Security/QoS-Aware Route Selection in Multi-hop Wireless Ad Hoc Networks

Yang Xu[1], *Member, IEEE*, Jia Liu[2], *Student Member, IEEE*, Yulong Shen[3], *Member, IEEE*,
Xiaohong Jiang[2], *Senior Member, IEEE* and Tarik Taleb[4], *Senior Member, IEEE*
[1]School of Economics and Management, Xidian University, Xian 710071, China.
Email: yxu@xidian.edu.com
[2]School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan.
Email: jliu871219@gmail.com, jiang@fun.ac.jp
[3]State Key Laboratory of ISN, Xidian University, Xi'an 710071, China.
Email: ylshen@mail.xidian.edu.cn
[4]Department of Communications and Networking, Aalto University, Helsinki, 11000 Finland.
Email: talebtarik@gmail.com

***Abstract*—Recently extensive works have been devoted to the performance analysis of physical layer security in wireless communication systems. However, the combination of physical layer security and quality of service (QoS) for route selection in multi-hop wireless ad hoc networks (WANETs) still remains an open technical challenge. As an initial step towards this end, this paper focuses on a multi-hop WANET with two typical transmission schemes amplify-and-forward (AF) and decode-and-forward (DF), and explores the route selection with the consideration of both security and QoS. We first derive the closed-form expressions of secrecy outage probability (SOP) and connection outage probability (COP) for a single hop link, and further extend the results to an end-to-end route. Then we conduct the performance comparison between the AF scheme and DF scheme. Finally, based on both the SOP and COP of a route, we formulate the route metric and propose a flexible route selection algorithm which enables us to select the suitable route for message delivery according to different security and QoS requirements.**

***Index Terms*—Route selection, physical layer security, QoS, AF, DF.**

I. Introduction

Network security has become a major concern in modern communication networks [1]. For wireless ad hoc networks (WANETs), protecting the secrecy of user messages is more challenging due to both the broadcast nature of wireless channel and the lack of central administration [2]. The traditional approach for guaranteeing the security in a wireless environment is to employ the cryptographic techniques at network layer [3]. However, the cryptographic-based method is not applicable in a resource-limited WANET since it incurs high computing complexity and thus the high energy consumption.

Physical layer security, an information-theoretic approach which exploits the fundamental characteristics of wireless channel to achieve perfect secrecy [4]–[6], has attracted considerable attention in literature. Specifically, Tekin and Yener [7] explored the achievable secrecy rate region in the two-way wiretap channels. Lai and Gamal [8] studied the relay-eavesdropper channel and presented some cooperation strategies for security. Later, some approaches were proposed to improve the security performance in a two-hop wireless networks, such as the position-based jamming approach in [9], and the artificial noise generation approach in [10]. Recently, the asymptotic behaviors of network performance (i.e., the scaling laws) in large-scale WANETs with the consideration of physical layer security were explored in [11]–[13].

Although extensive works have been devoted to this research filed, the combination of physical layer security and quality of service (QoS) for route selection in multi-hop wireless ad hoc networks (WANETs) still remains an open technical challenge (some works related to secure routing can be found in [14]–[17]). As an initial step towards this end, in this paper we focus on a multi-hop WANET which consists of legitimate nodes and malicious eavesdroppers, and explore the route selection issue with the consideration of both security performance and quality of service (QoS) requirement. The main contributions of this paper are summarized as follows:

- We consider both the amplify-and-forward (AF) and decode-and-forward (DF) transmission schemes in a multi-hop WANET, and derive the corresponding closed-form expressions of secrecy outage probability (SOP) and connection outage probability (COP) for a single hop link.
- Based on the SOP and COP of a single hop link, we further derive the expressions of SOP and COP for an end-to-end route, which serve as the performance metrics of security and QoS, respectively.
- We compare the performance between the two transmission schemes, which indicates that the AF scheme outperforms in the sense of security performance while the DF scheme outperforms in the sense of QoS performance.
- We formulate the metric for route selection with the consideration of both SOP and COP, and propose a

This work is partially supported by Japan JSPS Grant 15H02692, China NSFC Grants 61571352, 61373173 and U153620014.

978-1-4799-6664-6/16/$31.00 ©2016 IEEE

flexible route selection algorithm which enables us to select the suitable route for message delivery according to different security and QoS requirements.

The remainder of this paper is organized as follows. Section II presents the preliminaries involved in this paper. We analyze the outage probabilities in Section III. The route metric and route selection algorithm are proposed in Section IV. Finally, we provide the numerical results in Section V and conclude this paper in Section VI.

II. Preliminaries

In this section, we present the system model, two transmission schemes (AF and DF) and the performance metrics involved in this study.

A. System Model

We consider a WANET which consists of arbitrarily distributed legitimate nodes and malicious eavesdroppers, where each node is equipped with a single omni-directional antenna. A message is delivered from its source to its destination through a multi-hop route. We use the notation $\Pi_K = \langle l_1, \ldots, l_K \rangle$ to denote a route which is formed by K links l_1 to l_K. A link $l_k \in \Pi_K$ connects two node R_{k-1} and R_k on route Π_K, and it is exposed to a set of eavesdroppers denoted as $\mathcal{E}_k$, so we use the notation $l_k = (R_{k-1}, R_k, \mathcal{E}_k)$ to identify link l_k. We assume that the eavesdroppers do not collude with each other, and both the main links (between two legitimate nodes) as well as wiretap links (between a legitimate node and an eavesdropper) can be modeled as non-selective Rayleigh fading channels. Let h_k denote the fading coefficient of the channel from R_{k-1} to R_k, then $\mathbb{E}[|h_k|^2] = 1/d_{k-1,k}^{\alpha}$, where $d_{k-1,k}$ is the distance between nodes R_{k-1} and R_k, and α is the path-loss exponent (typically between 2 and 6). In the remainder of this paper, $d_{k-1,k}$ is abbreviated to d_k if there is no ambiguity. The noise received at each node is assumed to be an additive white Gaussian noise with power N_0.

B. Amplify-and-Forward

Under the AF transmission scheme, the source signal will be decoded only at the destination. Suppose that the source node R_0 transmits its signal s with power P and let n_k denote the additive white Gaussian noise at node R_k, then the received signal r_1 at R_1 is given by

$$r_1 = \sqrt{P} h_1 s + n_1. \tag{1}$$

After receiving the signal r_1, R_1 first performs coherent detection by multiplying r_1 with h_1^* and normalizes $h_1^* r_1$ with a scaling factor $\frac{1}{\sqrt{P}|h_1|^2}$. Then, R_1 transmits the normalized signal with power P to R_2. Thus, the received signal r_2 at R_2 is given by

$$\begin{aligned} r_2 &= \sqrt{P} h_2 \frac{h_1^* r_1}{\sqrt{P}|h_1|^2} + n_2 \\ &= \sqrt{P} h_2 s + \frac{h_2 h_1^*}{|h_1|^2} n_1 + n_2. \end{aligned} \tag{2}$$

By conducting the recursion, the received signal r_k at R_k can be determined as

$$r_k = \sqrt{P} h_k s + \sum_{i=1}^{k} \frac{h_k h_i^*}{|h_i|^2} n_i. \tag{3}$$

Due to the broadcast nature of wireless channel, for a main link l_k, each corresponding eavesdropper $e_{k_m} \in \mathcal{E}_k$ will also receive the signal from the transmitter R_{k-1}, and the received signal at eavesdropper e_{k_m} can be determined as

$$r_{e_{k_m}} = \sqrt{P} h_{e_{k_m}} s + \sum_{i=1}^{k-1} \frac{h_{e_{k_m}} h_i^*}{|h_i|^2} n_i + n_e, \tag{4}$$

where $h_{e_{k_m}}$ represents the channel fading coefficient of the wiretap link from R_{k-1} to e_{k_m}, $\mathbb{E}[|h_{e_{k_m}}|^2] = 1/d_{k-1,e_{k_m}}^{\alpha}$ ($1/d_{k-1,e_{k_m}}$ is abbreviated to $1/d_{e_{k_m}}$), and n_e denotes the additive white Gaussian noise at eavesdropper e_{k_m}.

C. Decode-and-Forward

Under the DF transmission scheme, each node first decodes the signal from per-hop node. If the decoding is successful, then the node transmits the re-coded original signal to the next-hop node. Suppose that node R_{k-1} decodes the signal from R_{k-2} successfully, then it will transmit the original signal s with power P. Thus, the received signals at node R_k and a corresponding eavesdropper $r_{e_{k_m}}$ are given by

$$r_k = \sqrt{P} h_k s + n_k, \tag{5}$$

$$r_{e_{k_m}} = \sqrt{P} h_{e_{k_m}} s + n_e. \tag{6}$$

D. Performance Metrics

As previous work [18], we define the events of secrecy outage and connection outage as follows:

Secrecy Outage: The SINR (signal-to-interference-plus-noise) at one or more eavesdroppers is above a fixed threshold γ_E. Hence, the message is not perfectly secure against eavesdropping. The secrecy outage probability (SOP) P_{so} is defined as the probability that the event of secrecy outage occurs.

Connection Outage: The SINR at the intended receiver is below the required threshold γ_C. Hence, the message cannot be correctly decoded by the intended receiver. The connection outage probability (COP) P_{co} is defined as the probability that the event of connection outage occurs.

In this paper, SOP and COP serve as the metrics of security performance and communication QoS, respectively.

III. Outage Probabilities Analysis

In this section, we first derive the SOP and COP for a link, based on which we further extend the results to an end-to-end route. Then, we compare the outage probabilities between the WANETs with AF and DF transmission schemes.

A. Link Outage Probabilities

We first derive the SOP for a link under both two transmission schemes. Regarding the link l_k which is exposed to a set of eavesdroppers $\mathcal{E}_k$, to calculate its SOP we only need to focus on the wiretap link with the maximum capacity among all wiretap links. Let $C_{e_k}^{AF}$ and $C_{e_k}^{DF}$ denote the maximum capacity of wiretap links from the relay node R_{k-1} to its eavesdroppers under the AF scheme and DF scheme, respectively, then $C_{e_k}^{AF}$ and $C_{e_k}^{DF}$ are given by

$$C_{e_k}^{AF} = \max_{m\leq|\mathcal{E}_k|} \log_2\left(1+\frac{P|h_{e_{k_m}}|^2}{(\sum_{i=1}^{k-1}\frac{|h_{e_{k_m}}|^2}{|h_i|^2}+1)N_0}\right), \quad (7)$$

$$C_{e_k}^{DF} = \max_{m\leq|\mathcal{E}_k|} \log_2\left(1+\frac{P|h_{e_{k_m}}|^2}{N_0}\right), \quad (8)$$

where $|\mathcal{E}_k|$ denotes the number of elements in set $\mathcal{E}_k$.

Notice that γ_E is the required SINR for an eavesdropper successfully intercepting the message, thus the SOP of link l_k under the AF scheme $P_{so}^{AF}(k)$ can be determined as

$$\begin{aligned}
P_{so}^{AF}(k) &= \mathbb{P}\left\{\max_{m\leq|\mathcal{E}_k|}\frac{P|h_{e_{k_m}}|^2}{(\sum_{i=1}^{k-1}\frac{|h_{e_{k_m}}|^2}{|h_i|^2}+1)N_0}>\gamma_E\right\}\\
&= 1-\mathbb{P}\left\{\max_{m\leq|\mathcal{E}_k|}\frac{P|h_{e_{k_m}}|^2}{(\sum_{i=1}^{k-1}\frac{|h_{e_{k_m}}|^2}{|h_i|^2}+1)N_0}<\gamma_E\right\}\\
&= 1-\prod_{m=1}^{|\mathcal{E}_K|}\mathbb{P}\left\{\frac{P|h_{e_{k_m}}|^2}{(\sum_{i=1}^{k-1}\frac{|h_{e_{k_m}}|^2}{|h_i|^2}+1)N_0}<\gamma_E\right\}\\
&= 1-\prod_{m=1}^{|\mathcal{E}_K|}\underbrace{\mathbb{P}\left\{\sum_{i=1}^{k-1}\frac{1}{|h_i|^2}+\frac{1}{|h_{e_{k_m}}|^2}>\frac{P}{\gamma_E N_0}\right\}}_{(a)}.
\end{aligned} \quad (9)$$

Since the expression (a) is not mathematically tractable, to address this issue, we refer to the approximation approach proposed in [19], which enables us to approximate (a) as

$$\begin{aligned}
(a) &= 1-\mathbb{P}\left\{\sum_{i=1}^{k-1}\frac{1}{|h_i|^2}+\frac{1}{|h_{e_{k_m}}|^2}<\frac{P}{\gamma_E N_0}\right\}\\
&\approx 2\sqrt{\hat{\lambda}_{k-1}\lambda_{e_{k_m}}}\left(\frac{P}{\gamma_E N_0}\right)^{e^{-(\hat{\lambda}_{k-1}+\lambda_{e_{k_m}})\frac{P}{\gamma_E N_0}}}\\
&\cdot\mathcal{K}_1\left(\frac{2P}{\gamma_E N_0}\sqrt{\hat{\lambda}_{k-1}\lambda_{e_{k_m}}}\right)\\
&\triangleq F\left(\hat{\lambda}_{k-1},\lambda_{e_{k_m}},\frac{P}{\gamma_E N_0}\right),
\end{aligned} \quad (10)$$

where $\hat{\lambda}_{k-1}=\sum_{i=1}^{k-1}\frac{1}{d_i^\alpha}$, $\lambda_{e_{k_m}}=\frac{1}{d_{e_{k_m}}^\alpha}$, and $\mathcal{K}_v(z)$ is the modified Bessel function of the second kind of order v [20]. Substituting (10) into (9), we have

$$P_{so}^{AF}(k)\approx 1-\prod_{m=1}^{|\mathcal{E}_k|}F\left(\hat{\lambda}_{k-1},\lambda_{e_{k_m}},\frac{P}{\gamma_E N_0}\right). \quad (11)$$

Regarding the SOP of link l_k under the DF scheme $P_{so}^{DF}(k)$, it can be determined as

$$\begin{aligned}
P_{so}^{DF}(k) &= \mathbb{P}\left\{\max_{m\leq|\mathcal{E}_k|}\frac{P|h_{e_{k_m}}|^2}{N_0}>\gamma_E\right\}\\
&= 1-\mathbb{P}\left\{\max_{m\leq|\mathcal{E}_k|}\frac{P|h_{e_{k_m}}|^2}{N_0}<\gamma_E\right\}\\
&= 1-\prod_{m=1}^{|\mathcal{E}_k|}\mathbb{P}\left\{\frac{P|h_{e_{k_m}}|^2}{N_0}<\gamma_E\right\}\\
&= 1-\prod_{m=1}^{|\mathcal{E}_k|}\left\{1-e^{\left(\frac{-\gamma_E N_0}{P}d_{e_{k_m}}^\alpha\right)}\right\}.
\end{aligned} \quad (12)$$

We then derive the COP under the two transmission schemes. Notice that γ_C is the required SINR for the intended receiver correctly decoding the message, thus the COP of link l_k under the AF scheme $P_{co}^{AF}(k)$ can be determined as

$$\begin{aligned}
P_{co}^{AF}(k) &= \mathbb{P}\left\{\frac{P|h_k|^2}{\sum_{i=1}^{k}\frac{|h_k|^2}{|h_i|^2}N_0}<\gamma_C\right\}\\
&= \mathbb{P}\left\{\sum_{i=1}^{k}\frac{1}{|h_i|^2}>\frac{P}{\gamma_C N_0}\right\},\\
&\approx F\left(\hat{\lambda}_{k-1},\lambda_k,\frac{P}{\gamma_C N_0}\right),
\end{aligned} \quad (13)$$

where $\lambda_k=\frac{1}{d_k^\alpha}$ and (13) follows from the approximation approach same as (10).

The COP of link l_k under the DF scheme $P_{co}^{DF}(k)$ can be determined as

$$\begin{aligned}
P_{co}^{DF}(k) &= \mathbb{P}\left\{\frac{P|h_k|^2}{N_0}<\gamma_C\right\}\\
&= 1-e^{\left(\frac{-\gamma_C N_0}{P}d_k^\alpha\right)}.
\end{aligned} \quad (14)$$

B. Route Outage Probabilities

Based on the outage probabilities of a link, we can further derive the outage probabilities for an end-to-end route. Considering the route $\Pi_K=\langle l_1,\ldots,l_K\rangle$, the secrecy outage happens if there is at least one link which is intercepted. Thus, the SOP of route Π_K under the AF scheme $P_{so}^{AF}(\Pi_K)$ and the DF scheme $P_{so}^{DF}(\Pi_K)$ can be determined as

$$\begin{aligned}
P_{so}^{AF}(\Pi_K) &= 1-\prod_{l_k\in\Pi_K}\left\{1-P_{so}^{AF}(k)\right\})\\
&\approx 1-\prod_{l_k\in\Pi_K}\prod_{m=1}^{|\mathcal{E}_k|}F\left(\hat{\lambda}_{k-1},\lambda_{e_{k_m}},\frac{P}{\gamma_E N_0}\right),
\end{aligned} \quad (15)$$

$$\begin{aligned}
P_{so}^{DF}(\Pi_K) &= 1-\prod_{l_k\in\Pi_K}\left\{1-P_{so}^{DF}(k)\right\}\\
&= 1-\prod_{l_k\in\Pi_K}\prod_{m=1}^{|\mathcal{E}_k|}\left(1-e^{\frac{-\gamma_E N_0}{P}d_{e_{k_m}}^\alpha}\right).
\end{aligned} \quad (16)$$

Regarding the COP of route Π_K, the connection outage happens if there is at least one link which is not connected. Thus, the COP of route Π_K under the AF scheme $P_{co}^{AF}(\Pi_K)$ and the DF scheme $P_{co}^{DF}(\Pi_K)$ can be determined as

$$\begin{aligned} P_{co}^{AF}(\Pi_K) &= 1 - \prod_{l_k \in \Pi_K} \left\{1 - P_{co}^{AF}(k)\right\} \\ &\approx 1 - \prod_{l_k \in \Pi_K} \left\{1 - F\left(\hat{\lambda}_{k-1}, \lambda_k, \frac{P}{\gamma_C N_0}\right)\right\}, \end{aligned} \tag{17}$$

$$\begin{aligned} P_{co}^{DF}(\Pi_K) &= 1 - \prod_{l_k \in \Pi_K} \left\{1 - P_{co}^{DF}(k)\right\} \\ &= 1 - e^{\frac{-\gamma_C N_0}{P} \sum\limits_{l_k \in \Pi_K} d_k^{\alpha}}. \end{aligned} \tag{18}$$

C. Comparison Between AF and DF

Based on the outage probabilities analysis, we further compare the security and QoS performance of a route between the AF and DF transmission schemes, which can provide us the insights that how to conduct route selection according to the users' requirements.

Considering the SOPs of link l_k, from (9) and (12) we have

$$\begin{aligned} P_{so}^{AF}(k) &= 1 - \prod_{m=1}^{|\mathcal{E}_k|} \mathbb{P}\left\{\sum_{i=1}^{k-1} \frac{1}{|h_i|^2} + \frac{1}{|h_{e_{k_m}}|^2} > \frac{P}{\gamma_E N_0}\right\} \\ &\le 1 - \prod_{m=1}^{|\mathcal{E}_k|} \mathbb{P}\left\{\frac{1}{|h_{e_{k_m}}|^2} > \frac{P}{\gamma_E N_0}\right\} \\ &= P_{so}^{DF}(k), \end{aligned} \tag{19}$$

where (19) follows since $\sum_{i=1}^{k-1} \frac{1}{|h_i|^2} \ge 0$.

Thus, regarding the security performance of route Π_K we have

$$\begin{aligned} P_{so}^{AF}(\Pi_K) &= 1 - \prod_{l_k \in \Pi_K} \left(1 - P_{so}^{AF}(k)\right) \\ &\le 1 - \prod_{l_k \in \Pi_K} \left(1 - P_{so}^{DF}(k)\right) \\ &= P_{so}^{DF}(\Pi_K). \end{aligned} \tag{20}$$

It indicates that AF transmission scheme outperforms DF transmission scheme in the sense of security performance.

Considering the COPs of link l_k, from (13) and (14) we have

$$\begin{aligned} P_{co}^{AF}(k) &= \mathbb{P}\left\{\sum_{i=1}^{k} \frac{1}{|h_i|^2} > \frac{P}{\gamma_C N_0}\right\} \\ &\ge \mathbb{P}\left\{\frac{1}{|h_k|^2} > \frac{P}{\gamma_C N_0}\right\} \\ &= P_{co}^{DF}(k). \end{aligned} \tag{21}$$

Thus, regarding the QoS performance of route Π_K we have

$$\begin{aligned} P_{co}^{AF}(\Pi_K) &= 1 - \prod_{l_k \in \Pi_K} \left(1 - P_{co}^{AF}(k)\right) \\ &\ge 1 - \prod_{l_k \in \Pi_K} \left(1 - P_{co}^{DF}(k)\right) \\ &= P_{co}^{DF}(\Pi_K). \end{aligned} \tag{22}$$

It indicates that DF transmission scheme outperforms AF transmission scheme in the sense of QoS performance.

Remark 1: The intuition of the performance comparison between the two transmission schemes is that under the AF scheme, the noise at the relay node of each link is cumulative, which not only degrades the SINR at the next intended receiver, but also degrades the SINR at the corresponding eavesdroppers. The comparison also indicates that improving the security performance comes with a cost in terms of the QoS degradation.

IV. Route Selection

Route selection is the process of selecting best end-to-end route(s) which can minimize (or maximize) some route metric(s). In this section, we propose the route selection algorithm which can select and adjust the end-to-end route(s) in a concerned WANET according to different QoS and security requirements of network users.

Based on the results of outage probabilities, we combine the SOP and COP of a route to constitute the corresponding route metric. In order to enable the route selection to perform tradeoff between the QoS and security requirements, we also introduce a control parameter β to adjust the "weights" of the route metric. More formally, let $Q(\Pi_K)$ denote the metric of route $\Pi_K = \langle l_1, \ldots, l_K \rangle$, then $Q(\Pi_K)$ is defined as

$$Q(\Pi_K) = \beta P_{co}(\Pi_K) + (1 - \beta) P_{so}(\Pi_K), \tag{23}$$

where β ranges from 0 to 1. It is notable that the QoS (resp. security) performance of the selected route will be improved (resp. degraded) by increasing β. When we set $\beta = 0$, it indicates that the route selection is depended only on the security requirement, which is suitable to the WANET with dense eavesdroppers. When we set $\beta = 1$, it indicates that the route selection is depended only on the QoS requirement, which will be efficient in the WANET with sparse eavesdroppers.

Substituting (15)−(18) into (23), the expressions of route metrics under AF scheme $Q^{AF}(\Pi_K)$ and DF scheme $Q^{DF}(\Pi_K)$ are determined as

$$\begin{aligned} Q^{AF}(\Pi_K) &= \beta P_{co}^{AF}(\Pi_K) + (1 - \beta) P_{so}^{AF}(\Pi_K) \\ &= 1 - \beta \prod_{l_k \in \Pi_K} \left\{1 - F\left(\hat{\lambda}_{k-1}, \lambda_k, \frac{P}{\gamma_C N_0}\right)\right\} \\ &\quad - (1 - \beta) \prod_{l_k \in \Pi_K} \prod_{m=1}^{|\mathcal{E}_k|} F\left(\hat{\lambda}_{k-1}, \lambda_{e_{k_m}}, \frac{P}{\gamma_E N_0}\right), \end{aligned} \tag{24}$$

$$Q^{DF}(\Pi_K) = \beta P_{co}^{DF}(\Pi_K) + (1-\beta) P_{so}^{DF}(\Pi_K)$$
$$= 1 - \beta e^{\frac{-\gamma_C N_0}{P} \sum\limits_{l_k \in \Pi_K} d_k^{\alpha}}$$
$$- (1-\beta) \prod_{l_k \in \Pi_K} \prod_{m=1}^{|\mathcal{E}_k|} \left(1 - e^{\frac{-\gamma_E N_0}{P} d_{e_{k_m}}^{\alpha}}\right). \quad (25)$$

Applying the route metrics of (24) and (25) into the classical on-demand routing protocols [21], we then propose the following algorithm which can conduct the route selection to satisfy different requirements of network users on both QoS and security, as summarized in Algorithm 1.

Algorithm 1 Route Selection Algorithm

1: The source node sends the route request message (RREQ) for route discovery.
2: After the relay node R_k receives the RREQ message, it calculates the distance between its pre-hop node R_{k-1} and itself, as well as the distance between the corresponding eavesdroppers and itself, respectively. Then, R_k loads the distance information into the RREQ message and sends it to the next-hop node.
3: After the destination receives the first RREQ message, it waits a certain time T to collect more RREQ messages. Based on the requirements on QoS and security, the destination chooses the transmission scheme and set the control parameter β.
4: The destination extracts the distance information from all the RREQ messages and calculates the corresponding route metrics.
5: The destination chooses the route with the minimum route metric to send route reply message (RREP) to the source node.
6: After the source node receives the RREP, the route selection is complete.

V. Numerical Results

In this section, we present the numerical results to illustrate the SOP and COP performance of a specific route, as well as the route selection under the AF scheme and DF scheme.

We first show that how the outage probabilities of a specific route vary with the network parameters, such as the number of hops and the density of eavesdroppers. We set that the distance between two nodes of a link is fixed as $d_k = 1$, and the distance between a legitimate node and its corresponding eavesdropper is fixed as $d_{e_{k_m}} = 5$. The number of eavesdroppers $|\mathcal{E}_k|$ is same for each link. Regarding other basic parameters, we set $P = 10$, $N_0 = 1$, $\alpha = 3$, $\gamma_E = 0.3$ and $\gamma_C = 0.1$.

Fig. 1 summarizes the SOP performance. We can see from Fig. 1 that when the route hops is 1, the SOP under AF and DF schemes are the same; when the route hops is larger than 1, the SOP under the AF scheme is smaller than that under the DF scheme. It indicates that for a multi-hop route, the advantage of AF scheme is that it can lead to a better security

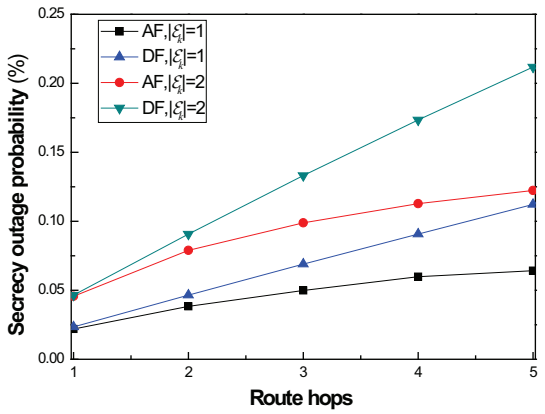

Fig. 1. Secrecy outage probability varies with the number of hops of a route under AF and DF schemes.

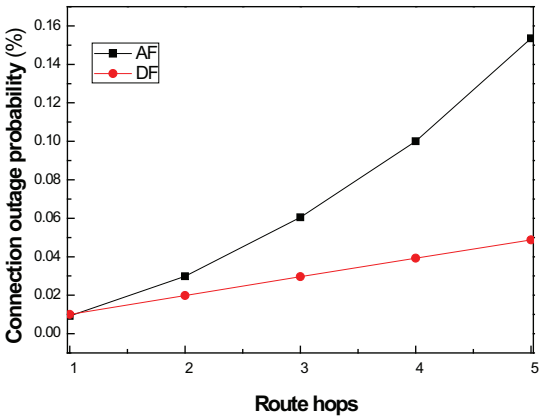

Fig. 2. Connection outage probability varies with the number of hops of a route under AF and DF schemes..

performance. Another interesting observation from Fig. 1 is that the growth trend of SOP under the DF scheme is almost linear with the number of hops, while under the AF scheme it tends to be flat as the number of hops becomes large. This is because that under the AF scheme, the noise at the relay node of each link is cumulative, which will lead that the SOP of a link decreases as the number of hops increases.

Fig. 2 summarizes the COP performance. It can be seen from Fig. 2 that when the route hops is 1, the COP under AF and DF schemes are the same; when the route hops is larger than 1, the COP under the DF scheme is smaller than that under the AF scheme. It indicates that for a multi-hop route, the advantage of DF scheme is that it can lead to a better QoS performance. We can also see that the growth rate of COP under the AF scheme is much faster than that under the DF scheme. This is because that under the AF scheme, the cumulative noise will degrade the SINR at the intended receiver.

We further illustrate in Fig. 3 and Fig. 4 that how the route selection is conducted in a WANET based on the different security and QoS requirements. We consider a multi-hop WANET where 30 legitimate nodes (shown by dots) are placed randomly on a 10×10 square area. The source node is placed

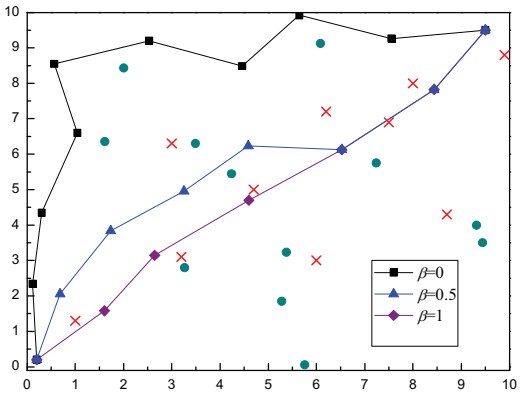

Fig. 3. Illustration of route selection with different route metrics under AF scheme.

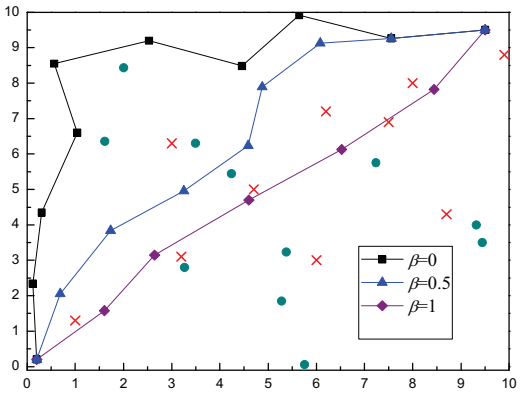

Fig. 4. Illustration of route selection with different route metrics under DF scheme.

at the lower left corner and the destination is placed at the upper right corner. In order to gain more insights into the route selection with different requirements on security and QoS, we strategically place 10 eavesdroppers (shown by "×") close to the line that connects the source and destination.

We can see from Fig. 3 and Fig. 4 that when the network user does not care about the security for data transmission, the route metric will be set as $\beta = 1$, and the selected route will be the one with the minimum connection outage probability even though it may pass through the eavesdroppers. When the network user only care about the security for data transmission, the route metric will be set as $\beta = 0$, and the selected route will be the one with the minimum secrecy outage probability (i.e., avoid the eavesdroppers as much as possible). When the network user takes into account both the security and QoS for data transmission, for example the route metric is set as $\beta = 0.5$, the selected route will be the one which can avoid parts of the eavesdroppers while ensure the hops is not too long. It is notable that the selected routes under AF and DF schemes are different when $\beta = 0.5$. This is because that the cumulative noise under AF scheme leads to a very small SOP for link l_k when k is large, thus the remaining hops will be selected only with the consideration of their QoS performance.

VI. Conclusion

This paper focuses on the security and QoS of route selection in multi-hop WANETs with eavesdroppers. For such a WANET under two typical transmission schemes AF and DF, we have derived the SOP and COP of a single hop link and extended the results to an end-to-end route. Based on the results of outage probabilities, we have formulated the route metric by combining the SOP and COP, and proposed the algorithm which enables the route selection to be flexibly conducted and adjusted according to the different security and QoS requirements.

References

[1] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*. Prentice Hall Press, 2002.
[2] C. E. Perkins, *Ad Hoc Networking*. Addison-Wesley Professional, 2008.
[3] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, 1998.
[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[5] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
[6] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.
[7] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.
[8] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.
[9] J. Vilela, P. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 616–627, 2011.
[10] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, 2011.
[11] S. Vasudevan, D. Goeckel, and D. F. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *ACM Mobihoc,*, 2010, pp. 21–30.
[12] C. Zhang, Y. Song, Y. Fang, and Y. Zhang, "On the price of security in large-scale wireless ad hoc networks," *IEEE/ACM Trans. Netw*, vol. 19, no. 2, pp. 319–332, 2011.
[13] O. Koyluoglu, C. Koksal, and H. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, 2012.
[14] W. Saad, X. Zhou, B. Maham, T. Başar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, 2012.
[15] L. Chen, "Secure network coding for wireless routing," in *Proc. IEEE ICC*, 2014, pp. 1941–1946.
[16] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Minimum energy routing and jamming to thwart wireless network eavesdroppers," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1433–1448, 2015.
[17] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, in press, 2015. DOI: 10.1109/TCOMM.2015.2514094.
[18] X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, 2011.
[19] G. Amarasuriya, C. Tellambura, and M. Ardakani, "Asymptotically-exact performance bounds of af multi-hop relaying over nakagami fading," *IEEE Trans. Commun.*, vol. 59, no. 4, pp. 962–967, 2011.
[20] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products, 7th edition*. Academic Press, 2000.
[21] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad Hoc Networks*, vol. 2, no. 1, pp. 1–22, 2004.