A Terminal Trust Assessment Method Based on Consensus Trust Aggregation

Shixin Cheng*, Jinzhe Zhang*, Liping Han*

**State Grid Qinghai Information & Telecommunication Company, Xining, China*

1713147519@qq.com, rubymelloroad@gmail.com, 2690618708@qq.com

***Abstract*—Due to the numerous terminal devices in a power network environment, it is difficult to defend against the attack of malicious nodes, like deception and data tampering in common trust models. A terminal trust assessment method based on consensus trust aggregation is proposed in this paper. Aimed at the direct trust of a goal node, standard quantitative trust value is predicted based on records of historical access nodes after filtering great trust factors. Trustworthy consensus nodes are selected to participate in the feedback trust consensus module. The consensus trust verification module is designed to ensure the security of the consensus, including consensus verification and malicious node replacement. The simulation results demonstrate the proposed method can reflect the trust level of terminal nodes more effectively, which has a better constraint on suspicious nodes.**

***Keyword*—trust assessment; consensus; power mobile network; terminal node**

Shixin Cheng born in 1995, received the Bachelor degree in Electronic Engineering from Tsinghua University in 2020. His research interests include Cyberspace Security and Data Security.

Jinzhe Zhang born in 1997, received the Bachelor degree in Software Engineering from Chongqing University in 2020. His research interests include Terminal Security and Network Penetration.

Liping Han born in 1997, received the Bachelor degree in Computer Science and Technology from Qinghai University in 2020. Her research interests include Network Security Defense Based on Honeypot Technology.