IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 December 2022, accepted 20 December 2022, date of publication 13 January 2023, date of current version 19 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3236879

RESEARCH ARTICLE

On the Effect of Malicious User on D2D Cluster: CSI Forgery and Countermeasures

INKYU BANG[1], (Member, IEEE), VENISSA ADZO SEDEM MANYA[1], (Student Member, IEEE), JONGHYUN KIM[2], (Member, IEEE), AND TAEHOON KIM[3], (Member, IEEE)

[1]Department of Intelligence Media Engineering, Hanbat National University, Daejeon 34158, Republic of Korea
[2]Electronics and Telecommunications Research Institute (ETRI), Daejeon 34129, Republic of Korea
[3]Department of Computer Engineering, Hanbat National University, Daejeon 34158, Republic of Korea

Corresponding author: Taehoon Kim (thkim@hanbat.ac.kr)

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.

ABSTRACT Device-to-device (D2D) communication in cellular networks refers to a technology that enables direct transmission and reception between devices in proximity without infrastructures such as base stations (BSs). It has consistently attracted attention due to its key role extending cellular coverage through the configuration of clusters, in which the D2D devices belonging to a cluster can either be a cluster head or a cluster member. In this paper, we investigate the effect of channel state information (CSI) forgery attacks of a single malicious user (i.e., attacker) belonging to a cluster. Particularly, we investigate two major threat models: 1) clustering failure attack, where an attacker reports its *overestimated* CSI instead of the original one to the BS during clustering, 2) quality of service (QoS) degradation attack where an attacker reports its *underestimated* CSI instead of the original one to the cluster head during the intra-cluster D2D communications (i.e., D2D multicasting). We define metrics to measure each CSI forgery attack as *clustering failure probability* and *cluster sum-rate*, respectively, and further derive a closed-form expression for the clustering failure probability. In addition, we propose threshold-based defense mechanisms as countermeasures against CSI forgery attacks and find suboptimal threshold values. Through simulations, we evaluate the performance of the defense mechanisms in terms of clustering failure probability and cluster sum-rate, comparing with optimal simulation results.

INDEX TERMS Wireless network security, device-to-device (D2D) communications, D2D clustering, channel state information (CSI), CSI forgery.

I. INTRODUCTION

The massive growth in the number of mobile devices using applications such as voice and video has led to an exponential surge of data traffic in cellular networks [1]. Accordingly, cellular networks have evolved to accommodate this rise in demand with advanced techniques such as massive multiple-input and multiple-output (MIMO), intelligent reflecting surface (IRS), and device-to-device (D2D) techniques. The notion of D2D communications in cellular networks was first introduced in 4G cellular networks and it has been recently highlighted again due to its potential in 6G cellular networks for applications of smart factories (e.g., industry 5.0) and vehicular communications (e.g., autonomous driving, vehicular platooning) [2].

D2D communication in cellular networks refers to a technology that enables direct data transmission and reception between devices in proximity without the infrastructures such as base stations [1]. D2D communication provides several advantages such as efficient utilization of available resources, improved data rates, and reduced latency. Thus, D2D communication has been considered one of the

The associate editor coordinating the review of this manuscript and approving it for publication was Ruofei Ma.

promising technologies to improve overall performance in cellular networks by efficiently utilizing the spectrum [3].

There have been many studies developing D2D communication techniques to improve spectral efficiency and reduce traffic overload in the network for key applications of D2D communications: content sharing, data computation offloading, and coverage extension [4], [5], [6], [7]. Especially, content sharing through D2D communications can contribute to the efficient use of radio resources by avoiding the repeated transmission of the same contents from the base station to different users, respectively. In content sharing, the user devices are grouped as a cluster including a cluster head (CH) and cluster members (CMs), and the CH is responsible for the dissemination of content received from the base station to CMs (i.e., D2D multicasting scenario).

D2D multicasting data rate for content sharing is dependent on the channel state information (CSI) between the CH and the base station, and also the CH and CMs due to the randomness in wireless fading channels. Thus, it is an important issue to properly form a cluster and select a cluster head in D2D multicasting scenarios. Accordingly, there have been several studies on clustering algorithms [8], [9], [10], [11]. It is important to note that most of the existing works considered CSI between users and the base station during clustering to enhance the performance of cluster-based D2D communication such as multicast data rate and latency. CSI-based clustering itself is beneficial in D2D communications. However, there exist potential security threats in cluster-based D2D communications when a malicious user is a member of the cluster. Several types of D2D attacks have been reported recently such as eavesdropping, free-riding, CSI forgery, denial-of-service, key compromise impersonation, and gray-hole attacks [12], [13], [14], [15].

In this paper, we focus on CSI forgery attacks in D2D communication where the malicious user in the cluster intentionally reports its overestimated or underestimated CSI (i.e., CSI forgery) instead of the original one to the base station or to the CH. CSI forgery can degrade the quality of service (QoS) such as data rate, spectral efficiency, and energy consumption. Tung et al. [16] investigated the vulnerability of forged CSI feedback in multiuser MIMO networks. They showed that an attacker can exploit the forged CSI to eavesdrop on other users' transmissions. Wang et al. [17] further investigated a sniffing attack using forged CSI in multiuser MIMO networks and proposed a defense mechanism able to compare a mismatch between downlink and uplink angular spectra for received CSI feedbacks. Wang et al. [18] analyzed the effect of CSI forgery in orthogonal frequency division multiple access (OFDMA) networks on physical-layer security related metrics such as eavesdropping probability and secrecy loss.

To the best of our knowledge, the effect of CSI forgery in cluster-based D2D communications has been less highlighted rather than other topics (e.g., multiuser MIMO, infrastructure-based communications). In this paper, we investigate vulnerabilities of D2D communication for cluster-based service in cellular networks. *To be specific, the main contributions of our work are summarized as follows;*

1) **Security problem formulation with new metrics:** we investigate a threat model that considers a single malicious user (i.e., an attacker) exploiting CSI forgery during clustering and cluster-based D2D communications, and define metrics to measure the impact of overestimated and underestimated CSI forgery: *clustering failure probability* and *cluster sum-rate*;
2) **Threshold-based defense with analysis:** we propose threshold-based countermeasures (i.e., defense mechanisms) against CSI forgery attacks (i.e., clustering failure attack and QoS degradation attack) and further derive a closed-form expression for clustering failure probability when the attacker reports overestimated CSI to deny the service of the entire cluster by being selected as a cluster head;
3) **Procedure to set threshold values:** we set suboptimal threshold values for defense mechanisms and evaluate their performance in terms of clustering failure probability and cluster sum-rate, compared with optimal simulation results.

The rest of this paper is organized as follows. In Section II, we clearly summarize several related studies and compare them with ours. In Section III, we describe our system model including threat model and related performance metrics. In Section IV, we investigate threshold-based countermeasures and analyze the performance of our defense mechanisms in terms of clustering failure probability and cluster sum-rate. Then, we evaluate the performance of our defense mechanisms through extensive simulations and provide additional discussions in Section V. Finally, we draw conclusions in Section VI.

II. RELATED WORKS

D2D communication has become an integral component of the cellular system due to its ability to improve spectral efficiency, reduce latency and increase system coverage. Accordingly, extensive research has been conducted to guarantee regular operations of D2D users under limited radio resource constraints. A number of studies have been done on user access control strategies in D2D communication networks in a bid to deal with the radio resource-limited environment [19], [20], [21]. Yu et al. [19] proposed a power-allocation algorithm to maximize the network throughput by efficiently adjusting the transmission power based on the distances between D2D users. The authors specifically used a booster to restrict D2D transmission power and reduce user interference. Lee et al. [20] analyzed a random network model for a D2D underlaid cellular system using stochastic geometry and proposed centralized and distributed power control algorithms to provide sufficient coverage and maximize the sum rate of the D2D links, respectively. Further, Lin and Tang [21] discussed the issue of user access and proposed optimal user

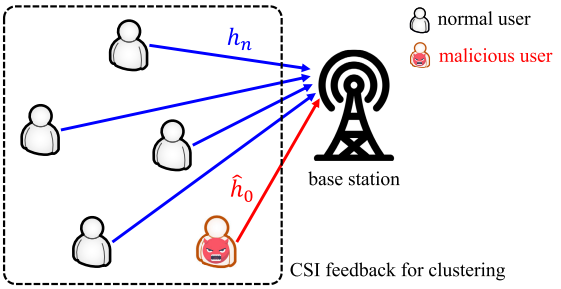
access strategies for data-intensive applications based on a blockchain consensus-based scheme.

The above-mentioned studies are based on the assumption that users in the D2D network provide authentic CSI values for their transmissions. They focused on user access schemes to enhance the performance of D2D links. On the other hand, it is also important to consider a malicious scenario where a user intentionally forges its CSI to gain an undue advantage over others, from the perspective of wireless network security. Many studies have investigated CSI forgery and its effects [16], [17], [18], [21], [22], [23], [24], [25]. In [16], [17], and [18], the effects of CSI forgery were investigated by focusing on infrastructure-based networks (e.g., MIMO and OFDMA systems) rather than cluster-based D2D communications. In recent times, there are still lots of studies [21], [22], [23], [24], [25] focusing on CSI forgery but only a few of them [21] consider D2D communication environments, which motivates us to tackle the problem in this paper. In [21], the authors focused on establishing the framework of D2D cellular networks for the authenticity of CSI using blockchain consensus methods. However, we newly introduce the notion of metrics to describe the impacts of CSI forgery attacks on D2D clustering and also derive the closed-form of analytical results. In [22], [23], [24], and [25], CSI forgery problems in MIMO networks were investigated. Zhang et al. [22] analyzed the impact of channel state misreporting on multiuser (MU) scheduling performance in massive MIMO networks. They specifically presented a throughput attack that misleads power allocation with CSI forgery. Yang et al. [23] investigated a theoretical analysis on the construction of forged CSI in MU-MIMO systems and demonstrated the possibility of malicious users launching sniffing attacks with carefully-calculated forged CSI. Hou et al. [24] showed the potential attacks against CSI-based user selection algorithms in MU-MIMO systems. The authors presented a user selection subversion, which fabricates CSI to manipulate user selection in the multiuser system. Lin et al. [25] worked on optimizing the spectral efficiency of mobile users by authenticating each user's CSI. Additionally, notions of channel-based physical-layer authentication and feature selection in abnormal detection can be extended to enhance security in D2D clustering problems [26], [27].

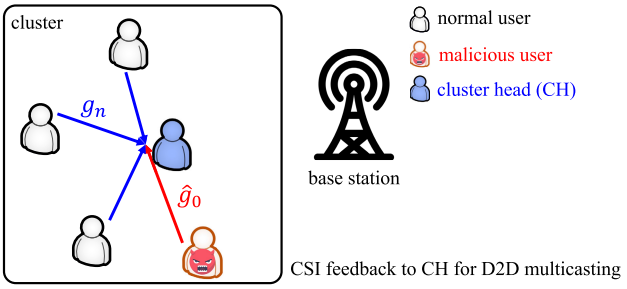
III. SYSTEM MODEL

In this section, we introduce the basic parameters for our system model, describe the threat model including two types of attacks (i.e., clustering failure attack and QoS degradation attack), and define performance metrics: clustering failure probability and cluster sum-rate.

We consider a cellular network that consists of a single base station and N users (or devices) including a single malicious user (i.e., the attacker), as described in Fig. 1. We assume that all the N devices and the base station are equipped with a single antenna and D2D communication is available at



(a) An example of CSI feedback from each device to the base station during a clustering failure attack



(b) An example of CSI feedback from each cluster member to the cluster head during a QoS degradation attack after clustering

FIGURE 1. An example of system model for $N = 5$.

every device.[1] We consider a scenario where N devices are forming a single cluster consisting of one cluster head (CH) and $N-1$ cluster members and then the CH is multicasting the common data to cluster members (CMs).

Let $n \in \mathcal{N} \triangleq \{0, \cdots, N-1\}$ denote a device index. We assume the Rayleigh channel fading model and let $h_n \in \mathbb{C}$ and $g_n \in \mathbb{C}$ denote channel fading coefficients between the base station and device n, and the selected CH and device n, respectively. Thus, h_n and g_n are assumed to be complex Gaussian random variables with zero mean and variances $\sigma_{h_n}^2$ and $\sigma_{g_n}^2$ respectively, i.e., $h_n \sim \mathcal{CN}(0, \sigma_{h_n}^2)$ and $g_n \sim \mathcal{CN}(0, \sigma_{g_n}^2)$.[2] We further assume that h_n and g_n are independent and identically distributed (i.i.d.), i.e., $\sigma_{h_n}^2 = \sigma_h^2$ and $\sigma_{g_n}^2 = \sigma_g^2$ $\forall n$, for analytical tractability.

The base station selects the CH considering the largest value of $|h_n|^2$ among N devices as follows:

$$n^\star = \arg\max_{n \in \mathcal{N}} |h_n|^2, \tag{1}$$

where $n^\star$ denotes the index of the CH. Note that using CSI as the CH selection criterion as in (1) is common in D2D clustering [11].

[1] Throughout the paper, we interchangeably use the terms 'user' and 'device', and 'malicious device' and 'attacker', respectively. We consider a single antenna case for analytical tractability but our model can be extended to a multi-antenna case.

[2] Note that we consider Rayleigh fading channel in our system model. However, when we consider other fading channel models such as Rician and Nakagami-m fading channels, which require more complicated analysis, the expected results and general trends will be similar.

After the cluster is formed (i.e., the CH is selected based on (1)), the CH multicasts data to its CMs requesting data from it, considering the minimum rate among them. We define $\mathcal{M} \subseteq \mathcal{N}$ as an index set of CMs requesting the data from the CH. Then, the minimum data rate of devices in $\mathcal{M}$ is given by

$$R_{\min}(\mathcal{M}) = \min_{n\in\mathcal{M}} \left\{\log_2\left(1+|g_n|^2\rho\right)\right\} = \log_2\left(1+\min_{n\in\mathcal{M}}\left\{|g_n|^2\right\}\rho\right), \quad (2)$$

where ρ denotes the transmit signal-to-noise ratio (SNR).

A. THREAT MODEL

The purpose of the malicious device is to disturb the cluster-based D2D communications among normal devices by exploiting the clustering failure attack and the QoS degradation attack. We introduce how the attacker can launch those attacks using CSI forgery.

Without loss of generality, we denote $n = 0$ as an index for the malicious device for notational simplicity. The attacker forges CSI values of $|h_0|^2$ and $|g_0|^2$ as follows:

$$|\hat{h}_0|^2 = \alpha|h_0|^2, \quad (3)$$
$$|\hat{g}_0|^2 = \alpha|g_0|^2, \quad (4)$$

where we define $\alpha \in [0, \infty)$ as a CSI forgery factor able to be set by the attacker.[3]

1) CLUSTERING FAILURE ATTACK

For this attack, the attacker reports an overestimated CSI feedback to the base station (i.e., $|\hat{h}_0|^2$ with $\alpha > 1$) in order to be selected as the CH, as described in Fig. 1. We assume that the malicious device intentionally denies its cluster members' service request when it is selected as the CH in order to cause a failure in the clustering of the N devices. Thus, we consider that the clustering failure attack is a success if the malicious device is selected as the CH (i.e., $n^\star = 0$ in (1)).

2) QoS DEGRADATION ATTACK

We assume that the attacker tries to launch the QoS degradation attack if the attacker is not selected during clustering. We consider the QoS of the cluster-based D2D communications in terms of the multicasting data rate of the CMs in $\mathcal{M}$. For this attack, the attacker reports an underestimated CSI feedback to the CH (i.e., $|\hat{g}_0|^2$ with $\alpha \leq 1$) in order to degrade the multicasting data rate of the CMs in $\mathcal{M}$, as described in Fig. 1b. Note that the attacker's goal is to set the forgery factor α such that $|\hat{g}_0|^2 = \min_{n\in\mathcal{M}}\left\{|g_n|^2\right\}$. Thus, if the QoS degradation attack is a success, then, the minimum data rate for D2D multicasting in (2) is rewritten as follows:

$$R_{\min}(\mathcal{M}) = \log_2\left(1+|\hat{g}_0|^2\rho\right). \quad (5)$$

[3]Note that the received signal strength indicator (RSSI) can alternatively be used in the wireless system instead of CSI. However, the similar security issue of forgery channel reporting will be the same and our framework can be applicable even if we consider RSSI instead of CSI.

B. PERFORMANCE METRIC

We define the following two performance metrics to measure the impacts of the clustering failure attack and the QoS degradation attack on the cluster-based D2D communications, respectively.

1) CLUSTERING FAILURE PROBABILITY

The clustering failure probability is the probability that the attacker is selected as the CH among all the N devices during the clustering. In other words, it indicates the impact of the clustering failure attack on the clustering process. For example, when we only consider the attack without any defense mechanisms, the clustering failure probability is given by

$$p_{\text{ref}} = \Pr\left[\max_{n\in\mathcal{N}\setminus\{0\}} |h_n|^2 < |\hat{h}_0|^2\right], \quad (6)$$

where $\mathcal{N} \setminus \{0\}$ indicates subtraction of the index 0 from $\mathcal{N}$.

Note that the clustering failure probability can be significantly reduced when the defense mechanism is applied at the base station. The derivation of (6) and the effect of defense mechanism will be analyzed and discussed in Section IV.

2) CLUSTER SUM-RATE

The cluster sum-rate is a summation of the data rates of CMs requesting data from the CH. For example, if the attacker successfully executes the QoS degradation attack, the CH multicasts the data to CMs in $\mathcal{M}$ based on (5). Thus, in this case, the cluster sum-rate is given by

$$R_{\text{ref}}^{\text{sum}} = |\mathcal{M}| \times \log_2\left(1+|\hat{g}_0|^2\rho\right), \quad (7)$$

where $|\mathcal{M}|$ denotes the number of elements in $\mathcal{M}$.

Note that the cluster sum-rate jointly considers the number of served devices by the CH using D2D communications in the cluster and the minimum multicasting data rate among corresponding CMs.

IV. THRESHOLD-BASED DEFENSE MECHANISM

In this section, we propose threshold-based defense mechanisms and analyze their effectiveness against the clustering failure attack and the QoS degradation attack.

Note that threshold-based defense mechanisms can filter out the candidates of the malicious devices suspected to forge the CSI values by comparing the given threshold values and estimated CSI values. The effect of threshold-based defense depends on the attacker's strategy (value of α in our case) and thus threshold values should be carefully determined. Further, several studies verify that properly setting threshold values can provide performance gain (e.g., outage probability) [28], [29].

A. THRESHOLD AGAINST CLUSTERING FAILURE ATTACK

For the clustering failure attack, the attacker intentionally reports the *overestimated* CSI (i.e., $|\hat{h}_0|^2$) to the base station. We consider that the base station employs a threshold β to

filter out the overestimated CSI by the attacker during the clustering process. In other words, the base station considers the following criterion on each CSI feedback from each device for the defense,

$$|h_n|^2 > \beta \text{ for } n \in \mathcal{N}. \tag{8}$$

If there exists any CSI feedback satisfying the condition in (8), then the base station regards such CSI as overestimated CSI feedback by the attacker and excludes the corresponding device from the list of candidates for the CH selection. Note that if we set a large β value, then we cannot properly defend the clustering failure attack. However, a small β value causes failure in the clustering process since the CH selection process cannot be completed due to the empty candidate set. Accordingly, β should be carefully determined and it will be discussed further in Section V.

1) CLUSTERING FAILURE PROBABILITY WITHOUT DEFENSE

For reference, we first analyze the clustering failure probability without considering the threshold condition in (8), summarized in the following theorem.

Theorem 1: For given N, σ_h^2, and α, the clustering failure probability without any defense mechanism is given by

$$p_{\text{ref}} = \sum_{k=0}^{N-1} \binom{N-1}{k} \frac{(-1)^k}{\alpha k + 1}. \tag{9}$$

Proof: When we do not consider the defense mechanism, the clustering failure probability is given in (6). To derive the closed-form of (6), we use the following notation: $X = |\hat{h}_0|^2 = \alpha |h_0|^2$ and $Y = \max_{n \in \mathcal{N} \setminus \{0\}} |h_n|^2$.

Thus, (6) is rewritten as follows:

$$p_{\text{ref}} = \Pr[Y < X] = \int_0^\infty F_Y(x) f_X(x)\, dx, \tag{10}$$

where $F_Y(\cdot)$ and $f_X(\cdot)$ denote the cumulative distribution function (CDF) of Y and the probability density function (PDF) of X, respectively.

Since $|h_n|^2$ is exponentially distributed with a parameter σ_h^2, Y is a maximum of $N-1$ i.i.d. exponential random variables and X is also exponentially distributed. Using the probability theory [30], $F_Y(y)$ and $f_X(x)$ are obtained as follows:

$$F_Y(y) = \left(1 - \exp\left(-\frac{y}{\sigma_h^2}\right)\right)^{N-1} \tag{11}$$

$$= \sum_{k=0}^{N-1} \binom{N-1}{k} (-1)^k \exp\left(-\frac{ky}{\sigma_h^2}\right), \tag{12}$$

$$f_X(x) = \frac{1}{\alpha\sigma_h^2} \exp\left(-\frac{x}{\alpha\sigma_h^2}\right), \tag{13}$$

where the equality in (12) holds due to the binomial theorem [31].

Finally, we can obtain (9) by plugging (12) and (13) into (10). ■

2) CLUSTERING FAILURE PROBABILITY WITH DEFENSE

Now, we focus on deriving the clustering failure probability with the threshold-based defense mechanism, summarized in the following theorem.

Theorem 2: For given N, σ_h^2, α, and β, the clustering failure probability with the threshold-based defense mechanism is given by

$$\begin{aligned} p_{\text{def}} = {} & \left(1 - e^{\left(-\frac{\beta}{\alpha\sigma_h^2}\right)}\right) \sum_{k=0}^{N-1} \binom{N-1}{k} \left(1 - e^{\left(-\frac{\beta}{\sigma_h^2}\right)}\right)^k \\ & \times e^{\left(-\frac{\beta(N-1-k)}{\sigma_h^2}\right)} \\ & \times \eta_\alpha \eta_0^k \sum_{m=0}^{k} \binom{k}{m} \frac{(-1)^m}{\alpha m + 1} \left(1 - e^{\left(\frac{-(\alpha m+1)\beta}{\alpha\sigma_h^2}\right)}\right) \\ & + e^{\left(-\frac{\beta}{\alpha\sigma_h^2}\right)} e^{\left(-\frac{\beta(N-1)}{\sigma_h^2}\right)}, \end{aligned} \tag{14}$$

where $\eta_0 = \left(1 - \exp\left(-\frac{\beta}{\sigma_h^2}\right)\right)^{-1}$ and $\eta_\alpha = \left(1 - \exp\left(-\frac{\beta}{\alpha\sigma_h^2}\right)\right)^{-1}$.

Proof: Let us define the following probability events to derive (14).

- S: an event that the base station fails to form the cluster,
- B: an event of $\alpha|h_0|^2 \le \beta$,
- B^c: a complement of B (i.e., $\alpha|h_0|^2 > \beta$),
- A_k: an event that the number of devices whose CSI is less than or equal to β (i.e., $|h_n|^2 \le \beta$) is exactly k among $N-1$ normal devices.

Then, the clustering failure probability with the threshold-based defense mechanism is expressed as follows:

$$\begin{aligned} p_{\text{def}} &= \sum_{k=0}^{N-1} \Pr[A_k \cap B] \Pr[S \mid A_k \cap B] \\ &\quad + \Pr\left[B^c\right] \Pr\left[S \mid B^c\right] \\ &= \sum_{k=0}^{N-1} \Pr[A_k] \Pr[B] \Pr[S \mid A_k \cap B] \\ &\quad + \Pr\left[B^c\right] \Pr[A_0], \end{aligned} \tag{15}$$

where the second equality holds since the A_k and B are independent events and $\Pr[S \mid B^c]$ is reduced to $\Pr[A_0]$ for given B^c.

Using the fact that $|h_n|^2$ is exponentially distributed with a parameter σ_h^2, we can obtain $\Pr[A_k]$, $\Pr[B]$, and $\Pr[B^c]$ as follows:

$$\Pr[A_k] = \binom{N-1}{k} \left(1 - e^{\left(-\frac{\beta}{\sigma_h^2}\right)}\right)^k e^{\left(-\frac{\beta(N-1-k)}{\sigma_h^2}\right)}, \tag{16}$$

$$\Pr[B] = 1 - e^{\left(-\frac{\beta}{\alpha\sigma_h^2}\right)}, \tag{17}$$

$$\Pr\left[B^c\right] = 1 - \Pr[B] = e^{\left(-\frac{\beta}{\alpha\sigma_h^2}\right)}. \tag{18}$$

Further, we use the following notation: $X = |\hat{h}_0|^2 = \alpha|h_0|^2$ and $W = \max_{n\in\{1,\cdots,k\}} |h_n|^2$. Then, $\Pr[S \mid A_k \cap B]$ is rewritten as follows:

$$\Pr[S \mid A_k \cap B] = \Pr[W < X] = \int_0^\beta F_W(x) f_X(x)\, dx, \tag{19}$$

where $F_W(\cdot)$ and $f_X(\cdot)$ denote the CDF of W and the PDF of X, respectively.

For given A_k and B, X is a truncated exponential random variable and W is a maximum of k truncated exponential random variables [30]. Thus, $F_W(w)$ and $f_X(x)$ are obtained as follows:

$$F_W(w) = \eta_0^k \left(1 - \exp\left(-\frac{w}{\sigma_h^2}\right)\right)^k \tag{20}$$

$$= \eta_0^k \sum_{m=0}^{k} \binom{k}{m} (-1)^m \exp\left(-\frac{mw}{\sigma_h^2}\right), \tag{21}$$

$$f_X(x) = \frac{\eta_\alpha}{\alpha\sigma_h^2} \exp\left(-\frac{x}{\alpha\sigma_h^2}\right), \tag{22}$$

where we consider $\eta_0 = \left(1 - \exp\left(-\frac{\beta}{\sigma_h^2}\right)\right)^{-1}$ and $\eta_\alpha = \left(1 - \exp\left(-\frac{\beta}{\alpha\sigma_h^2}\right)\right)^{-1}$ as factors for truncated distributions.

By plugging (21) and (22) into (23), we can obtain $\Pr[S \mid A_k \cap B]$ as follows:

$$\Pr[S \mid A_k \cap B] = \eta_\alpha \eta_0^k \sum_{m=0}^{k} \binom{k}{m} \frac{(-1)^m}{\alpha m + 1} \left(1 - e^{\left(\frac{-(\alpha m+1)\beta}{\alpha\sigma_h^2}\right)}\right). \tag{23}$$

Finally, we can obtain (14) by plugging (16), (17), (18), and (23) into (15). ∎

Remark 1: The clustering failure probability in (14) is a function of α and β. Thus, the α value should be given in advance to the base station in order to set an optimal β value that minimizes the clustering failure probability against the clustering failure attack. However, the attacker determines the α value and it is unavailable at the base station. For practical use of the defense mechanism, the β value should be set without considering the α value. We have empirically investigated a way of determining suboptimal β values without considering the α value through simulation and it will be discussed in Section V.

B. THRESHOLD AGAINST THE QoS DEGRADATION ATTACK

For the QoS degradation attack, the attacker intentionally reports the *underestimated* CSI (i.e., $|\hat{g}_0|^2$) to the CH. We consider that the base station employs a threshold γ to filter out the underestimated CSI by the attacker during D2D multicasting by the CH. We assume that the base station determines the threshold γ and securely transmits its value to the CH.[4] Thus, the CH is able to consider the following criterion on each CSI feedback from each device to the CH for the defense.

$$|g_n|^2 < \gamma \text{ for } n \in \mathcal{M}. \tag{24}$$

Similarly to the overestimated CSI case (i.e., the clustering failure attack), if there exists any CSI feedback satisfying the condition in (24), then the CH regards such CSI as underestimated feedback by the attacker and excludes a corresponding device from $\mathcal{M}$.

Let $\mathcal{K}$ denote an index set of cluster members considered as sending normal CSI feedback to the CH (i.e., $|g_n|^2 \geq \gamma$). Then, the CH sets data rate of D2D multicasting based on $\mathcal{K}$ and the cluster sum-rate is given by

$$R_{\text{def}}^{\text{sum}} = |\mathcal{K}| \times \log_2\left(1 + \min_{n\in\mathcal{K}} \left\{|g_n|^2\right\} \rho\right). \tag{25}$$

Remark 2: The cluster sum-rate in (25) is dependent on the γ value. For example, if we set too large γ value, the cluster sum-rate is zero since $\mathcal{K}$ can be an empty set (i.e., $|\mathcal{K}| = 0$). Thus, the γ value should be carefully determined. In average sense, we can theoretically determine an optimal γ value using an expected value of the cluster sum-rate in (25), which is given by[5]

$$\begin{aligned}\mathbb{E}\left[R_{\text{def}}^{\text{sum}}\right] = {} & \Pr\left[|\hat{g}_0|^2 \geq \gamma\right] \sum_{m=0}^{N-1} \Pr[|\mathcal{K}| = m] \\ & \times \mathbb{E}\left[(m+1)\log_2\left(1 + \min_{n\in\mathcal{K}} \left\{|g_n|^2, |\hat{g}_0|^2\right\} \rho\right)\right] \\ & + \Pr\left[|\hat{g}_0|^2 < \gamma\right] \sum_{m=1}^{N-1} \Pr[|\mathcal{K}| = m] \\ & \times \mathbb{E}\left[m \log_2\left(1 + \min_{n\in\mathcal{K}} \left\{|g_n|^2\right\} \rho\right)\right].\end{aligned} \tag{26}$$

However, it is difficult to exactly derive the closed-form of (26) and to analytically find an optimal γ value. Instead, similar to β, we have empirically investigated a way of determining suboptimal γ values through simulations and it will be discussed in Section V.

V. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we first introduce an algorithm to set optimal or suboptimal values for β and γ. Then, we evaluate the performance of threshold-based defense mechanisms in terms of clustering failure probability and cluster sum-rate. We investigate the performance by considering two cases: the proposed suboptimal value and the optimal threshold values (i.e., $\beta^\star$ and $\gamma^\star$).

[4] Note that setting γ at the base station can prevent the attacker from learning details of the defense mechanism when it is selected as the CH.

[5] We consider $(m+1)$ in the first term of (26) since the malicious user satisfies the threshold condition (i.e., $\Pr\left[|\hat{g}_0|^2 \geq \gamma\right]$) and thus it is considered together during the cluster sum-rate calculation.

Algorithm 1 shown at the next page describes a procedure to set threshold values (i.e., β^* and γ^*) against both clustering failure attack and QoS degradation attack. Note that we can set optimal threshold values when α is given. However, it is very difficult to accurately predict (or estimate) the value of α. Thus, we alternatively propose to set suboptimal threshold values, as described in lines 8 and 17 of Algorithm 1. Through simulations, we find that the following threshold values are able to provide near-optimal (i.e., suboptimal) performance in terms of the clustering failure probability and the cluster sum-rate, respectively,

$$\beta^* = \sigma_h^2, \tag{27}$$

$$\gamma^* = \frac{1}{5} \times \sigma_g^2. \tag{28}$$

Algorithm 1 Threshold Determination

Input: N, h_n, σ_h^2, g_n, σ_g^2, and α (optional)
Output: β^* or γ^*

1: **if** ready for clustering **then**
2: /* Set β against the clustering failure attack */
3: **if** α is estimated **then**
4: /* α is available */
5: For p_{def} in (14), $\beta^* = \frac{\partial p_{\text{def}}}{\partial \beta}$
6: **else**
7: /* Independent of α */
8: $\beta^* = \sigma_h^2$
9: **end if**
10: **else**
11: /* Set γ against the QoS degradation attack */
12: **if** α is estimated **then**
13: /* α is available */
14: For $\mathbb{E}\left[R_{\text{def}}^{\text{sum}}\right]$ in (26), $\gamma^* = \frac{\partial \mathbb{E}\left[R_{\text{def}}^{\text{sum}}\right]}{\partial \gamma}$
15: **else**
16: /* Independent of α */
17: $\gamma^* = \frac{1}{5} \times \sigma_g^2$
18: **end if**
19: **end if**

Remark 3: Determining the β and γ values based on (27) and (28) does not depend on the attacker's decision on the α value. Thus, the threshold-based defense mechanisms with the proposed beta and gamma values can be practically used against the CSI forgery attacks.

We use MATLAB R2021a (version 9.10.0) for the simulation results, and we consider $N = 5$, $\sigma_h^2 = 1.0$, $\sigma_g^2 = 1.0$, and 1,000,000 iterations by default. In addition, we consider 'CSI forgery' and 'No CSI forgery' schemes for baseline schemes. 'CSI forgery' scheme indicates the performances of CSI forgery attacks when we do not employ the proposed defense mechanism and 'No CSI forgery' scheme indicates the performances when the attacker does not execute CSI forgery (i.e., $\alpha = 1$), respectively.

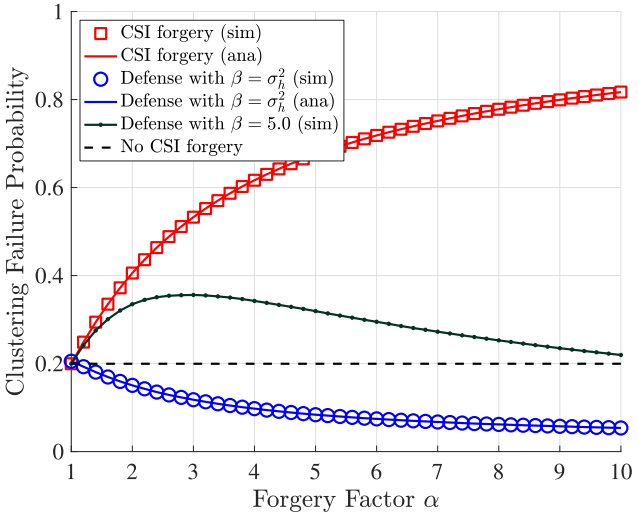
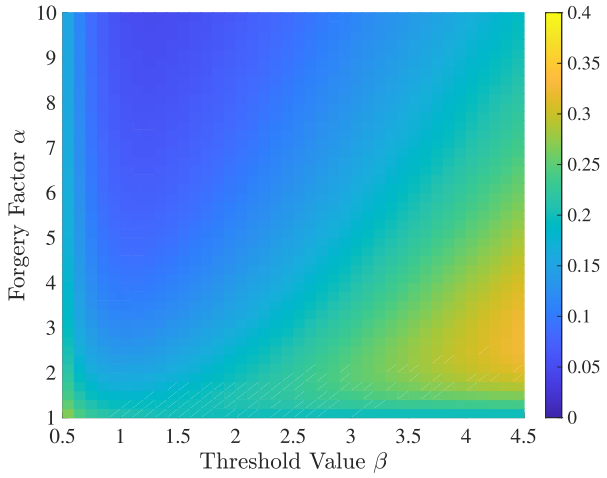


FIGURE 2. Clustering failure probability for varying α.

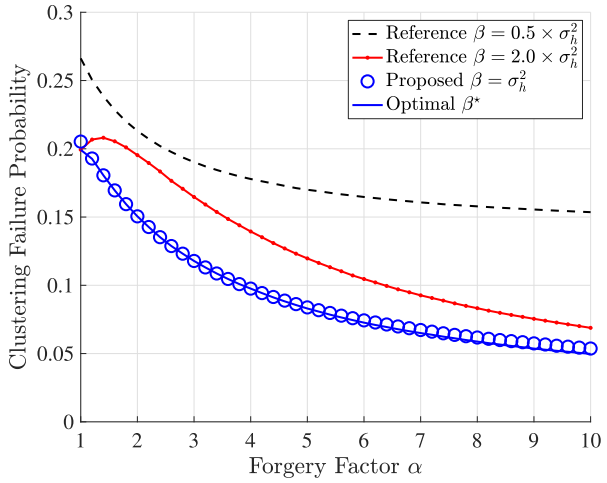
A. IMPACT OF THE CLUSTERING FAILURE ATTACK

Fig. 2 shows the clustering failure probability for varying α. When we do not employ the defense mechanism (i.e., 'CSI forgery' scheme), the clustering failure probability increases as the α value increases since the attacker is selected as the CH with a high probability when the α value is large. When the attacker does not forge the CSI feedback (i.e., 'No CSI forgery'), the clustering failure probability is $\frac{1}{N} = 0.2$ since the attacker only has the chance of being selected as the CH equally with the other normal users. When we consider the defense mechanism with the proposed β value in (27), we can achieve the low clustering failure probability for various α values. However, we should carefully set the β value as the inappropriate β value (e.g., $\beta = 5.0$) will not ensure the effectiveness of the defense mechanism. Note that the simulation ('sim') and analysis ('ana') results are exactly the same. Analytical results of CSI forgery and threshold-based defense schemes are obtained based on (9) and (14) in Theorems 1 and 2, respectively.

Fig. 3 shows two subfigures to determine the suboptimal β values achieving near-optimal performance in terms of the clustering failure probability. Fig. 3a shows the clustering failure probability for varying β and α values. The color of each point represents the probability value for given β and α values: high clustering failure probability colored in yellow and low clustering failure probability colored in deep blue. For all α values, we can find an optimal β value that minimizes the clustering failure probability. Fortunately, we can approximate the optimal $\beta^\star$ value as σ_h^2 proposed in (27). Fig. 3b shows a comparison of the clustering failure probabilities when we consider optimal $\beta^\star$ based on exhaustive searching in Fig. 3a for given the α values, suboptimal β proposed in (27), and two reference threshold values (i.e., $0.5\sigma_h^2$ and $2\sigma_h^2$). Using (27), we can achieve almost near-optimal performance in terms of the clustering failure probability, but we incur a performance loss if threshold values are arbitrarily set. Note that we should carefully verify



(a) Clustering failure probability for varying β and α



(b) A comparison of the clustering failure probability when we consider optimal $\beta^\star$, proposed β in (27), and two reference threshold values (i.e., $0.5\sigma_h^2$ and $2\sigma_h^2$) for varying α

FIGURE 3. The clustering failure probability for various β and α values to determine the suboptimal β values achieving near-optimal performance.

the feasibility of our proposed method to determine suboptimal β value on different simulation parameters such as channel variance σ_h^2.

Fig. 4 compares the clustering failure probabilities using the optimal $\beta^\star$ and proposed β in (27) for different channel variance σ_h^2 values. As we discussed, for any α values, our proposed method to set suboptimal β values can achieve near optimal performance in terms of the clustering failure probability. Note that the absolute error between clustering failure probability using the optimal $\beta^\star$ value and the one using the proposed β value decreases as the α value increases. Thus, the threshold-based defense mechanism with the proposed β value can be practically employed against the clustering failure attack.

B. IMPACT OF THE QoS DEGRADATION ATTACK

Fig. 5 shows the cluster sum-rate for varying α. When the threshold-based defense mechanism is not employed by the

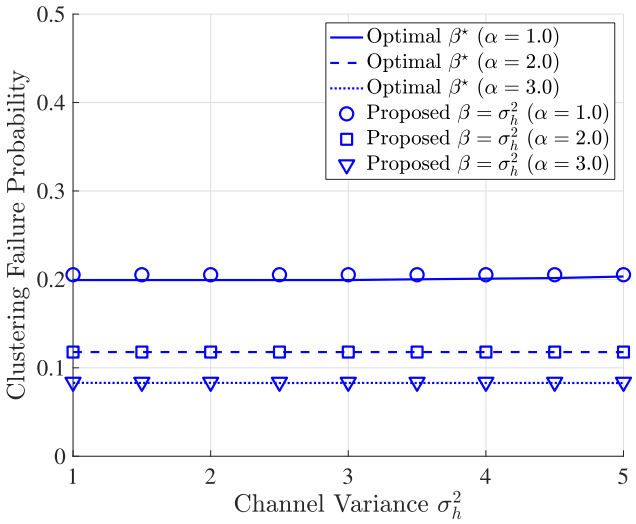


FIGURE 4. A comparison of the clustering failure probability when we consider both optimal $\beta^\star$ and proposed β for varying σ_h^2.

CH, the CH sets the minimum data rate to consider all the CMs in the cluster (i.e., 'CSI forgery' and 'No CSI forgery' schemes). For 'CSI forgery' scheme, the cluster sum-rate decreases as the α value decreases since the CH sets the minimum data rate for CMs based on the attacker's underestimated CSI feedback. 'No CSI forgery' scheme shows the constant cluster sum-rate as the α value decreases since it only considers original CSI feedback by the attacker (i.e., $\alpha = 1.0$) instead of the forged one. When we consider the defense mechanism with the proposed γ value in (28), we can achieve the higher cluster sum-rate compared with baseline schemes. Note that the threshold-based defense mechanism filters out some cluster members satisfying the condition (24) and thus it results in the decrease of the size of served CMs (i.e., $|\mathcal{K}|$ in (25)). However, this filtering effect contributes to increasing the minimum data rate (i.e., $\log_2\left(1 + \min_{n\in\mathcal{K}}\left\{|g_n|^2\right\}\rho\right)$ in (25)). Thus, the cluster sum-rate can increases even if we only consider some of CMs instead of all the CMs. Similarly to setting the β value, we should carefully set the γ value since the effect of defense mechanism varies depending on γ values (e.g., $\gamma = 0.01$ and $\gamma = 1.0$).

Fig. 6 shows two subfigures to determine the suboptimal γ values achieving near-optimal performance in terms of the cluster sum-rate. Fig. 6a shows the cluster sum-rate for varying γ and α values. The color of each point represents the sum-rate for given γ and α values: high sum-rate colored in yellow and low sum-rate colored in deep blue. For all α values, we can find an optimal γ value that maximizes the cluster sum-rate. Similarly to β in (27), we can approximate the optimal $\gamma^\star$ value as $\frac{1}{5}\sigma_g^2$ proposed in (28). Fig. 6b compares the cluster sum-rates when we consider optimal $\gamma^\star$ based on exhaustive searching in Fig. 6a for given α values, suboptimal γ proposed in (28), and two reference threshold values (i.e., $0.1\sigma_g^2$ and $0.5\sigma_g^2$). Note that we can achieve near-optimal performance in terms of the cluster sum-rate using (28), but

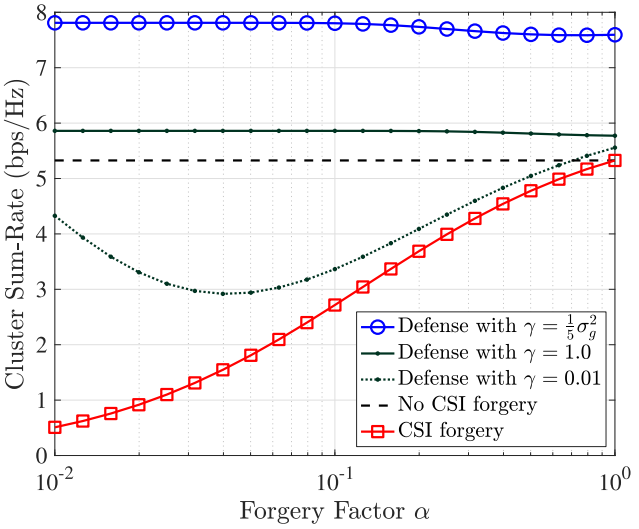
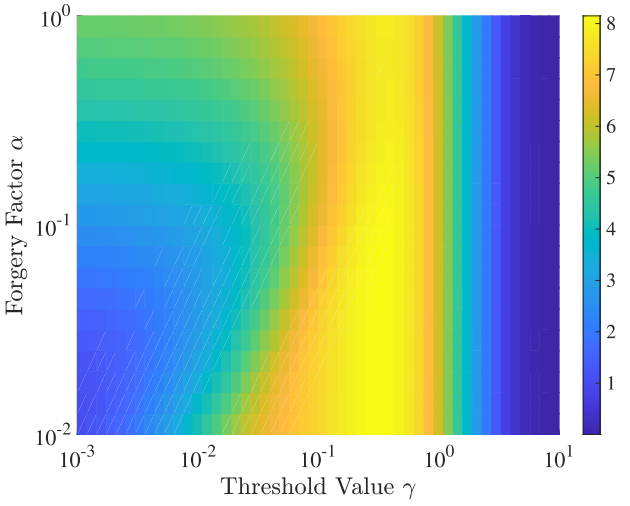
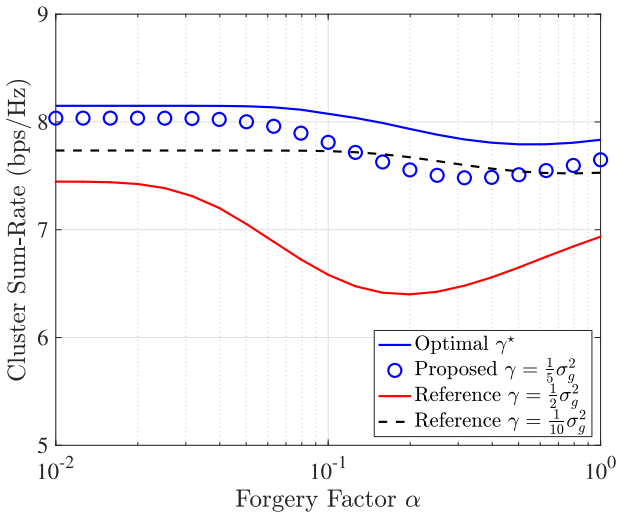


FIGURE 5. Cluster sum-rate for varying α.



(a) Cluster sum-rate for varying γ and α



(b) A comparison of the cluster sum-rate when we consider optimal $\gamma^\star$, proposed γ in (28), and two reference threshold values (i.e., $0.1\sigma_g^2$ and $0.5\sigma_g^2$) for varying α

FIGURE 6. The cluster sum-rate for various γ and α values to determine the suboptimal γ values achieving suboptimal performance.

we incur a performance loss if threshold values are arbitrarily set. Our proposed defense mechanism is suboptimal and thus it shows worse performance in some ranges, compared with the $\gamma = 0.1$ case. Accordingly, we should carefully verify the feasibility of our proposed method to determine suboptimal γ value on different simulation parameters such as channel variance σ_g^2.

Fig. 7 compares the cluster sum-rates using the optimal $\gamma^\star$ and proposed γ in (28) for different channel variance σ_g^2 values. There are no significant differences when we consider the optimal $\gamma^\star$ value and the proposed γ value for various α values. Thus, the threshold-based defense mechanism with the proposed γ value can be practically employed against the QoS degradation attack.

C. DISCUSSIONS

In this subsection, we additionally discuss some issues of our work such as the computational complexity analysis of the threshold-based defense algorithm, advanced attack models, the difficulty of CSI forgery in practice, and limitations.

1) COMPUTATIONAL COMPLEXITY ANALYSIS

Our proposed defense mechanism sets threshold values (i.e., β and γ) based on Algorithm 1. Its calculation depends on the availability of the α value (i.e., the attacker's strategy). We can determine an optimal threshold value (e.g., β) for given α but it requires computations proportional to N^2, based on the derivative of (14) (or (26) in the case of γ). On the other hand, we can determine the suboptimal threshold values (e.g., β) based on (27) (or (28) in the case of γ) and it does not require any further calculation. Thus, the computational complexity of the proposed algorithm is $\mathcal{O}(N^2)$ if α is available and it is reduced to $\mathcal{O}(1)$ if we do not exploit any information for the attacker, where $\mathcal{O}(\cdot)$ denotes big $\mathcal{O}$ notation for computational complexity analysis [32]. Note that we mostly achieve $\mathcal{O}(1)$ in general since the attacker's strategy is unknown in practice.

2) ADVANCED ATTACK MODEL

The complexity of the attack models in the CSI forgery problem varies depending on both the fabrication of CSI and the resulting vulnerability in the systems. For example, instead of clustering failure and performance degradation, CSI forgery can launch more complicated attacks such as eavesdropping if we carefully manipulate forged CSI values. In [17], the authors explored the eavesdropping attack in a novel and practical context in which CSI forgery entangles MU-MIMO scheduling in a many-users regime. The aim of the attacker was to optimize both the eavesdropping opportunity by being selected with the victim and the corresponding decoding

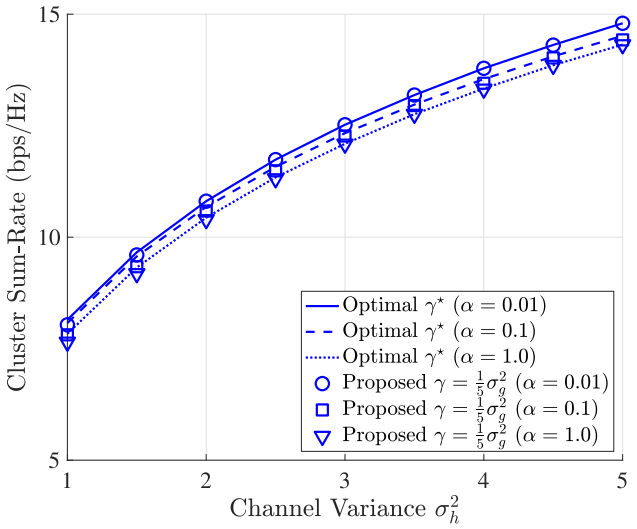


FIGURE 7. A comparison of the cluster sum-rates when we consider both optimal $\gamma^\star$ and proposed γ for varying σ_g^2.

quality. The manipulation of the CSI was done by constructing orthogonal CSI against victims followed by stepwise refinements. In [33], the authors proposed a mathematically formulated strategy for eavesdropping attacks in MU-MIMO systems, called polynomial attack. The attack aims at the messages transmitted to target clients and is launched by exploiting the explicit CSI feedback mechanism in MU-MIMO systems. The eavesdropping attackers can sniff the CSI feedback from target clients, and use them to maliciously forge the feedback to the access points. Note that there are several attack models related to CSI forgery problems and it is important to remember that the CSI forgery attacks can be an initial step to launch the more complicated attacks such as eavesdropping and the denial of service.

3) PRACTICAL ISSUE IN CSI FORGERY

Practically, we need some requirements to successfully launch the CSI forgery attacks. For example, in an experimental setting, the malicious user can execute the CSI forgery attacks using software-defined radio devices such as universal software radio peripheral (USRP) B210 [34]. Thus, it is easy to successfully launch the attacks if software-defined radio (SDR) devices are available to the attacker. On the other hand, in case of using commercial devices instead of SDRs, forging the CSI would be difficult and it might require kernel programming to read (or write) information in hardware modem [35], [36]. It is worth noting that CSI forgery problems are one of the common and important security issues in wireless networks.

4) LIMITATIONS

Threshold-based defense mechanisms have some limitations. First, suboptimal threshold values (i.e., β and γ) might vary depending on various environmental setting, and thus they should be carefully estimated. Second, we assume that it is difficult for the attackers to know the information related to threshold values. However, if this information is available on the attacker's side, then attackers can bypass our defense and cause more severe results to normal users. Thus, more accurate and complicated defense mechanisms should be studied for future work.

VI. CONCLUSION

In this paper, we investigated two CSI forgery attacks (i.e., clustering failure attack and QoS degradation attack) where the malicious user in cellular D2D networks intentionally reports its overestimated or underestimated CSI feedbacks instead of the original one to the base station or to the cluster head. We introduced two metrics to measure the impact of both clustering failure and QoS degradation, caused by CSI forgery attacks. We proposed threshold-based defense mechanisms and further derived a closed-form expression of the clustering failure probability. Furthermore, we proposed to set suboptimal threshold values for defense mechanisms without considering the attacker's decision on the α values. Our future research will focus on exploring more efficient methods of preventing CSI forgery attacks in cluster-based D2D communications, including more complicated attack vectors able to launch more destructive results from CSI forgery problems. In addition, robust defense mechanisms using advanced techniques such as deep learning-based abnormal detection and physical authentication against CSI forgery problems can be further investigated as an extension of our work.

REFERENCES

[1] F. S. Shaikh and R. Wismüller, "Routing in multi-hop cellular device-to-device (D2D) networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2622–2657, 4th Quart., 2018.
[2] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.
[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. Surveys Tuts.*, vol. 20, no. 3, pp. 2133–2168, 3rd Quart., 2018.
[4] D. Wu, L. Zhou, Y. Cai, and Y. Qian, "Collaborative caching and matching for D2D content sharing," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 43–49, Jun. 2018.
[5] D. Wu, L. Zhou, Y. Cai, H.-C. Chao, and Y. Qian, "Physical–social-aware D2D content sharing networks: A provider–demander matching game," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7538–7549, Aug. 2018.
[6] U. Saleem, Y. Liu, S. Jangsher, X. Tao, and Y. Li, "Latency minimization for D2D-enabled partial computation offloading in mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4472–4486, Apr. 2020.
[7] X. Liu, Z. Li, W. Meng, G. Gui, Y. Chen, F. Adachi, and N. Zhao, "Transceiver design and multihop D2D for UAV IoT coverage in disasters," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1803–1815, Apr. 2019.
[8] L. Yang, D. Wu, S. Xu, G. Zhang, and Y. Cai, "Social-energy-aware user clustering for content sharing based on D2D multicast communications," *IEEE Access*, vol. 6, pp. 36092–36104, 2018.
[9] H. Zheng, S. Hou, Z. Song, Y. Hao, and H. Li, "Power allocation and user clustering for uplink MC-NOMA in D2D underlaid cellular networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1030–1033, Dec. 2018.
[10] 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 Things J.*, vol. 6, no. 5, pp. 8645–8657, Oct. 2019.
[11] M. Gharbieh, A. Bader, H. ElSawy, H. Yang, M. Alouini, and A. Adinoyi, "Self-organized scheduling request for uplink 5G networks: A D2D clustering approach," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1197–1209, Feb. 2019.

[12] O. N. Hamoud, T. Kenaza, and Y. Challal, "Security in device-to-device communications: A survey," *IET Netw.*, vol. 7, no. 1, pp. 14–22, Jan. 2018.
[13] D. Barik, J. Sanyal, and T. Samanta, "Denial-of-service attack mitigation in multi-hop 5G D2D wireless communication networks employing double auction game," *J. Netw. Syst. Manage.*, vol. 31, no. 1, pp. 1–30, Mar. 2023.
[14] R. Hajian, A. Haghighat, and S. H. Erfani, "A secure anonymous D2D mutual authentication and key agreement protocol for IoT," *Internet Things*, vol. 18, May 2022, Art. no. 100493.
[15] V. Balaji and P. Selvaraj, "Gray-hole attack minimization in IoMT with 5G based D2D networks," *Comput. Syst. Sci. Eng.*, vol. 42, no. 3, pp. 1289–1303, 2022.
[16] Y.-C. Tung, S. Han, D. Chen, and K. G. Shin, "Vulnerability and protection of channel state information in multiuser MIMO networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 775–786.
[17] 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 Conf. Comput. Commun.*, Apr. 2019, pp. 1963–1971.
[18] X. Wang, M. Tao, and Y. Xu, "Analysis of false CSI attack by a malicious user in OFDMA networks," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2012, pp. 1–5.
[19] C.-H. Yu, K. Doppler, C. B. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2752–2763, Aug. 2011.
[20] N. Lee, X. Lin, J. G. Andrews, and R. W. Heath Jr., "Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 1–13, Jan. 2015.
[21] 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.
[22] Z. Zhang, Y. Sun, A. Sabharwal, and Z. Chen, "Impact of channel state misreporting on multi-user massive MIMO scheduling performance," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2018, pp. 917–925.
[23] Y. Yang, Y. Chen, W. Wang, and G. Yang, "Securing channel state information in multiuser MIMO with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3091–3103, May 2020.
[24] 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 Conf. Comput. Commun.*, May 2022, pp. 140–149.
[25] D. Lin, S. Hu, Y. Gao, and W. Tang, "Heuristic-learning-based network architecture for device-to-device user access control," *IEEE Commun. Mag.*, vol. 57, no. 11, pp. 96–101, Nov. 2019.
[26] M. Roopak, G. Y. Tian, and J. Chambers, "Multi-objective-based feature selection for DDoS attack detection in IoT networks," *IET Netw.*, vol. 9, no. 3, pp. 120–127, May 2020.
[27] Y. Ran, H. Al-Shwaily, C. Tang, G. Y. Tian, and M. Johnston, "Physical layer authentication scheme with channel based tag padding sequence," *IET Commun.*, vol. 13, no. 12, pp. 1776–1780, Jul. 2019.
[28] F. Kara and H. Kaya, "Threshold-based selective cooperative NOMA: Capacity/outage analysis and a joint power allocation-threshold selection optimization," *IEEE Commun. Lett.*, vol. 24, no. 9, pp. 1929–1933, Sep. 2020.
[29] X. Ding and Y. Wang, "Misbehavior detection and optimal threshold analysis in DF cooperative relay networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2718–2721, Dec. 2021.
[30] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stocahstic Processes*. New York, NY, USA: McGraw-Hill, 2002.
[31] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*. London, U.K.: Academic, 2003.
[32] D. E. Knuth, "Big omicron and big Omega and big theta," *ACM SIGACT News*, vol. 8, no. 2, pp. 18–24, Apr./Jun. 1976.
[33] X. Wang, Y. Liu, X. Lu, S. Lv, Z. Shi, and L. Sun, "On eavesdropping attacks and countermeasures for MU-MIMO systems," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 40–45.
[34] *Ettus Research USRP B210*. Accessed: Dec. 6, 2022. [Online]. Available: https://www.ettus.com/all-products/ub210-kit/
[35] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11 n traces with channel state information," *ACM SIGCOMM CCR*, vol. 41, no. 1, p. 53, 2011.
[36] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity WiFi," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2015, pp. 53–64.

INKYU BANG (Member, IEEE) received the B.S. degree in electrical and electronic engineering from Yonsei University, Seoul, South Korea, in 2010, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2012 and 2017, respectively. He was a Research Fellow with the Department of Computer Science, National University of Singapore (NUS), from 2017 to 2019. From March 2019 to July 2019, he was a Senior Researcher with the Agency for Defense Development (ADD), Daejeon. He is currently an Associate Professor with the Department of Intelligence Media Engineering (Adjunct with the Department of Information and Communication Engineering), Hanbat National University, Daejeon. His research interests include information-theoretic security (physical-layer security), wireless network security, 6G/5G/IoT, satellite communications, and deep learning application in wireless communications.

VENISSA ADZO SEDEM MANYA (Student Member, IEEE) received the B.S. degree in telecommunications engineering from the Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana, in 2020. She is currently pursuing the M.S degree with the Department of Intelligence Media Engineering, Hanbat National University, Daejeon, South Korea. Her research interests include wireless network security and device-to-device (D2D) communication in cellular networks.

JONGHYUN KIM (Member, IEEE) received the Ph.D. degree in computer science from The University of Oklahoma, Norman, OK, USA, in 2005. He was a Researcher with Samsung Electronics, from 1995 to 1997. He is currently a Principal Researcher with the Electronics Telecommunications Research Institute (ETRI), Daejeon, South Korea. He is also working as a Project Leader of the Intelligence Security Group, ETRI. He is involved in standardization activities as the vice chair of WP1 and a rapporteur of Q.4 (cybersecurity) in ITU-T Study Group 17. His research interests include information security, cyber security, cloud security, AI-based malware detection, and 5G/6G security.

TAEHOON KIM (Member, IEEE) received the B.S. degree in media communications engineering from Hanyang University, Seoul, South Korea, in 2011, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2013 and 2017, respectively. From September 2017 to February 2020, he was a Senior Researcher with the Agency for Defense Development (ADD), South Korea. He is currently an Associate Professor with the Department of Computer Engineering, Hanbat National University, Daejeon. His research interests include wireless communications, resource management for 5G/IoT, machine learning applications in wireless communications, wireless network security, and satellite communications.