

# Interference of Overhearing by Eavesdropper Nodes for Secure Wireless Ad-Hoc Networks

Hinano Amano and Hiroaki Higaki(✉)

Department of Robotics and Mechatronics, Tokyo Denki University, Tokyo, Japan
{amano,hig}@uni-heidelberg.de

**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 directional antenna and it is not difficult for an eavesdropper wireless node to overhear the wireless signal to get the data message. Some researches show that it is useful to transmit a noise wireless signal which collides to the data message wireless signal in order for interfering the overhearing. However, some special devices such as directional antennas and/or high computation power for complicated signal processing are required. For wireless multihop networks with huge number of wireless nodes, small and cheap wireless nodes without such special devices are mandatory for construction of the network. This paper proposes a novel method for interfering the overhearing by the eavesdropper wireless nodes by a routing protocol and a data message transmission protocol with cooperative noise signal transmissions by 1-hop and 2-hop neighbor wireless nodes of each intermediate wireless node. The results of simulation experiments show that the proposed intentional collision method provides enough coverage of noise wireless signals especially by help of part of 2-hop neighbor wireless nodes.

**Keywords:** Wireless multihop communication · Overhearing avoidance · Jamming wireless signals · Collisions · Routing protocol

## 1 Introduction

In wireless ad-hoc networks and wireless sensor networks, data messages are transmitted along a wireless transmission route from a source wireless node to a destination one. A wireless transmission route consists of a sequence of intermediate wireless nodes each of which forwards 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

© Springer Nature Switzerland AG 2020
O. Gervasi et al. (Eds.): ICCSA 2020, LNCS 12252, pp. 246–260, 2020.
https://doi.org/10.1007/978-3-030-58811-3_18

transmission range to overhear the data message signal. That is, the neighbor wireless node, even if it is an eavesdropper one, receives the data message.

Usually, the data messages are securely transmitted by cryptography. The source wireless node encrypts a clear text and the data message carries a cryptogram. In order for achieving the clear text from the cryptogram in the overheard data message, a cryptography key is required for both the destination wireless node and an eavesdropper wireless node. Especially, in sensor networks where sensor data messages initiated by source sensor nodes with sensor and wireless communication devices are transmitted to a wireless sink node connected to a high performance sensor database computer, it is impossible for each sensor node to implement highly secure cryptography methods since its implementation, operation and maintenance costs are high. Thus, even in sensor networks with simple and facile cryptography methods, the sensor data is required to be transmitted securely.

For this requirement, some secure wireless transmission methods have been proposed as described in the next section. One method requires each intermediate wireless node to devise a directional antenna and wireless signals are required to be transmitted only in the specified direction by using a beam-forming method. Another one requires each intermediate wireless node to support high performance signal processing with complex calculation. However, it is difficult to introduce these conventional methods to wireless multihop networks consisting of small, light and cheap wireless nodes such as sensor nodes. Therefore, this paper proposes a novel secure wireless multihop transmission method without special hardwares such as directional antennas and/or processors supporting high performance signal processing in each intermediate wireless node. That is, under an assumption that wireless signals are transmitted according to the unit disc model [8] by using an omni directional antenna by each intermediate wireless node, it makes difficult for eavesdropper wireless nodes to overhear the data messages transmitted along a wireless multihop transmission route.

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 Sect. 3. Both the routing and the data message transmission protocols are proposed. Section 4 evaluates our proposed method by simulation experiments.

## 2 Related Works

There are various security problems in wireless multihop networks and a lot of solutions have been discussed and proposed. The selfish wireless node problem and the black-hole attack problem are well known peculiar problems in wireless multihop networks. On the other hand, a so-to-speak eavesdropper problem is a common one for wired and wireless networks and a countermeasure solution is mandatory. Especially in wireless networks, since all the data messages are carried by wireless signals which are inherently broadcasted and are easily overheard by any neighbor wireless node, much more advanced method has been required

to be developed. The dominant technology is an cryptography. Due to the characteristics of the mobile wireless nodes, simple and facile encryption/decryption methods have been proposed for achieving enough security with reasonably low computational complexity.

However, the cryptography is only a method which makes difficult for eavesdroppers to achieve the clear text from the cryptogram carried by the data message. That is, it may fall behind. Thus for taking the initiative, a method to make difficult or impossible for eavesdropper wireless nodes to overhear the data messages carrying the cryptograms is much effective. Combination of the method interfering the overhearing and the cryptography for wireless multihop networks is expected to provide an acceptable tradeoff between required security and inevitable overhead. In wireless multihop sensor networks and IoT (Internet of Things) consisting of huge number of low-power wireless nodes without computational power enough to support highly secure communication methods, a novel secure communication method not depending only on the cryptography is required.

One of such methods makes difficult for eavesdropper wireless nodes to overhear the transmitted data messages by intentional collisions with noise wireless signals [2,6]. Paper [2] proposes a method for secure wireless data message transmissions under an assumption 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). A sender wireless node $N_s$ transmits a wireless signal carrying a data message to a receiver wireless node $N_r$ by using beam forming such that $N_r$ and only its limited neighbor wireless nodes receive it. Concurrently with the transmission of the wireless signal, $N_r$ also transmits a noise wireless signal called a jamming wireless signal to all its neighbor wireless nodes by its omni directional antenna. Since the wireless signal transmission range of the noise wireless signal covers the wireless signal transmission range of the wireless signal carrying the data message, no wireless nodes can receive the data message itself without any collision. Here, one of the neighbor wireless nodes $N_f$ of $N_r$ forwards its receiving collided wireless signal which is the superposition of these wireless signals to $N_r$. On receipt of the collided wireless signal from $N_f$, $N_r$ removes the original noise wireless signal from the received wireless signal and achieves the original wireless signal carrying the data message since the noise signal was transmitted by $N_r$ itself. This signal processing is only possible by $N_r$ since no other wireless nodes have the original noise wireless signal transmitted by $N_r$.

This method by using the intentional collisions with the noise wireless signals seems excellent for secure communication. However, the assumptions of the directional antennas for beam forming and high performance processors for complex signal processing to remove a noise wireless signal from a collided wireless signal 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 their networks consist of huge number of such wireless nodes that it is difficult or impossible to have such functionalities.

## 3 Proposal

This section proposes a novel method for secure wireless multihop transmissions of data messages which interferes eavesdropper wireless nodes achieving the clear texts carried by the data messages. Our method makes difficult for the eavesdropper wireless nodes to overhear the data message signals which are broadcasted by intermediate wireless nodes in a wireless multihop transmission route. Here, no additional special hardware such as directional antennas for beam forming and high performance processors to support highly complex signal processing is needed in the intermediate wireless nodes. That is, the transmissions of the wireless signals from omni directional antennas of the wireless nodes are modeled by the unit disc model [4].

### 3.1 Noise Signal Transmission for Ad-Hoc Wireless Communications

This section discusses the method for secure wireless transmissions of data messages in wireless ad-hoc communication between neighbor wireless nodes, i.e., only 1-hop wireless transmissions. Wireless nodes $N_s$ and $N_r$ are a sender and a 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 a possible eavesdropper wireless node $N$ in the wireless signal transmission range of $N_s$ receives $m$ as shown in Fig. 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 signals never reach $N_r$. If $N_r$ is in one of the noise wireless signal transmission ranges, $N_r$ cannot receive $m$ due to the collision caused by $m$ and the noise wireless signal.

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

**[Noise Wireless Signal 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 $N_r$. $N_j$ is out of the wireless signal transmission range of $N_r$.

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

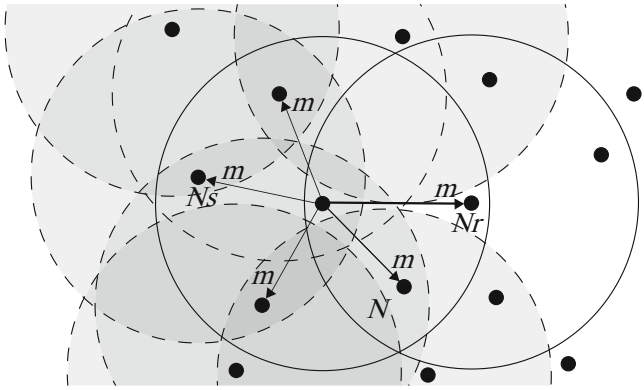


**Fig. 1.** Noise wireless signal transmissions by neighbor nodes.

the wireless nodes. Hence the possible eavesdropper wireless nodes are prevented to receive $m$ by the collision. 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 1-hop 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 also out of the wireless signal transmission range of $N_j$. Thus, the noise wireless signal from $N_j$ never reaches $N_r$ and no collisions of $m$ 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.

### 3.2 Extended Noise Signal Transmission for Ad-Hoc Wireless Communications

The previous subsection proposes a method to prevent eavesdropper wireless nodes to overhear the data message transmitted between neighbor wireless nodes. Here, secure ad-hoc wireless communication is realized by noise wireless signals transmitted by the neighbor wireless nodes of a sender wireless node out of the wireless signal transmission range of a receiver wireless node. The wireless nodes and the time duration required to transmit the noise wireless signals are also specified by the RTS/CTS control message transmissions and no additional control messages are required to be transmitted.

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 Fig. 2, if the distance $|N_sN_r|$ 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 Fig. 3, if $|N_sN_r|$ is relatively short, the common area of the wireless signal transmission ranges 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.

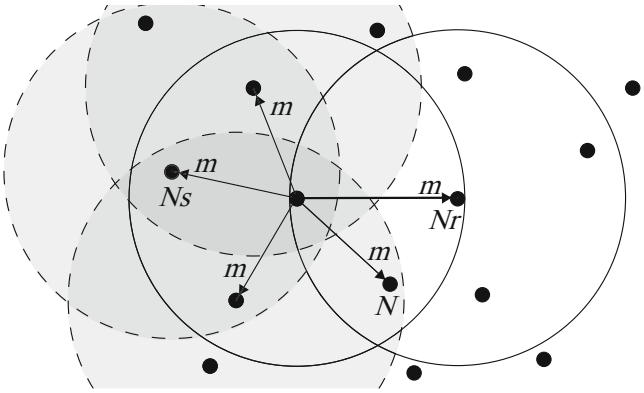


**Fig. 2.** Eavesdropper interfering for far sender/receiver wireless nodes.

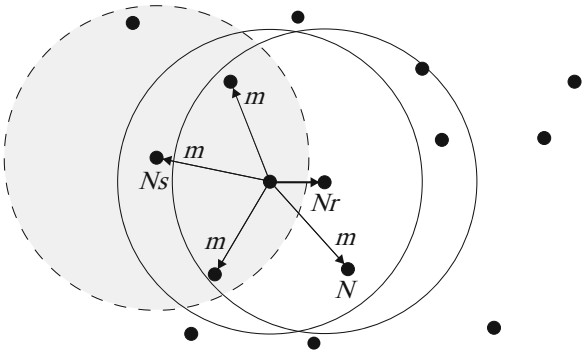


**Fig. 3.** Eavesdropper interfering for near sender/receiver wireless nodes.

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 signal transmission ranges of both $N_s$ and $N_r$ are expected to be efficient. Therefore, wireless nodes out of the both wireless transmission ranges of $N_s$ and $N_r$ are required to transmit the noise wireless signals if its wireless signal transmission range covers even a part of the wireless signal transmission range of $N_s$. Such wireless nodes are 2-hop neighbor wireless nodes of $N_s$ and are not 1-hop neighbor wireless nodes of $N_r$. This paper proposes that transmissions of noise wireless signals are required to be common 2-hop neighbor wireless nodes of $N_s$ and $N_r$ as shown in Fig. 4. By this extension, even if $|N_s N_r|$ is relatively short, the coverage of transmission ranges of noise wireless signals overlapping the wireless transmission ranges of $N_s$ is improved.

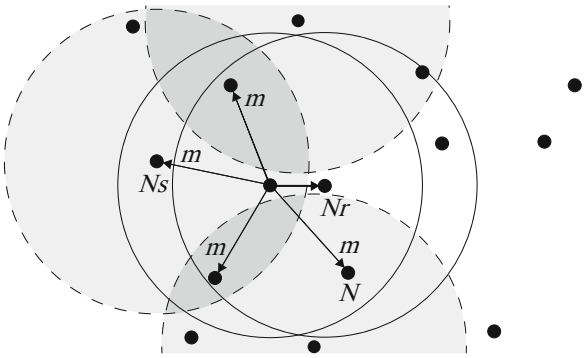


**Fig. 4.** Coverage improvement with help of common 2-hop neighbor wireless nodes.

### 3.3 Noise Signal Transmission for Wireless Multihop Communications

Different from the wireless nodes transmitting the noise wireless signals for a secure data message transmission in 1-hop ad-hoc communications discussed in the previous subsection, it is difficult to require the 2-hop neighbor wireless nodes of $N_s$ to transmit the noise wireless signals without additional control messages to the original RTS/CTS control. Since 2-hop neighbor wireless nodes are both out of the wireless signal transmission ranges of $N_s$ and $N_r$, additional control messages are required to be transmitted to notify them to transmit the noise wireless signals. In addition, it is impossible for 1-hop neighbor wireless nodes of $N_s$ to transmit the additional control message concurrently with the

CTS control message from $N_r$ after receipt of the RTS control message since the transmitted control message collides with the CTS control message at $N_s$. Therefore, the 2-hop neighbor wireless nodes of intermediate wireless nodes being required to transmit the noise wireless signals are determined in a routing protocol which detects the wireless multihop transmission route $||N_0 \dots N_n\rangle\rangle$ which is a sequence of intermediate wireless nodes from a source wireless node $N^s = N_0$ to a destination wireless node $N^d = N_n$. Since a certain control messages is transmitted along the detected wireless multihop transmission route in most of the ad-hoc routing protocols, 1-hop neighbor wireless nodes of each intermediate wireless node can transmit some control messages to notify a part of its 2-hop neighbor wireless nodes to be required to transmit the noise wireless signals simultaneously with the data message transmissions.

The 2-hop neighbor wireless nodes of $N_s$ selected to transmit the noise wireless signals according to the conditions for 1-hop ad-hoc communications described in the previous subsection are also required to transmit the noise wireless signals for secure wireless multihop communications. That is, 1-hop neighbor wireless nodes of an intermediate wireless node $N_i$ out of the wireless signal transmission range of its next-hop wireless node $N_{i+1}$ is required to transmit the noise wireless signals concurrently with the data message transmissions from $N_i$ to $N_{i+1}$. In addition to cover wider part of the wireless signal transmission range of $N_i$ by the noise wireless signal transmission ranges to prevent eavesdropper wireless nodes to overhear the data message, a part of the 2-hop neighbor wireless nodes are also required to transmit the noise wireless signals. Though the transmission ranges of the 2-hop neighbor nodes of $N_i$ surely overlap the wireless signal transmission range of $N_i$, they do not transmit the noise wireless signals if $N_{i+1}$ is their 1-hop neighbor wireless node for avoidance the collisions with the receiving data message transmissions at $N_{i+1}$.

Therefore, for wireless multihop data message transmissions from a source wireless node $N^s = N_0$ to a destination one $N^d = N_n$ along the wireless multihop transmission route $||N_0 \dots N_n\rangle\rangle$, the wireless nodes $N_j$ satisfying either of the following conditions transmits the noise wireless signals to prevent the data messages to be overheard by possible eavesdropper wireless nodes in the wireless signal transmission range of $N_i$ (Fig. 5).

**[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 $N_{i+1}$.

### 3.4 Routing and Noise Wireless Signal Transmission Protocol

As mentioned in the previous subsection, a wireless signal transmission range of an intermediate wireless node $N_i$ is covered by wireless signal transmission ranges of 1-hop neighbor wireless nodes of $N_i$ out of the wireless signal transmission rage

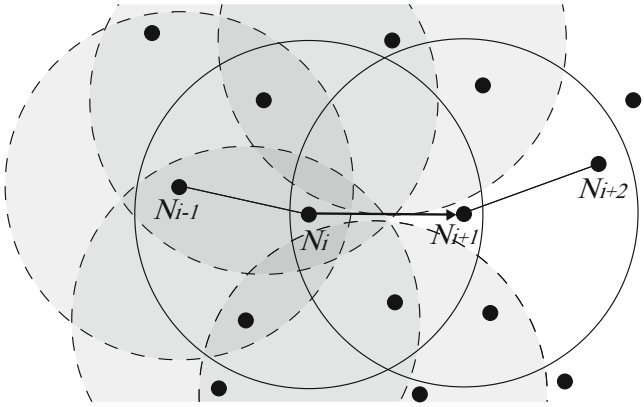


**Fig. 5.** Noise wireless signal transmissions for wireless multihop communication.

of $N_{i+1}$ and of common 2-hop neighbor wireless nodes of $N_i$ and $N_{i+1}$ to prevent possible eavesdropper wireless nodes by noise wireless signal transmissions. In order to determine the common 2-hop neighbor wireless nodes, certain control messages are required to be transmitted by 1-hop neighbor wireless nodes of both $N_i$ and $Ni + 1$. It is realized by forwarding of both an RTS and a CTS control messages by 1-hop neighbor wireless nodes of $N_i$ and $N_{i+1}$, respectively. Though these forwarded RTS/CTS control messages might be collide to the original RTS/CTS control messages. Hence, the method results in longer transmission delay of data messages.

Different from this dynamic determination of 2-hop neighbor noise wireless signal transmission nodes, this paper proposes the method by which they are determined in a flooding based routing protocol such as AODV. Same as in [3], in addition to a flooding of an *Rreq* control message and a unicast transmission of an *Rrep* control message along a detected wireless multihop transmission route, additional control messages are transmitted during the transmission of the *Rrep* control message to the 2-hop neighbor noise wireless signal transmission nodes.

Figure 6 shows an overview of the proposed protocol based on AODV. When an intermediate wireless node $N_{i+1}$ transmits an *Rrep* control message to its previous-hop intermediate wireless node $N_i$, a 1-hop neighbor wireless node $N^n_{i+1}$ of $N_{i+1}$ overhears the *Rrep* control message. Just after this reception of *Rrep*, $N^n_{i+1}$ broadcasts a noise wireless signal transmission request control message *Jreq*$(i + 1)$ in its wireless signal transmission range. By this extended routing protocol, 1-hop neighbor wireless node of $N_i$ out of the wireless signal transmission range of $N_{i+1}$ receives *Rrep* control message from $N_i$ but does not receive *Rrep* control message from $N_{i+1}$ transmits a noise wireless signal while $N_i$ transmits data messages to $N_{i+1}$. On the other hand, common 2-hop neighbor wireless nodes of $N_i$ and $N_{i+1}$ receive *Jreq*$(i)$ and *Jreq*$(i+1)$ from 1-hop neighbor wireless nodes of $N_i$ and $N_{i+1}$, respectively. These wireless nodes transmit noise wireless signals while a data message is transmitted from $N_i$ to $N_{i+1}$.

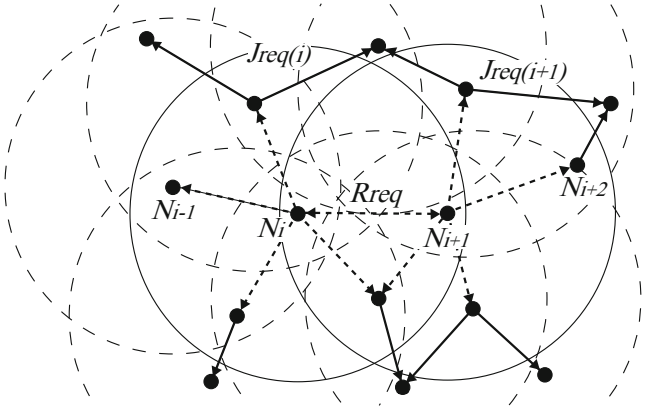


**Fig. 6.** Routing protocol with selection of 2-hop neighbor wireless nodes transmitting noise wireless signal.

**[Noise Signal Transmitting Wireless Node Determination]**

(1) On receipt of an *Rrep* control message from an intermediate wireless node $N_i$, a neighbor wireless node $N_i^n$ broadcasts a $Jreq(i)$ control message in its wireless signal transmission range.
(2) A wireless node $N$ which has received *Rrep* control message not from $N_{i+1}$ but from $N_i$ transmits a noise wireless signal while a data message is transmitted from $N_i$ to $N_{i+1}$.
(3) A wireless node $N$ which has received both $Jreq(i)$ and $Jreq(i+1)$ control messages from its neighbor wireless nodes transmits a noise wireless signal while a data message is transmitted from $N_i$ to $N_{i+1}$.

A wireless node $N$ which has received *Rrep* control message not from $N_{i+1}$ but from $N_i$, i.e., which is a 1-hop neighbor wireless node of $N_i$ and is not a 1-hop neighbor wireless node of $N_{i+1}$ identifies the time duration when it transmits a noise wireless signal while a data message is transmitted from $N_i$ to $N_{i+1}$ by receipt of an RTS control message as discussed in the previous subsection. On the other hand, a wireless node $N$ which has received both $Jreq(i)$ and $Jreq(i+1)$ control messages from its neighbor wireless nodes does not receive either an RTS control messages from $N_i$ or a CTS control messages from $N_{i+1}$ since $N$ is out of the wireless signal transmission ranges of both $N_i$ and $N_{i+1}$ and $N$ cannot identify the time duration when it transmits a noise wireless signal while a data message is transmitted from $N_i$ to $N_{i+1}$. As also discussed in the previous subsection, if the RTS and the CTS control messages are forwarded to $N$, though $N$ can identify the time duration, it requires higher communication overhead, i.e., longer transmission delay for a 1-hop data message transmission from $N_i$ to $N_{i+1}$, which results in longer end-to-end transmission delay of the data message along a wireless multihop transmission route from its source wireless node to its destination one. Hence, this paper proposes another simple way for $N$ to identify

the time duration. That is, $N$ starts to transmit a noise wireless signal when it receive any noise wireless signal from one of its neighbor node. Since it is satisfied one of the conditions of a noise signal transmission wireless node mentioned in the previous subsection in advance, $N$ is surely required to transmit a noise wireless signal. In addition, if $N$ has received a noise wireless signal from one of its neighbor wireless nodes, it may be the 1-hop neighbor wireless node of $N_i$ and $N$ may be required to start to transmit a noise wireless signal. Even if $N$ receives a noise wireless signal transmitted by its different neighbor wireless node from the 1-hop neighbor wireless node of $N_i$, a noise wireless signal transmitted from $N$ never disturbs a data message transmission if $N$ has not received a CTS control message for the data message. In order to avoid unnecessary collisions of the noise wireless signal and a data message, the time duration of the noise wireless signal from $N$ is adjusted to the required transmission time for the shortest data message since $N$ cannot achieve the NAV information for the data message carried by the RTS and the CTS control messages.

### 3.5 Notification of Noise Signal Transmission Time

In order to solve this problem, this paper proposes a method to notify the initiation time and duration of noise signal transmission to common 2-hop neighbor wireless nodes of an intermediate wireless node $N_i$ and its next-hop intermediate wireless node $N_{i+1}$. Since $N_i$ is an intermediate wireless node of a wireless multihop transmission route, $N_i$ surely receives a data message from its previous-hop intermediate wireless node $N_{i-1}$ before sending it to $N_{i+1}$. In the RTS/CTS collision avoidance control for a data message transmission from $N_{i-1}$ to $N_i$, a common neighbor wireless node $N_i'$ of $N'$ and $N_i$ receives a *CTS* control message from $N_i$. By referring NAV contained in the *CTS* control message, $N_i'$ gets required time duration of a data message transmission. $N_i'$ transmits an *NTTN* (Notification of Transmission Time of Noise Signal) control message containing the required time duration of a data message transmission to $N'$ which becomes possible to transmit noise signal for the required time duration to interfere eavesdropper wireless node trying to overhear a data message transmitted from $N_i$ to $N_{i+1}$. Though $N_i'$ should suspend transmission of any message due to receipt of the *CTS* control message from $N_i$ for avoidance of collision with the data message from $N_{i-1}$ to $N_i$ at $N_i$, $N_i'$ transmits the *NTTN* control message to $N'$ concurrently with an *ACK* control message from $N_i$ to $N_{i-1}$. This is because both the *ACK* and the *NTTN* control messages are correctly received without any collisions by $N_{i-1}$ and $N'$, respectively as shown in Fig. 7.

## 4 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 (Fig. 8).

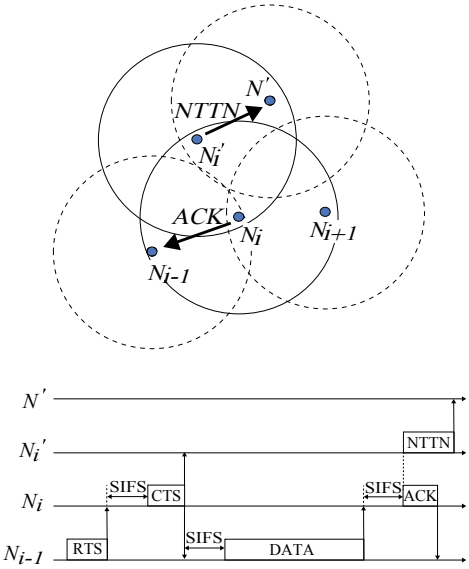


**Fig. 7.** Notification of time for noise signal transmission by NTTN control message.

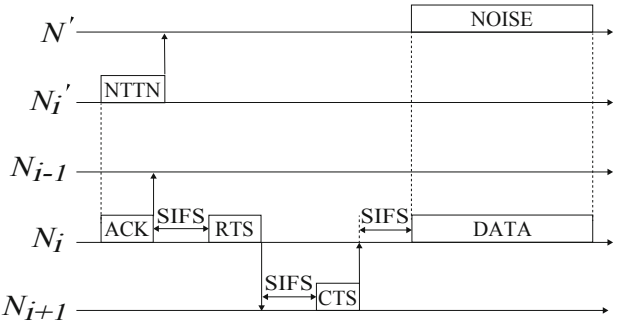


**Fig. 8.** Time starting transmission of noise signal by common 2-hop neighbor node $N'$.

A wireless transmission range of a wireless node is 100 m 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 0–100 m. 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 9 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 in simulation and the distance between the source and the destination wireless nodes. In the case (1), 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 case (3), 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.

Next, we evaluate the performance of the proposed method in wireless multihop transmissions of data messages. Here, 100–1,000 wireless nodes with 50 m wireless signal transmission ranges are randomly distributed according to the unique distribution randomness in a 700 m × 700 m square field. A source and a destination wireless nodes are fixed at locations of (200, 200) and (500, 500), respectively. The coverage of the wireless signal transmission area of intermediate wireless nodes by those of 1- and 2-hop neighbor wireless nodes transmitting noise wireless signals is evaluated by using 1,000 different distribution of the wireless nodes.

Figure 10 shows the results of the experiments. (1) represents the coverage by the method in which only 1-hop neighbor wireless nodes of the intermediate wireless nodes transmit noise wireless signals and (2) represents the coverage by the proposed method in this paper in which part of 2-hop neighbor wireless nodes also transmit noise wireless signals to improve the coverage. Averagely, about 11% higher coverage is realized by (2) in comparison with (1). In addition, though the coverage is sensitive to the locations of wireless nodes, i.e., the coverage highly depends on length and angle of successive wireless communication links in (1), by introduction of the help of part of 2-hop neighbor wireless nodes, the coverage becomes more stable in (2) than in (1). Therefore, additional wireless noise transmitted by part of 2-hop neighbor wireless nodes of the intermediate wireless nodes highly contributes to more secure wireless multihop transmissions of data messages against silent eavesdropper wireless nodes.

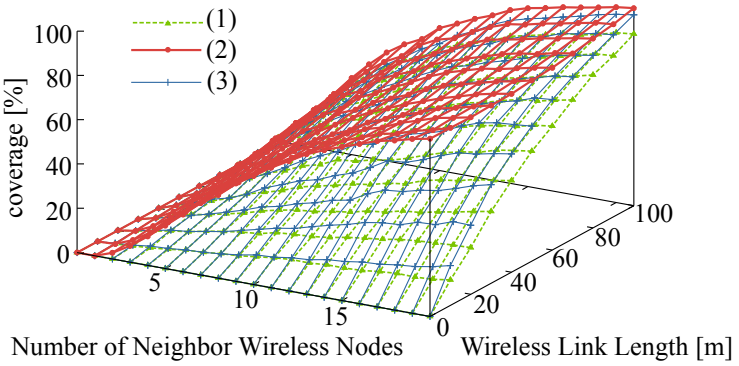


**Fig. 9.** Noise wireless signal coverage in 1-hop ad-hoc communication.

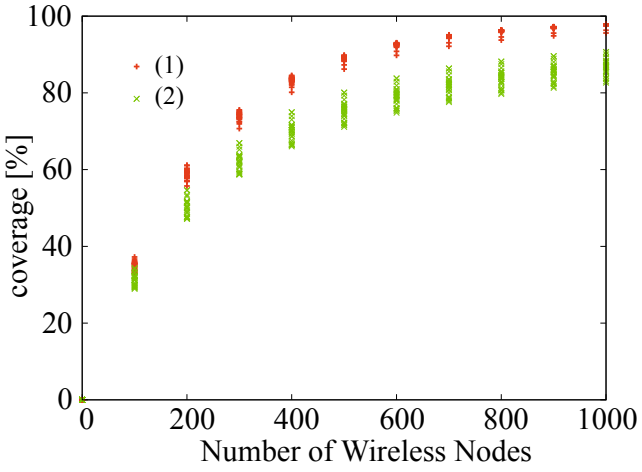


**Fig. 10.** Noise wireless signal coverage in wireless multihop communication.

## 5 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 design an extended method to make better trade-off between coverage of the noise wireless signals, i.e, degree of security and transmission

power consumption of the noise wireless signals in 1-hop and 2-hop neighbor wireless nodes.

## References

1. Boneh, D., Dunworth, C., Lipton, R.J.: Breaking DES Using a Molecular Computer. In: Proceedings of the 1st International Workshop on DNA Based Computers, pp. 37–66 (1995)
2. He, X., Yener, A.: Two-hop secure communication using an untrusted relay: a case for cooperative jamming. In: Proceedings of the IEEE Global Telecommunications Conference 2008 (2008)
3. Kanachi, T., Higaki, H.: Wireless multihop transmissions for secret sharing communication. In: Proceedings of the 14th IEEE International Conference on Scalable Computing and Communications, pp. 808–813 (2014)
4. Kranakis, E., Singh, H., Urrutia, J.: Compass routing on geometric networks. In: Proceedings of the 11th Canadian Conference on Computational Geometry, pp. 51–54 (1999)
5. Shigeyasu, T., Matsuno, H., Morinaga, N.: Proposal of a method for improving MAC level fairness in the coexisting environment with legacy IEEE802.11DCF terminals. IPSJ J. **50**(3), 1156–1169 (2009)
6. Tekin, E., Yener, A.: The general Gaussian multiple-access and two-way wiretap channels: avhievable rates and cooperative jamming. IEEE Trans. Inf. Theory **54**(6), 2735–2750 (2008)
7. Toh, C.K., Vassiliou, V., Guichal, G., Shih, C.H.: MARCH: a medium access control protocol for multihop wireless ad hoc networks. In: Proceedings of IEEE/AFCEA Military Communication Conference, pp. 512–516 (2000)
8. Urrutia, J.: Two problems on discrete and computational geometry. In: Proceedings of Japan Conference on Discrete and Computational Geometry, pp. 42–52 (1999)