https://doi.org/10.7840/kics.2024.49.6.807

QoS Degradation Attack in D2D Multicasting Networks : Analysis and Countermeasure

Venissa Adzo Sedem Manya[◆], Taehoon Kim[*], Jonghyun Kim[**], Inkyu Bang[°]

ABSTRACT

Device-to-device (D2D) communication in cellular networks enables mobile users in proximity to communicate with each other without the intervention of infrastructures such as base stations (BSs). Accordingly, networks should configure a cluster for cluster-based D2D content sharing. However, potential threats may arise since signaling among D2D devices is not mostly controlled by the centralized entity (e.g., BS). In this paper, we investigate a quality of service (QoS) degradation attack where channel feedback is incorrectly reported by the attacker (i.e., channel state information (CSI) forgery) in order to decrease the cluster sum-rate in a cluster-based D2D communication scenario. We first derive a closed-form of the cluster sum-rate under the QoS degradation attack. We also analyze the effect of a threshold-based defense scheme on the cluster sum-rate and further evaluate the impact of the QoS degradation attack using a system-level simulator in 5G networks (i.e., Simu5G).

Key Words: device-to-device (D2D) communication, channel state information (CSI), CSI forgery, cluster sum-rate, quality of service (QoS)

Ⅰ. Introduction

Over the past decade, there has been extensive use of smart devices in cellular networks, which results not only in a stupendous increase in data traffic but also in the demand for a better quality of service (QoS). In addition to mobile phones, laptops, wearable devices, tablets, and even vehicles can also be wirelessly connected to the internet in recent times. Cellular networks have evolved over the years to satisfy these diverse demands. Accordingly, several advanced technologies such as device-to-device (D2D) communication, cell-free massive multiple-input and multiple-output(MIMO), intelligent reflecting surfaces (IRS), and mobile edge computing have been investigated and developed to improve the performance of cellular networks[1,2].

D2D communication in cellular networks is a technology that enables mobile users in proximity to communicate with each other without infrastructures such as base stations. D2D communication has been highlighted as one of the leading technologies in cellular networks due to its potential to improve performance in terms of latency, throughput, and resource utilization for various applications such as content sharing, data and computation offloading, coverage extension, and the Internet of Things (IoT)[3]. Furthermore, many applications, such as content

※ This work was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korea Government (MSIT), Research on Foundational Technologies for 6G Autonomous Security-by-Design to Guarantee Constant Quality of Security, under Grant 2021-0-00796.

◆ First Author : McMaster University, Department of Electrical and Computer Engineering, manyav@mcmaster.ca(This research is done while studying at Hanbat National University), 학생회원
° Corresponding Author : Hanbat National University, Department of Intelligence Media Engineering, ikbang@hanbat.ac.kr, 정회원
* Hanbat National University, Department of Computer Engineering; thkim@hanbat.ac.kr, 정회원
** Electronics and Telecommunications Research Institute (ETRI); jhk@etri.re.kr, 정회원

논문번호 : 202401-005-B-RU, Received December 30, 2023; Revised February 5, 2024; Accepted February 16, 2024

sharing, require the formation of clusters, and thus several studies have investigated the development of cluster-based D2D communications.

In cluster-based D2D communication, nearby users are grouped into a cluster with a designated cluster head (CH) to facilitate the dissemination of information. D2D clustering has been proven to improve network performance in terms of throughput, energy consumption, and spectral efficiency. Accordingly, various clustering algorithms have been presented in D2D cellular networks[4,5]. Channel state information(CSI) feedback is essential in cluster-based D2D communication since it can directly or indirectly affect the achievable rate between devices (or users) in the cluster. Thus, the availability of the CSI of individual users in the cluster is beneficial for every user to receive and correctly decode the information transmitted. However, CSI feedback itself can be exploited by a malicious user, and thus it has been considered one of the potential threats in wireless networks.

Tung *et al.* analyzed the vulnerability of CSI forgery in multiuser MIMO systems[6], which can be exploited to eavesdrop on other transmissions. Wang *et al.* investigated a sniffing attack in multiuser MIMO networks using manipulated CSI and proposed a countermeasure based on differences in angular spectra[7]. Hou *et al.* presented possible attacks in multi-user MIMO networks that adopted CSI-based user selection algorithms[8]. A number of studies investigated the impacts of CSI forgery in wireless communication systems but most of them considered infrastructure-based networks rather than D2D communication environments[6-8].

Only a few studies considered CSI forgery problems in D2D communications[9,10]. They mainly focused on analyzing the impact of cluster failure attacks, not QoS degradation attacks, and considered only link-level simulations. Bang *et al.* investigated CSI forgery problems in D2D clustering scenarios[10]. They newly presented threat models such as clustering failure attack and QoS degradation attack. However, they only formulated the QoS degradation attack and did not provide details of the analysis in the closed-form.

To the best of our knowledge, the QoS degradation attack in D2D communication has not been investigated in detail in terms of analysis and simulations. To this end, in this paper, we investigate the QoS degradation attack in cluster-based D2D communication in detail, particularly deriving a closed-form expression of cluster sum-rate and performing a system-level simulation to verify its validity. Our main contributions are summarized as follows:

✓ We investigate the QoS degradation attack in cluster-based D2D communication and derive the closed-form of the cluster sum-rate under the attack;

✓ We further analyze the effect of a threshold-based defense scheme against the QoS degradation attack and derive mathematical formulation in the closed-forms;

✓ We perform system-level simulations to evaluate the impact of the QoS degradation attack on cluster-based D2D communication with Simu5G.

The rest of the paper is organized as follows. Section II describes the system model, the threat model, and the performance metric. In Section III, we introduce a countermeasure against possible threats and mathematically analyze the performance of the countermeasure. In Section IV, we perform a simulation to evaluate the performance of the defense mechanism and to verify our mathematical analysis. Finally, we draw our conclusions in Section V.

Ⅱ. System Model

Fig. 1 depicts a system model where we consider a single D2D cluster of multiple devices including a single malicious device as a cluster member. We assume that all the devices and the base station are equipped with a single antenna. Additionally, we assume that a malicious device acts as the cluster member under the situation that the cluster head (CH) was already designated. The CH is responsible for D2D multicasting in the cluster and decides the data rate for D2D multicasting based on CSI feedback

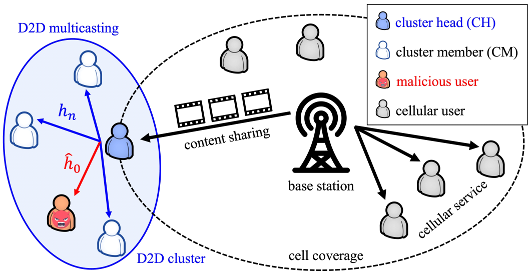


Fig. 1. A system model where we consider a single D2D cluster of five devices (i.e., N = 3) including a single malicious device as a cluster member

from each user to the CH[10]. We define $n \in \mathscr{N} \triangleq \{0, \cdots, N\}$ as an index of each device except for the CH (i.e., only cluster members of the D2D cluster). We consider total $N+1$ cluster members: N normal cluster members and a single malicious cluster member. Let h_n denote the channel fading coefficient between the CH and device n. We assume a Rayleigh fading channel and thus $h_n \in \mathbb{C}$ is a complex Gaussian random variable with zero mean and variance $\sigma^2_{h_n}$.

The CH multicasts data to only cluster members who request content sharing. Let $\mathscr{D} \subseteq \mathscr{N}$ indicate the set of active cluster members who request content sharing. We assume that the CH sets multicasting data rate to consider the minimum quality of service (in terms of data rate) for all devices in $\mathscr{D}$. Then, the minimum achievable data rate for all cluster members in $\mathscr{D}$ is given as follows:

$$R_{\min}(\mathscr{D}) = \log_2(1 + \min_{n \in \mathscr{D}}\{|h_n|^2\}\rho), \tag{1}$$

where ρ represents the signal-to-noise ratio (SNR) for transmission.

2.1 Threat Model: QoS Degradation Attack

The main purpose of the malicious device is to degrade the quality of service (QoS) in the D2D cluster by exploiting CSI forgery. Note that the data rate for D2D multicasting in (1) is mainly determined by the device that experiences the worst channel condition (i.e., minimum value of $|h_n|^2$, $\forall n \in \mathscr{D}$). Thus, the malicious device can intentionally report its *underestimated* CSI instead of the original one for the purpose of degrading the date rate in (1).

We define this attack as the *QoS degradation attack*[10]. Without loss of generality, we assume $n = 0$ for the index of the malicious device. Then, we can model the forged CSI of the original $|h_0|^2$ as follows:

$$|\hat{h}_0|^2 = \alpha |h_0|^2, \tag{2}$$

where $\alpha \in (0, 1]$ denotes the CSI forgery factor by the malicious user.

To execute the QoS degradation attack, the malicious user deliberately reports an *underestimated* CSI (i.e., $|\hat{h}_0|^2$ in (2)) to the CH in order to lower the data rate for D2D multicasting in (1). Consequently, if the QoS degradation attack is successfully done from the perspective of the malicious device, then the base station believes that the malicious device experiences the worst channel fading. Thus, the base station sets the minimum achievable data rate for the D2D multicasting as follows:

$$R_{\min}(\mathscr{D}) = \log_2(1 + |\hat{h}_0|^2 \rho). \tag{3}$$

2.2 Performance Metric: Cluster Sum-Rate

For the QoS degradation attack, all cluster members in the D2D cluster suffer from the data rate degradation. Thus, we consider the sum-rate in the D2D cluster as a performance metric to quantitatively measure the level of QoS degradation, instead of a single device's data rate in (1).

We define the *cluster sum-rate* as a sum of all data rates of the cluster members that require content sharing from the CH and it is given by

$$R^{\text{sum}}_{\text{ref}} = |\mathscr{D}| \times \log_2(1 + \min_{n \in \mathscr{D}}\{|h_n|^2\}\rho), \tag{4}$$

where $|\mathscr{D}|$ represents the number of cluster members in $\mathscr{D}$.

Note that the cluster sum-rate jointly considers the number of cluster members (i.e., served D2D devices by the CH) and the data rate for D2D multicasting together. We will compare the expectation of the cluster sum-rate with and without the QoS degradation attack in detail with mathematical analysis in Section

Ⅲ and extensive simulations in Section Ⅳ, respectively.

Ⅲ. Analysis and Countermeasure

In this section, we first investigate the closed-form of cluster sum-rate in (4) without considering a countermeasure. Next, we introduce threshold-based countermeasures proposed in [10] and derive the closed-form of cluster sum-rate in (4) when the countermeasure is applied, which has not been studied in previous work[10].

3.1 Sum-Rate Analysis without Countermeasure

For^{h} analytical tractability, we consider an independent and identically distributed (i.i.d.) condition for channel coefficient h_n (i.e., $\sigma_{h_n}^2 = \sigma_h^2\ \forall n$). When we do not consider a countermeasure against QoS degradation attack (i.e., defense mechanism), we assume that all devices in the D2D cluster request content sharing (i.e., $\mathscr{D} = \mathscr{N}$). We analyze the expectation of the cluster sum-rate without a defense mechanism for reference and it is summarized in the following theorem.

Theorem 1. *For a given N, σ_h^2, and α, the expectation of the cluster sum-rate without any defense is given by*

$$\mathbb{E}\left[R_{ref}^{sum}\right] = \frac{N+1}{\log(2)} \exp\left(\frac{\mu}{\rho}\right) E_1\left(\frac{\mu}{\rho}\right), \quad (5)$$

where $\mu = \frac{1+\alpha N}{\alpha\sigma_h^2}$, and $\mathrm{E}_1(x)$ indicates an exponential integral function defined as $\mathrm{E}_1(x) = \int_x^\infty \frac{\exp(-t)}{t}dt$[11].

Proof. In the absence of the defense mechanism, the cluster sum-rate in (4) is rewritten by

$$\begin{aligned} &R_{\mathrm{ref}}^{\mathrm{sum}}(\mathscr{D}) \\ &= |\mathscr{D}| \log_2\left(1 + \min\left\{\min_{n \in \mathscr{D}\setminus\{0\}}\{|h_n|^2\}, |h_0|^2\right\}\rho\right) \quad (6) \\ &= |\mathscr{D}| \log_2(1 + Z\rho), \end{aligned}$$

where $\mathscr{D} \setminus \{0\}$ denotes a subtraction of index 0 from a set $\mathscr{D}$ and the second equality holds with notation substitutions with $X = \min_{n\in\mathscr{D}\setminus\{0\}} |h_n|^2$, $Y = |\hat{h}_0|^2 = \alpha|h_0|^2$ and $Z = \min(X, Y)$.

Consequently, the expectation of (6) is derived as follows:

$$\mathbb{E}[R_{\mathrm{ref}}^{\mathrm{sum}}] = (N+1)\int_0^\infty \log_2(1+z\rho) f_Z(z)dz, \quad (7)$$

where $|\mathscr{D}| = N+1$ and $f_Z(\cdot)$ denotes the probability density function (PDF) of Z.

Using the fact that X corresponds to the minimum of N i.i.d. exponential random variables with a parameter σ_h^2 and Y is also exponentially distributed, we can obtain the cumulative distribution function (CDF) of Z (i.e., $FZ(z)$) as follows:

$$\begin{aligned} F_Z(z) &= \Pr[Z \le z] = 1 - \Pr[X > z]\Pr[Y > z] \\ &= 1 - \exp\left(-\frac{Nz}{\sigma_h^2}\right)\exp\left(-\frac{z}{\alpha\sigma_h^2}\right). \end{aligned} \quad (8)$$

In addition, the PDF of Z is given by

$$\begin{aligned} f_Z(z) &= \frac{\mathrm{d}}{\mathrm{d}z}F_Z(z) \\ &= \frac{1+\alpha N}{\alpha\sigma_h^2}\exp\left(-\frac{z(1+\alpha N)}{\alpha\sigma_h^2}\right). \end{aligned} \quad (9)$$

We can finally obtain (5) by substituting (9) into (7).

3.2 Sum-Rate Analysis with Countermeasure

To mitigate CSI forgery attacks such as underestimated or overestimated CSI reporting, threshold-based filtering mechanisms were investigated in [10]. We also employ the threshold-based defense scheme to defend the D2D multicasting against the QoS degradation attack. The main idea of the threshold-based defense scheme is for the CH to set a proper threshold value in order to filter out the forged (underestimated) CSI by the malicious user during the D2D multicasting for content sharing. Similar to [10], we define a criterion for the filtering using the threshold value γ and it is expressed as follows:

$$|h_n|^2 < \gamma \text{ for } n \in \mathscr{D}. \tag{10}$$

Remark 1. *Threshold-based defense mechanisms inherently have a disadvantage such that a legitimate device could even be considered as a malicious device if its actual CSI feedback is less than the criterion. Thus, the CH could exclude those devices satisfying* (10) *from the D2D multicasting for content sharing. However, we can minimize this negative effect by properly setting a threshold value as discussed in* [10]. *It will be further discussed in Section IV.*

Let $\mathscr{M}$ represent the set of cluster members who are considered to report their original CSI feedback to the CH (i.e., $|h_n|^2 \geq \gamma$). Then, the CH sets the D2D multicasting data rate based on $\mathscr{M}$, which is a subset of $\mathscr{D}$ (i.e., $\mathscr{M} \subset \mathscr{D}$). Thus, when we apply the defense mechanism, the cluster sum-rate is expressed as follows:

$$R_{\text{def}}^{\text{sum}} = |\mathscr{M}| \times \log_2(1 + \min_{n \in \mathscr{M}}\{|h_n|^2\}\rho). \tag{11}$$

Note that the number of elements in M varies depending on the γ value and it is the main factor to determine the value of (11). Thus, the value of γ must be chosen carefully. For example, setting a very low γ value might allow the malicious device to launch the attack and it results in approaching an almost zero cluster sum-rate. Accordingly, we analyze the expectation of the cluster sum-rate with a defense mechanism and it is summarized in the following theorem.

Theorem 2. *For a given N,* σ_h^2, *and* α, *the expectation of the cluster sum-rate with the defense mechanism is derived as* (12), *shown at the top of the next page where* $\eta = \exp\left(-\frac{1}{\sigma_h^2}\right)$, $\beta = (1+\gamma\rho)$, $\mu = \frac{1+\alpha N}{\alpha\sigma_h^2}$ *and* $E_1(x) = \int_x^\infty \frac{\exp(-t)}{t}dt$.

Proof. Using the condition of whether the malicious device is filtered out by (10) or not, and given the number of devices in the D2D cluster (i.e., $|\mathscr{M}| = k$), we reformulate (11) into (13), shown at the top of the next page.

To derive the closed-form of (13), we define the probability events as follows:

H: an event that $|\hat{h}_0|^2 \geq \gamma$,

H^c: a complement of H (i.e., $|\hat{h}_0|^2 \geq \gamma$),

A_k: an event that exactly k out of N devices have their CSI values greater than or equal to γ (i.e., $|\mathscr{M}| = k$).

Then, the expectation of the cluster sum-rate with the defense mechanism can be derived as follows:

$$\begin{aligned}
&\mathbb{E}[R_{\text{def}}^{\text{sum}}] \\
&= \sum_{k=0}^{N} \Pr[H \cap A_k]\, \mathbb{E}\left[|\mathscr{M}| \log_2(1 + \min_{n\in\mathscr{M}}\{|\bar{h}_n|^2\}\rho)\right] \\
&+ \sum_{k=1}^{N} \Pr[H^c \cap A_k]\, \mathbb{E}\left[|\mathscr{M}| \log_2(1 + \min_{n\in\mathscr{M}}\{|\bar{h}_n|^2\}\rho)\right] \\
&= \sum_{k=0}^{N} \Pr[H] \Pr[A_k]\, \mathbb{E}\left[|\mathscr{M}| \log_2(1 + \min_{n\in\mathscr{M}}\{|\bar{h}_n|^2\}\rho)\right] \\
&+ \sum_{k=1}^{N} \Pr[H^c] \Pr[A_k]\, \mathbb{E}\left[|\mathscr{M}| \log_2(1 + \min_{n\in\mathscr{M}}\{|\bar{h}_n|^2\}\rho)\right],
\end{aligned} \tag{14}$$

$$\begin{aligned}
\mathbb{E}[R_{\text{def}}^{\text{sum}}] =& \eta^{\frac{\gamma}{\alpha}} \times \sum_{k=0}^{N} \binom{N}{k} \eta^{\gamma k}\, (1-\eta)^{\gamma(N-k)} \times \frac{(k+1)}{\log(2)} \left[\log(\beta) + \exp\left(\frac{\beta\mu}{\rho}\right) \times \mathrm{E}_1\left(\frac{\beta\mu}{\rho}\right)\right] \\
&+ \left(1 - \eta^{\frac{\gamma}{\alpha}}\right) \times \sum_{k=1}^{N} \binom{N}{k} \eta^{\gamma k}\, (1-\eta)^{\gamma(N-k)} \times \frac{k}{\log(2)} \left[\log(\beta) + \exp\left(\frac{\beta k}{\rho\sigma_h^2}\right) \times \mathrm{E}_1\left(\frac{\beta k}{\rho\sigma_h^2}\right)\right].
\end{aligned} \tag{12}$$

$$\begin{aligned}
\mathbb{E}[R_{\text{def}}^{\text{sum}}] =& \Pr\left[|\hat{h}_0|^2 \geq \gamma\right] \sum_{k=0}^{N} \Pr[|\mathscr{M}| = k] \times \mathbb{E}\left[(k+1)\log_2\left(1 + \min_{n\in\mathscr{M}}\left\{|h_n|^2, |\hat{h}_0|^2\right\}\rho\right) \middle| |h_n|^2 \geq \gamma, |\hat{h}_0|^2 \geq \gamma\right] \\
&+ \Pr\left[|\hat{h}_0|^2 < \gamma\right] \sum_{k=1}^{N} \Pr[|\mathscr{M}| = k] \times \mathbb{E}\left[k\log_2\left(1 + \min_{n\in\mathscr{M}}\left\{|h_n|^2\right\}\rho\right) \middle| |h_n|^2 \geq \gamma\right].
\end{aligned} \tag{13}$$

where $/\bar{h}_n/^2$ indicate channel gain satisfying condition of $/h_n/^2 \geq \gamma$, which follows a truncated exponential distribution, and the second equality holds due to the independence between each probability event. Further, Pr[H], Pr[H^c], and Pr[A_k] are obtained as follows:

$$\Pr[H] = \exp\left(-\frac{\gamma}{\alpha\sigma_h^2}\right), \tag{15}$$

$$\Pr[H^c] = 1 - \Pr[H] = 1 - \exp\left(-\frac{\gamma}{\alpha\sigma_h^2}\right), \tag{16}$$

$$\Pr[A_k] = \binom{N}{k}\eta^{\gamma k}\,(1-\eta)^{\gamma(N-k)}, \tag{17}$$

where we define Pr[$/h_n/^2 \geq \gamma$] for $n \in \{1, \cdots, N\}$ as $\eta = \exp\left(-\frac{1}{\sigma_h^2}\right)$.

Let W denote $\min_{n\in\mathcal{M}}\{|\bar{h}_n|^2\}$ in (14). If $/\mathcal{M}/ = k$ and $0 \in \mathcal{M}$ (i.e., malicious device is in the D2D cluster), the PDF of W is given by

$$f_W(w) = \frac{1+\alpha k}{\alpha\sigma_h^2}\exp\left(-\frac{(w-\gamma)(1+\alpha k)}{\alpha\sigma_h^2}\right). \tag{18}$$

Otherwise (i.e., $/\mathcal{M}/ = k$ and $0 \notin \mathcal{M}$), the PDF of W is given by

$$f_W(w) = \frac{k}{\sigma_h^2}\exp\left(-\frac{k(w-\gamma)}{\sigma_h^2}\right). \tag{19}$$

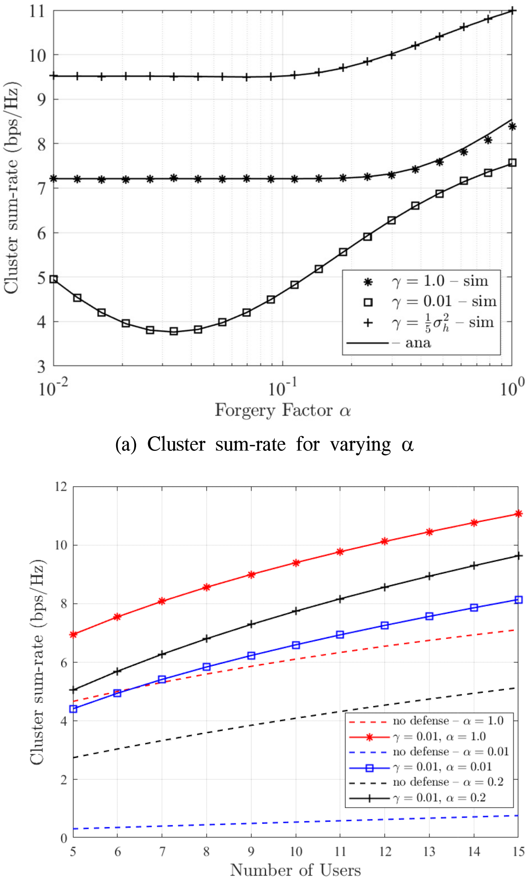
We can finally obtain (12) by plugging Pr[H] in (15), Pr[H^c] in (16), Pr[A_k] in (17), (18), and (19) into (14). □

Ⅳ. Numerical Results

In this section, we consider two types of simulation tools: MATLAB[12] and Simu5G[13]. First, we verify our analysis on the expectation of cluster sum-rate using simulations with MATLAB. Next, we evaluate the performance of the defense mechanism under the QoS degradation attack using Simu5G, a practical simulation tool that implemented 5G specifications-based protocol stacks.

4.1 Simulations with MATLAB

Fig. 2 shows the cluster sum-rate when we consider different values of α and N, respectively. Fig. 2a shows the cluster sum-rate for different values of α. We verify that our derivation (indicated by 'ana') in (12) correctly matches with the simulation results (indicated by 'sim'). We observe that the cluster sum-rate decreases when the malicious user aggressively adjusts the forgery factor (i.e., small α value) since the CH sets the minimum data rate for the multicast process based on the minimum value of CSI feedback reports. It should be noted that the defense scheme excludes cluster members who meet the requirement in (10), which can reduce the number of multicast devices and thus also decrease the cluster



(a) Cluster sum-rate for varying α

(b) Cluster sum-rate for varying N

Fig. 2. Cluster sum-rate when we consider various α and N

sum-rate. However, we can achieve a better cluster sum-rate if we carefully set threshold value (e.g. $\gamma = \frac{1}{5}\sigma_h^2$). Fig. 2b shows the cluster sum-rate for different number of users N in the D2D cluster. The cluster sum-rate increases with an increase in the number of users N in the D2D cluster regardless of the α value set by the malicious user. We can achieve a better cluster-sum rate when the defense scheme is employed. It implies that the threshold-based defense scheme filters out the unqualified devices (i.e., devices that fall under the category in (10)) but the cluster sum-rate is expected to increase if we carefully set threshold γ value, as discussed in Fig. 2a.

4.2 Simulations with Simu5G

Simu5G is a network simulator that incorporates 5G New Radio access technology[13]. It is based on the OMNet++ framework and allows the simulation of 5G network scenarios so that researchers can benchmark their solutions to an easy-to-use framework.[1] It also embeds a possible extension to set up device-to-device (D2D) communication simulations, with a special focus on the main parameters that might affect the performance of the D2D network[13].

As part of the system-level simulation using Simu5G, we consider a cluster of $N = 5$ devices leveraging cellular links in order to stream video packets from the server through the base station. Each device is to receive the video based on the device with the worst channel quality indicator (CQI). We manually set two types of CQI value ranges for [0-15] in our simulations as follows: [0-6] and [7-15] to indicate poor and good channel conditions, respectively.

Fig. 3 shows the cluster sum-rate of using Simu5G when the various scenarios are considered. In the “attack” scenario, we consider that the malicious device reports a very low CQI value (i.e., CQI = 4) which drastically reduces the cluster sum-rate as observed from the bar graph. However, the cluster sum-rate can be improved when the defense scheme is implemented (i.e., threshold ɣ corresponding to CQI = 9). Depending on CQI values to filter out suspected users, the cluster sum-rate can dramatically vary. For example, we can achieve a non-degraded cluster sum-rate in the case of “no attack” (i.e., CQI = 15). Note that we do not fully consider incorporating D2D links due to some limitations of Simu5G simulations. However, our simulation is similar to that of the D2D scenario discussed in this paper and advanced simulation results using Simu5G will be studied in depth in our future research.

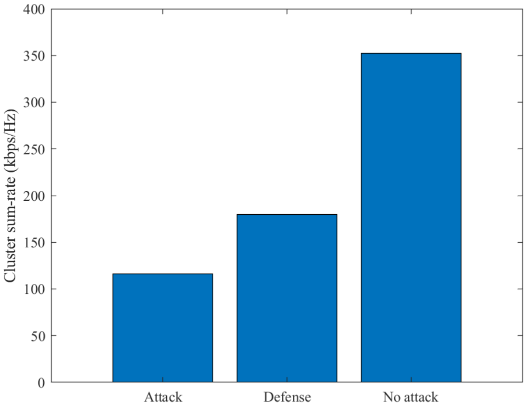


Fig. 3. Cluster sum-rate considering video streaming service through Simu5G based simulations

V. Conclusion

In this paper, we investigated a CSI forgery attack, specifically, a QoS degradation attack in a D2D cluster where a malicious user in the cluster intentionally reports an underestimated CSI instead of the original one to the cluster head. We defined the cluster sum rate as our evaluation metric against the QoS degradation attack. We introduced a threshold-based countermeasure commonly used against CSI forgery attacks. Further, we derived the closed-form expression of expectation on the cluster sum-rate. Finally, we verified our mathematical derivations using simulations and evaluated the threshold-based defense mechanism considering 5G protocol-based advanced simulation tools (i.e., Simu5G).

[1] https://github.com/Unipisa/Simu5G

References

[1] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 334-366, 2021. (https://doi.org/10.1109/OJCOMS.2021.3057679)

[2] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84-90, 2019. (https://doi.org/10.1109/MCOM.2019.1900271)

[3] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, and M. A. Javed, "A survey of device-to-device communications: Research issues and challenges," *IEEE Commun. Surv. & Tuts.*, vol. 20, no. 3, pp. 2133-2168, 2018. (https://doi.org/10.1109/COMST.2018.2828120)

[4] H. Rong, Z. Wang, H. Jiang, Z. Xiao, and F. Zeng, "Energy-aware clustering and routing in infrastructure failure areas with D2D communication," *IEEE Internet of Things J.*, vol. 6, no. 5, pp. 8645-8657, 2019. (https://doi.org/10.1109/JIOT.2019.2922202)

[5] M. Gharbieh, A. Bader, H. ElSawy, H.-C. Yang, M.-S. Alouini, and A. Adinoyi, "Selforganized scheduling request for uplink 5G networks: A D2D clustering approach," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1197-1209, 2019. (https://doi.org/10.1109/TCOMM.2018.2876008)

[6] Y.-C. Tung, S. Han, D. Chen, and K. G. Shin, "Vulnerability and protection of CSI in multiuser MIMO networks," in *Proc. ACM Conf. CCS*, pp. 775-786, 2014. (https://doi.org/10.1145/2660267.2660272)

[7] S. Wang, Z. Chen, Y. Xu, Q. Yan, C. Xu, and X. Wang, "On user selective eavesdropping attacks in MU-MIMO: CSI forgery and countermeasure," in *Proc. IEEE INFOCOM*, pp. 1963-1971, 2019. (https://doi.org/10.1109/INFOCOM.2019.8737412)

[8] T. Hou, S. Bi, T. Wang, Z. Lu, Y. Liu, S. Misra, and Y. Sagduyu, "MUSTER: Subverting user selection in MU-MIMO networks," in *Proc. IEEE INFOCOM*, pp. 140-149, 2022. (https://doi.org/10.1109/INFOCOM48880.2022.9796815)

[9] D. Lin and Y. Tang, "Blockchain consensus based user access strategies in D2D networks for data-intensive applications," *IEEE Access*, vol. 6, pp. 72683-72690, 2018. (https://doi.org/10.1109/ACCESS.2018.2881953)

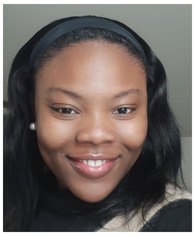
[10] I. Bang, V. A. S. Manya, J.-H. Kim, and T. Kim, "On the effect of malicious user on D2D cluster: CSI forgery and countermeasures," *IEEE Access*, 2023. (https://doi.org/10.1109/ACCESS.2023.3236879)

[11] I. Gradshteyn and I. Ryzhik, *Table of integrals, series, and products*, London, UK: Academic Press, 2003. (https://doi.org/10.1016/C2010-0-64839-5)

[12] MATLAB, *version 23.2.0.2358603* (*R2023b*). The MathWorks Inc., 2023. [Online]. Available: https://www.mathworks.com/products/matlab.html)

[13] G. Nardini, D. Sabella, G. Stea, P. Thakkar, and A. Virdis, "Simu5G-An OMNeT++ library for end-to-end performance evaluation of 5G networks," *IEEE Access*, vol. 8, pp. 181176-181191, 2020. (https://doi.org/10.1109/ACCESS.2020.3028550)

Venissa Adzo Sedem Manya



Aug. 2020 : B.Eng. degree, Kwame Nkrumah University of Science and Technology (KNUST), Ghana

Aug. 2023 : M.Eng. degree, Hanbat National University, South Korea

Sept. 2023~Current : Ph.D. student, McMaster University, Canada

<Research Interest> wireless network security and device-to-device (D2D) communication

[ORCID:0009-0008-5082-2834]

Taehoon Kim

2017 : Ph.D. Electrical Engineering, KAIST, South Korea

2017~2020 : Senior Researcher, Agency for Defense Development, South Korea

2020~Current : Associate Professor, Department of Computer Engineering, Hanbat National University, South Korea

<Research Interests> wireless communications, resource management for 6G/IoT, machine learning applications in wireless communications, and wireless network security.

[ORCID:0000-0002-9353-118X]

Jonghyun Kim

2005 : Ph.D. Computer Science, University of Oklahoma, USA

1995~1997 : Researcher, Samsung Electronics, South Korea

2005~Current : Principal Researcher, ETRI, South Korea

<Research Interests> information security, cyber security, cloud security, AI-based malware detection and 5G/6G security

[ORCID:0000-0002-5532-2117]

Inkyu Bang

2017 : Ph.D. Electrical Engineering, KAIST, South Korea

2017~2019 : Research Fellow, National University of Singapore, Singapore

2019~2019 : Senior Researcher, Agency for Defense Development, South Korea

2019~Current : Associate Professor, Department of Intelligence Media Engineering, Hanbat National University, South Korea

<Research Interests> wireless network security, physical-layer security, information-theoretic security, 6G/5G/IoT, and deep learning application in wireless communications.

[ORCID:0000-0001-7109-1999]