-related | 9,716,094 |
| ICMP Black Nurse | 1,786,694 |
| DNS Amplification | 1,615,122 |
| Brute Force Login via RDP | 1,067,895 |

As seen in table 1 and 2 the top 5 inbound and outbound attacks among the other numerous attacks not mentioned is alarming and due to human ignorance and advancing technology these attacks evolve and are difficult to curtail.



## RELATED WORKS

The paper "intrusion prevention/intrusion detection system (ips/ids) for WIFI networks" written by Michal Korčák et al

The paper illustrates designing and evaluating a system that would passively monitor wireless network traffic of small home networks. The experiment was carried out with DOS by ICMP flooding

on the access point. An IDPS system was used to disassociate the attacker from the access point when the attack was initiated
In my opinion using this system can be very expensive for small office home office networks Experimental methods in this research are preferred and cultivating this experiment in my research will be beneficial in my findings [5]

From the SOHO Wireless Intrusion Detection Systems - Cure or Placebo paper, written by Peter Wolski, a series of 4 tests were carried out on SOHO networks with different detection systems. Snort Commview and wireless watch. The results varied as per the criteria used in the tests. Each test had a little bit of sophistication to the attack. From the paper I deduced that some of the attacks were as a result of old operating systems. There tests carried out in my reach may be restricted only to modern operating systems in order to acquire streamlined results.[6]

The paper," Supervised Machine Learning Techniques for Trojan Detection with Ring Oscillator Network" conducted by Kyle Worley and Md Tauhidur Rahman. They we presented a quantitative comparison of four supervised machine learning algorithms' performance when classifying ICs based on their ring oscillator network frequencies. Acquiring information from the best supervised learning algorithm and implementing it in my methodology would be beneficial.[7]

## PROBLEM STATEMENT

Small office home office businesses range from startup companies to online shops and these offices sometimes handle substantial amounts of data. Cyberattacks on these small businesses due to their sheer size can leave them bankrupt and tarnish their image in terms of shopping securely or running any activity securely with their services. Hence the need to provide an extra layer of protection that is a machine learning algorithm capable of detecting a wide variety of intrusion attacks. Some research questions that will be addressed in the paper includes but not limited to.

1. How secured it the small office network going to be after integration of supervised machine learning algorithm?
2. Which attacks occurs frequently on the small office home office networks.

## METHODOLOGY

Solving this problem requires experimentation. The main method used will be training a supervised neural network algorithm by using data generated from a SOHO simulated network using NS3. A network will be simulated and will have data packets created and sent over the network .Packets will be attacked with different types of network attacks associated with SOHO networks and will be captured using Wireshark to collect the dataset for the algorithm to train. Its output will be to flag any malicious or suspicious intrusions. To implement the supervised neural network algorithm, both data generated with attacks and non-attacks data must be introduced to the algorithm in the training phase. Then testing the algorithm with different scenarios would further ensure its robustness in the network. The figure below shows a supervised learning algorithm a similar model will be created and trained to detect intrusions in the network. Below are some other tools that will be used in this study.
NS3
Python (NumPy, pandas' library)
Kali Linux
Wireshark

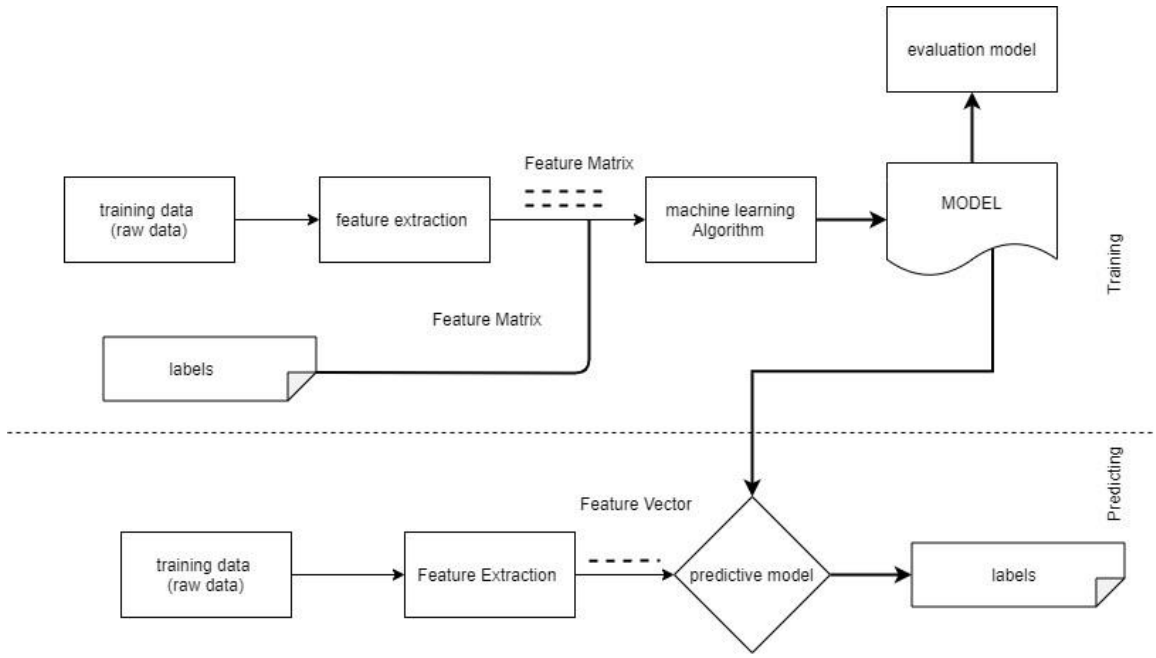


Figure 2 A flowchart of a supervised machine learning model [8]

## CONCLUSION

The integration of an anomaly detector in a small office home office network will be able to keep users informed by providing them with notifications of the changes on their networks. Also, it should be able to keep the users network secured even when there is a problem of misconfiguration of some components on the networks. Since a network anomaly detection dataset for a SOHO is going to be used by the algorithm, it will help with classifying attacks which will also help users distinguish between the varies attacks identified on the network.

**REFERENCES**

**[1]** Exam collection: SOHO network: Requirements, planning and implementation.

**[2]** CISCO. How do I set up a small business network : https://www.cisco.com/c/en/us/solutions/smallbusiness/resource-center/networking/how-to-set-up-a-network.html

**[3]** what-when-how: Small Office/Home Office LANs (Networking)

**[4]** Trend micro. A Look into the Most Noteworthy Home Network Security Threats of 2017. 2018 https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-look-intothe-most-noteworthy-home-network-security-threats-of-2017

**[5]** Michal Korčák1 and Jaroslav Lámer2 and František Jakab. 2014 *intrusion prevention/ intrusion detection system (ips/ids) for Wi-Fi networks*: https://www.researchgate.net/publication/273011407_Intrusion_PreventionIntrusion_Detection_System_IPSIDS_for_Wifi_Networks doi: 10.5121/ijcnc.2014.6407

**[6]** Peter Wolski 2004 *SOHO Wireless Intrusion Detection Systems - Cure or Placebo:* https://pdfs.semanticscholar.org/d0fd/d1d285f23eb37bcc0f9cb2d3cd3f0b56b776.pdf?_ga=2.229290716.1715069632.1583270978-1610647827.1583270978

**[7]** Kyle Worley and Md Tauhidur Rahman *2019 Supervised Machine Learning Techniques forTrojan Detection with Ring Oscillator Network:* https://www.researchgate.net/publication/331700603_Supervised_Machine_Learning_Techniques_for_Tro jan_Detection_with_Ring_Oscillator_Network

**[8]** Dong Nguyen Canh Nguyen Thuan Hong Duong-Ba et all 2017 *Joint network coding and machine learning for error-prone wireless broadcast:* https://www.researchgate.net/publication/314202159_Joint_network_coding_and_machine_learning_for_e rror-prone_wireless_broadcast doi: 10.1109/CCWC.2017.7868415