International Journal of ASRO
Volume 13, Number 04, pp.46-53
December 2022

SECOND NAVAL FLEET COMMAND DISINFOLAHTA INFORMATION SYSTEM NETWORK COMMUNICATION PROCEDURE FOR SUPPORTING THE NAVAL TASK

Adi Widodo[1], Chairul Imron[2], Sutrisno[3], Zainal Syahlan[4]

[1,3,4] *Indonesian Naval Technology College, Bumimoro-Morokrembangan, Surabaya 60187, Indonesia*
[2]*Mathematic Department, Institute Technology Ten November, Surabaya, Indonesia*
Emaiil: Adiwidodo@gmail.com

ABSTRACT

Disinfolahta's second naval fleet command has the Main task of assisting with the field of development, data collection, and processing as well as presenting information, research, and development within the Koarmada II environment and acting as an information technology service center. Telegraphic communication radio within the Indonesian Navy is used for long-distance communication between ships, aircraft, and international shore radio. RTG Telegraphic communication radio uses international Morse signs, Q codes, and Z code procedural signs to convey information or news. The application of Radio Communication Telegraphy is very vulnerable to information theft. Important information conveyed from ship to ship, ship to aircraft, or to shore radio or vice versa can be accessed publicly. Information system security defense at Disinfolahta Koarmada II has not shown a level of efficiency and effectiveness, due to the absence of a special section in the field of information system security issues related to data transactions in communication networks. Improvement or improvement of information security is needed which plays a role in maintaining the confidentiality of information. Increasing the security and confidentiality of information is very necessary so that important information that is distributed is not known by unauthorized parties. This study plans a communication protocol scenario using the Mavlink and AX2.5 communication protocols. Each scenario will be run using a simulation to get network performance. The results of network performance measurements will be modeled using a dynamic system to get the best communication protocol as a proposal in order to improve the information security system at the Second naval fleet command.

Keywords: *RTG, Mavlink, AX2.5, network performance, communication protocols*

1. INTRODUCTION

Information technology is currently one of the problematic issues because in addition to contributing to increasing human welfare, progress, and civilization, it is also an effective means of unlawful acts including criminal acts (crime). Information security is a way of preventing theft or detecting theft in a business. information-based systems, where the information itself has no physical meaning. (Raharjo, 2002). Journal of Network Security with the title "The principles of network security design", describes network security that provides system protection against threats originating from outside the network. Information system security is used to control the risks associated with the use of information and distribution of information (Stawowski, 2007). The Naval Information and Data Processing Service (Disinfolahta) is one of the Work Units (Satker) in Koarmada II which carries out special functions in the field of Naval Information Systems and Data Processing Development. In the Organization and Procedures (Orgapros) Disinfolahta Koarmada II has the Main Duties of assisting the Pangkoarmada II in the fields of coaching, data collection and processing and presentation of information, research, and development within the Koarmada II environment and acting as an information technology service center. The use of information technology in Koarmada II is strategic support for operations in achieving the goals listed in the vision and mission.

2. MATERIALS AND METHODOLOGY

2.1 Research Approach

The research carried out is research in the context of providing advice on the development of information security technology in Koarmada II which carries out a special function in the field of Information Systems Development and Naval Data Processing. Development of information security technology in answering the problem of the application of Telegraphic Communication Radio which is very prone to information theft. Important information conveyed from ship to ship, ship to aircraft, or to shore radio or vice versa can be accessed publicly. This explains the weak points of information security using RTG Telegraphic Communication Radio although in general, the information is encrypted.

2.2 Data Source, Subject, and Object Research

Sources of data in special research on data that affect the governance of information systems.

2.2.1 Data Source

The data collected was obtained from primary data and secondary data. Primary data were obtained from informant sources, namely individuals or individuals, through interviews conducted by researchers. While secondary data means that research data sources are obtained by researchers in the form of studies, evidence, historical records, or reports arranged in archives.

2.2.2 Subject

Research subjects are parties directly involved as resource persons or data providers. This research will be conducted at Disinfolahta Koarmada II Surabaya by studying information systems in relation to the distribution and exchange of data using a wireless communication system.

2.2.2 Object

In this study, the object of research was Disinfolata Second naval fleet command in Surabaya.

2.3 Research Design

VmeS implementation on VHF frequency is very vulnerable to information theft. Important information conveyed or otherwise can be accessed publicly. This is a weak point of information security using VmeS on VHF frequencies. Variable identification is carried out to determine the variables involved in modeling the system. In this step, historical patterns or hypothetical patterns are identified that describe the behavior of the problem. These patterns are integrated into an arrangement so that they can represent internal tendencies in the system. Variables are arranged based on the results of a literature study and in-depth interviews with The personel second naval fleet command.

2.3.1 Design ModelFormulation

The concept of dynamic systems refers to closed systems or systems that have feedback. The feedback loop structure links the output of the previous period with the input of the next period. So the feedback system has the ability to control itself in achieving certain goals that it identifies itself. These feedback loops are the basic framework of the system. This closed loop is a sequential circuit. The components are decisions that control the actions, levels (stats) of a system, and information about the system level. This information is the feedback.

2.3.2 Verification and Validation Model

Verification is carried out to check units or units of variables. While model validation is done to compare the behavior of the simulated model with the behavior of the actual system. If in testing there are significant differences in behavior, then the system variables can be reviewed again or modified as necessary. However, if appropriate behavior is achieved, then the model can be accepted as a valid representation of the actual system.

2.3.3 Design Scenario Of Communication Protocol

The results of interviews with the Disinfolahta Koarmada II Surabaya obtained several variables that will be used in making the simulation model, such as *Throughput, Packet Loss, and End-to-End Delay.*

2.3.4 Causal Loop Diagram

From the existing Network Security modeling references, the Causal Loop Diagram concept was created for planning the development of information technology security in implementing communication protocols. The four main behaviors in the loop clause;

a. Training strengthens awareness (loop R1).
b. Incidents of information theft can increase the likelihood of other information theft incidents (R2).
c. Management invests in training to improve resilience and information security (loop B1).
d. Management invests in technical security to increase resilience and information security (loop B2).

2.3.5 Stock and Flow Diagram

The attack model is described as consisting of two stocks, namely, the success of information theft and the development of an information security system. The success of information theft arises due to the vulnerability of the security system, as the value of the probability rate of information theft. Information security resilience capability arises as a result of efforts to increase information security

resilience. Risk assessment efforts are also needed to be able to assess which parts of the system are vulnerable to information theft so that efforts to reduce vulnerability can be carried out in accordance with the results of the risk assessment carried out.

2.3.6. Formulation

The model is built consistently in the use and measurement of its variables on system elements. The next step is to create equations to connect variables and constants that are defined in each element of the system. Errors in determining and using units, variables, and constants will result in unnecessary confusion and complexity.

2.3.7. Trial Model

Model testing is carried out to determine the feasibility of the model that has been made. The model testing consists of:

a. Verify the model to avoid errors.

b. Does the model resemble the actual system?

2.3.8. Analysis and Interpretation

Analysis and interpretation are done to compare with the actual system. How do the variables influence each communication parameter that has been made?

3. RESULT AND DISCUSSION

In the process of implementation, radiotelegraphy can be formed in a communication network consisting of two or more radios at the same frequency. In transmitting data, a modulation system model is used, namely FSK modulation. The Matlab simulation model with the message configuration sent via the FSK modulator and received and processed on the demodulator is shown in the waveform figure Figure 1. The simulation modeling is set up by sending a message 'Telegram message'.

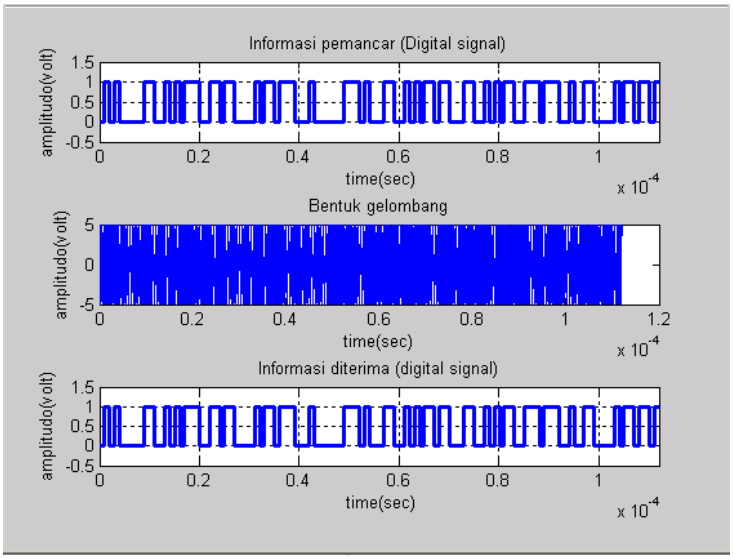

Figure 1. Transmitter Information Waveform, Modulated Waveform, and Receiver Information Waveform

Binary data when displayed in Figure 2.

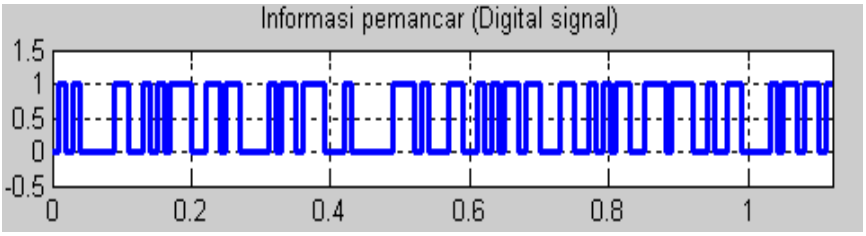

Figure 2. Transmitter Data Information In Binary

Network performance simulation tests using the AX2.5 and Mavlink protocols will be explained in the following discussion. The initial number of nodes used as a successful trial configuration is 8 nodes. The source node is node 0 in red and the destination node is node 4 in blue. Node 0 performs the process of sending data to be submitted to node 4.

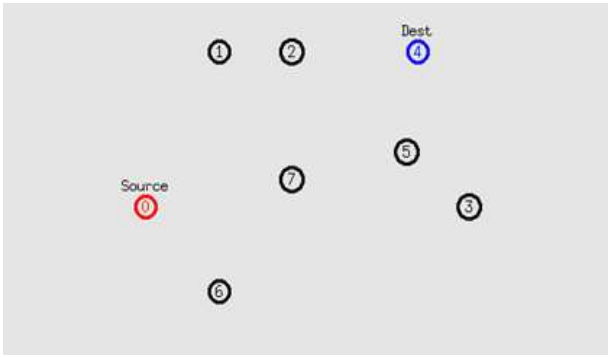

Figure 3. Protocol AX2.5 simulation

The RREP process is given by all nodes other than node 0, which aims as a routing process to get the shortest route from node 0 to node 4. From the simulation process, the shortest routes are node 0, node 7, and node 4.

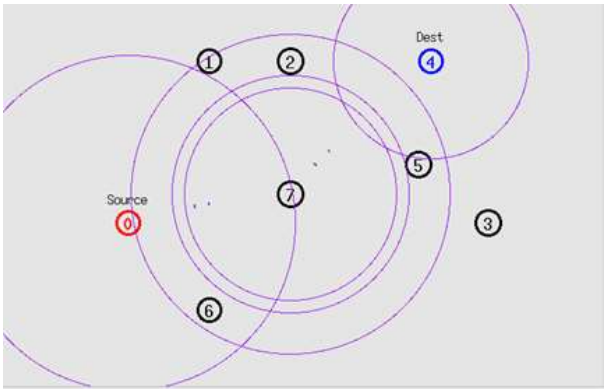

Figure 4. Route discovery

The simulation displays the process of sending packets from node 0 to node 4 via node 7. The process of sending packets will be carried out until 100 packets are sent.

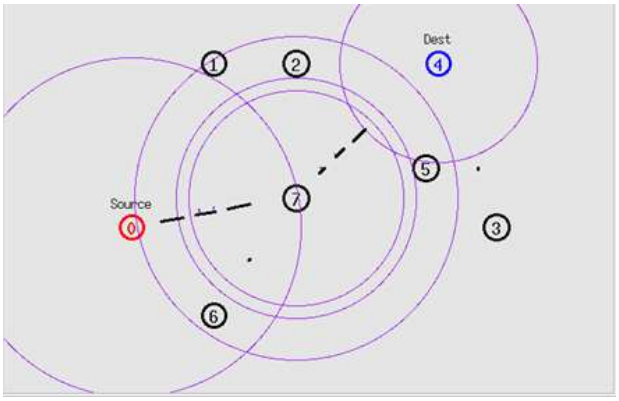

Figure 5. Send Packet from Node 0 – Node 7-Node 4

The test results obtained a Packet Delivery Ratio of 1.0 or a percentage is 100%. This proves that the number of Packet Losses is 0 or there are no lost packets in the shipping process. In the large test packets sent were 8631 packets and those received by node 4 were 8631 packets.

```
Packet delivery ratio
 Sending          :8631
 Receive          :8631
 Ratio            :1.0000
```

Figure 6. Packet Delivery Ratio

Throughput measurement results obtained a value of 16580 Kbps, throughput is data sent in units that represent how much bandwidth capacity is actually used.

Figure 7. Measure Throughput

Graph Figure 8 describes the graph of AX2.5 network performance with a variable throughput of 0.009948, packet loss of 0, and end-to-end delay of 0.002501 In the graph, the maximum network performance figure is 3.58 The results of network performance against time series are shown in Table 1.

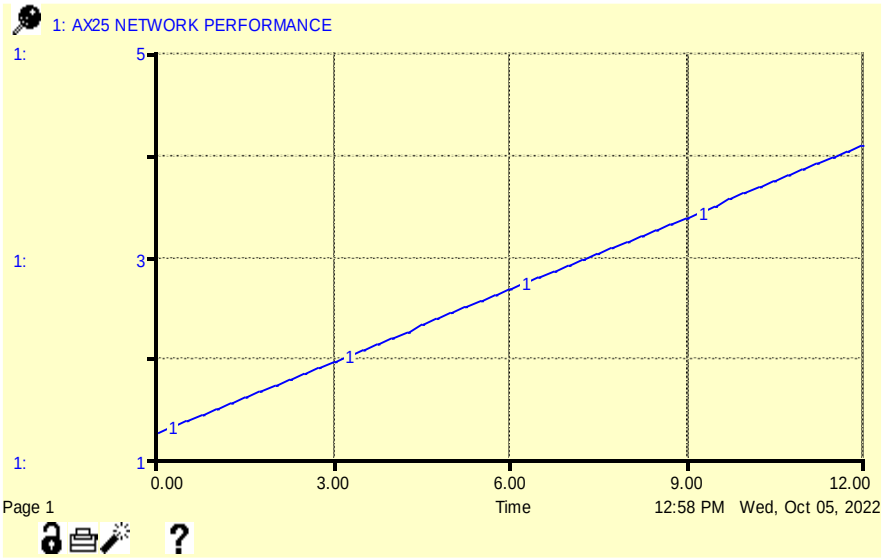

Figure 8. AX2.5 Protocol Performance

Table 1. AX2.5 Protocol Performance

Time	**Performance AX2.5**	***End to end delay***	***Packet loss***	***Throughput***
0	0.74000	0.00250	0.00000	0.00995
0.25	0.80000	0.00250	0.00000	0.00995
0.5	0.86000	0.00250	0.00000	0.00995
0.75	0.92000	0.00250	0.00000	0.00995
1	0.97000	0.00250	0.00000	0.00995
11	3.35000	0.00250	0.00000	0.00995
11.25	3.41000	0.00250	0.00000	0.00995
11.5	3.47000	0.00250	0.00000	0.00995
11.75	3.52000	0.00250	0.00000	0.00995
Final	3.58000	0.00250	0.00000	0.00995

Graph Figure 9 explains the MAVLINK network performance graph with throughput variables of 0.152617, packet loss of 0.083482996, and end-to-end delay of 0.127451. In the graph, the maximum network performance figure is 3.03. The results of network performance against time series are shown in Table 2.

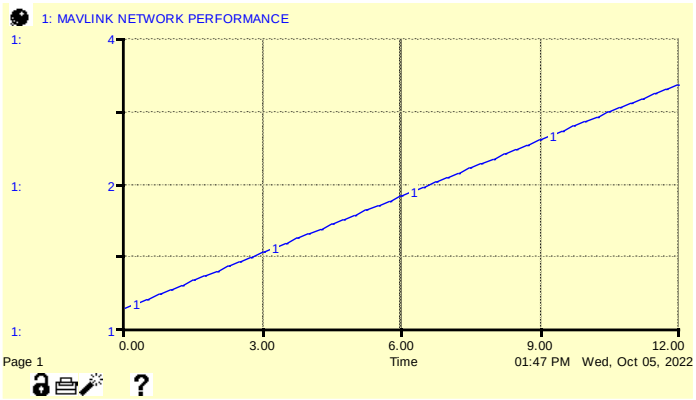

Figure10. MAVLINK Protocol Performance

Table 2. MAVLINK Protocol Performance

Time	**Performance MAVLINK**	***End to end delay***	***Packet loss***	***Throughput***
0	0.69	0.0025	0	0.00995
0.25	0.74	0.0025	0	0.00995
0.5	0.79	0.0025	0	0.00995
0.75	0.84	0.0025	0	0.00995
1	0.89	0.0025	0	0.00995
11	2.83	0.0025	0	0.00995
11.25	2.88	0.0025	0	0.00995
11.5	2.93	0.0025	0	0.00995
11.75	2.98	0.0025	0	0.00995
Final	3.03	0.0025	0	0.00995

4. CONCLUSION

From the results of collecting, processing, analyzing data, and presenting the results of data processing that has been done, conclusions can be drawn based on the results that have been obtained as follows:

a. Based on the simulation results and analysis of the AX2.5 and MAVLink communication protocols, the AX2.5 network performance has a throughput of 16580 bps, a delay of 0.005274 seconds, and a packet loss of 0. Meanwhile, the performance of the MAVLink network has a throughput of 142759 bps, a delay of 0.113181, and a packet loss of 20794. From the measurement results and analysis, it can be concluded that the AX.2.5 communication protocol has better network performance than MAVLink, this is evidenced by the packet loss value of 0, which means that the AX 2.5 communication protocol does not lose data. The test and analysis results show that the AX2.5 communication protocol is the recommended communication protocol in an effort to increase information security.

b. In the dynamic system modeling that has been implemented with the planning stage Causal Loop Diagram is detailed with Stock and flow diagrams, which can explain the relationship between variables and determine the effect of time on the decision of the composition of the communication protocol. Stock shows the accumulation of variable values while rate shows the rate of change of the system over time. Based on the results of the dynamic system modeling that has been implemented, the final result of the network performance of the AX 2.5 communication protocol is 3.58 and the MAVLink communication protocol is 3.03. The validation and verification results of the model on field events obtained an average MAPE error value of 2.8% for AX2.5 and the results of the MAVLink network performance validation obtained an average MAPE error value of 2.9%.

c. Telegraphic communication radio is used for long-distance communication between ships, aircraft, and international shore radio at Disinfo Surabaya. RTG Telegraphic communication radio uses international Morse signs, Q codes, and Z code procedural signs to convey information or news. In the process of implementation, radiotelegraphy can be formed in a communication network consisting of two or more radios at the same frequency.

Parameters based on the Quality of service of radio communication networks to represent overall network performance are throughput, packet loss, and delay. Throughput represents how much bandwidth capacity is actually used, packet loss describes how many data packets are not delivered to the recipient and delay is the time required for data transmission.

ACKNOWLEDGEMENT

The authors greatly acknowledge the support from Indonesia Naval Technology College STTAL Surabaya Indonesia for providing the necessary resources to carry out this research work. The authors are also grateful to the anonymous reviewers and journal editorial board for their many insightful comments, which have significantly improved this article.

REFERENCES

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network*, *2*(1), 123–138. https://doi.org/10.3390/network2010009

Aprillya, M. R., Suryani, E., & Dzulkarnain, A. (2019). System Dynamics Simulation Model to Increase Paddy Production for Food Security. *Journal of Information Systems Engineering and Business Intelligence*, *5*(1), 67. https://doi.org/10.20473/jisebi.5.1.67-75

Chai, T., & Draxler, R. R. (2014). Root mean square error (RMSE) or mean absolute error (MAE)? -Arguments against avoiding RMSE in the literature. *Geoscientific Model Development*, *7*(3), 1247–1250. https://doi.org/10.5194/gmd-7-1247-2014

Forrester, J. W. (1994). *System dynamics, systems thinking, and soft OR*.

Ghafiqie, A. (2012). Pengembangan Model Sistem Dinamis Untuk Menganalisa Kontribusi MRT Jakarta Terhadap PAD DKI Jakarta. *Universitas Indonesia Library*, 1–82. http://lib.ui.ac.id/file?file=digital/20309768-T31003 - Pengembangan model.pdf

Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *8*(2), 137. https://doi.org/10.17933/mti.v8i2.108

Korcz, K. (2017). Maritime Radio Information System. *Journal of KONES*, *24*(3), 127–134. https://doi.org/10.5604/01.3001.0010.3060

Koubaa, A., Allouch, A., Alajlan, M., Javed, Y., Belghith, A., & Khalgui, M. (2019). Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey. *IEEE Access*, *7*, 87658–87680. https://doi.org/10.1109/ACCESS.2019.2924410

Lázaro, F., Raulefs, R., Wang, W., Clazzer, F., & Plass, S. (2019). VHF Data Exchange System (VDES): an enabling technology for maritime communications. *CEAS Space Journal*, *11*(1), 55–63. https://doi.org/10.1007/s12567-018-0214-8

Maesaroh, S., Kusumaningrum, L., Sintawana, N., Lazirkha, D. P., & O., R. D. (2022). Wireless Network Security Design And Analysis Using Wireless Intrusion Detection System. *International Journal of Cyber and IT Service Management*, *2*(1), 30–39. https://doi.org/10.34306/ijcitsm.v2i1.74

Menteri Pertahanan Republik Indonesia. (2015). *Buku Putih Pertahanan Indonesia 2015*.

Natamiharja, R. (2018). A Case Study on Facebook Data Theft in Indonesia. *FIAT JUSTISIA:Jurnal Ilmu Hukum*, *12*(3), 206. https://doi.org/10.25041/fiatjustisia.v12no3.1312

permenhan. (2014). *PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA NOMOR 36 TAHUN 2014*.

Raharjo, A. (2002). *Cybercrime : pemahaman dan upaya pencegahan kejahatan berteknologi* (Citra Aditya Bakti (ed.); Cet.1).

Sabadina, U. (2021). Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online. *Jurnal Lex Renaissance*, *6*(4), 799–814. https://doi.org/10.20885/jlr.vol6.iss4.art11

Salahuddin, Bakhtiar, Yusman, & Fadhli. (2019). Efficiency of AX.25 Protocol in a Wireless SCADA Communication System for Monitoring Performance of Micro-Hydro Power Plants. *IOP Conference Series: Materials Science and Engineering*, *536*(1). https://doi.org/10.1088/1757-899X/536/1/012051

Stateczny, A., Gierlowski, K., & Hoeft, M. (2022). Wireless Local Area Network Technologies as Communication Solutions for Unmanned Surface Vehicles. *Sensors*, *22*(2), 1–30. https://doi.org/10.3390/s22020655

Stawowski, B. M. (2007). The Global Voice of Information Security The Principles of Network Security Design. *Information Security*, *October*, 29–31.

Xu, X., Ngoc Cuong, T., Lee, S.-D., & You, S.-S. (2020). Secure communication system in

maritime navigation using state observer with linear matrix inequality. *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, *4*(3), 70–75. https://doi.org/10.1080/25725084.2020.1790102

Yau, K. L. A., Syed, A. R., Hashim, W., Qadir, J., Wu, C., & Hassan, N. (2019). Maritime Networking: Bringing the Internet to the Sea. *IEEE Access*, *7*(January), 48236–48255. https:// doi.org/ 10. 1109 / ACCESS.2019. 2909921