AfanEnglish2

by Wiyan Hera

Submission date: 05-Jun-2022 05:39PM (UTC+0300)
Submission ID: 1850764015
File name: on_for_Unmanned_Aerial_Vehicle_System_Using_SNORT_english2.docx (88.57K)
Word count: 2485
Character count: 13999

Network Intrusion Detection for Unmanned Aerial Vehicle System Using SNORT-IDS

Nur Afan Syarifudin[1], Djuniadi[2]

1. *Department of Computer Science, Faculty of Mathematics and Natural Sciences, Semarang State University*
2. *Department of Electrical Engineering, Faculty of Engineering, Semarang State University*

*** Corresponding Author:** Email: afan_syarifudin10@students.unnes.ac.id

Abstract

The development of IoT devices has brought changes a large material in this world. IoT devices can *now be applied* to *a variety of things to deal with specific problems. One of them is the Unmanned Aerial Vehicle (UAV) device. The use of IoT devices in this UAV is like doing system work in more real time and can be monitored such as image processing and others. The integration of IoT devices on UAVs requires communication using internet protocol (IP). However, IP has the disadvantage that it can* be *easily hit by attacks such as DDoS, Ping Attack, and others. This can cause communication on drones and computer ground devices to be disrupted. Moreover, drone devices* are devices *that have a very dangerous can if there is loss control. Therefore, it is necessary to have a system* that *can detect* the *presence of these disturbances so that actions can be taken to avoid loss control from the drone. The system is an intrusion detection system (IDS). Snort is a device that can detect interference with devices that are opensource and easy to use. In this study, results were obtained that showed* the *average accuracy* of *snort in detecting attacks on IoT UAV devices.*

Key Words: Network Intrusion Detection; UAVs; SNORT-IDS

1. Introduction

The tremendous development in the use of services and applications has brought great benefits in the communication network uniqueness. This is what is behind the emergence of the Internet of Things (IoT) (Condomines et al., 2019). There are many IoT devices that have been developed today such as smart homes, drones, and etc. One of the devices currently in use is a drone. Drone is widely used in certain matters such as disaster monitoring, surveillance, transportation, forestry and environmental protection (Deebak & Al-Turjman, 2020). Drones can also be used as a means of transportation in lieu of land transportation to avoid accidents caused by human errors (Shafique et al., 2021).

Drones have massive development both in terms of hardware and software such as written by Oren and Verity which states the Internet of Things is implanted in drones (Oren & Verity, 2020). The working principle of IoT has been widely applied in the manufacture of other smart drones, such as drones that use navigation in the form of image processing and drones that can fly with an autopilot system (Deebak & Al-Turjman, 2020).

Smart drones consist of sensors that can work collaboratively between other electric lifters such as sensors, cameras, mini personal computers, flight controllers, and supported devices for drones. Smart drones also require Internet Protocol (IP) as means of their network communication media (Aggarwal & Kumar, 2020). In order for drones to carry out their extensive mission in scanning drone land, it needs integration with IoT (Kumar et al., 2021). The integration of smart drones with IoT systems can add to the quality of monitoring in the world of agriculture. However, drones have vulnerabilities to security attacks such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks (Elrawy et al., 2018). The existence of this attack can interfere with network communication using TCP / IP protocols between the drone and computer devices embedded in the smart drone can be disrupted, causing loss of control due to communication errors (Rodrigues et al., 2017) .

An intrusion detection system (IDS) is needed as a security scheme that works in the main security of the network layer on IoT devices (Elrawy et al., 2018). an IDS is required to work on monitoring traffic in the network from IoT devices such as smart drones with strict conditions of low process capability as well as high volume data processing (Elrawy et al., 2018) . Therefore, the most up-to-date IoT security is needed and also an understanding of the security vulnerabilities related to smart drones is needed.

Due to the dependence of smart drones on internet protocol (IP) as a communication medium, a system is needed that can detect interference in IoT devices (Sicato et al., 2020). IDS can effectively, simply, and accurately detect threats on IoT networks. Other similar studies such as Sedjelmaci, Senouci and Messous's on how to detect cyberattacks on unmanned devices can be monitored using IDS (Sedjelmaci et al., 2016). In addition, research by Condomines, Zhang, and Larrieu that uses IDS as an intrusion in UAV devices states IDS can detect attacks that occur on aircraft without crew (Condomines et al., 2019).

There are many types of IDS that are usable and open source. Of the many types, there are several of the most popular ones including SNORT-IDS and Suricata-IDS. Based on research conducted by Risyad, Data and Pramukantoro stated that SNORT-IDS is superior in detecting TCP SYN flood attacks. In addition, SNORT-IDS also has better reliability in measuring detection accuracy, detection speed, and detection effectiveness (Risyad et al., 2018). With the advantages of SNOR-IDS, research was conducted on Network Intrusion Detection for Unmanned Aerial Vehicle Using SNORT-IDS.

2. Methodology

This stage contains a methodology used in the study entitled Network Intrusion Detection on Raspberry-Pi for Unmanned Aerial Vehicle System Using SNORT-IDS in detecting intrusion attacks or interference on IoT devices embedded in smart drones. At this stage, it is expected to be a guide for work in research so

that it can run according to the target. Such stages are carried out systematically and specifically as described in the figure below.

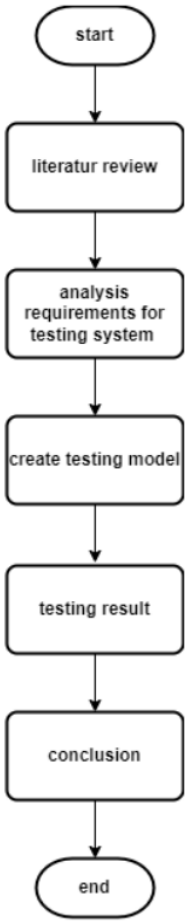

Fig 1: Methodology flowchart

The flowchart explanation is as follows

2.1 Literature review

At this stage, it discusses literature studies carried out to support research carried out such as the type of IDS used, the application or application of IDS in UAVs, as well as supporting devices used in IDS which are described as follows.

2.1.1 IDS

Intrusion detection system is the process of monitoring a series of processes in a computer or network system and analyzing them as a sign of possible threats and crimes in an attempted disruption in computer security. IDS is able to detect the emergence of intrusions in a network (Tasneem et al., 2018).

2.1.1.1 SNORT-IDS

As explained in the previous stage SNORT-IDS is software that can detect intrusion interference in an activity on a computer. SNORT-IDS is a type of signature based on IDS. The advantage of this software is that it has rules that can be created and designed to block traffic and send interference notifications (Tasneem et al., 2018).

2.1.2 UAV

Unmanned Aerial Vehicle (UAV) is an alternative device that can help facilitate human work. UAVs are also increasingly experiencing a very rapid development, namely by automating IoT devices that become smart drones. However, many researchers have complained of some threats such as in the study

conducted by Codomines, Zhang and Larrieu which stated the possibility of attacks such as jamming, spoofing, or interference network on devices within the internet protocol (Condomines et al., 2019).

2.1.3 Raspberry Pi

Raspberry Pi is a minicomputer device that can be operated on IoT. Raspberry pi is portable and can be planted in intelligent system systems including smart drones. Raspberry pi functions as a computer that can run programs to carry out image processing, processing documents, etc. on smart drones Raspberry pi is used as the main tool to run IDS as a monitoring of the occurrence of all intrusions in the drone system (Parag Vadher, 2020). Raspberry pi devices are particularly vulnerable to DoS attacks that can compromise drone communication with IoT devices. In this study, the Raspberry 4B model was used because it has a high level of accuracy compared to other devices in the IDS (Samrat Krishna et al., 2021).

2.2 Analysis requirements for testing system

The needs analysis needed to perform this test includes:

- Computer with processor AMD Ryzen 7
- Raspberry Pi 4B
- SNORT software
- Ethernet cable

2.3 Create testing model

The testing model used is arranged in the flowchart below

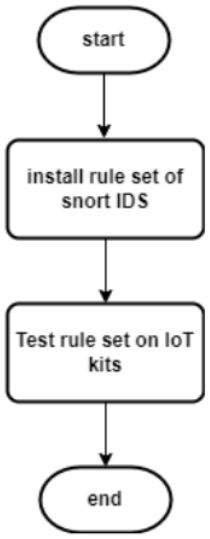

Fig 2: Testing flowchart models

2.4 Testing results

Contains IDS testing results on smart drone devices. The experiment refers to the research of Pampattiwar and Chhangani by conducting experiments using SNORT-3 (Pampattiwar & Chhangani, 2017).

2.5 Conclusion

The results of the discussion are based on the experiments carried out.

3. Result and Discussion

Testing and trial

3.1 Testing model

No.	Rule set Snort 3
1.	app-detect
2.	browser-chrome
3.	browser-firefox
4.	browser-ie
5.	browser-other
6.	browser-plugins
7.	browser-webkit
8.	content-replace
9.	exploit-kit
10.	executable-file
11.	flash-file
12.	file-identify
13.	-image files
14.	file-java
15.	file-office
16.	file-other
17.	pdf-file
18.	indicator-compromise
19.	indicator-obfuscation
20.	indicator-scan
21.	indicator-shellcode
22.	malware-backdoor
23.	malware-cnc
24.	malware-other
25.	malware-tools
26.	os-linux
27.	os-mobile
28.	os-other
29.	os-solaris
30.	os-windows
31.	policy-multimedia
32.	policy-other
33.	policy-social
34.	policy-spam
35.	protocol-dns
36.	protocol-finger
37.	protocol-ftp
38.	protocol-icmp
39.	protocol-imap
40.	protocol-nntp
41.	protocol-other
42.	protocol-pop
43.	protocol-rpc
44.	protocol-scada
45.	protocol-services
46.	protocol-snmp
47.	protocol-telnet
48.	protocol-tftp
49.	protocol-voip
50.	pua-adware
51.	pua-other
52.	pua-p2p
53.	pua-toolbars
54.	server-apache
55.	server-iis
56.	mail-server
57.	server-mssql
58.	server-mysql
59.	oracle-server
60.	server-other
61.	server-samba
62.	Sql
63.	x11

3.2 Testing results

Based on the results of experiments conducted using the rule set on Snort 3 applied to smart drone UAVs, it was observed with the following parameters.

a. Transfer rate (throughput)

On snort experiments using raspberry pi 4. The average speed of transfer is in units of Mbit/s. On connections connected to computer devices using cables, an average speed of up to 30.5 Mbit/s is obtained. while connections. While the speed by connecting wirelessly can produce a speed of 27.8%. This shows that the use of a network connection using cables can speed up the transfer rate in the snort rule 3 test.

b. CPU Load Average

Testing at average CPU load can show all the rules that were configured at the beginning. This is in line with research conducted by

Krisna, at all (Samrat Krishna et al., 2021). It supports the use of Snort on IoT devices in this case i.e. on UAV devices.

c. Memory Load

Snort testing on average memory load against the rule set that was configured at the beginning was 55.60%. From several experiments carried out obtained data that are not too far away.

In the application of UAV devices, testing is also carried out on the rule set including:

a. Port rule test

In port testing using FIN scan which is used to find open ports. In this experiment using FTP 21, SSH 65001, and HTTP:8080 can open. This is in accordance with previous studies, namely (Erlansari et al., 2020).

b. FTP rule test

In ftp testing used a "brute force" attack scheme. In this scheme, IDS can recognize intrusions that occur due to FTP access without going through authorization.

4. Conclusion

Based on experiments using Snort 3 using Raspberry pi can be generated the following conclusions. S

1) The first stage of the experiment focused on the performance produced by snort 3 on raspberry pi devices in carrying out all forms of intrusion with the application of the snort 3 rule set. The results obtained are not far from the previous research, namely average performance. In the experiment, there was also a difference in the transfer rate between using cables and wireless.
2) The phase 2 experiment focused on testing port performance on snort with several schemes including "brute force". With this scheme snort 3 can serve to detect the presence of intrusions in the IP address.

Based on the tests that have been carried out, snort 3 on raspberry pi can be used on IoT Unmanned Aerial Vehicle devices. In this research, there are still many shortcomings, especially in testing rule sets that are not carried out all only on the equipment needed in IoT. So that if you want to apply it to other devices, it is necessary to test the rules in accordance with the required device specifications.

5. Acknowledgments

This research is the result of collaboration with supervisors in the information system security course.

6. References

[1] Aggarwal, S., & Kumar, N. (2020). Path planning techniques for unmanned aerial vehicles: A review, solutions, and

challenges. *Computer Communications*, *149*, 270–299. https://doi.org/10.1016/j.comcom.2019.10.014

[2] ondomines, J. P., Zhang, R., & Larrieu, N. (2019). Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. *Ad Hoc Networks*, *90*, 101759. https://doi.org/10.1016/j.adhoc.2018.09.004

[3] Deebak, B. D., & Al-Turjman, F. (2020). Aerial and underwater drone communication: potentials and vulnerabilities. In *Drones in Smart-Cities*. Elsevier Inc. https://doi.org/10.1016/b978-0-12-819972-5.00001-x

[4] Elrawy, M. F., Awad, A. I., & Hamed, H. F. A. (2018). Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing*, *7*(1), 1–20. https://doi.org/10.1186/s13677-018-0123-6

[5] Erlansari, A., Coastera, F. F., & Husamudin, A. (2020). Early Intrusion Detection System (IDS) using Snort and Telegram approach. *Sisforma*, *7*(1), 21–27. https://doi.org/10.24167/sisforma.v7i1.2629

[6] Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Gadekallu, T. R., & Srivastava, G. (2021). SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. *Computer Networks*, *187*(November 2020). https://doi.org/10.1016/j.comnet.2021.107819

[7] Oren, C., & Verity, A. (2020). Artificial Intelligence (AI) Applied to Unmanned Aerial Vehicles (UAVs) and its impact on Humanitarian Action. *Digital Humanitarian Network*, *May*, 60. https://www.academia.edu/43359673/Artificial_Intelligence_AI_Applied_to_Unmanned_Aerial_Vehicles_UAVs%0Ahttps://www.digitalhumanitarians.com/artifical_intelligence_applied_to_uavs/

[8] Pampattiwar, S. R., & Chhangani, P. A. Z. (2017). Hybrid Intrusion Detection System Using Snort. *International Research Journal of Engineering and Technology(IRJET)*, *4*(4), 1–6. https://www.irjet.net/archives/V4/i4/IRJET-V4I4439.pdf

[9] Parag Vadher. (2020). Snort IDPS using Raspberry Pi 4. *International Journal of Engineering Research And*, *V9*(07), 151–154. https://doi.org/10.17577/ijertv9is070099

[10] Risyad, E., Data, M., & Pramukantoro, E. S. (2018). Comparison of Intrusion Detection System (IDS) Performance of Snort And Suricata In Detecting TCP SYN Flood Attacks. *Journal of Information Technology Development and Computer Science*, *2*(9), 2615–2624.

[11] Rodrigues, M., Pigatto, D. F., Fontes, J. V.C., Pinto, A. S. R., Diguet, J.-P., & Branco, K. R. L. J.C. (2017). UAV Integration Into IoIT: Opportunities and Challenges. *International Conference on Autonomic and Autonomous Systems (ICAS)*, *January*, 6.

[12] Samrat Krishna, G., Srinivasa Ravi Kiran, T., & Srisaila, A. (2021). Testing performance of RaspberryPi as IDS using SNORT. *Materials Today: Proceedings*, *xxxx*, 1–4. https://doi.org/10.1016/j.matpr.2021.01.607

[13] Sedjelmaci, H., Senouci, S.M., & Messous, M. A. (2016). How to detect cyber-attacks in unmanned aerial vehicles network? *2016 IEEE Global Communications Conference, GLOBECOM 2016* -

Proceedings. https://doi.org/10.1109/GLOCOM.2016.7841878

[14] Shafique, M. A., Afzal, M. S., Riaz, N., & Ahmed, A. (2021). Public Perception regarding Autonomous Vehicles in Developing Countries: A Case study of Pakistan. *Pakistan Journal of Engineering and Applied Sciences*, *28*, 1–6.

[15] Sicato, J.C. S., Singh, S. K., Rathore, S., & Park, J. H. (2020). A comprehensive analyses of intrusion detection system for IoT environment. *Journal of Information Processing Systems*, *16*(4), 975–990. https://doi.org/10.3745/JIPS.03.0144

[16] Tasneem, A., Kumar, A., & Sharma, S. (2018). Intrusion Detection Prevention System using SNORT. *International Journal of Computer Applications*, *181*(32), 21–24. https://doi.org/10.5120/ijca2018918280

AfanEnglish2

ORIGINALITY REPORT

4%	3%	2%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	link.springer.com Internet Source	1%
2	Submitted to University of Hertfordshire Student Paper	1%
3	Bakkiam David Deebak, Fadi Al-Turjman. "Aerial and underwater drone communication: potentials and vulnerabilities", Elsevier BV, 2020 Publication	<1%
4	peerj.com Internet Source	<1%
5	netapps.internetworks.my Internet Source	<1%
6	Ebrima Jaw, Xueming Wang. "A novel hybrid-based approach of snort automatic rule generator and security event correlation (SARG-SEC)", PeerJ Computer Science, 2022 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		