# CONCLUSION

In this paper, we propose a CTI modeling and threat type identification system based on HIN, called Hin CTI. We design meta-schema and a set of meta-paths and meta-graphs to model CTI on HIN, which can extract and incorporate higher-level semantics of cyber-threat infrastructure nodes involved in CTI. Through the proposed MIIS measure-based heterogeneous GCN-based threat type identification approach, we overcome the challenge of limited labels of cyber-threat infrastructure nodes. Through the hierarchical regularization, our identification approach can also alleviate the problem of over fitting. Experiments based on real-world dataset demonstrate that our developed system Hin CTI that integrates our proposed approach can significantly improve the performance of threat type identification compared with the existing state-of-the-art baseline methods.

For future work, we plan to explore other information to enrich the node features and relations of the cyber threat intelligence HIN for further improving the performance of our approach. Another interesting direction for future work is the extraction of fine-grained structured data (including node and their relationships) from intelligence reports recorded in natural language, leveraging topic modeling and natural language processing techniques. Doing so will greatly enrich the heterogeneous information network and enhance the performance of threat identification.