# Cover Letter with Summary of Differences

Dear editor,

This manuscript builds on top of our prior work published as a regular 6-pages paper in the 26th IEEE Symposium on Computers and Communications (ISCC' 2021), titled "FLPhish: Reputation-based Phishing Byzantine Defense in Ensemble Federated Learning". The manuscript in hand has been significantly revised, in which we provide an extended system design, with more theoretical and evaluation results. Below, we highlight the major changes/extensions we made in the submission over the prior conference paper.

* In this manuscript, we summarize the previous works about robust federated learning in Section II, which is not part of our ISCC' 2021 paper (See more details in Section II).
* In this manuscript, we provided the algorithm details of the phishing mechanism (See more details in Section IV).
* In this manuscript, we provided more mathematical details about the reputation mechanism, especially about the derivation process based on Bayesian Inference (See more details in Section IV).
* In this manuscript, we provided a theoretical security analysis of the proposed FLPhish scheme, which explains how the proposed FLPhish scheme defends against Byzantine attacks (See more details in Section IV).
* Going beyond the aggregation algorithm in our ISCC' 2021 paper, we proposed a better aggregation algorithm, FLPhish-weight, which not only has better performance but also is more reliable than the aggregation algorithm, FLPhish-threshold (which we just named FLPhish, but did not give a specific name) in our ISCC' 2021 paper. This brand-new aggregation algorithm provides a solid study on Byzantine attack defense in federated learning from validation to explanation (See more details in Section IV and V).
* In this manuscript, we evaluate our framework against one more type of attack, named "random attack." The experiment results show our framework's robustness against this type of attack (In our ISCC'2021 paper, we only evaluated our framework against untargeted attacks. See more details in Section V).
* In this manuscript, two more datasets, Fashion-MNIST and CIFAR-10, are used in our evaluation. The experiment performance on these two datasets further proves our framework's reliability (In our ISCC' 2021 paper, only the MNIST dataset was used. See more details in Section V).
* In this manuscript, we evaluate our framework against more state-of-the-art frameworks. We compare our FLPhish with FedAvg, Trimmed Mean, and Median (In our ISCC' 2021 paper, we did not compare our FLPhish with any frameworks). And the performance comparison proves our FLPhish's performance over FedAvg, Trimmed Mean, and Median (See more details in Section V).

Sincerely,

Beibei Li, Peiran Wang, Qinglei Kong, Yuan Zhang, Rongxing Lu

Dec. 18th, 2021