A Two-Way Secrecy Scheme for the Scalar Broadcast Channel with Internal Eavesdroppers
Chee Yen Leow, Dennis L. Goeckel and Kin K. Leung

Abstract
In a broadcast channel where idle users are internal eavesdroppers, the secrecy capacity approaches zero when the number of users is large. We propose a two-way secrecy scheme to improve the secrecy capacity and analyse it in large network. The proposed scheme makes use of the forward and backward channels to transmit a secret key and a one-time pad encoded secret message. Relays are also used to prevent the eavesdropper from gaining an advantage of multi-user diversity. Analytical and simulation results justify that the proposed two-way secrecy scheme achieves positive secrecy rate even when the number of users approaches infinity.

I. Introduction
In a wireless scalar broadcast channel, opportunistic transmission where the source transmits to the user with the best instantaneous channel gain is sum-rate optimal due to multi-user diversity gain. However, [1] shows that multi-user diversity could be detrimental to secrecy capacity. In particular, [1] studies the secrecy capacity of the opportunistic broadcast with $K$ users using Wyner wiretap coding [2]. We want only the legitimate user to be able to decode the message, thus the $K-1$ idle users are potential eavesdroppers in the network. As $K$ goes to infinity, the secrecy capacity reduces to zero, due to the fact that the channel gain of the best eavesdropper approaches the channel gain of the active user (legitimate user). The problem worsens in non-opportunistic broadcast where the active user does not necessarily have the best channel. In this case, only eavesdroppers benefit from multi-user diversity. As a result, the secrecy capacity goes to zero when $K$ is large.

In this paper, we propose a two-way secrecy scheme for the scalar broadcast channel with internal eavesdroppers. The propose scheme leverages multi-user diversity to achieve positive secrecy capacity in the network even when the number of users is large. We consider the scalar broadcast channel under opportunistic and non-opportunistic transmissions. In opportunistic broadcast, the proposed two-way secrecy scheme utilises forward and backward channels between the source and the legitimate user to communicate secret messages. The proposed scheme is then generalised to non-opportunistic broadcast. In non-opportunistic broadcast, the proposed scheme invites a pair

Chee Yen Leow and Kin K. Leung are with Dept. of Electrical & Electronic Engineering, Imperial College London, SW7 2AZ, UK. Dennis L. Goeckel is with Dept. of Electrical & Computer Engineering, University of Massachusetts, Amherst, MA 01003, US. The review category is C. Networks : 3. Network Information Theory. The Point of Contact is Dennis L. Goeckel, Tel:(413) 545-3514, Email: goeckel@ecs.umass.edu
of idle users as relays and utilises forward and backward channels of source-to-relay and relay-to-destination to forward secret messages. The performance of the proposed scheme under the effect of Rayleigh fading and path loss are studied. Analytical and simulation results verify that the proposed scheme is able to achieve non-zero secrecy capacity even when the number of users is large.

II. PROTOCOL FOR OPPORTUNISTIC BROADCAST

The proposed two-way secrecy scheme makes use of the forward and backward channels between the source and the legitimate user to average out the channel gain of the best eavesdropper in order to achieve positive secrecy rate. The proposed scheme can be described in two time slots. In the first time slot, the legitimate user transmits a secret key, \( x \) encoded with wiretap codes to the source node at a secrecy rate \( r_s \). The source node decodes the secret key and uses it as a one-time pad for the secret message intended for the legitimate user. In the second time slot, the source node broadcasts the secret message \( m \) using wiretap codes at secrecy rate \( r_s \). Since the legitimate user has the knowledge of the secret key \( x \) and the one-time pad encoded message \( m \), the secret message can be decoded. The eavesdroppers are not able to decode the secret message unless they have the knowledge of both \( x \) and \( m \). The protocol only needs to ensure that the eavesdroppers would not be able to decode either \( x \) or \( m \).

Using extreme value theory, the secrecy rate \( r_s \) when \( K \rightarrow \infty \) is summarised in the following theorem.

**Theorem 1.** Assuming wiretap coding, unit transmission power and i.i.d. Rayleigh fading, the achievable secrecy rate of the proposed two-way secrecy scheme under opportunistic broadcast converges to \( r_s = 1 \) bits/s/Hz as \( K \rightarrow \infty \).

III. PROTOCOL FOR NON-OPPORTUNISTIC BROADCAST

The proposed two-way secrecy scheme is generalised to non-opportunistic broadcast. The proposed protocol makes use of the two-way secrecy scheme developed in the previous section and employs two idle users to relay the secret messages from the source to the destination to achieve a positive secrecy rate. The protocol ensures that the secret messages are hidden from all idle users (internal eavesdroppers), including the relays which help to forward the source messages.

A secret message \( d \) is demultiplexed into two data streams, \( b \) and \( c \), such that \( d = b \oplus c \). The proposed protocol can be described in two phases. In each phase, the two-way secrecy scheme proposed in the previous section is used to communicate the secret message, i.e. message \( b \) and \( c \) in first phase and second phase respectively. In the first phase, three time slots are used. See fig. 1. In particular, in the first time slot, the first relay, \( R_1 \) sends a wiretap encoded secret key \( \tilde{b} \) to the source, \( S \) and destination, \( M \) at rate \( r_s \). The source then broadcasts the one-time pad encoded source message and secret key, \( m_1 = b \oplus \tilde{b} \) using wiretap coding at rate \( r_s \). In the third time slot, the
relay $R_1$ forwards $m_1$ to the destination using wiretap coding at rate $r_s$. A similar process is repeated in the second phase, for the source to communicate message $c$ to the destination with the help of relay $R_2$. The destination is able to recover the secret message $d$ using the knowledge of $m_1$, $m_2$, $\tilde{b}$ and $\tilde{c}$, since $d = m_1 \oplus \tilde{b} \oplus m_2 \oplus \tilde{c}$. The protocol only needs to ensure that eavesdroppers and relays would miss one of the required messages, $m_1$, $m_2$, $\tilde{b}$ and $\tilde{c}$.

Using extreme value theory, the secrecy rate $r_s$ when $K \to \infty$ is summarised in the following theorem.

**Theorem 2.** Assuming wiretap coding, unit transmission power and i.i.d. Rayleigh fading, the achievable secrecy rate of the proposed two-way secrecy scheme under non-opportunistic broadcast converges to $r_s = \log_2 \frac{3}{2}$ bits/s/Hz as $K \to \infty$.

### IV. Conclusion

A two-way secrecy scheme which combines a one-time pad and wiretap coding is proposed for the scalar broadcast channel. Analytical results shows that a positive secrecy rate is achievable when $K$ approaches infinity, under both opportunistic and non-opportunistic broadcast.

### References
