Proceedings of Machine Learning Research vol 245:1–8, 2024 2024 International Conference on Machine Learning and Intelligent Computing

A Trust Evaluation Method with Collaborative Active Detection for D2D-enabled Networks

Gang Yang* YANG199599GG@GMAIL.COM
School of Computer and Cyberspace Security, Xiangtan University, Xiangtan, China

Pan Liu
School of Computer and Cyberspace Security, Xiangtan University, Xiangtan, China

Yan Liu
School of Computer and Cyberspace Security, Xiangtan University, Xiangtan, China

Editors: Nianyin Zeng and Ram Bilas Pachori

Abstract

Device-to-Device (D2D) communication emerges as a pivotal technology for enhancing the capacity and coverage of networks. Nonetheless, these networks are vulnerable to threats posed by malicious devices (MDs) that have the potential to tamper with transmitted content, thereby compromising the network's reliability. The trust model is one of the effective methods to solve such internal attacks. Previous research mainly evaluated device trust based on social similarity and passive trust models. These methods make it difficult to obtain accurate evaluation results. Even though there are some active trust models, they have limitations such as high cost and limited scope of application. To solve the above problems, we propose a low-cost collaborative active detection trust evaluation method. In this method, the device first generates some smaller detection packets, verification codes and sends them directly to the trusted alliance party. Then, during each trust evaluation process, the device determines the trust of nodes on the multi-hop path by actively sending these detection packets to the trusted alliance party. Experimental results show that, compared with existing strategies, our proposed strategy can achieve higher trust evaluation accuracy with lower energy consumption.

Keywords: D2D, Collaborative Active Detection, Trust Evaluation

1. Introduction

As the computing, caching, and communication capabilities of mobile devices continue to increase, the feasibility of device-to-device (D2D) communication technology has also significantly improved (Li et al., 2021). D2D communication refers to a process where various devices can directly exchange information with each other without the need for data to be relayed through Base Station (BS) or other similar central facilities. This mode of communication can offer shorter latencies and higher data transfer rates, significantly enhancing the overall performance of the network (Mayer et al., 1995). Especially in recent years, video resources have become the main-stream of network traffic. D2D technology assists base stations in video content distribution, which can significantly reduce the load on base stations.

However, in a D2D-enabled network, since devices act as service providers, there could be the presence of malicious devices (MD) which might transmit false information or attempt to launch offline attacks to disrupt the stable operation of the network. The trustworthiness of D2D devices within the network plays a decisive role in enhancing user enthusiasm for utilizing D2D technology; hence, there is a necessity to accurately assess device trustworthiness. Additionally, the MDs

in the network may also initiate trust attacks such as ballot-stuffing, bad-mouthing, etc., further complicating the challenge of trust assessment.

Early studies broke down social trust into three main dimensions: competence, benevolence, and integrity (Liu et al., 2004). Most of the literature on trust management in wireless networks focuses on whether nodes can perform specific tasks reliably (Li et al., 2010; Chen et al., 2018; Li et al., 2024). The current mainstream trust method is mainly a passive trust acquisition method (Chen et al., 2016). Their sources of trust evidence may be based on direct observations of device behavior. However, when there is little interaction data, and it is difficult to meet the timeliness requirements of the system for trust values. In response to the problems existing in the passive trust acquisition method, Li et al. (2024) proposed an active detection method (TEAD), which effectively makes up for the shortcomings of the passive method and can accurately assess the trust of devices in the network. However, this method requires high additional costs in the early stage of establishing a trust relationship.

In response to the above problems, this paper proposes a collaborative active detection method. Accurately evaluate the trust of the device at a lower cost through active detection and multi-hop collaborative verification, thereby increasing users' enthusiasm for sharing content through D2D communication. The contributions of this paper are as follows:

1. This paper proposes a D2D communication trust model with collaborative active detection. Different from existing research, it is a distributed model for unstable malicious behaviors.

2. Different from previous active detection, our strategy performs collaborative active detection by generating some smaller detection packets.

3. Experimental results show that our strategy outperforms other existing strategies in different network environments. Even when the proportion of malicious users is 60%, the trust knowledge correctness is still about 1. In addition, in terms of energy consumption, our strategy only consumes a small amount of additional energy.

2. System model and problem statement

2.1. System model

The system model considered in this article is a D2D network, as shown in Figure 1. The network contains some base stations and several mobile devices equipped with D2D communication distributed in the BS range.

We assume that there are N mobile devices in the network, represented by $U = \{u_1, u_2, \cdots, u_N\}$, among which the proportion of malicious device (MD) is p and the proportion of normal device (ND) is 1-p. In addition, the total number of videos transmitted between network users is K, represented by $M = \{v_1, v_2, \cdots, v_k\}$. The check code of each video file is represented by $TVC = \{tvc_1, tvc_2, \cdots tvc_k\}$. The check code can be used to verify whether the transmission is successful. Each device stores some videos locally for sharing.

2.2. Problem statement

As mentioned above, due to the existence of MD in the D2D network, MD may provide false information when serving as content providers. At the same time, MD can also send correct information

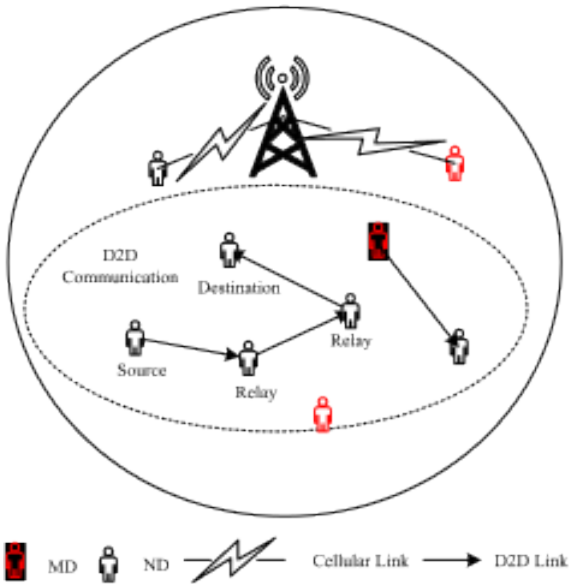

Figure 1: D2D-enabled networks.

to other devices to improve their trust. Therefore, there may be MD with high trust in the network, and every device in the network may be attacked by MD. In order to solve the above problems, we establish a new trust model of D2D network to evaluate the trust of devices, using U^N and U^M to represent the ND set and MD set respectively, and evaluate our trust model through the following factors.

2.2.1. TRUST KNOWLEDGE CORRECTNESS (TKC)

TKC refers to the accuracy of each normal device's trust evaluation. Let $F_{i,j} = 1$ means that u_i's trust perception of u_j is correct, and $F_{i,j} = 0$ means u_i's trust perception of u_j is wrong. Assuming that the set of devices that has the trust relationship with $u_i \in U^N$ is u_i. Then, the trust knowledge correctness TKC can be obtained by the following formula:

$$TKC = \frac{\sum_{u_i \in U^N} \sum_{u_j \in \mu_i} F_{ij}}{\sum_{u_i \in U^N} |\mu_j|} \tag{1}$$

2.2.2. ENERGY COST (EC)

Let P_X^t and T^t denote the transmit power of the transmitting device in the t^{th} interaction and the duration of the interaction, respectively (Chen et al., 2016). Then, the energy cost of the system over a period of time can be calculated by

$$EC = \frac{\sum_{t=1}^{N} P_X^t T^t}{|U|} \tag{2}$$

where N represents the total number of a interaction in the system during the period, and $|U|$ is the number of devices in the network.

3. Solutions

3.1. Collaborative active detection

In order to accomplish trust evaluation of devices in a fast, accurate, and low-energy manner, this paper proposes a collaborative active detection method. Referring to Figure 2 to explain the basic principles of the collaborative active detection method. As illustrated in Figure 2, this paper categorizes devices into two types based on their neighboring devices: the first type includes trusted devices with a comprehensive trust value greater than 0.5 (represented by u_j in Figure 2), and the second type consists of untrusted devices with a comprehensive trust value less than 0.5 (represented by u_k in Figure 2). Additionally, the vicinity of the device is divided into four areas: Area 1, 2, 3, and 4. Within each area, devices select the most credible among the trusted devices as their collaborative active detection device, ensuring all nodes within the device's vicinity are covered during the detection process.

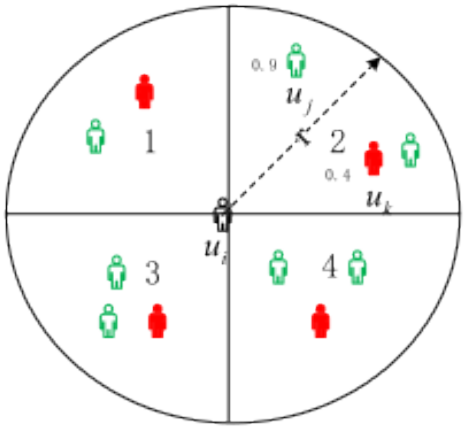

Figure 2: The division map of device neighbor area.

As the approach is similar across all areas, we will only consider one area as an example. Referencing Figure 2 and Figure 3, this example explains the process involving detection packets and checksums between a device and its collaborative active detection device. Assume u_j is the most trusted device within u_i's trusted devices, with the highest comprehensive trust value. u_i generates a low-data detection packet and checksum, then sends them to u_j. Upon receiving them, u_j sends an acknowledgment message (ACK) back to u_i, forming a collaborative active detection pair. When u_i needs to conduct collaborative active detection in the area, as shown in Figure 3 (b), it uses the mentioned detection packet to request a relay from devices, with u_k forwarding the message to u_j. u_j then checks the checksum of the received packet; if it matches, u_j sends a detection success message to u_i, otherwise, it sends a detection failure message. u_i determines the reliability of u_k based on the received message—if the detection is successful, u_i adds a successful interaction evidence to both u_j and u_k. If not, u_i only records one failed interaction evidence with u_k.

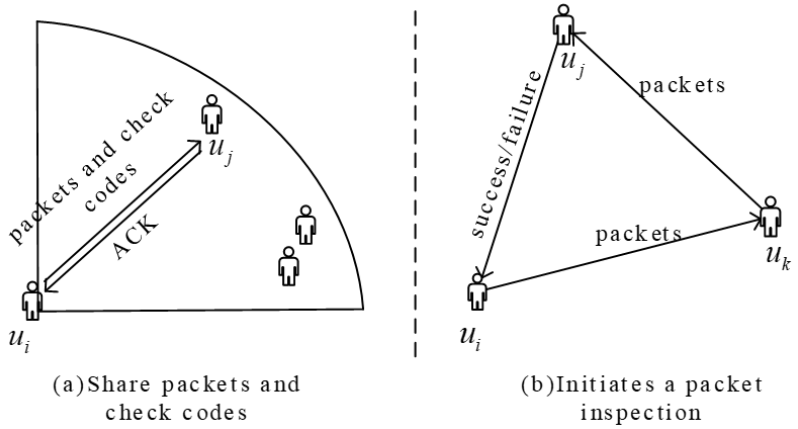

Figure 3: Collaborative Active Detection.

3.2. Trust model

Comprehensive trust: The comprehensive trust of the device to the device is obtained by the weighted sum of direct trust and recommended trust. The specific formula is as follows:

$$T^t_{C(i,\,j)} = \lambda T^t_{\mathrm{D}(i,\,j)} + (1-\lambda) T^t_{R(i,\,j)} \tag{3}$$

where λ is the weight parameter, $\lambda \in [0, 1]$.The calculation process of direct trust and recommended trust is introduced in detail below.

Direct trust: The direct trust of the device at the t^{th} moment can be calculated by the following formula:

$$T^t_{D(i,\,j)} = \begin{cases} 0.4 * T^{t-1}_{C(i,\,j)} + \ 0.6 * \frac{s_{i,j}}{s_{i,j}+f_{i,j}} & , if\ t > 1 \\ \frac{s_{i,j}}{s_{i,j}+f_{i,j}} & ,\ if\ t = 1 \end{cases} \tag{4}$$

Among them, which $T^{t-1}_{C(i,\,j)}$ is the comprehensive trust of u_i to u_j at the $(t-1)^{th}$ moment, where $s_{i,j}$ represents the success factor and $s_{i,j}$ represents the failure factor. $f_{i,j}$ is equal to the number of successful interactions at the t^{th} moment, and the initial value of $f_{i,j}$ is 0, and each time the interaction fails $f_{i,j} = f_{i,j} + w_{i,j}$. $w_{i,j}$ is the penalty factor, which is adjusted based on the number of failed interactions between devices, $w_{i,j} = \log_2(2 + 2f_{i,j})$.

Recommend trust: In the process of trust evaluation, u_i requests the presenter for recommendation trust about u_j. After u_i collects recommendation information from different presenters, u_i calculates the recommendation trust for u_j through the following formula:

$$T^t_{R(i,\,j)} = \frac{\sum_{k=1}^{N_i} W_k * T^t_{D(k,\,j)}}{\sum_{k=1}^{N_i} T^t_{C(i,\,k)}} \tag{5}$$

Where N_i is the set of devices with direct interaction at the t^{th} moment, w_k and is the confidence weight value.

4. Experimental design and implementation

In order to verify the effectiveness of the method we proposed. In this section, we mainly introduce the environment settings of this article, and evaluate our algorithm from the following indicators.

4.1. The Environment Settings

The core parameter settings of the experiment are shown in Table 1.

Table 1: Core parameters.

Parameters	Value
The proportion of MDs p	0.1-0.6
λ	0.6
$\mathrm{Th_T}$	0.5
The malicious degree of MDs e	0.4-0.9
r, R	25m, 200m

Extensive study on trust models in D2D-enable networks can typically categorize these models into two main groups: active trust evaluation and passive trust evaluation. Active trust evaluation was notably demonstrated by Li et al. (2024) through a classic and exemplar trust management model embedded with active detection, conveniently referred to as TEAD. On the other hand, passive trust evaluation is represented by Chen et al. (2016) who proposed a pioneering trust management model predicated on social relationships, dubbed SOA-Based for simplicity. To demonstrate the efficiency of our strategy, we compare it against both TEAD and SOA-Based.

4.2. Trust Knowledge Correctness (TKC)

As depicted in Figure 4 (a), we present the variance in trust accuracy under differing ratios of MDs p and e=0.5. The results clearly indicate that as the proportion of MDs increases, our strategy and TKC value of TEAD remain significantly stable, close to 1. Conversely, the TKC value achieved by the SOA-Based model significantly drops, demonstrating its vulnerability. This decrease is especially pronounced when the proportion of MDs p reaches 0.6, at which point the TKC value falls to approximately 0.5.

As illustrated in Figure 4 (b), we further delineate the shifts in trust accuracy under varying malicious degrees of MDs (e) and p=0.4. The results indicate conditions where the MD's malicious degrees are high, different strategies demonstrate high TKC values. Especially when e = 0.9, their TKC values are close to 1. In contrast, when the MD's level of malice is lower, the TKC values of different strategies show certain variations. For instance, at e = 0.4, both our strategy and the TEAD strategy have a TKC value of 0.98, while the SOA-Based strategy has only 0.75.

4.3. Energy Cost (EC)

As shown in Figure 5, we show the changes in energy consumption of each strategy when the proportion of MDs p=0.4 and e=0.5. It can be seen from the results that the energy consumption of our strategy tends to be stable, and our energy consumption is relatively small compared with TEAD. Compared with the SOA-Based strategy, our strategy uses less additional energy consumption to

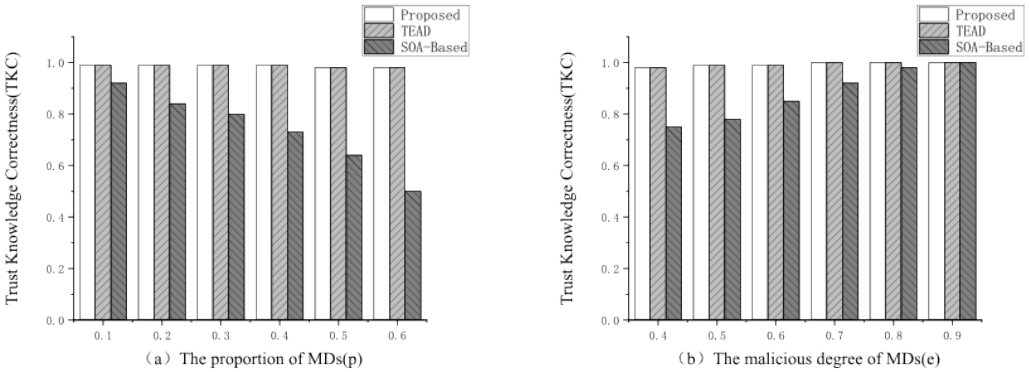

Figure 4: TKC values for different methods across various scenarios after 100 intervals.

obtain higher trust evaluation performance. All in all, the overall performance of our strategy is better than other strategies.

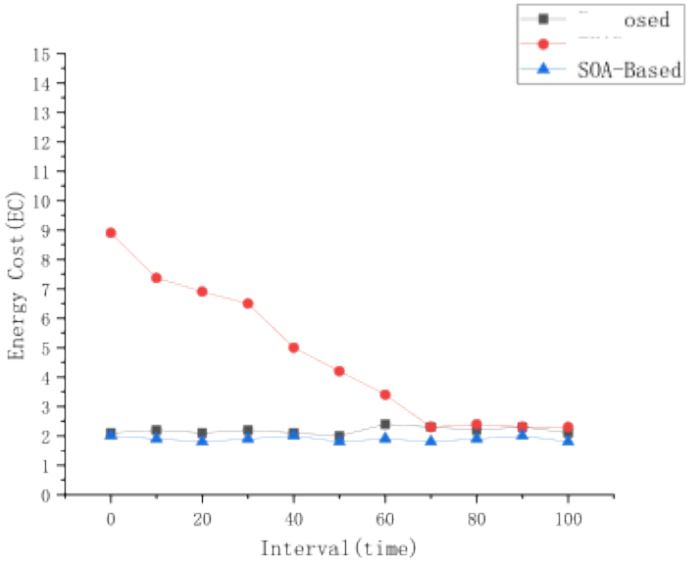

Figure 5: The mean energy cost of different methods with p=0.4, e=0.5.

5. Conclusion

In this paper, we introduce a trust evaluation method with collaborative active detection for D2D-enabled networks. In line with this, we took into account several variants of malicious attacks, including opportunistic service attacks, ballot-stuffing and bad-mouthing attacks. The resultant simulations auspiciously illustrate a marked advantage of our model over current ones. When dissecting the comparative results, it was observed that even with 60% of the nodes being malicious in nature, our model's TKC stays at 1. In terms of energy consumption, our method can maintain a

high level of TKC with low energy expenditure. In future work, we hope to implement the proposed model within realistic liquidity frameworks and benchmark the comparative outcomes.

References

Gaojie Chen, Jinchuan Tang, and Justin P. Coon. Optimal routing for multihop social-based d2d communications in the internet of things. *IEEE Internet of Things Journal*, 5(3):1880–1889, 2018. doi: 10.1109/JIOT.2018.2817024.

Ing-Ray Chen, Jia Guo, and Fenye Bao. Trust management for soa-based iot and its application to service composition. *IEEE Transactions on Services Computing*, 9(3):482–495, 2016. doi: 10.1109/TSC.2014.2365797.

Ting Li, Anfeng Liu, Neal N. Xiong, Shaobo Zhang, and Tian Wang. A trustworthiness-based vehicular recruitment scheme for information collections in distributed networked systems. *Information Sciences*, 545:65–81, 2021. ISSN 0020-0255. doi: https://doi.org/10.1016/j.ins.2020.07.052.

X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang. Trust-based on-demand multipath routing in mobile ad hoc networks. *IET Information Security*, 4:212–232(20), December 2010. ISSN 1751-8709.

Zhetao Li, Jianhui Wang, Saiqin Long, Jianming Fu, Min Yang, and Jian Weng. A trust evaluation joint active detection method in video sharing d2d networks. *IEEE Transactions on Mobile Computing*, 23(7):7739–7752, 2024. doi: 10.1109/TMC.2023.3339652.

Zhaoyu Liu, A.W. Joy, and R.A. Thompson. A dynamic trust model for mobile ad hoc networks. In *Proceedings. 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2004. FTDCS 2004.*, pages 80–85, 2004. doi: 10.1109/FTDCS.2004.1316597.

Roger C. Mayer, James H. Davis, and F. David Schoorman. An integrative model of organizational trust. *The Academy of Management Review*, 20(3):709–734, 1995. ISSN 03637425.