

The paper presents an adaptive routing protocol for underwater sensor networks. To prevent malicious attacks, the paper uses GAN to identify malicious nodes, and hence provides more resilient routing under hostile environments. The authors simulated the performance of their schemes and compare with two other approaches and the results show that their schemes can provide better identification of malicious nodes under various conditions. The paper is presented very well and readily read. The following is some revision comments:

1. Suggested change and revision in writing:

- ~~and~~-disaster warning, and 31
- ~~changes~~ in the net- 39
- ~~P~~roposed a method for data collection, transmission and storage of the marine Internet of 181
- In order to fur- 200 //should start a new paragraph
- There is not comment in the related work to contrast the proposed work with them. It is suggested to do so, especially with GAN based trust evaluation model.
- Some strange symbols need to be corrected.

$$RE_j = \begin{cases} 0 & Energy_j \leq Energy_{rated} \\ \frac{Energy_j - Energy_{rated}}{Energy_{rated}} & Energy_{rated} < Energy_j \leq 2Energy_{rated}, \\ 1 & Energy_j > 2Energy_{rated} \end{cases} \quad (7)$$

- 6.3. Performance Analysis of Data Forwarding 911

should use a table to summarize these scenarios.

2. The authors explained in the paper that since the environment changes and hence the trust model may become less accurate and need to be updated at some threshold. However, in the paper I cannot see what are the value of the threshold and how the threshold is defined and included in the whole process of dynamic tuning of the system. Besides, the simulation does not mention about this and hence the results become less convincing.