SYSTEM DYNAMIC MODELING OF COMMUNICATION PROTOCOL FOR INCREASING SECURITY AND CONFIDENTIALITY OF INFORMATION SYSTEM IN SECOND FLEET COMMAND

Adi Widodo[1], Eko Krisdiono[2], Zainal Syahlan[3]

[1,2,3]Indonesian Naval Technology Collage
Bumimoro-Morokrembangan, Surabaya 60178, Indonesia

ABSTRACT

The progress of information technology science is a current problem because, in addition to being able to contribute to improving welfare, progress, and the level of human civilization, it can also have a negative impact that causes unlawful actions and actions including criminal acts (crimes). Department of Information and Data Processing of Second Fleet Command has the main task of collecting, managing, and processing data as well as presenting information, research, and development in the Second Fleet Command 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 coastal radio. Radio communication Telegraphy RTG uses international Morse signs, Q code, and Z code procedural signs to convey information or news. This research is planning a communication protocol scenario using the Mavlink and AX2.5 communication protocols. Each scenario will be run using simulation to get network performance. The results of the network performance measurement will be modeled using a dynamic system to get the best communication protocol as a proposal to improve the information security system at the Department of Information and Data Processing Second Fleet Command.

Keywords: RTG, Mavlink, AX2.5, Radio communication Telegraphy, Communication protocol, network performance

.

1. INTRODUCTION

The development of information technology is currently a dilemmatic problem because it can contribute to improving welfare, progress, and human civilization, but on the other hand, it becomes an effective means for unlawful acts, namely a crime. Information security is how to prevent theft or detect theft in an information-based system, where the information itself has no physical meaning (Raharjo, 2002).

Network security in the journal "The principles of network security design", is the main network security as system protection against threats originating from outside the network. Information system security is used to control risks associated with the use of information and distribution of information (Stawowski, 2007). The application of Radio Telegraphy communication is very vulnerable to information theft. Important information that is conveyed from ship to ship, ship to aircraft, or to coastal radio or vice versa can be accessed publicly. This explains the weak point of information security using Radio Telegraphy RTG communication even though in general the information has been encoded in international Morse signs, Q code, and Z code procedure marks.

Information system security defense in the Department of Information and Data Processing Second Fleet Command has not shown a level of efficiency and effectiveness, due to the absence of a special section on the field of information system security issues related to data transactions in communication networks, which fully plays a role and has responsibility in handling the security of existing Information Technology resources. There is no Standard Operating Procedure (SOP) for defense from information system attacks and recovery from attacks or data theft. The need for the importance of network security in information or news transactions from ship to ship, ship to aircraft, or to coastal radio or vice versa requires improvement or enhancement of information security that plays a role in maintaining the confidentiality of information. The Navy Information and Data Processing Service (Department of Information and Data Processing) is the Working Unit in Second Fleet Command which carries out special functions in the field of Information System Development and Naval Data Processing. The usage of information technology in Second Fleet Command is strategic support for operations in achieving the objectives stated in the vision and mission. The application of Radio Telegraphy communication is very vulnerable to information theft.

Important information that is conveyed from ship to ship, ship to aircraft, or to coastal radio or vice versa can be accessed publicly. This explains the weak point of information security using Radio Telegraphy RTG communication even though in general the information has been encoded in international Morse signs, Q code, and Z code procedure marks. Information system security defense in the Department of Information and Data Processing Second Fleet Command has not shown a level of efficiency and effectiveness, due to the absence of a special section on the field of information system security issues related to data transactions in communication networks, which fully plays a role and has responsibility in handling the security of existing Information Technology resources. There is no Standard Operating Procedure for defense against information system attacks and recovery from attacks or data theft. The need for the importance of network security in information or news transactions from ship to ship, ship to aircraft, or to coastal radio or vice versa requires improvement or enhancement of information security that plays a role in maintaining the confidentiality of information.

2. MATERIALS AND METHODS

2.1 Research Approach

The research to be carried out is a type of quantitative research carried out by developing using mathematical models, theories, and hypotheses related to empirical observations. Second Fleet Command is the largest Indonesian navy Fleet in the central region of Surabaya. The Navy Information and Data Processing Service are one of the Working Units in the Second Fleet Command which carries out special functions in the field of Information System Development and Naval Data Processing. The application of Radio Telegraphy communication is very vulnerable to information theft. Important information that is conveyed from ship to ship, ship to aircraft, or to coastal radio or vice versa can be accessed publicly. This explains the weak point of information security using RTG Telegraph Radio communication even though in general the information has been encoded.

2.2 Data Sources, Subjects, and Research Objects

The data sources, subjects, and objects of this research are devoted only to data that affect infrastructure, software, hardware, security, and information system network governance.

2.2.1 Data Source

The information collected was obtained from the essential information and auxiliary information. Essential information was obtained from informants, namely individuals or individuals, through interviews conducted by researchers. While secondary data means the source of research data obtained by researchers within the frame of studies, proving historical records or reports orchestrated in files.

2.2.2 Subjects

Research subjects are parties who are directly involved as resource persons or data providers. This research will be conducted at the Department of Information and Data Processing

Second Fleet Command Surabaya by examining the information system in its fabric in the distribution and exchange of data using a wireless communication system.

2.2.3 Objects

The object of this research is the Disinfolata Second Fleet Command Surabaya. It has tasks to manage, and secure all data in the Second Fleet Command. Moreover, disinfolahta second fleet command is the nearest place and can represent the research in the navy.

2.3 Research design

VmeS is a communication that uses radio intermediaries in the Very High Frequency (VHF) frequency to send messages or data from the sending station to the receiving station. The VMeS terminal is at the sending station and the VMeS gateway is at the base station or receiving station. The application of VmeS on the VHF frequency is very vulnerable to information theft. Important information submitted or otherwise can be accessed publicly. This is a weak point of information security using VmeS on VHF frequencies. Variable identification is done to find out 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 (fabrication) so that they can represent the internal tendencies that exist in the system. The variables were arranged based on the results of literature studies and in-depth interviews with the Department of Information and Data Processing Second Fleet Command Surabaya.

2.3.1 Model Design and Formulation

A dynamic system is basically a system where the modeler will take into account the value of the taste of the system, not just the logic of a system. In the Dynamic System method, the system concept refers to a closed system or a system that has feedback. The feedback system has the ability to control itself in achieving certain goals that it identifies itself.

2.3.2 Model Verification and Validation

Performed to test the accuracy of the logic of the model and there are no errors. The process of checking units or unit variables is carried out in this process. While the model validation is done to compare the behavior of the simulation model with the actual system behavior. If in the test there is a significant difference in behavior, then the system variables can be reviewed again or modified as necessary. However, if behavioral conformity is achieved, then the model can be accepted as a valid representation of the actual system.

2.3.3 Communication Protocol Scenario Design

The design and formulation of the simulation model were built based on the results of in-depth interviews with the Department of Information and Data Processing Second Fleet Command Surabaya. The interview results obtained an overview of the wireless communication system that is applied today. This stage is supported by some literature and data from the Department of Information and Data Processing Second Fleet Command Surabaya. The data is used as initial input when designing the model. Furthermore, a mathematical formulation of the model is made, so that the model can describe the state of the real system. Variable identification is carried out through in-depth interviews. Based on the comes about of the meeting, several variables were gotten that will be used in making the simulation model, such as:

a. Throughput. Throughput is communicated as the volume of information that’s effectively sent in unit time. It could be a degree of how quickly or moderately the arrangement is being measured.

b. Packet Loss Is a measurement of how many packets are lost in the process of sending data.

c. End-to-End Delay is a measurement of the time interval required to transmit data from the sender to the receiver.

2.3.4 Causal Loop Diagram

Causal Loop Diagram (CLD) (Ghafiqie, 2012), serves to describe the relationship between variables that have been defined previously. From the existing Network Security modeling references,a Causal Loop Diagram concept was made for planning the development of information technology security in implementing communication protocols. The four main behaviors in the clause loop:

a. Training strengthens awareness (loop R1).

b. Incidents of theft of information can increase the likelihood of another incident of theft of information (loop R2).

c. Management contributes to make strides in data security and versatility (loop B1).

d. Management contributes to specialized security to increase versatility 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 information security systems. The success of information theft arises due to the vulnerability of the security system, as the probability value of the information theft rate. Information security resilience capabilities arise 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 made according to the results of the risk assessment carried out.

2.3.6 Formula Determination

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

2.3.7 Testing Model

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

a. Verify the model to avoid errors and,

b. The model resembles 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.

This chapter will explain the analysis and discussion of the research "Procedures of Communications Network Information System Department of Information and Data Processing Second Fleet Command to Support the Main Duties of the Indonesian Armed Forces in Facing Cyber Threats and Information Crime". At the beginning of the discussion will be described the data transmission system model on radiotelegraphy communication which is used for long-distance communication between ships, aircraft, and international coastal radio.

Radio communication Telegraphy RTG uses international Morse signs, Q code, and Z code procedural signs to convey information or news. In the implementation process, radiotelegraphy can be formed in a communication network consisting of two or more radios on the same frequency. In transmitting data, a modulation system model is used, namely FSK modulation. The Matlab simulation model with the configuration of messages sent through the FSK modulator and received and processed in the demodulator is shown in the waveform image Figure 1. The simulation model is set by sending the message 'Telegram message'.

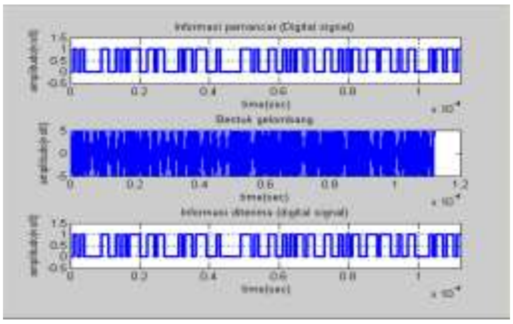


Figure 1. Transmitter and Receiver Information Wave

In the Figure 2 shows the data information that transmiting in binary form.

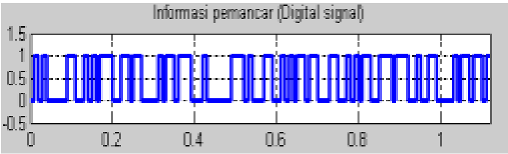


Figure 2. Transmitter Data Information in Binary

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

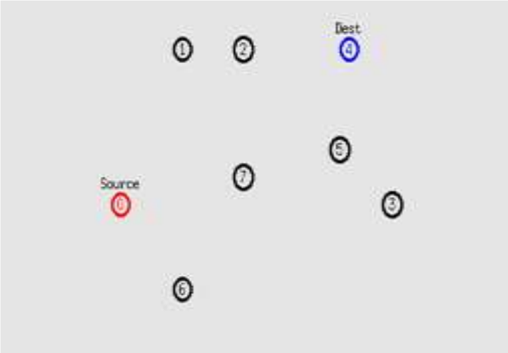


Figure 3. Simulation of The AX2.5 Protocol

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.

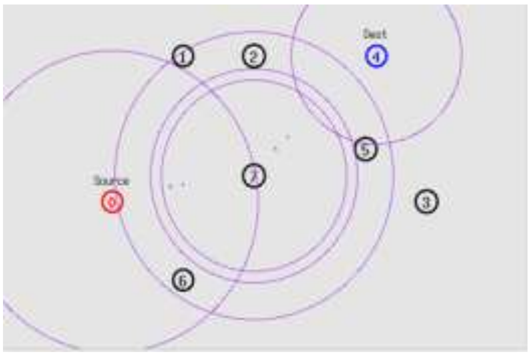


Figure 4. Route Search Process

The simulation shows the process of sending packets from node 0 to node 4 through node 7. The packet delivery process will be carried out until 100 packets are sent.

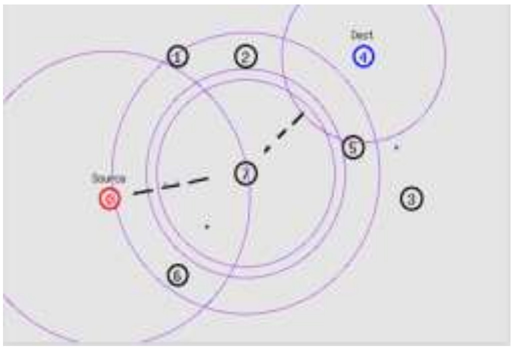
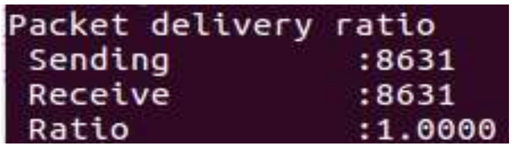


Figure 5. The Process of Sending Packets

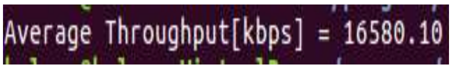
The test results in figure number 6 was obtained Packet Delivery Ratio of 1.0 or in percentage is 100%. This proves the number of Packet Loss is 0 or there are no packets lost in the transmitting process. In the large test, the packets sent were 8631 and received by node 4 was 8631 packets.



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

Figure 6. Packet Delivery Ratio

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



```
Average Throughput[kbps] = 16580.10
```

Figure 7. Throughput Measurement

4. CONCLUSION.

Based on the comes about of the investigate recreation with the title "Modeling Communication Protocol Dynamic Systems in Improving the Security and Confidentiality of the Information Systems of the Second Fleet Command Surabaya" is as follows, namely, with no packet loss found in the AX2.5 protocol communication test, the AX2.5 protocol has the highest level of the best coefficient and become a proposal in an effort to improve security and confidentiality in the information system at Second Fleet Command Surabaya.

ACKNOWLEDGEMENT

In this paper, the authors greatly acknowledge the support from 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

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*,

Ghafiqie, A. (2012). Pengembangan Model Sistem Dinamis Untuk Menganalisa Kontribusi MRT Jakarta Terhadap PAD DKI Jakarta. Universitas Indonesia Library, 1–82.

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.*

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.

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.

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

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