증폭 후 전송 중계기 기반 차량 간 은닉 통신

MD Sakil Hasan, 문지환*
국립한밭대학교

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

Amplify-and-Forward Relay-Aided Vehicular Covert Communications

MD Sakil Hasan, Jihwan Moon*
Hanbat National Univ.

요 약

In this paper, we study vehicular covert communications in an amplify-and-forward (AF) relay system. Along with a public message to a destination node via an AF relay, a source node attempts to transmit a covert message while evading the surveillance of the AF relay. We derive and minimize the detection error probability (DEP) of the covert message detector at the AF relay. The numerical results present the covert rates for different DEP requirements.

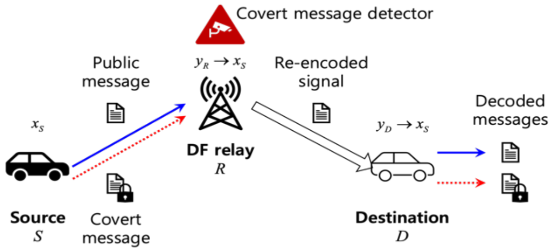
Ⅰ. 서 론

The recent advance in vehicular communications has enabled various applications that enrich our livings [1]. Meanwhile, although the combination of cryptography and physical layer security may successfully hinder adversaries from eavesdropping, one may require a higher level of security in which the existence of vehicular communications should also be concealed. An opponent, instead of the actual information, would make use of the nature of transmission and carry out a traffic analysis by collecting metadata such as the source and destination addresses of packets. These threats called for covert communications or low-probability-of-detection communications.

In this paper, we study vehicular covert communications strategies in an amplify-and-forward (AF) relay system. Along with a public message to a destination node via an AF relay, a source node attempts to transmit a covert message while evading the surveillance of the AF relay. We derive and minimize the detection error probability (DEP) of the covert message detector at the AF relay. The numerical results present the covert rates for different DEP requirements.

Ⅱ. 본론

The source node S and the destination node D communicates via the relay R. We make an assumption that a direct link between the source and destination nodes is absent due to environmental conditions, such as being located in shadowed areas or being separated by a considerable distance. In addition to transmitting public messages, the source node also attempts to transmit a covert message and wishes that the covert message detector incorporated within the relay fails to identify it. The received signal at the relay is written as



$$y_R = h_{SR}\sqrt{P_S}\left(\sqrt{\alpha}x_P + \sqrt{1-\alpha}x_C\right) + z_R$$

where $x_P \sim CN(0,1)$ and $x_C \sim CN(0,1)$ indicate the public and covert messages, respectively, P_S means the source transmit power, α controls the proportion of P_S for x_P, and $z_R \sim CN(0,\sigma_R^2)$ denotes the additive noise. As in [1], we assume that the noise variance varies uncertainly in this work such that $\sigma_{R,\text{dB}}^2 \sim U\left(\bar{\sigma}_{R,\text{dB}}^2 - \zeta_{\text{dB}}, \bar{\sigma}_{R,\text{dB}}^2 + \zeta_{\text{dB}}\right)$ in decibel range. It is assumed that every node keeps the global channel state information (CSI) since the covert transmission occurs internally under the normal operation of relay.

The destination receives an amplified version of y_R from the AF relay as

$$y_D = h_{RD}\sqrt{P_R}x_R + z_D$$

where $x_R = y_R/\sqrt{|h_{SR}|^2 P_S + \sigma_R^2}$ represents the normalized unit-power signal from the AF relay. With some manipulations, we can derive the achievable rates for the public and covert messages as

$$r_{P,\mathrm{AF}} = \log_2\left(1 + \frac{|h_{SR}|^2 P_S \alpha}{|h_{SR}|^2 P_S(1-\alpha) + \sigma_R^2 + \tilde{\sigma}_D^2}\right)$$

$$r_{C,\mathrm{AF}} = \log_2\left(1 + \frac{|h_{SR}|^2 P_S(1-\alpha)}{\sigma_R^2 + \tilde{\sigma}_D^2}\right)$$

where $\tilde{\sigma}_D^2 = (|h_{SR}|^2 P_S + \sigma_R^2)\sigma_D^2/(|h_{RD}^2|P_R)$.

The covert message detector at the AF relay is designed to identify the presence of any additional messages apart from the public message. To achieve this, it first removes the public message from the received signal y_R. This process results in an effective residual signal $\tilde{z}_R \triangleq y_R - h_{SR}\sqrt{P_S}x_P$ assuming that the relay perfectly knows h_{SR} and P_S [1]. We then establish null and alternative hypotheses as

$$H_0\colon \tilde{z}_R = z_R$$

$$H_1\colon \tilde{z}_R = h_{SR}\sqrt{P_S}\left(\left(\sqrt{\alpha}-1\right)x_P + \sqrt{1-\alpha}x_C\right) + z_R$$

where the null hypothesis H_0 represents an event that the source node did not transmit a covert message, and the alternative hypothesis H_1 denotes an event that a covert message exists. With a radiometer [1] as a detection measure, the detector can utilize the sufficient test statistic T for the hypotheses after collecting an $N \to \infty$ number of ample signals, which reduces to the average power $\mathrm{E}[|\tilde{z}_R|^2]$ as

$$H_0\colon T = \sigma_R^2$$

$$H_1\colon T = 2|h_{SR}|^2 P_S\left(1-\sqrt{\alpha}\right) + \sigma_R^2$$

and the covert message detector decides that a covert link exists if $T \geq \tau$ for some threshold τ.

The DEP $\Pr(\mathrm{e})$ is composed of false alarm and miss probabilities as

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

where the detector assumes that the covert transmission occurs at random, i.e., $\Pr(H_0) = \Pr(H_1) = 0.5$. The threshold τ minimizing the DEP can be obtained from [2] as

$$\tau^\star = 2|h_{SR}|^2 P_S\left(1-\sqrt{\alpha}\right) + \frac{1}{\zeta}\bar{\sigma}_R^2$$

and the corresponding minimum DEP is given by [2]

$$\Pr(\mathrm{e})\,|_{\tau=\tau^\star} = \frac{1}{2}\left(1 - \frac{1}{2\ln\zeta}\left(\ln\frac{\tau^\star}{\tau^\star - 2|h_{SR}|^2 P_S\left(1-\sqrt{\alpha}\right)}\right)\right)$$

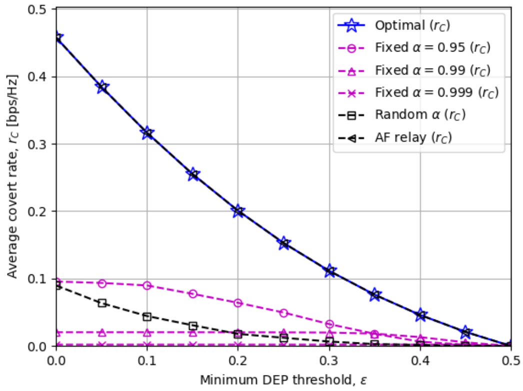
as long as $\zeta\bar{\sigma}_R^2 \geq 2|h_{SR}|^2 P_S\left(1-\sqrt{\alpha}\right) + \bar{\sigma}_R^2/\zeta$. Note that $\tau^\star$ yields the worst-case minimum DEP assuming that the detector uses the exact value of α.

We then optimize the following problem:

$$\begin{aligned} &(\mathrm{P1})\colon \max_{\alpha} r_{C,\mathrm{AF}}|_{\sigma_R^2=\zeta\bar{\sigma}_R^2} \\ &\textit{subject to}\colon r_{P,\mathrm{AF}}|_{\sigma_R^2=\zeta\bar{\sigma}_R^2} \geq \bar{r}_P \\ &\qquad \Pr(\mathrm{e})\,|_{\tau=\tau^\star} \geq \varepsilon \\ &\qquad \zeta\bar{\sigma}_R^2 \geq 2|h_{SR}|^2 P_S\left(1-\sqrt{\alpha}\right) + \bar{\sigma}_R^2/\zeta \\ &\qquad 0 \leq \alpha \leq 1 \end{aligned}$$

We maximize the worst-case covert rate subject to the worst-case rate for public messages by setting the noise variance at the AF relay to $\sigma_R^2 = \zeta\bar{\sigma}_R^2$.

The performance figure presents the average worst-case covert rate of compress-and-forward (CF) (blue star marker) and AF relay (black left triangle marker) when the minimum DEP threshold changes. It can be observed that both of the CF and AF relay covert communications exhibit the identical performance. Also, the optimal worst-case covert rate monotonically decreases as the required threshold increases and becomes zero when perfect DEP of 0.5 is desired.



III. 결론

In this paper, we studied vehicular covert communications strategies in an AF relay system. We derived and minimized the DEP of the covert message detector at the AF relay. The numerical results presented that the covert rate performance is equivalent for CF and AF relays.

.

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).

참 고 문 헌

[1] Jihwan Moon, "Performance Comparison of Relay-Based Covert Communications: DF, CF and AF," Sensors, vol. 23, no. 21, p. 8747, Oct. 2023.

[2] Jihwan Moon, "Covert Communications in a Compress-and-Forward Relay System," accepted for ICT Express.