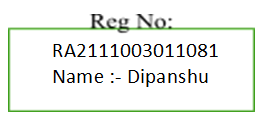
**JOURNAL ARTICLE EVALUATION OUTLINE**

****

# 

# TITLE: A Recurrent Reward Based Learning Technique for Secure Neighbor Selection in Mobile AD-HOC Networks

# AUTHOR(S): K. Sakthidasan Sankaran, N. Vasudevan, K. R. Devabalaji, Thanikanti Sudhakar Babu, Hassan Haes Alhelou, and T. Yuvaraj

# JOURNAL: IEEE Access

# DATE/YEAR: Jan 28 / 2021

# VOLUME: 9

# PAGES: 12 pages

# A. INTRODUCTION

1. Does the title of the research article give any indication of the type of study being reported; i.e., Descriptive, Correlational, or Causal – Comparative

Answer :- The title of the research article suggests that the study is focused on proposing a new technique for secure neighbor selection in mobile ad-hoc networks using recurrent reward-based learning. This indicates that the study is likely experimental or causal-comparative in nature.

2. Were the Independent and Dependent variables mentioned in the title?

Answer:- the research paper titled "Recurrent Reward Based Learning Technique for Secure Neighbor Selection in Mobile AD-HOC Networks" does not explicitly mention the independent and dependent variables in the title. The document primarily focuses on the background and qualifications of the authors, their research interests, and their publication history.

3. In what part of the article did you find what kind of statistical tools were being used?

Information about the statistical tools being used in the study can be found in the "RELATED WORKS" section of the article, where it discusses the proposed technique and compares it with existing methods. The research discusses various approaches such as trust- based multi-objective optimization, communication, energy, and recommendation-based trust evaluation, as well as hybrid weighted trust-based algorithms for tackling security issues like black hole attacks.

# B. Analyzing the Variables

1. What is(are) the independent variables, Be specific!

Packet Dispatching Rate (PDR)

Transmission Quality (QTX)

Node Availability (AN)

TR (transmitting/receiving) and I (idle) states of the nodes

1. What is(are) the nature of the measurements: i.e., Nominal, Ordinal, Ratio, Interval, as well as whether or not they are continuous or discrete.

1)--Packet Dispatching Rate (PDR): This variable is estimated based on packet transmission and reception attributes and is considered a continuous ratio variable.

2)--Transmission Quality (QTX): The quality of transmission is assessed for the path through the neighbor and is viewed as a continuous ratio variable.

3)--Node Availability (AN): The availability of nodes for communication is determined and can be classified as a continuous ratio variable.

4)--TR (transmitting/receiving) and I (idle) states of the nodes:- The measurements are related to the network functions and neighbor attributes, which are analyzed using a recurrent learning method.

2. What is(are) the Dependent variables, Be specific!

The dependent variables in the proposed technique for secure neighbor selection in mobile ad-hoc networks are the detection ratio of malicious nodes.

1. What is(are) the nature of the measurements: i.e., Nominal, Ordinal, Ratio, Interval, as well as whether or not they are continuous or discrete.

Detection ratio of malicious nodes is taken with respect to hop-count and malicious nodes ratio.

These measurements are continuous in nature.

# C. Hypothesis

1. Were the hypotheses clear and understandable?

Answer:- The provided excerpts do not explicitly state the hypotheses in traditional scientific terms (such as explicitly stating a null hypothesis and an alternative hypothesis). However, they clearly outline the goals and the expectations from the proposed technique, which suggests an implicit hypothesis that applying recurrent reward-based learning for secure neighbor selection in mobile ad-hoc networks (MANETs) would improve throughput, packet delivery ratio, detection ratio, and reduce delay when compared to existing methods

2. What was the hypotheses? What was the Null hypothesis? Was it appropriate for the study?

Answer:-

--The implicit hypothesis can be inferred as: The application of recurrent reward-based learning for secure neighbor selection in MANETS significantly improves network performance metrics (throughput, packet delivery ratio, detection ratio) and reduces delay, indicating an effective method for mitigating adversaries and anomalies.

--A potential Null hypothesis (not explicitly stated) might be: The application of recurrent reward-based learning for secure neighbor selection in MANETs does not significantly improve network performance metrics or reduce delay compared to existing methods.

--Given the focus on improving MANET security and performance through a novel technique, this hypothesis is appropriate for the study as it aims to test the effectiveness of the proposed method against existing challenges in the field.

3. Did the introduction adequately set up the hypothesis?

Answer:- Yes, the introduction and subsequent sections of the document establish a clear foundation for the study's aims by highlighting the significance of secure neighbor selection in MANETS, the challenges posed by adversaries and anomalies, and the potential of recurrent reward-based learning as a solution. While not stating the hypotheses in a traditional format, the document effectively sets up the expectation that the proposed technique could offer substantial improvements in network performance and security, thereby indirectly setting up the hypotheses for the study.

4.If the authors did not provide hypothesis, try to “Creatively” generate what you think they should have been.

Answer:-While not stating the hypotheses in a traditional format, the document effectively sets up the expectation that the proposed technique could offer substantial improvements in network performance and security, thereby indirectly setting up the hypotheses for the study.

Attempt to state the null hypothesis for each alternative hypothesis

Answer:- The application of recurrent reward-based learning for secure neighbor selection in MANETs does not significantly improve network performance and security.

Did the authors specify a specific Alpha Risk level for rejecting the Null hypothesis? If so, what was it? If they did not specify the Alpha Risk level, what do you think it must have been?

Answer:- The author does not specify an Alpha Risk level for rejecting the Null hypothesis. Generally, in scientific studies, an Alpha Risk level (significance level) of 0.05 is commonly used. This level represents a 5% risk of concluding that a difference exists when there is no actual difference. Without specific mention in the provided context, it would be reasonable to assume that the authors might have adhered to this conventional standard if they were conducting statistical tests to evaluate their hypotheses.

# D. Sample

1. Do you believe that the sample was large enough?

Answer:- The author does not explicitly mention the sample size (N) or the standard deviation required for computing the standard error of the mean. Without these specific values, it's not possible to directly compute the standard error or discuss the appropriateness of the sample size for the study.

1. Given the sample size could you compute the standard error of the mean to accomplish this you would need the values for both N and the standard deviation. Did they provide you with this data. What do you believe the “Critical region” for rejection of the null hypothesis should have been.

Answer:- Regarding the critical region for rejection of the null hypothesis, the document does not provide information on the significance level (alpha) chosen for the hypothesis tests, which is essential to determining the critical region. Typically, a common choice is alpha = 0.05, but without explicit information, one cannot assert what the "Critical region" should have been for this particular study.

The document content focuses on the effectiveness of a recurrent reward-based learning technique for secure neighbor selection in mobile ad-hoc networks, specifically discussing improvements in packet delivery ratio, detection ratio, and delay reductions. It details the methodology for evaluating node reliability and selection but lacks detailed statistical analysis data such as sample size, standard deviation, or specifics on hypothesis testing parameters.

# E. Results and Conclusions

# 1. Are appropriate statistical tools used?

The author details the learning process, detection ratio comparisons, and the use of probability factors for determining the legitimacy of nodes in the routing process. This implies a methodological approach that involves statistical analysis to classify nodes and evaluate the system's performance.

The recurrent learning process and the conditions for node selection outlined in the document further suggest a structured analytical approach to optimize neighbor selection, which is critical for enhancing security and performance in MANETS.

Therefore, based on the information provided, it is reasonable to conclude that appropriate statistical tools were likely utilized in the experimental analysis to support the claims of the proposed technique's effectiveness, although the specific statistical tools and tests employed are not detailed in the provided excerpts.

A.Ex. Was the “Homogeneity of variance” assumption tested (An F-max Test) could you do one?

Answer:- It does not explicitly list specific statistical tests or methods like the "Homogeneity of variance" or an F-max Test, the nature of the experimental analysis and the quantitative metrics used imply a comprehensive statistical evaluation was part of the research methodology. The focus on detection ratio comparisons, for instance, hints at comparative statistical analysis, possibly involving techniques such as Analysis of Variance (ANOVA) or regression analysis to examine the relationships between variables like hop count, malicious nodes ratio, and the performance metrics mentioned

B. Ex. The nature of measurement for the independent and dependent variables and how many of them might indicate the type of statistical tool that should have been used?

Answer:-The nature of measurement for the independent and dependent variables (such as hop count, malicious nodes ratio, packet delivery ratio, and average delay) and their relationship with the detection of malicious nodes and network performance metrics indicate a complex analytical approach.

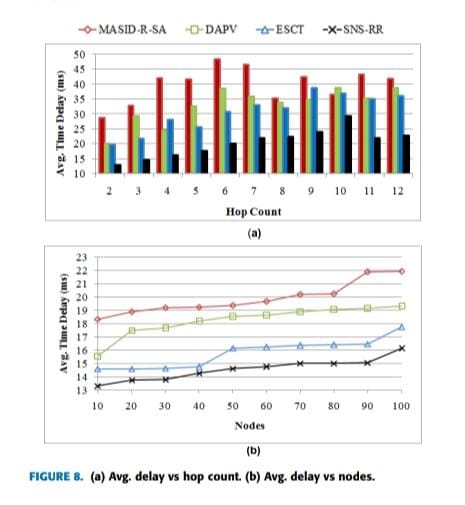
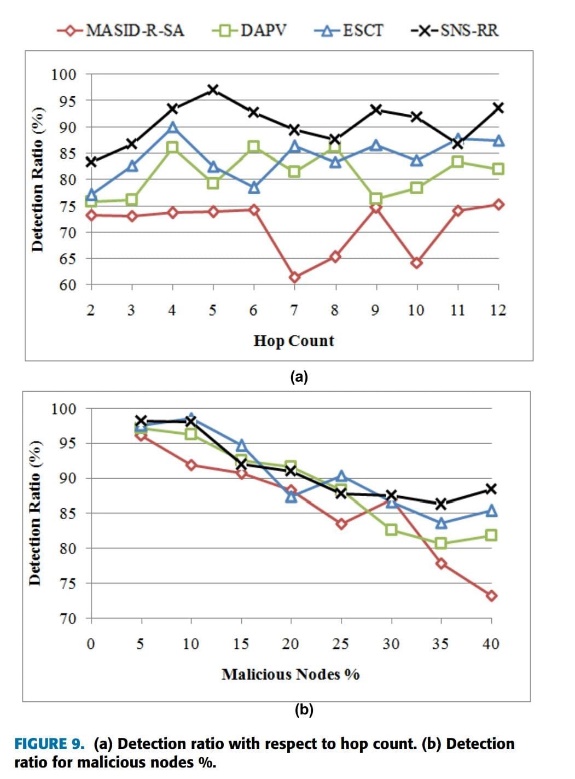
The methodology seems to involve analyzing network behavior under various conditions to optimize the detection and mitigation of adversaries and anomalies. In general, when assessing network performance and security, statistical tools suitable for such analysis might include regression analysis, analysis of variance (ANOVA), and machine learning algorithms for pattern recognition and anomaly detection.

2. Were Graphic charts used?

If so, Were they helpful in showing the results

If graphic charts were not used, try to construct them from the reported data: i.e. Sketch out a Bar graph, Histogram or Frequently Polygon

Answer:-Yes, graphic charts were used in the document to present the results of the research. Specifically, Figures 8(a) and 8(b) showed average delay versus hop count and nodes, respectively, while Figures 9(a) and (b) depicted the detection ratio of malicious nodes in relation to hop-count and malicious nodes ratio. These graphical representations were likely helpful in visually demonstrating the outcomes of the experimental analysis, allowing for easier interpretation of the data regarding how the proposed technique impacts network performance and security.

Given the context and the specific mention of figures in the document, it's evident that these graphical tools were integral to showcasing the effectiveness of the recurrent reward-based learning technique for secure neighbor selection in MANETS, particularly in terms of improving

key metrics like packet delivery ratio, detection ratio, and reducing delay.

3. Does the investigator relate the results to the hypothesis?

Answer:-The investigator seems to relate the results to the hypothesis by designing a secure neighbor selection technique that utilizes recurrent reward for optimal path node discovery to enhance end-to-end communication reliability. Additionally, the researcher aims to enhance security in Mobile Ad-Hoc Networks (MANETs) communication by categorizing nodes based on their states and behavior, with reward estimation through a recurrent machine learning algorithm to determine neighbor reliability.

4. Does the investigator over-conclude, that is, are the conclusions supported by the data?

Answer:- Regarding over-conclusion, the document mentions the performance of a comparative analysis of the proposed method with existing techniques to demonstrate its consistency. By conducting this analysis, the investigator aims to ensure that the conclusions drawn are supported by the data and are not overstated. This approach helps in substantiating the validity of the findings and avoiding unwarranted claims based on the research outcomes.