Covert Communications for a Disguised Full-Duplex Vehicle With Channel Distribution Information

Refat Khan, Jihwan Moon*

Hanbat National Univ.

refatkhanuits@gmail.com, *anschino@staff.hanbat.ac.kr

채널 분포 정보를 활용한 위장 전이중 통신 차량용 은닉 통신

Refat Khan, 문지환*
국립한밭대학교

Abstract

In this paper, we investigate a covert communications system that consists of a source vehicle communicating with a disguised full-duplex (FD) destination node. Supposedly receive-only, the destination vehicle covertly transmits confidential messages to a hidden vehicle while avoiding the surveillance of a warden vehicle. With channel uncertainty of the warden vehicle, we derive the lower bound of the expected minimum detection error probability (DEP) at the warden vehicle. Numerical results present the covert rate performance for different DEP requirements.

Ⅰ. Introduction

An opponent may utilize the nature of transmission to carry out a traffic analysis by collecting metadata, e.g., the source and destination addresses. These threats call for covert communications or low-probability-of-detection communications [1].

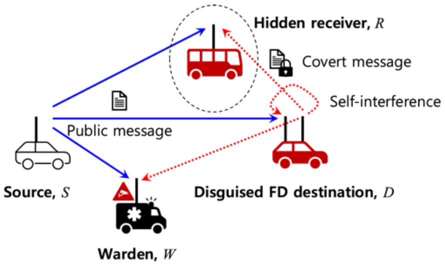
In this paper, we investigate a covert communications system that consists of a source vehicle communicating with a disguised full-duplex (FD) destination vehicle. Supposedly receive-only, the destination vehicle covertly transmits confidential messages to a hidden vehicle while avoiding the surveillance of a warden vehicle. With channel uncertainty of the warden vehicle, we derive the lower bound of the expected minimum detection error probability (DEP) at the warden vehicle. Numerical results present the covert rates for different DEP requirements.

Ⅱ. Method

The source vehicle S delivers a public message to the destination vehicle D. At the same time, the seemingly receive-only destination vehicle carries out a covert transmission through an unseen antenna to the hidden receiver R in FD while the warden vehicle W surveils suspicious communications. The received signal at the disguised FD destination can be written as

$$y_D = h_{SD}\sqrt{P_S}x_P + \tilde{h}_{DD}\sqrt{P_D}x_C + z_D$$

Here, $x_P \sim CN(0,1)$ and $x_C \sim CN(0,1)$ specify the public and covert messages, respectively, P_D and P_S stand for the transmit power at the destination and source, respectively, $\tilde{h}_{DD} \sim CN\left(0,\sigma_{\mathrm{SI}}^2\right)$ denotes the residual self-interference channel, and $z_X \sim CN(0,\sigma_X^2)$ means the additive noise at node $X \in \{D,R,W\}$.



We consider the uncertainty on the D−W channel as

$$h_{DW} = \sqrt{\rho}\bar{h}_{DW} + \sqrt{1-\rho}\tilde{h}_{DW}$$

in which h_{DW}, $\bar{h}\_DW$ and $\tilde{h}_{DW} \sim CN(0,L_{DW})$ represent the ground-truth channel, estimated channel, and estimation error, respectively, with $\rho \in [0,1]$ denoting the level of estimation.

The achievable public data rate $\bar{r}_{P,D}$ is calculated as

$$\bar{r}_{P,D} = \log_2\left(1 + \frac{|h_{SD}|^2 P_S}{\left|\tilde{h}_{DD}\right|^2 P_D + \sigma_D^2}\right)$$

As for the hidden receiver, both a direct-link public message from the source vehicle and a covert message from the destination vehicle are received as

$$y_R = h_{SR}\sqrt{P_S}x_P + h_{DR}\sqrt{P_D}x_C + z_R$$

The hidden receiver then decodes and eliminates public messages in prior to recovering covert messages. For successful decoding of public messages, it is required that the public data rate be limited by its achievable amount $\bar{r}_{P,R}$ as

$$\bar{r}_{P,R} = \log_2\left(1 + \frac{|h_{SR}|^2 P_S}{|h_{DR}|^2 P_D + \sigma_R^2}\right)$$

Therefore, the achievable covert rate after removing x_P from y_R is expressed by

$$r_{C,R} = \log_2\left(1 + \frac{|h_{DR}|^2 P_D}{\sigma_R^2}\right)$$

During communications, the warden vehicle receives

$$y_W = h_{SW}\sqrt{P_S}x_P + h_{DW}\sqrt{P_D}x_C + z_W$$

In this work, we take a conservative assumption that the warden vehicle perfectly knows necessary parameters such as h_{SW}, h_{WD}, P_S. Upon this worst-case assumption, the warden node first removes public messages from y_W and obtain the effective residual signal $\tilde{z}_W \triangleq y_W - h_{SW}\sqrt{P_S}x_P$. We then have null and alternative hypotheses as

$$H_0: \tilde{z}_W = z_W$$
$$H_1: \tilde{z}_W = h_{DW}\sqrt{P_D}x_C + z_w$$

The null hypothesis H_0 represents an event that a covert message is not transmitted, and the alternative hypothesis H_1 indicates the other event where the disguised FD destination vehicle sent a convert message. Using a radiometer [1], the sufficient test statistic T for the hypotheses after observing $N \to \infty$ transmissions becomes $E[|\tilde{z}_W|^2]$ as

$$H_0: T = \sigma_W^2$$
$$H_1: T = |h_{DW}|^2 P_D + \sigma_W^2$$

The warden vehicle decides that a covert link exists if $T \geq \tau$ and otherwise when $T < \tau$ for threshold τ.

We consider the noise uncertainty at the warden vehicle as in [1]. Hence, $\sigma_{W,\text{dB}}^2 \sim U\left(\bar{\sigma}_{W,\text{dB}}^2 - \zeta_{\text{dB}}, \bar{\sigma}_{W,\text{dB}}^2 + \zeta_{\text{dB}}\right)$ in decibel scale with $\bar{\sigma}_{W,\text{dB}}^2$ and $\zeta_{\text{dB}} \geq 0$ being the mean and maximum range, respectively. The resulting DEP $\Pr(\text{e})$ is then calculated by

$$\Pr(\text{e}) = \underbrace{\Pr(T \geq \tau|H_0)}_{\text{False alarm}}\Pr(H_0) + \underbrace{\Pr(T < \tau|H_1)}_{\text{Miss}}\Pr(H_1)$$

with random $\Pr(H_0) = \Pr(H_1) = 0.5$ [1][2].

τ that minimizes the DEP is obtained from [1] as

$$\tau^\star = |h_{DW}|^2 P_D + \frac{\bar{\sigma}_W^2}{\zeta}$$

and the resulting minimum DEP becomes [1]

$$\Pr(\text{e})|_{\tau=\tau^\star} = \frac{1}{2}\left(1 - \frac{1}{2\ln\zeta}\left(\ln\frac{\tau^\star}{\tau^\star - |h_{DW}|^2 P_D}\right)\right)$$

We then optimize the following problem:

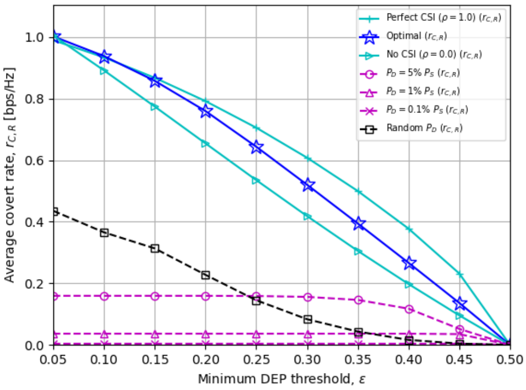
$$\begin{aligned}
(\text{P1}):\ &\max_{P_D, r_P} r_{C,R} \\
\text{subject to:}\ &\bar{r}_P \leq r_P \leq \min\left(\bar{r}_{P,R}, \bar{r}_{P,D}\right) \\
&\mathrm{E}_{h_{DW}}[\Pr(\text{e}|h_{DW})|_{\tau=\tau^\star}] \geq \varepsilon \\
&\zeta\bar{\sigma}_W^2 \geq |h_{DW}|^2 P_D + \bar{\sigma}_W^2/\zeta \\
&0 \leq P_D \leq \bar{P}_D
\end{aligned}$$

It is analytically intractable to find the exact expectation of the DEP. We thus resort to Jensen's inequality [2] by noting the concavity of the logarithm

$$\mathrm{E}_{h_{DW}}[\Pr(\text{e}|h_{DW})|_{\tau=\tau^\star}]$$
$$\geq \frac{1}{2}\left(1 - \frac{1}{2\ln\zeta}\left(\ln\frac{\left(\rho\left|\bar{h}_{DW}\right|^2 + (1-\rho)L_{DW}\right)P_D\zeta + \bar{\sigma}_W^2}{\bar{\sigma}_W^2}\right)\right)$$

which provides a lower bound of the expected DEP.

The performance figure presents the average worst-case covert rate with perfect and imperfect CSI when the minimum DEP threshold changes. The importance of obtaining decent CSI for performance is highlighted.



Ⅲ. Conclusion

In this paper, we investigated a covert communications system that consists of a source vehicle communicating with a disguised FD destination node. With channel uncertainty of the warden vehicle, we derived the lower bound of the expected minimum DEP at the warden vehicle. The importance of decent channel information for performance was highlighted.

ACKNOWLEDGMENT

This research was partially supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2021R1I1A3050126)

This work was partially supported by Korea Research Institute for defense Technology planning and advancement(KRIT) grant funded by the Korea government(DAPA(Defense Acquisition Program Administration)) (21-106-A00-007, Space-Layer Intelligent Communication Network Laboratory, 2022)

This research was partially supported by the MSIT (Ministry of Science and ICT), Korea, under the ICAN (ICT Challenge and Advanced Network of HRD) program (IITP-2024-RS-2022-00156212) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation).

REFERENCES

[1] Jihwan Moon, "Disguised Full-Duplex Covert Communications," Sensors, vol. 23, no. 14, p. 6515, Jul. 2023.

[2] Jihwan Moon, "The Channel Uncertainty of Warden on Disguised Full-Duplex Covert Communications," The Journal of Korean Institute of Communications and Information Sciences (J-KICS), Nov. 2023.