Interference with Overhearing for Secure Ad-Hoc Networks

Isamu SHIMADA and Hiroaki HIGAKI∗

Department of Robotics and Mechatronics Tokyo Denki University 5 Senju-Asahimachi,
Adachi-ku, Tokyo, Japan

*Corresponding author

Keywords: Ad-Hoc networks, Interfering overhearing, Noise wireless signals, Intentional collisions,
Routing protocol.

Abstract. In ad-hoc networks, data messages are transmitted from a source wireless node to a
destination one along a wireless multihop transmission route consisting of a sequence of
intermediate wireless nodes. Each intermediate wireless node forwards data messages to its next-
hop wireless node. Here, a wireless signal carrying the data message is broadcasted by using an
omni antenna and it is not difficult for a eavesdropper wireless node to overhear the wireless signal
to get the data message.

Introduction

A wireless transmission route consists of a sequence of intermediate wireless nodes which
forward data messages from its previous-hop wireless node to its next-hop one. Each intermediate
wireless node broadcasts a wireless signal for the data message transmission by using an omni
directional antenna. Hence, it is possible for all its neighbor wireless nodes within its wireless
transmission range to receive the data message. That is, the neighbor wireless node, even if it is an
eavesdropper, overhears the data message. The next section overviews related works. Our proposal
for interfering the overhearing by eavesdropper wireless nodes by cooperation with neighbor
wireless nodes of each intermediate one is shown in Section 3. Both the routing and the data
message transmission protocols are proposed. Section 4 evaluated our proposed method in
simulation experiments.

Related Works

One of such methods makes difficult for eavesdropper wireless nodes to overhear the transmitted
secure wireless data message transmission under assumptions that beam forming by using
directional antennas is available for all the wireless nodes (at least all the wireless nodes which is
possible to transmit data messages to their neighbor nodes). This seems an excellent secure
communication method by using the intentional collisions with the noise wireless signals. However,
the assumptions of the directional antennas for beam forming and high performance processors for
complex signal processing to remove the noise wireless signals from the collided wireless signals
are not reasonable to apply to the wireless multihop networks such as sensor networks and IoT.
This is because the sensor nodes and the IoT devices may be so small, light and cheap and the
networks consist of huge number of such wireless nodes that it is difficult or impossible to have
such functionalities.

Proposal

This section proposes a novel method for secure wireless multihop transmissions of data messages
which interferes eavesdropper wireless nodes trying to achieve the clear texts carried by the data
messages. That is, the transmissions of the wireless signals from omni antennas of the wireless
nodes are modeled by the unit disc model [2].
Wireless nodes $N_s$ and $N_r$ are the sender and receiver ones, respectively. $N_r$ is in the wireless signal transmission range of $N_s$. A data message $m$ is broadcasted by $N_s$ to all the neighbor wireless node of $N_s$ in the wireless signal transmission range of $N_s$. Hence, $N_r$ surely receives $m$. At the same time all the neighbor wireless nodes including possible eavesdropper wireless nodes $N$ in the wireless signal transmission range of $N_s$ receive $m$ as shown in Figure 1. In order to prevent $N$ to receive $m$, noise wireless signals are introduced same as the related works discussed in the previous section. Only noise wireless signals transmitted by wireless nodes whose wireless signal transmission ranges cover at least a part of the wireless signal transmission range of $N_s$ contribute to the secure wireless transmission of $m$ from $N_s$ to $N_r$. At the same time, the noise wireless signal never reach $N_r$. If $N_r$ is in the noise wireless signal transmission range, $N_r$ cannot receive $m$ due to the collision caused by $m$ and the noise wireless signal.

![Figure 1. Noise Wireless Signal Transmissions by 1-Hop Neighbor Nodes.](image1)

This paper proposes the following conditions for a wireless node $N_j$ to transmit a noise wireless signal to prevent possible eavesdropper wireless node to receive the data message transmitted from a sender wireless node $N_s$ to a receiver one $N_r$ (2).

**[Noise Wireless Transmitting Node $N_j$]**

1. $N_j$ is a neighbor wireless node of $N_s$. $N_j$ is in the wireless signal transmission range of $N_s$.
2. $N_j$ is not a neighbor wireless node of $N_r$. $N_r$ is out of the wireless signal transmission range of $N_r$.

![Figure 2. Noise Wireless Signal Transmissions for Ad-Hoc Communication.](image2)
The condition (1) is a sufficient condition for the wireless signal transmission range of \( N_j \) to cover a part of the wireless signal transmission range of \( N_s \). Since both \( m \) and the noise wireless signal reach the wireless nodes in the common area of both the wireless signal transmission ranges, a collision of them occurs at the wireless nodes. Hence the possible eavesdropper wireless nodes are prevented to receive \( m \) by the collisions. In addition as discussed in the later subsection, the wireless nodes satisfying the condition (1) does not require any additional control message transmission to synchronously transit the noise wireless signals with \( m \) from \( N_s \) to \( N_r \). Thus, this subsection proposes that the neighbor wireless nodes of \( N_s \) transmit the noise wireless signals.

The condition (2) is a necessary condition for the wireless signal transmission range of \( N_j \) not to include \( N_r \). Because of the assumption of the unit disc model for the wireless signal transmission range, \( N_r \) is out of the wireless signal transmission range of \( N_j \), either. Thus, the noise wireless signal from \( N_j \) never reach \( N_r \) and no collisions between \( m \) and the noise wireless signal occur at \( N_r \). Thus, this subsection proposes that the neighbor wireless nodes of \( N_r \) do not transmit the noise wireless signals.

However, the existence probability of the neighbor wireless nodes transmitting the noise wireless signals preventing the overhearing of possible eavesdropper wireless nodes depends on the distribution of the wireless nodes, i.e., the density of the wireless nodes, and the distance \( |N_s N_r| \) between the sender wireless node \( N_s \) and the receiver one \( N_r \). As shown in Figure 3, if the distance \( |N_s N_r| \) is relatively long, the common area of the wireless signal transmission ranges of \( N_s \) and \( N_r \) is small and the area including the wireless nodes satisfying the conditions in the previous subsection is large. Hence, the coverage of the noise wireless signals overlapping the wireless signal transmission range of \( N_s \) in which possible eavesdropper wireless nodes overhear the data messages is relatively high. On the other hand as shown in Figure 4, if \( |N_s N_r| \) is relatively short, the common area of the wireless signal transmission range of \( N_s \) and \( N_r \) is small. Since the wireless nodes in this area cannot transmit the noise wireless signals which reach \( N_r \), the coverage of the noise wireless signals overlapping the wireless signal transmission range of \( N_s \) is relatively low and it is difficult to prevent eavesdropper wireless nodes to overhear the data message.

![Figure 3. Eavesdropper Interfering with Far Sender/Receiver Wireless Nodes.](image)
In order to solve the problem, additional wireless nodes are required to transmit the noise wireless signals to improve the coverage, i.e., the area where wireless nodes does not receive the noise wireless signals though they receive the data message from $N_S$ is required to be reduced. It is clear that no wireless nodes in the wireless signal transmission range of $N_R$ can transmit the noise wireless signals without collisions at $N_R$, noise wireless signal transmissions by the wireless nodes out of the wireless transmission ranges of both $N_S$ and $N_R$ are expected to be efficient. Therefore, for wireless multihop data message transmissions from a source wireless node $N_S$ to a destination one $N^d$ along the wireless multihop transmission route $\| N_0 \cdots N_d \rangle$, the wireless nodes $N_j$ satisfying the following conditions transmits the noise wireless signals to prevent the data messages to be overheard by possible eavesdropper wireless nodes.

[Noise Wireless Signal Transmitting Node $N_j$]

1. A wireless node $N_j$ is a 1-hop neighbor wireless node of $N_i$ and in not a 1-hop neighbor wireless node of $N_{i+1}$.
2. $N_j$ is not a 1-hop neighbor wireless node of $N_i$ and $N_{i+1}$ either and a 2-hop neighbor wireless node of both $N_i$ and $N_{i+1}$.

Evaluation
This section evaluates the coverage of the wireless signal transmission ranges of the intermediate wireless nodes of the wireless multihop transmission routes by the noise wireless signals transmitted in accordance with the proposed method in simulation experiments. A wireless transmission range of a wireless node is 10m and its 1-hop and 2-hop neighbor nodes are randomly distributed according to the unique distribution randomness. Here average numbers of neighbor wireless nodes are 0–20 and the distance between an intermediate wireless node and its next-hop wireless node is 0–100m. For each density of the wireless nodes and the distance between the successive intermediate wireless nodes, the coverage is evaluated for 1,000 different distributions of the wireless nodes. For each distributions of the wireless nodes, the coverage of the wireless signal transmission ranges of the intermediate wireless nodes along the wireless multihop transmission routes by the noise wireless signal transmission ranges for the following three cases:

1. Only 1-hop neighbor wireless nodes of the intermediate wireless nodes satisfying the proposed conditions transmit the noise wireless signals.
2. All the 1-hop neighbor wireless nodes of the intermediate wireless nodes and the 2-hop ones satisfying the proposed conditions transmit the noise wireless signals.
3. All the 1-hop neighbor wireless nodes of the intermediate wireless nodes and only the limited 2-hop neighbor wireless nodes which is a neighbor of the 1-hop neighbor wireless nodes which transmit the noise wireless signals transmit the noise wireless signals.

Figure 7 shows the results of the simulation experiments. The coverage monotonically increases according to the average numbers of neighbor wireless nodes, i.e., the total numbers of wireless nodes.
nodes in simulation and the distance between the source and the destination wireless nodes. In the (1) case, the coverage for the low density of neighbor wireless nodes and the short distance between the successive intermediate wireless nodes is relatively low. However, in the (3) case, the coverage is sufficiently improved by introduction of the noise wireless signal transmissions by the 2-hop neighbor wireless nodes of the intermediate wireless node.

Concluding Remarks

This paper proposes a novel secure wireless multihop data message transmissions by the intentional collisions with the noise wireless signals. Here, the noise wireless signals are transmitted by a part of the 1-hop and 2-hop neighbor wireless nodes of the intermediate wireless nodes to make difficult for possible eavesdropper wireless nodes to overhear the data messages. To select the neighbor wireless nodes transmitting the noise wireless signals, we extends AODV routing protocol with additional control messages. The results of the simulation experiments show that the coverage of the noise wireless signals is reasonably high. In future work, we will further extend the routing and data message transmission protocol to increase the number of 2-hop neighbor wireless nodes transmitting the noise wireless signals to make more secure wireless multihop communications and will evaluate the performance of our proposed method in wireless multihop communication environments.

References
