Afan 5

by Wiyan Hera

Submission date: 05-Jun-2022 12:43PM (UTC+0300)
Submission ID: 1848819349
File name: ction_on_IoT_Unmanned_Aerial_Vehicle_System_Using_SNORT__5.docx (86.52K)
Word count: 1702
Character count: 11388

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

Nur Afan Syarifudin[1], Djuniadi[2]

1. *Departemen of Computer Science, Faculty of Mathematics and Natural Sciences, Universitas Negeri Semarang*
2. *Departemen of Electrical Engineering, Faculty of Engineering, Universitas Negeri Semarang*

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

Abstract

This is abstract

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

1. Introduction

Perkembangan luar biasa dalam penggunaan layanan dan aplikasi telah membawa manfaat yang besar dalam komunikasi jaringan. Hal inilah yang melatarbelakangi munculnya Internet of Things (IoT) (Condomines et al., 2019). Ada banyak perangkat IoT yang telah dikembangkan saat ini seperti smart home, drone, and etc. Salah satu dari perangkat yang saat ini digunakan yaitu drone. Drone banyak digunakan dalam hal-hal tertentu misalnya monitoring bencana, pengawasan, transportasi, kehutanan dan perlindungan lingkungan (Deebak & Al-Turjman, 2020). Drone juga dapat digunakan sebagai sarana transportasi alternatif pengganti transportasi darat untuk menghindari terjadinya kecelakaan yang disebabkan karena human eror (Shafique et al., 2021).

Drone memiliki pengembangan yang massive baik dari segi hardware maupun software seperti dalam tulisan Oren dan Verity yang menyatakan Internet of Things ditanamkan pada drone (Oren & Verity, 2020). Prinsip kerja IoT telah banyak diterapkan di dalam pembuatan smart drone yang lain, seperti drone yang menggunakan navigasi berupa pengolahan

citra dan drone yang dapat terbang dengan sistem autopilot (Deebak & Al-Turjman, 2020).

Smart drone terdiri dari sensor yang dapat bekerja berkolaborasi antara perangkat elektrik lainnya seperti sensor, camera, mini personal computer, flight controller, and supported devices for drones. Smart drone juga membutuhkan Internet Protocol (IP) sebagai media komunikasi jaringannya (Aggarwal & Kumar, 2020). Agar drone dalam menjalankan misinya yang yang luas dalam melakukan scanning lahan drone perlu integrasi dengan IoT (Kumar et al., 2021). Integrasi smart drone dengan sistem IoT dapat menambah kulitas dari monitoring dalam dunia pertanian. Akan tetapi, drone memiliki kerentanan terhadap serangan keamanan seperti serangan denial-of-service (DoS) dan distributed denial-of-service (DDoS) (Elrawy et al., 2018). Adanya serangan ini dapat menggangu komunikasi jaringan yang menggunakan procokol TCP/ IP antara drone dengan perangkat computer yang tertanam dalam smart drone dapat terganggu sehingga menyebabkan loss control karena kesalahan komunikasi (Rodrigues et al., 2017).

Sebuah intrusion detection system (IDS) dibutuhkan sebagai skema pengamanan yang bekerja dalam pengamanan utama layer jaringan pada perangkat IoT (Elrawy et al., 2018). sebuah IDS diperlukan untuk bekerja mengawasi lalu lintas dalam jaringan dari perangkat IoT seperti smart drone dengan kondisi ketat kemampuan proses yang rendah serta pemrosesan data volume tinggi (Elrawy et al., 2018). Oleh karena itu diperlukan keamanan IoT yang paling mutakhir dan juga pemahaman mengenai kerentanan kemanan yang berkaitan pada smart drone sangat diperlukan.

Karena ketergantungan smart drone terhadap internet protocol (IP) sebagai media komunikasinya maka dibutuhkan sistem yang dapat mendeteksi gangguan pada perangkat IoT (Sicato et al., 2020). IDS dapat mendeteksi secara efektif, sederhana, dan akurat ancaman pada jaringan IoT. Penelitian lain yang serupa seperti penelitian Sedjelmaci, Senouci dan Messous mengenai bagaimana cara mendeteksi serangan siber pada perangkat tanpa awak dapat dimonitoring menggunakan IDS (Sedjelmaci et al., 2016). Selain itu, penelitian Condomines, Zhang, and Larrieu yang menggunakan IDS sebagai pendeksi intrusi pada perangkat UAV menyatakan IDS dapat mendeteksi serangan yang terjadi pada pesawat tanpa awak (Condomines et al., 2019).

Ada banyak jenis IDS yang dapat digunakan dan bersifat open source. Dari sekian jenis ada beberapa yang paling popular diantaranya yaitu SNORT-IDS dan Suricata-IDS. Berdasarkan penelitian yang dilakukan Risyad, Data dan Pramukantoro menyatakan bahwa SNORT-IDS lebih unggul dalam mendeteksi serangan TCP SYN flood. Selain itu, SNORT-IDS juga memiliki reliabilitas yang lebih baik dalam mengukur akurasi deteksi, kecepatan deteksi, san efektifitas deteksi (Risyad et al., 2018). Dengan keunggulan SNOR-IDS maka dilakukan penelitian mengenai Network Intrusion Detection for Unmanned Aerial Vehicle Using SNORT-IDS.

2. Methodology

Pada tahap ini berisi methodology yang digunakan dalam penelitian yang berjudul Network Intrusion Detection on Raspberry-Pi for Unmanned Aerial Vehicle System Using

SNORT-IDS dalam mendeteksi serangan atau gangguan intrusi pada perangkat IoT yang tertanam dalam smart drone. Pada tahap ini diharapkan menjadi panduan pengerjaan dalam penelitian agar dapat berjalan sesuai dengan target. Tahapan tersebut dilaksanakan secara sistematis dan spesifik seperti yang dijelaskan pada gambar di bawah ini.

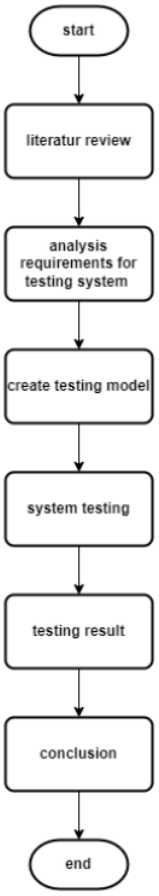

Fig 1: Methodology flowchart

Penjelasan flowchart adalah sebagai berikut

2.1 Literature review

Pada tahapan ini dibahas mengenai studi pustaka yang dilakukan untuk mendukung penelitian yang dilakukan seperti jenis IDS yang digunakan, penerapan atau aplikasi IDS pada UAV, serta perangkat pendukung yang digunakan dalam IDS yang diuraikan sebagai berikut.

2.1.1 IDS

Intrusion detection system merupakan proses monitoring dari serangkaian proses dalam sistem computer atau jaringan dan menganalisisnya sebagai tanda dari kemungkinan ancaman dan kejahatan dalam percobaan gangguan di dalam kemanan computer. IDS mampu mendeteksi kemunculan dari intrusi dalam sebuah jaringan (Tasneem et al., 2018).

2.1.1.1 SNORT-IDS

Seperti apa yang telah dijelaskan pada tahapan sebelumnya SNORT-IDS merupakan software yang dapat mendeteksi gangguan intrusi pada sebuah aktivitas di computer. SNORT-IDS merupakan salah satu jenis signature based on IDS. Keunggulan dari software ini yaitu dengan rule yang dapat dibuat dan didesign untuk mengeblok lalu lintas dan mengirimkan notifikasi gangguan (Tasneem et al., 2018).

2.1.2 UAV

Unmanned Aerial Vehicle (UAV) merupakan perangkat alternative yang dapat membantu memudahkan pekerjaan manusia. UAV juga semakin

mengalami perkembangan yang sangat pesat yaitu dengan otomasi perangkat IoT yang menjadi smart drone. Namun, banyak peneliti yang mengeluhkan beberapa ancaman seperti dalam penelitian yang dilakukan Codomines, Zhang dan Larrieu yang menyatakan kemungkinan serangan seperti jamming, spoofing, atau gangguan jaringan pada perangkat di dalam internet protocol (Condomines et al., 2019).

2.1.3 Raspberry Pi

Raspberry Pi merupakan perangkat minicomputer yang dapat dioperasikan pada IoT. Raspberry pi bersifat portable dan dapat ditanam pada sistem sistem cerdas diantaranya smart drone. Raspberry pi berfungsi sebagai computer yang dapat menjalankan program untuk melakukan image processing, processing documents, etc. pada smart drone Raspberry pi digunakan sebagai alat utama untuk menjalankan IDS sebagai monitoring terjadinya segala intrusi dalam sistem drone (Parag Vadher, 2020). Perangkat Raspberry pi sangat rentan terhadap serangan DoS yang dapat membahayakan komunikasi drone dengan perangkat IoT. Pada penelitian ini digunakan Raspberry model 4B karena memiliki tingkat keakurasian yang tinggi dibandingkan perangkat yang lain dalam IDS (Samrat Krishna et al., 2021).

2.2 Analysis requirements for testing system

Analisis kebutuhan yang dibutuhkan untuk melakukan pengujian ini diantaranya:

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

2.3 Create testing model

Testing model yang digunakan tersusun dalam flowchart di bawah ini

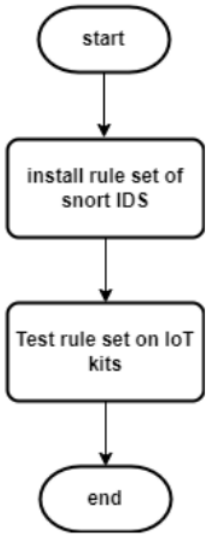

Fig 2: Testing model flowchart

2.4 System testing

Percobaan menggunakan model testing SNORT-IDS yang telah dirancang pada perangkat IoT tertanam pada smart

drone (Pampattiwar & Chhangani, 2017).

2.5 Testing result

Berisi hasil testing IDS terhadap perangkat smart drone.

2.6 Conclusion

Hasil discussion berdasarkan percobaan yang dilakukan.

3. Result and Discussion

Pengujian dan uji coba

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.	file-executable
11.	file-flash
12.	file-identify
13.	file-image
14.	file-java
15.	file-office
16.	file-other
17.	file-pdf
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.	server-mail
57.	server-mssql
58.	server-mysql
59.	server-oracle
60.	server-other
61.	server-samba
62.	sql
63.	x11

3.2 System testing

3.3 Testing result

4. Conclusion

Berdasarkan hasil penelitian yang dilakukan, dapat disimpulkan beberapa hal mengenai network intrusion detection menggunakan SNORT-IDS:

5. Acknowledgments

Penelitian ini merupakan hasil kolaborasi dengan dosen pembimbing pada mata kuliah keamanan sistem informasi.

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] Condomines, 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] 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

[6] 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/

[7] 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

[8] 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

[9] Risyad, E., Data, M., & Pramukantoro, E. S. (2018). Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(9), 2615–2624.

[10] 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.

[11] 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

[12] 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

13] 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.

[14] 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

[15] 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

Afan 5

ORIGINALITY REPORT

5%	6%	2%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Negeri Semarang Student Paper	1%
2	www.bukugue.com Internet Source	1%
3	Submitted to Universitas Pelita Harapan Student Paper	1%
4	download.garuda.kemdikbud.go.id Internet Source	1%
5	123dok.com Internet Source	1%
6	core.ac.uk Internet Source	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		