이동통신망에서 클러스터 기반 서비스를 위한 기기간 통신의 취약점에 관한 연구

Venissa Adzo Sedem Manya, 김태훈*, 김종현**, 방인규
한밭대학교 지능미디어공학과, *한밭대학교 컴퓨터공학과, **한국전자통신연구원

30215295@edu.hanbat.ac.kr, *thkim@hanbat.ac.kr, **jhkim@etri.re.kr, ikbang@hanbat.ac.kr

A Study on Vulnerability of D2D Communication for Cluster-based Service in Cellular Networks

Venissa Adzo Sedem Manya, Taehoon Kim, **Jong-Hyun Kim, Inkyu Bang
Hanbat National University, **Electronics and Telecommunications Research Institute

Abstract

In this paper, we investigate the vulnerability of D2D communications, focusing on cluster-based multicasting scenarios in cellular networks. We introduce a threat model for cellular D2D communication and show the impact of potential vulnerability on the performance degradation such as energy consumption and data rate through simulations.

I. Introduction

Device-to-device (D2D) communication refers to a technology that empowers devices (User Equipment (UE), smart meters, and sensors, among others) to send and receive data directly without going through the core wireless network infrastructure via base stations (or access points) [1]. One of the applications of D2D communication is multicasting/content-sharing where a user is responsible for the delivery of other users' contents received from a base station, to efficiently utilize cellular radio resources.

Forming clusters for content delivery is a way of setting up the D2D multicasting scenario. In addition, cluster-based D2D communications can improve network performance in terms of throughput, spectral efficiency, and energy consumption. Accordingly, several studies have been on clustering algorithms [2]-[4]. Although clustering is very beneficial in D2D communication, there are possible security threats associated with its implementation and it is important to investigate them from both theoretical and practical aspects [5]. One of these security threats is the focus of this paper.

In this paper, we investigate the vulnerability of D2D communication for cluster-based service in cellular networks. We analyze a threat model that considers forged channel state information (CSI) attacks on cluster-based D2D communications. The forged CSI attack consists of two phases. In the first phase, a malicious cluster member intentionally reports forged CSI to the base station to avoid being selected as a cluster head. In the second phase, the malicious cluster member intentionally reports forged CSI again to degrade the network performance in terms of data rate. Through simulations, we evaluate the impact of the forged CSI attack on the performance degradation.

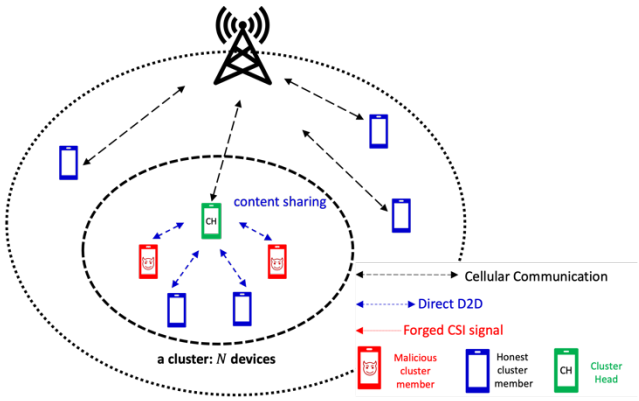

Figure 1. D2D cluster-based communication in cellular networks

II. Threat Model

We consider a single cluster using D2D communication in cellular network. Fig. 1 describes our system model that consists of a cluster of N devices: H honest and M malicious devices. The devices in the cluster leverage D2D communication for content sharing. The cluster head (CH) is responsible for delivering content from the base station to the cluster members after the members have reported their CSIs to the CH. We introduce possible vulnerability when we consider forged CSI reports by malicious devices. We call it as 'Forged CSI Attack', which consists of two phases: cluster head selection and performance degradation.

Phase 1 – Cluster Head Selection

When the base station wants to transmit data to all the devices, it sends it to one of the devices (cluster head), which broadcasts the data to the other devices by leveraging D2D communication. All the devices are required to report their CSIs to the base station for the selection of the cluster head. The device with the best channel quality is chosen as the cluster head.

In forged CSI attack, the malicious devices report forged CSIs to the base station to avoid being selected as cluster heads. The malicious devices should forge CSIs to be lower than their true CSIs in order to make the base station categorize them as cluster members with low channel quality instead of cluster header. We define a forged factor $\beta \in [0,1]$ to control a ratio of forged CSI. Then, the relationship between the true and forged CSI is expressed as:

$$f_n = \beta |g_n|^2. \quad (1)$$

where g_n denotes true CSI of the malicious device.

In addition, the wasted power ratio due to forged CSI attack compared with the normal case can be defined as follows:

$$\alpha = \left(\frac{M}{N-M}\right). \quad (2)$$

Phase 2 – Performance Degradation

After the selection of the CH, the newly chosen CH delivers content to the other members of the cluster. We assume a broadcasting mode of transmission for content sharing. The cluster members report their CSIs to the CH to receive contents. Since we are considering a broadcasting scenario, the achievable rate is set to the device with the worst CSI. Accordingly, the minimum achievable rate to make sure that all the cluster members receive the content is given by

$$R_{min} = \min[\log_2(1 + |g_n|^2 \mathrm{SNR}), \log_2(1 + |f_m|^2 \mathrm{SNR})], \quad (3)$$

$|g_n|^2, |f_m|^2$ are assumed to follow Rayleigh Fading channels. (3) shows that if any malicious device reports a forged CSI which is very low, the whole cluster will suffer performance degradation.

III. Numerical Results

In this section, we provide numerical results to evaluate the performance of a forged CSI attack. In the simulation setup, we consider a cellular network with N set to 15, 20, and 25 respectively.

Fig. 2 demonstrates the wasted power ratio in the cluster due to the presence of malicious devices and their avoidance of the cluster head selection.

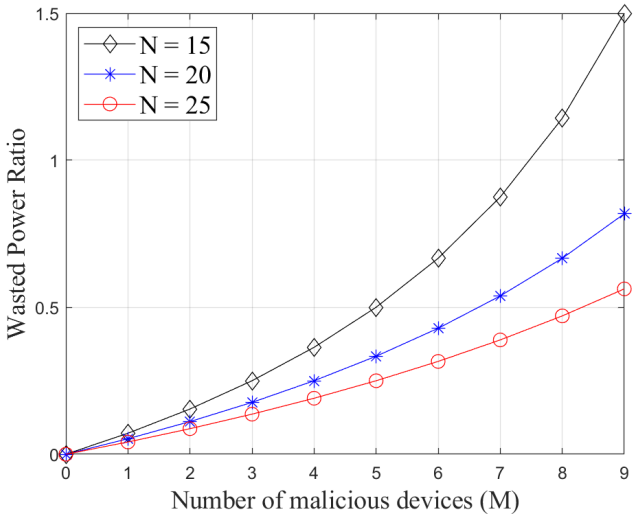

Figure 2. Wasted power ratio during cluster head selection with respect to different N.

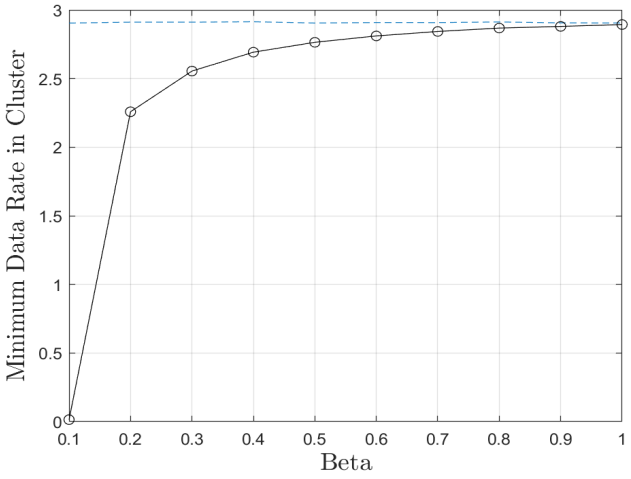

Figure 3. Reduction in cluster performance with respect to forged CSI.

Fig. 3 shows that the minimum data rate of the cluster is reduced due to the transmission of forged CSIs by malicious devices thereby degrading the overall performance of the cluster.

IV. Conclusion

We presented a potential threat of forged CSI attacks in cluster-based D2D communication in cellular networks. We analyze the wasted power ratio associated with the selection of a cluster head and evaluate the impact of the forged CSI attack on the performance degradation in data rate.

Acknowledgment

This work was supported by the Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No.2021-0-00796, Research on Foundational Technologies for 6G Autonomous Security-by-Design to Guarantee Constant Quality of Security).

References

[1] A. Asadi *et al.*, "A survey on device-to-device communication in cellular networks," *IEEE Communication Survey and Tutorials*, Vol. 16, No. 4, pp. 1801-1819, Apr. 2014.

[2] D. J. Son *et al.*, "Resource allocation based on clustering for D2D communications in underlaying cellular networks," *IEEE International Conference on Information and Communication Technology Convergence (ICTC)*, 2014.

[3] Hematian, A. *et al.*, "A clustering-based D2D communication to support diverse applications," *International Conference on Research in Adaptive and Convergent Systems (RACS)*, 2016.

[4] T. Girici and A. C. Kazez, "Clustering-based D2D discovery and content delivery in wireless networks," *ITU Journal on Future and Evolving Technologies*, vol. 2, no. 2, May 2021.

[5] N. Hamoud *et al.*, "Security in device-to-device communications: a survey," *Institution of Engineering and Technology (IET) Journals*, Vol. 7 Iss. 1, pp. 14-22, 2017.