ROBUST DEFENSE SCHEME AGAINST SELECTIVE DROP ATTACK IN WIRELESS AD HOC NETWORKS

B.S.Murthy [1], G.Naveena 2,

[1]**Assistant professor(HOD) , MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:-suryanarayanamurthy.b@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:- guttulanaveena@gmail.com

ABSTRACT

Performance and security are two critical functions of wireless ad-hoc networks (WANETs). Network security ensures the integrity, availability, and performance of WANETs. It helps to prevent critical service interruptions and increases economic productivity by keeping networks functioning properly. Since there is no centralized network management in WANETs, these networks are susceptible to packet drop attacks. In selective drop attack, the neighboring nodes are not loyal in forwarding the messages to the next node. It is critical to identify the illegitimate node, which overloads the host node and isolating them from the network is also a complicated task. In this paper, we present a resistive to selective drop attack (RSDA) scheme to provide effective security against selective drop attack. A lightweight RSDA protocol is proposed for detecting malicious nodes in the network under a particular drop attack. The RSDA protocol can be integrated with the many existing routing protocols for WANETs such as AODV and DSR. It accomplishes reliability in routing by disabling the link with the highest weight and authenticate the nodes using the elliptic curve digital signature algorithm. In the proposed methodology, the packet drop rate, jitter, and routing overhead at a different pause time are reduced to 9%, 0.11%, and 45%, respectively. The packet drop rate at varying mobility speed in the presence of one gray hole and two gray hole nodes are obtained as 13% and 14% in RSDA scheme

1 INTRODUCTION

MOVING target defense (MTD) is one of the cyberspace game-changing revolutionary technologies proposed by Federal Networking and Information technology Research and Development (NITRD) in recent years. Nowadays, network security configurations are typically deterministic, static and homogeneous. These features reduce the difficulties for cyber attackers scanning the network to identify specific targets and gather essential information. Thus, the attackers take the asymmetric advantages of building up, launching and spreading attacks, and the defenders are at a passive position. The existing defense mechanisms and approaches cannot reverse this situation. Therefore, MTD is proposed as a new revolutionary technology to alter the asymmetric situation of attacks and defenses. It keeps moving the attack surface of the protected target through dynamic shifting, which can be controlled and managed by the administrator. In this way, the attack surface exposed to attackers appears chaotic and changes all the time. Thus, the work effort, i.e., the cost and

complexity for the attackers to launch a successful attack, will be greatly increased. As a result, the probability of successful attacks will be decreased, and the resiliency and security of the protected target will be enhanced effectively. The revolutions of MTD can be summarized from the following three aspects: (i)Dynamic defense: the transformation from static to dynamic in system architecture. (ii)Active defense: the transformation from passive perception into actively setting blocks to the weakness and virus in security mechanism. (iii)Flexible defense: the transformation from regular into a flexible operation mode. The basic goal of MTD is to achieve the active defense to the external attacks based on unknown vulnerabilities and backdoors. To date, MTD has been studied in various contexts, including cloud computing, and web applications.

Literature Survey

Literature survey is that the most vital step in software development process. Before developing the tool, it's necessary to work out the time factor, economy and company strength. Once this stuff is satisfied, ten next steps are to work out which OS and language used for developing the tool. This literature survey is mainly used for identifying the list of resources to construct this proposed application.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

Literature survey is that the most vital step in software development process. Before developing the tool, it's necessary to work out the time factor, economy and company strength. Once this stuff is satisfied, ten next steps are to work out which OS and language used for developing the tool. This literature survey is mainly used for identifying the list of resources to construct this proposed application.

Proposed System & alogirtham

In this paper, we present an encryption scheme to improve DES under the concept of MTD, by means of (linear) network coding (NC), which advocates linearly combining coding along with data propagation. The following two reasons motivate us to choose NC. First, NC, which has been used in for encryption scheme design, changes the static nature of network information transmission, so it is a good match to achieve the dynamic, active and random features of MTD as defined. Second, the use of NC as an encryption scheme has the potential to resist the exhaustive attack, as an L-bit plaintext may correspond to possible ciphertexts.

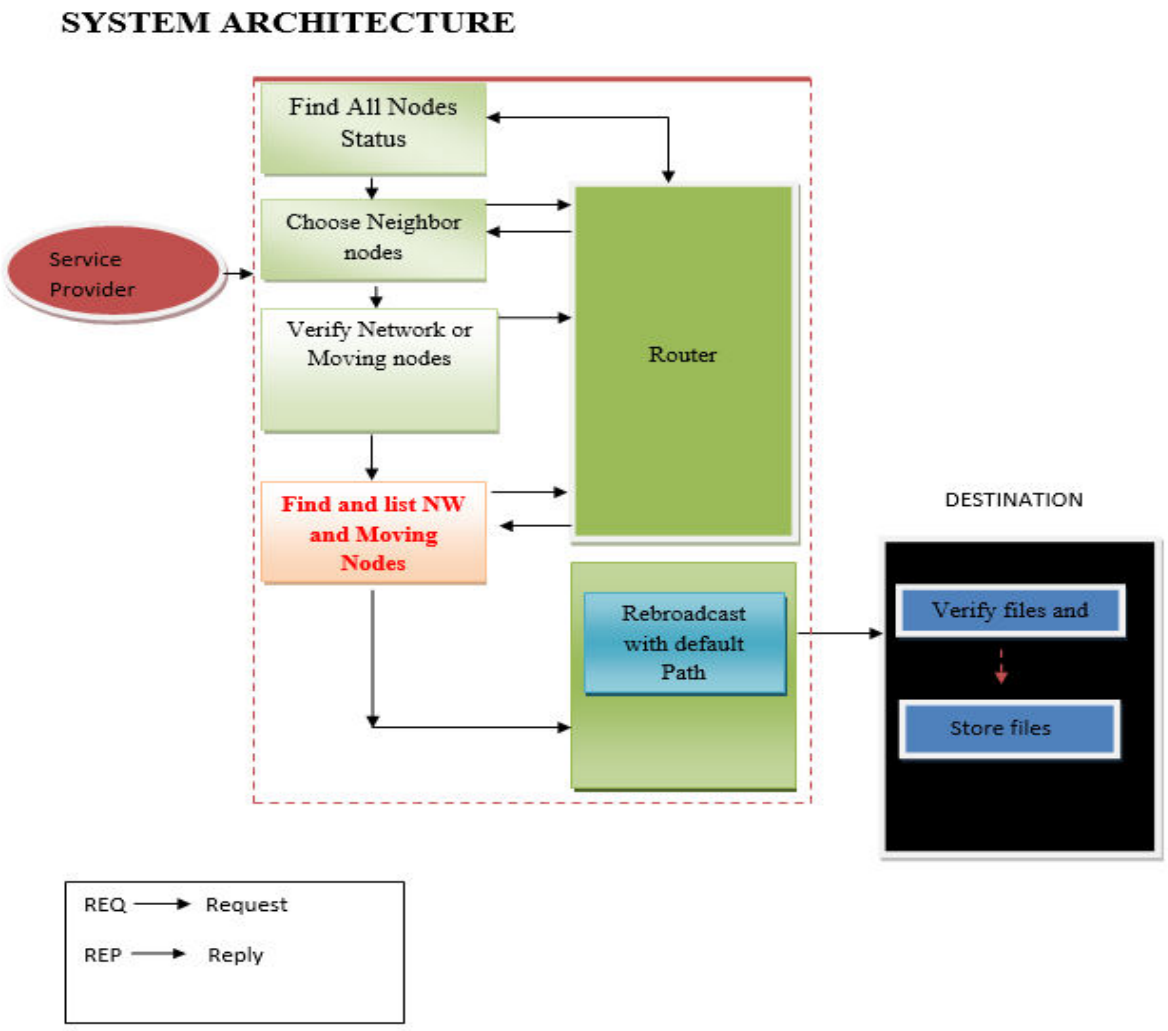


Fig:3.1 System Architecture

IMPLEMENTATION

MODULES:

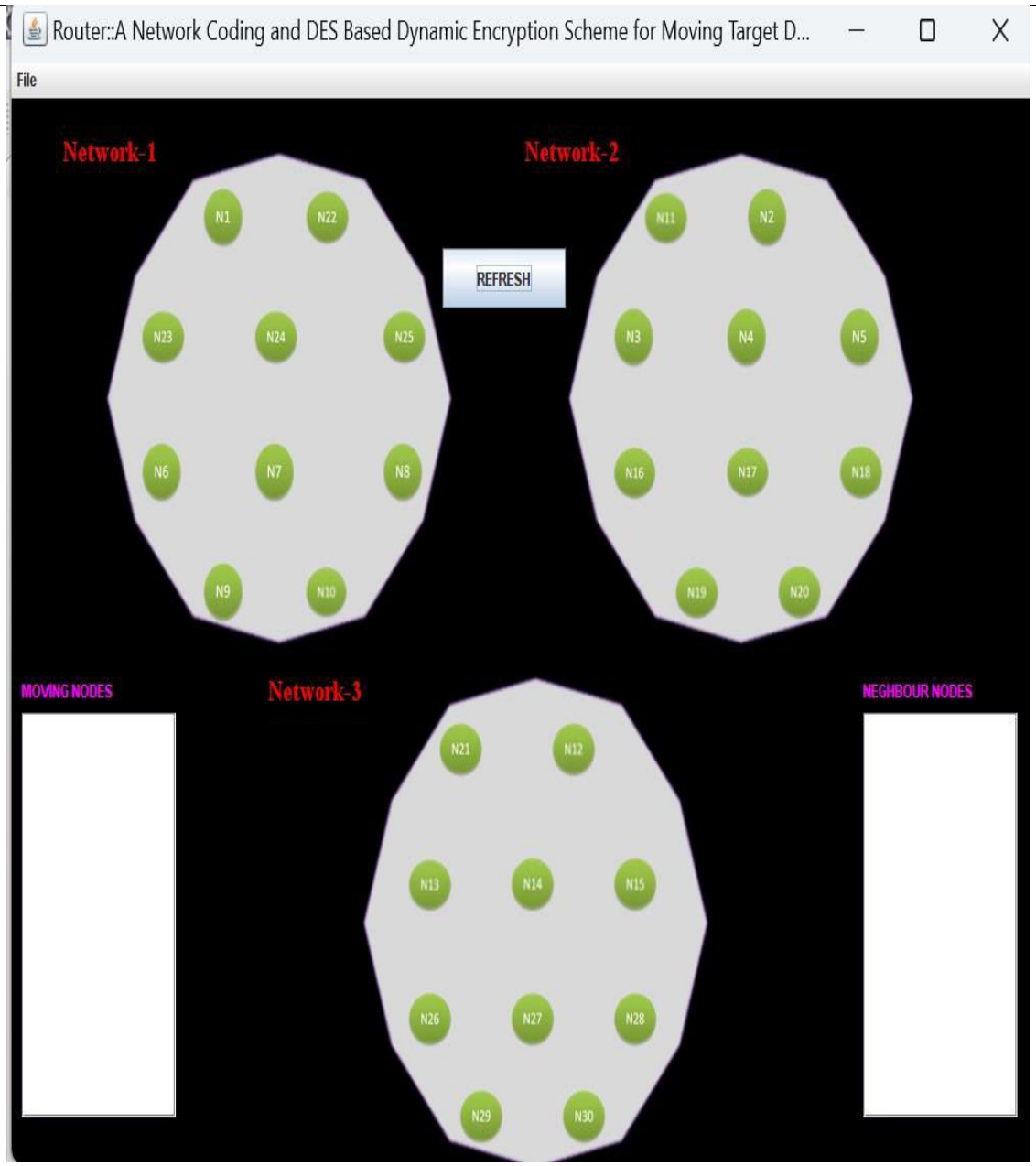
1. Inner Layer Encryption Embedding NC

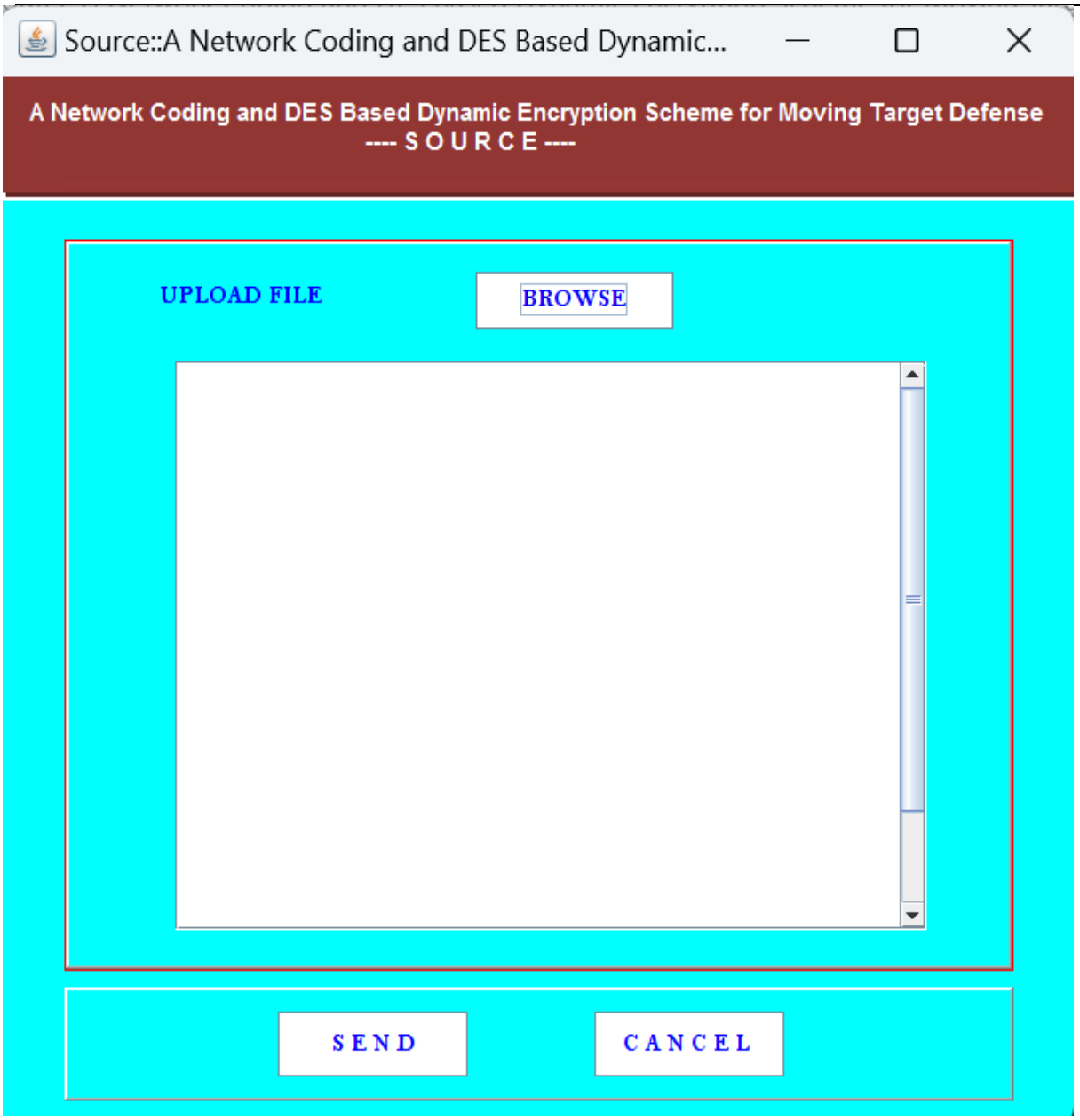
   In this step, the plaintext x, which is a binary row vector, is converted to a binary intermediate sequence z1 based on a high-dimensional binary invertible matrix Ka generated by the concept of NC. The main purpose of this step is to extend the key space of the algorithm, so as to resist the exhaustive attack.

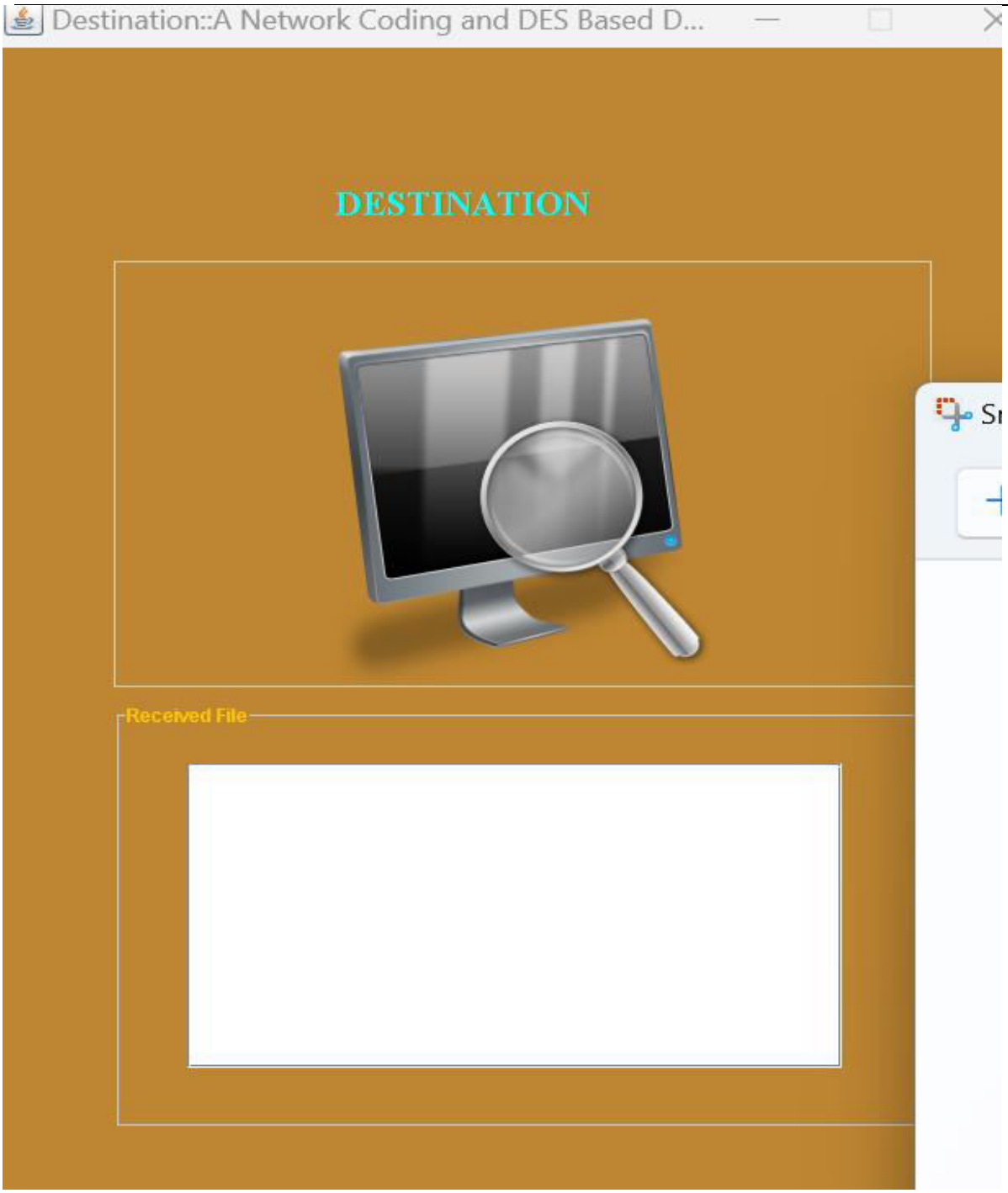
2. Middle Layer DES Encryption

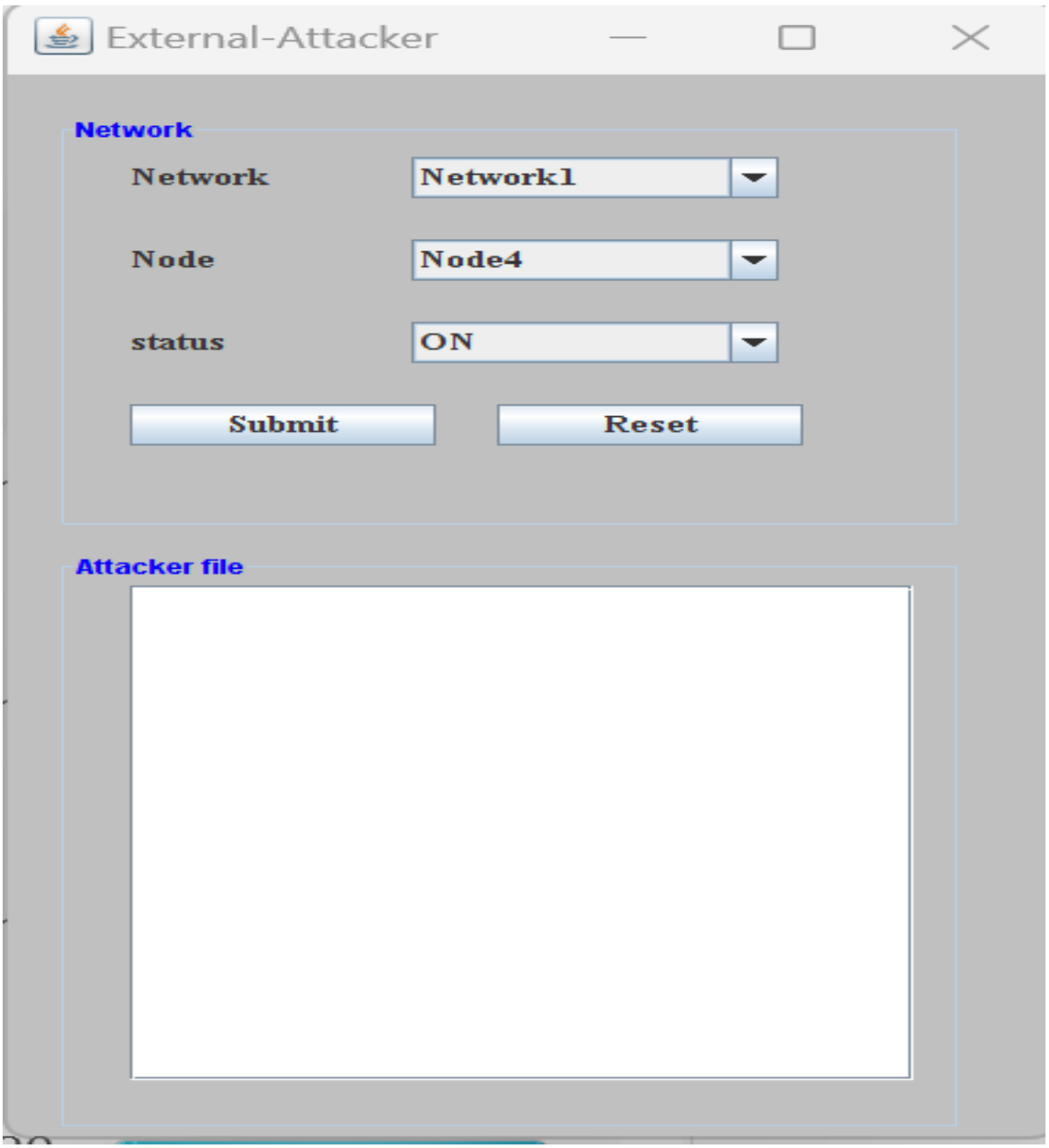
   The middle layer encryption step adopts DES to encode intermediate sequence z1, and get another intermediate sequence z2. The main purpose of this step is to exploit the design of S-box in DES to bring non-linearity into the encryption scheme, and hence to effectively defense the analysis attack.

5 RESULTS AND DISCUSSION


Router::A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target D...
File
Network-1
Network-2
N1
N22
N23
N24
N25
N6
N7
N8
N9
N10
REFRESH
N11
N2
N3
N4
N5
N16
N17
N18
N19
N20
MOVING NODES
Network-3
NEGHBOUR NODES
N21
N12
N13
N14
N15
N26
N27
N28
N29
N30


Source::A Network Coding and DES Based Dynamic...
A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense
---- S O U R C E ----
UPLOAD FILE
BROWSE
SEND
CANCEL


Destination::A Network Coding and DES Based D...
DESTINATION
Received File



6. CONCLUSION AND FUTURE WORK

CONCLUSION

In this paper, we proposed a novel encryption scheme which combines both the DES and the network coding characteristic, which has good behavior to resist both exhaustive and analysis attacks. The simulation results show that the running ratio of the proposed scheme is relatively lower than or comparable to the triple DES. The NC nature of the proposed scheme makes it endow the dynamic, active and random characteristics in the concept of Moving Target Defense (MTD). The security level of the proposed scheme will be tested in our future work.

7. REFRENCES

[1] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, X. S. Wang, Moving Target Defense—Creating Asymmetric Uncertainty for Cyber Threats, Germany: Springer, 2011.

[2] S. Jajodia, A. K. Ghosh, V. Subrahmanian, V. Swarup, C. Wang, and X. S. Wang, Moving target defense II, Application of Game Theory and Adversarial Modeling. Series: Advances in Information Security, Springer Science & Business Media, New York, 2013.

[3] M. Carvalho and R. Ford, ―Moving-target defenses for computer networks.‖ IEEE Security & Privacy, vol. 2, no.12, pp. 73-76, 2014.

[4] W. Peng, F. Li, C.-T. Huang, and X. Zou, ―A moving-target defense strategy for cloud-based services with heterogeneous and dynamic attack surfaces,‖ IEEE International Conference on Communications (ICC), Sydney, Jun., 2014.

[5] A. D. Keromytis, R. Geambasu, and S. Sethumadhavan, ―The meerkats cloud security architecture,‖ IEEE International Conference on Distributed Computing Systems Workshops, Macau, June, 2012.

[6] S. G. Vadlamudi, S. Sengupta, and S. Kambhampati, ―Moving target defense for web applications using bayesian stackelberg games,‖ International Conference on Autonomous Agents & Multiagent Systems, Singapore, May, 2016.

[7] M. Taguinod, A. Doupé, Z. Zhao, and G.-J. Ahn, ―Toward a moving target defense for web applications,‖ in Information Reuse and Integration (IRI), IEEE International Conference, San Francisco, Aug, 2015.

[8] L. Z. Gu, Z. H. Zheng, Y. X. Yang, Modern Cryptography. China: Publishing House of Beijing University of Posts and Telecommunications, 2015.

[9] W. Stallings. Cryptography and Network Security Principles and Practice. 5th ed, NJ, USA: Prentice Hall Press Upper Saddle River, 2010.

[10] A. Hevia, M. Kiwi, ―Strength of two data encryption standard implementations under timing attacks,‖ ACM Transaction Information and System Security, vol. 2, pp. 416-437, Nov. 1999.

[11] X. Wang, R. Zeng, ―The analysis and improvement of DES algorithm,‖ Journal of Shiyan Technical Institute, vol. 19, No.5, pp.84-86, Oct. 2006.

[12] B. Jiang, ―Analysis of DES Algorithm Implementation and Improvement Process,‖ Journal of Langfang Teachers College, vol. 10, No.5, pp.46-47, Oct. 2010.

[13] J. X. Gao, ―Implementation and improvement of DES algorithm,‖ Network Security Technology & Application, vol. 1, pp.61-62, 2014.