Invited Article

Modified Dijkstra's Routing Algorithm for Security with Different Trust Degrees

Chan Dai Truyen Thai[1], Vo Nguyen Quoc Bao[2], Tran Quang Nhu[1], Nguyen Thi Yen Linh[2], Huynh Van Hoa[2]

[1] Vietnamese-German University (VGU), Vietnam
[2] Posts and Telecommunications Institute of Technology (PTIT), Ho Chi Minh City, Vietnam

Correspondence: Chan Dai Truyen Thai, chan.ttd@vgu.edu.vn
Communication: received 18 February 2020, revised 2 March 2020, accepted 2 March 2020
Online publication: 10 June 2020, Digital Object Identifier: 10.21553/rev-jec.250
The associate editor coordinating the review of this article and recommending it for publication was Prof. Vo Nguyen Quoc Bao.

Abstract– **A great number of efficient methods to improve the performance of the networks have been proposed in physical-layer security for wireless communications. So far, the security and privacy in wireless communications is optimized based on a fixed assumption about the trustworthiness or trust degrees (TD) of certain wireless nodes. The nodes are often classified into different types such as eavesdroppers, untrusted relays, and trusted cooperative nodes. Wireless nodes in different networks do not completely trust each other when cooperating or relaying information for each other. Optimizing the network based on trust degrees plays an important role in improving the security and privacy for the modern wireless network. We proposed a novel algorithm to find the route with the smallest total transmission time from the source to the destination and still guarantee that the accumulated TD is larger than a trust degree threshold. Simulation results are presented to analyze the affects of the transmit SNR, node density, and TD threshold on different network performance elements.**

Keywords– **Physical-layer security, trust degree, trustworthiness, untrusted relay.**

1 Introduction

The wireless communications has been dramatically developed, especially in the last two decades, however, starts to face a lot of challenges in security and privacy [1–3]. In the past few years, the physical-layer security for wireless communications has given a great number of efficient methods to improve the performance of the networks [4]. However, several issues play important roles in optimizing the security in practical conditions such as energy [5], channel estimation [6], and trust factors [7–9].

So far, the security and privacy in wireless communications is optimized based on a fixed assumption about the trustworthiness of the wireless nodes. They are often classified into different types such as eavesdroppers, untrusted relays, and trusted cooperative nodes [10–12]. However, the trustworthiness or TD of a node may not be always clear and strongly depends on the social relationship of its and the legitimate nodes' users (such as friendship in social network) [13–15]. Consequently, TD issues should be considered when optimizing the network performance in order to provide better security and privacy in practice. Nowadays in the world, more and more wireless, especially tiny, devices are used in communication as well as supervising in transportation, security, health, education, and environment. Wireless nodes in different networks with different purposes and/or in different organizations, therefore, do not completely trust each other when relaying information for each other, in the meantime, need to cooperate due to remote or inaccessible locations. Solving this problem plays an important role in improving the security and privacy for the modern wireless network, especially when considering new aspects [7, 16, 17].

A great number of researches in physical-layer security have focused on the one-hop or two-hop wireless networks. Recently, a few works have investigated on the multi-hop scenarios. For example, a physical layer security-aware routing scheme is proposed for a multi-hop network with decode-and-forward (DF) relays. Several outage probabilities in close forms are analytically derived. However, in the routing algorithm, the security constraints are not considered in every route selection step. The well-known Bell-Ford algorithm is applied and the security metrics are calculated for the final solution only [18]. Another research also uses Bell-Ford algorithm to find the best route to the destination [19], however, like [18], it does not consider illegitimate nodes with different trust degrees but only fixed clearly malicious nodes, known as eavesdroppers. A Dijkstra algorithm is proposed to add randomization to the routing in order take less predictable paths. It focuses on the protocol characteristics and does not consider trust degrees in the model [20].

Recently a few research groups have investigated the issue of different trustworthiness levels or trust degrees

in two-hop communication as we mentioned above [4]. To the best of our knowledge, this paper is the one of the first works to consider trust degrees for multi-hop networks. The novelty of this work can be summarized as follows:

- We propose a novel algorithm to find the route with the shortest total transmission time from the source to the destination and still guarantee that the accumulated TD is larger than a trust degree threshold.
- We use accumulated TD along the considered route to calculate the expected probability that at least one of the relays use the extracted information for a malicious purpose.
- We analyze the affects of the transmit SNR, node density, and TD threshold to network performance factors such as the successful delivery ratio, total transmission time, and number of hops in a route.

The remaining of the paper is organized as follows. Section 2 presents the system model that the paper will follow. Section 3 describes the proposed routing algorithm. Section 4 describes the simulation scenarios, presents and analyzes the results; and section 5 concludes the paper.

2 System Model

We consider a network with n nodes. Node 1 wants to send message s to node n. Nodes 1 and n are legitimate and also respectively referred to as the source and destination nodes. However, they may not be directly linked by a reliable channel. Thus the other $n-2$ illegitimate nodes will help by decoding and forwarding the message in a hop-by-hop manner. Each node has a different TD of $t_i \in [0\ 1]$, $i = \{1, ..., n\}$, viewed from the legitimate nodes. It is the probability that a node will not use the information extracted, when decoding the message in the process of helping, for a malicious purpose. Certainly, the TD of the legitimate nodes is always 1. The directly connecting and available link between node i and node j is denoted by l_{ij}. Assume that all node have no buffer, i.e., they need to forward all bits they received and decoded.

Since all nodes use DF relaying mode, a relaying node needs to receive the signal from the previous node in the relaying route with enough SNR, fully decode the message, and re-encode it with a rate which is the capacity of the channel between it and the next node in the route as shown in Figure 1. It means that a relay will have complete information about s. What decides the security level of s is the TDs of the nodes in the relay set, that the message will go through, denoted here by $\mathcal{R}$. The probability that the message is used for a malicious purpose, by at least a certain node, is given by

$$p_{\mathrm{M}} = 1 - \prod_{i \in \mathcal{R}} t_i. \tag{1}$$

We assume that s is not a completely secured message, i.e., we accept that the message is used for a malicious purpose with probability lower than threshold probability p_{T}. If $p_{\mathrm{T}} = 0$, i.e., $p_{\mathrm{M}} \leq 0$, $\prod_{i \in \mathcal{R}} t_i \geq 1$, $\prod_{i \in \mathcal{R}} t_i = 1$ or all relays have TDs of 1, the message is completely secured.

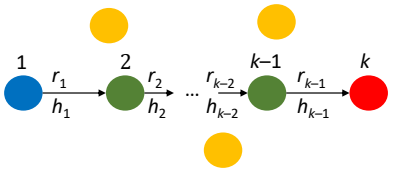

Figure 1. A certain considered route in the network with the blue source, green relays, and red destination. The yellow nodes are not in the considered route.

We also assume that when a node in a route transmits, only the next node[1] in the route receives the signal such that in this paper, we only consider the insecurity due to the low trust degrees of the relays but not the eavesdropping of certain eavesdroppers or other non-targeted illegitimate nodes. Two scenario examples with such a scenario are (*i*) a wire network with copper or optical cables; (*ii*) a wireless network with precise beamforming transmission between any two nodes.

Figure 1 shows a certain route ($\mathcal{R}$) in the network along which the nodes are re-numbered from 1 (the source) to k (the destination, also node n in the network). We denote the channel between node i and $i+1$ along the route as h_i. The maximum achievable rate (MAR) of the transmission from node i to node $i+1$ is given by

$$c_i = \log_2\left(1 + \frac{p|h_i|^2}{\sigma^2}\right),\ i \in \mathcal{R}, \tag{2}$$

where p and σ^2 are respectively the transmit and noise powers. If all nodes in the route transmit with the same rate, they can use the same constellation and the rate is given by

$$r = \min_{i \in \mathcal{R}} c_i \tag{3}$$

to make sure that all receivers along the route can decode the message. However, in order to optimize the routing and increase end-to-end transmission rate, each node along the route can re-encode the message with a different constellation and therefore a different rate of r_i (bits/s/Hz). Assume that all transmissions take place in 1-Hz bandwidth. The necessary time for transmitting f bits from node i to node $i+1$ is $\frac{f}{r_i}$. The time it takes to deliver f bits from the source to the destination via the considered route, excluding other processing times, is given by $T = \sum_{i \in \mathcal{R}} \frac{f}{r_i}$ (s). Since $r_i \leq c_i$, to minimize T, r_i should be chosen as c_i and $T = \sum_{i \in \mathcal{R}} \frac{f}{c_i}$ (s).

3 Proposed Routing Algorithm

The Dijkstra's algorithm is used to find the shortest path between a source and a destination in a network.

[1]In case of a more general scenario where other nodes along the route can receive or overhear parts of the signal, the consequence is also the same as in the assumed scenario in this paper.

Table I
STEPS OF THE PROPOSED ROUTING ALGORITHM FOR THE CASE OF $\alpha = 0.80$.
ONLY ROUTES WITH ACCUMULATED TD WHICH IS AT LEAST 0.8 ARE CONSIDERED

Iteration	$\mathcal{S}$	D_{12}	**Path**	T_{12}	D_{13}	**Path**	T_{13}	D_{14}	**Path**	T_{14}	D_{15}	**Path**	T_{15}	D_{16}	**Path**	T_{16}
1	1	1	1-2	0.9	1	1-3	0.9	∞	-	-	∞	-	-	9	1-6	1.00
2	1,2	1	1-2	0.9	1	1-3	0.9	∞	-	-	∞	-	-	9	1-6	1.00
3	1,2,3	1	1-2	0.9	1	1-3	0.9	3	1-3-4	0.81	∞	-	-	6	1-3-6	0.90
4	1,2,3,4	1	1-2	0.9	1	1-3	0.9	3	1-3-4	0.81	∞	-	-	4	1-3-4-6	0.81
5	1,2,3,4,6	1	1-2	0.9	1	1-3	0.9	3	1-3-4	0.81	11	1-6-5	0.80	4	1-3-4-6	0.81
6	1,2,3,4,6,5	1	1-2	0.9	1	1-3	0.9	3	1-3-4	0.81	11	1-6-5	0.80	4	1-3-4-6	0.81

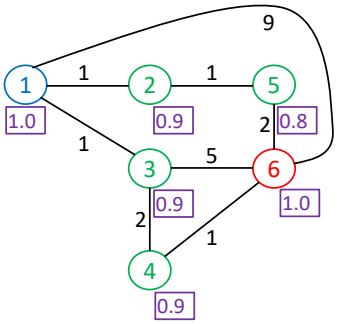

Figure 2. An example of the network with 6 nodes. The violet number below each node shows its TD. The number next to a link shows its cost.

The additive cost of each available link in the network is given beforehand. The shortest path is the path with the smallest accumulated cost when going from the source to the destination. The algorithm will check all possible routes by moving one by one node from the tentative list to the permanent list and expanding the known network gradually to the destination [21].

In this paper, we will find the path with the shortest delivery time, therefore, the time for transmitting 1Kbits from a node to the next node is the cost in the applied Dijkstra's algorithm. We define the cost of a link as $\frac{f}{c_i}$. However, in this paper, we also need to consider the TDs. We therefore modify the algorithm by adding the constraint regarding the TDs in the proposed routing algorithm. Denote the cost of link l_{ij} by d_{ij}. If $d_{ij} > c_{\max}$, where $c_{\max}$ is a very large number, there is no direct link between node i and node j.

In this section, we explain how the proposed routing algorithm is conducted. Consider an example of network as shown in Figure 2. There are 6 nodes with different TDs shown in violet boxes below the nodes. Each link has an associated cost shown next to it. We will find a path from node 1 to node 6 with the smallest accumulated cost and the accumulated TD must be larger than a certain TD threshold (α). In all possible routes from node i to node j in the network, we denote the route with the smallest accumulated cost from node i to node j by $\mathcal{P}_{ij}$, its corresponding cost by D_{ij}, and its corresponding accumulated TD by T_{ij}. If $\mathcal{R}_{ij}$ denotes the set of all nodes along path $\mathcal{P}_{ij}$, we can write $T_{ij} = \prod_{m \in \mathcal{R}_{ij}} t_m$. In case of general n, the routing algorithm is equivalent to the following optimization problem

$$\begin{aligned} &\min_{\mathcal{P}_{1n}} \ D_{1n} \\ &\text{subject to } T_{1n} \leq \alpha. \end{aligned} \tag{4}$$

The proposed routing algorithm for general n is given in Algorithm 1. Below we demonstrate it with the network example in Figure 2. To initialize the algorithm, we set permanent list $\mathcal{S} = \{1\}$ (only the source node is included in $\mathcal{S}$) and tentative list $\mathcal{S}' = \{2, ..., 6\}$. Using only the information about the costs of the links between 1 and its adjacent nodes (2 and 3), we calculate the path from 1 to all other nodes as shown in the first row in the Table I. Nodes 4 and 5 cannot be reached only via the links directly connected to the nodes in $\mathcal{S}$ (l_{12} and $l_{1,3}$). The cost of the route from 1 to 4 (or 5) with the minimum accumulated cost is ∞. The corresponding path and the accumulated TD are therefore not available.

Considering all nodes in $\mathcal{S}'$, we select the node with

Algorithm 1: Finding the shortest path from node 1 to node n such that the accumulated TD is smaller than α

Data: Link costs d_{ij}, $i, j \in \{1, ..., n\}$; cost threshold $c_{\max}$; TD threshold α.
Result: The shortest path p_o.

1) Initialize: permanent list of nodes $\mathcal{S} = \{1\}$; tentative list $\mathcal{S}' = \{2, 3, ..., n\}$; accumulated cost for the path from node 1 to node i as $D_{1i} = d_{1i}$, $i \in \{1, ..., n\}$.
2) Select the next node in $\mathcal{S}'$ to be moved to $\mathcal{S}$:
$$j = \arg\min_{m \in \mathcal{S}'} D_{1m}. \tag{5}$$
3) Add j to permanent list $\mathcal{S}$: $\mathcal{S} = S \cup \{k\}$.
4) Drop j from tentative list $\mathcal{S}'$: $\mathcal{S}' = \mathcal{S}' \backslash \{k\}$.
5) Define the set of all neighboring nodes of node j which are in $\mathcal{S}'$ and have the accumulated TD from node 1 of at least α as follows
$$\mathcal{N}_j = \{m | m \in \mathcal{S}', d_{jm} < c_{\max}, T_{1m} \geq \alpha\}. \tag{6}$$
6) Check for improvement in the minimum cost path from node 1 to each node in $\mathcal{N}_j$ as follows
$$D_{1m} = \min\{D_{1m}, D_{1j} + d_{jm}\}, \text{ for } m \in \mathcal{N}_j \cap \mathcal{S}'. \tag{7}$$
7) Go back to step (2) until $\mathcal{S}' = \emptyset$.

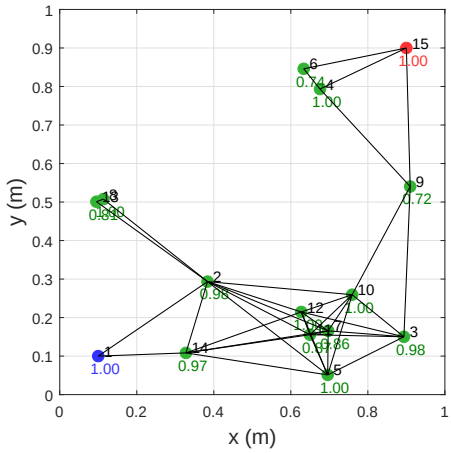

Figure 3. An example of the network with 15 nodes. The colorful number below each node shows its trust degree.

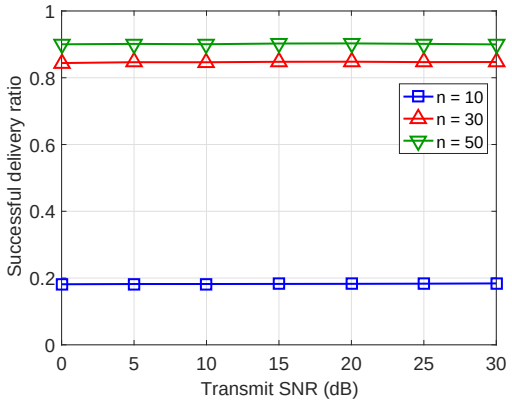

Figure 4. The successful delivery ratio in case $\alpha = 0.7$.

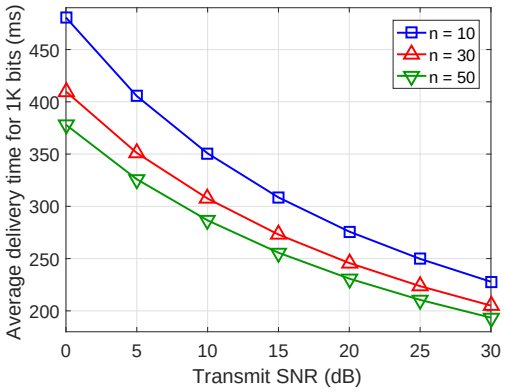

Figure 5. The average delivery time for 1K bits in case $\alpha = 0.7$.

the smallest accumulated cost when going from node 1 to it basing on the information in the first row. Since nodes 2 and 3 have the same accumulated cost to 1, either of them can be selected. Here node 2 is selected, added to $\mathcal{S}$, and also removed from $\mathcal{S}'$. After that, the adjacent nodes of 2 are considered as next destinations and we update the corresponding information in row 2. The process continues until all nodes are added to $\mathcal{S}$ and $\mathcal{S}'$ is empty. In each column of the last row, the shortest path to the corresponding node is shown. In row to the path to node 5 is not added since $T_{15} = 0.72 < \alpha$.

4 Simulation Results

In this section, we present the simulation results and analyze the different elements affecting the network performance. In the simulations, n nodes' positions are randomized with the uniform distribution in a square of 1m$\times$1m. Two nodes have reliable wireless connection only when the distance between them is small than a threshold of $d_{\text{th}} = 0.4$. A reliable wireless channel is randomly distributed with σ_{h}^2-variance and 0-mean complex Normal distribution where $\sigma_{\text{h}}^2 = \left(\frac{c_{\text{L}}}{4\pi f_{\text{R}} d}\right)^2$ in which c_{L} is the light velocity, f_{R} is the radio frequency, and d is the distance between the considered transmitter and receiver. We use $f_{\text{R}} = 900$ MHz, one of the unlicensed frequency bands in the US. The variance of the channel reflects the simplified path loss of the Friis Transmission Formula [22]. The TD of an illegitimate node is randomized with the 1-mean and 0.4-variance Normal distribution and truncated in the value range of [0 1], i.e., if the random value is larger than 1, the TD is set to 1 and if it is smaller than 0, the TD is set to 0. Figure 3 shows a network example with 15 nodes. The source, illegitimate, and destination nodes are filled with blue, green, and red colors, respectively. We find the route from node 1 to node n with the shortest transmission time for 1 Kbits and accumulated TD at least α.

In the first simulation, the transmit SNR is varied and different numbers of nodes are considered with fixed $\alpha = 0.7$. Figure 4 shows the successful delivery ratio (SDR) for 1 Kbits from node 1 to node n in every realization of topology, TDs, and channels. If in a random realization, a route from node 1 to node n satisfying the TD threshold does not exist, another random realization is generated until such a route exist and the data about the delivery time and number hops is accumulated. In a simulation, we need to generate a certain number of successful realizations. The ratio of the number of successful realizations and that of generated ones is the SDR. As shown, the SDR does not depend on the transmit SNR because a higher transmit SNR only improves the transmission between any two nodes, and consequently, the cost or the average delivery time. More nodes leads to a higher SDR since nodes can more easily find the next nodes for a route to the destination. However, when the node number is already high, increasing it does not increase SDR significantly since the nodes are already dense.

Figure 5 shows the average delivery time for 1 Kbits from node 1 to node n. As shown, all delivery times decrease with the transmit SNR of each hop since the receiver of each hope can receive a better signal and reduce the transmission time in each hop. More number of nodes in a network lead to a shorter delivery time because on average there is a shorter distance, and therefore, a better transmission rate or a shorter transmission time between any two nodes.

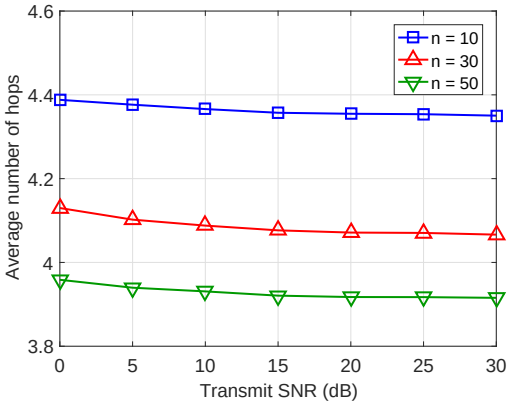

Figure 6. The average number of hops of the best route in case $\alpha = 0.7$.

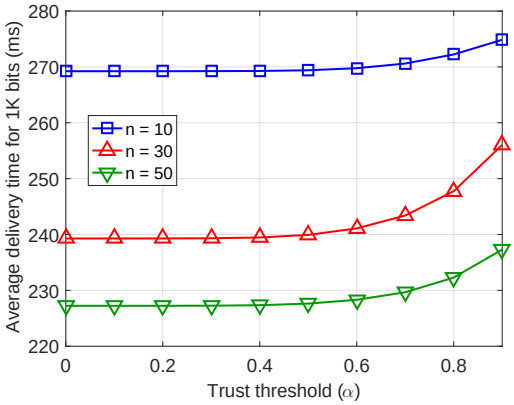

Figure 8. The average delivery time with varied TD threshold and fixed SNR at 20dB.

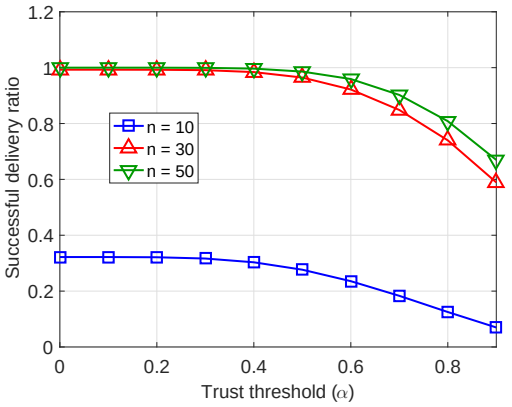

Figure 7. The successful delivery ratio with varied TD threshold and fixed SNR at 20dB.

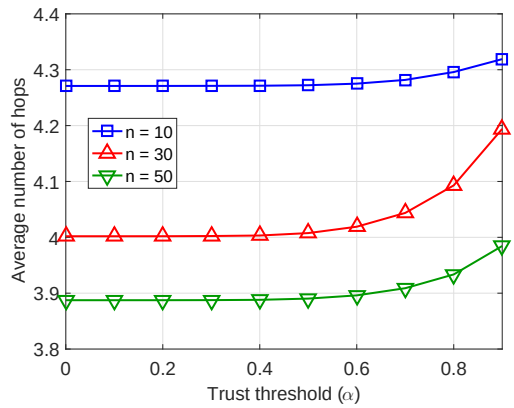

Figure 9. The average number of hops with varied TD threshold and fixed SNR at 20dB.

Figure 6 shows the average number hops that the best route from node 1 to node n goes through. It decreases slightly with the transmit SNR since a better transmit SNR can increase each hop transmission rate so routes with fewer hops but with worse channels can combat with the other routes and become the best ones. More nodes in the network lead to smaller number of hops since the nodes can find the next nodes more easily with a determined channel distance threshold d_{th}.

In the second simulation, we vary the trust threshold (α) to see the affects of this parameter on the performance of the network in terms of SDR, the average delivery time, and the average number of hops. In this case, we set the transmit SNR to 20 dB. Differently to the case in Figure 4, the SDR decreases when the trust threshold increases as it puts stricter trust threshold constraint (the accumulated TD must be greater than the trust threshold constraint). Similarly to other cases, denser nodes will so help to increase the SDR. When α is low enough (about 0.3) and n is large enough (about 30), almost all random realizations succeed.

Figure 8 shows the average delivery time from node 1 to node n. As expected, when a stricter TD constraint is put in the shortest route finding problem, the network performance gets worse, i.e., the average delivery time is longer. As usual, the case with more nodes performs better. Figure 9 shows the average number of hops. It also increases with α since a stricter TD constraint will not allow less trusted routes with fewer nodes to be considered.

5 Conclusion

In this paper, we proposed a modified algorithm to find the route with shortest total transmission time based on Dijsktra's shortest path algorithm with additional trust degree (TD) constraints for the multi-hop decode-and-forward relay network. The simulation results show that successful delivery ratio increases with transmit SNR and decreases when node number increases and the TD constraint is stricter. In the meantime, the time delivery time and average number of hops increases with the node number and the TD constraint and decreases when the transmit SNR increases. Therefore precisely determining the TDs of the nodes in a network is very important since it helps to better optimize the routing and increases the security and network performance. In case high-resolution TDs are not available, classifying into different types, with different TD ranges, also helps.

Acknowledgement

This work was supported by NAFOSTED Grant 102.02-2018.318.

References

[1] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 1550–1573, Feb. 2014.

[2] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6854–6868, 2015.

[3] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Secret group key generation in physical layer for mesh topology," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, Dec. 2015, pp. 1–6.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2009.

[5] L. Jiang, H. Tian, Z. Xing, K. Wang, K. Zhang, S. Maharjan, S. Gjessing, and Y. Zhang, "Social-aware energy harvesting device-to-device communications in 5G networks," *IEEE Wireless Communications*, vol. 23, no. 4, pp. 20–27, 2016.

[6] Q. Li and L. Yang, "Artificial Noise Aided Secure Precoding for MIMO Untrusted Two-Way Relay Systems With Perfect and Imperfect Channel State Information," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2628–2638, 2018.

[7] M. Zhao, J. Y. Ryu, J. Lee, T. Q. S. Quek, and S. Feng, "Exploiting trust degree for multiple-antenna user cooperation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 4908–4923, 2017.

[8] J. Ryu, J. Lee, and T. Q. S. Quek, "Trust Degree based Beamforming for MISO Cooperative Communication System," *IEEE Communications Letters*, vol. 19, no. 11, pp. 1957–1960, 2015.

[9] Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, "A scheme for trustworthy friendly jammer selection in cooperative cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3500–3512, 2019.

[10] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Communications Letters*, vol. 19, no. 3, pp. 463–466, 2014.

[11] J. Xiong, L. Cheng, D. Ma, and J. Wei, "Destination aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7274–7284, 2015.

[12] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1517–1530, 2015.

[13] Y. Li, T. Wu, P. Hui, D. Jin, and S. Chen, "Social-aware D2D communications: qualitative insights and quantitative analysis," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 150–158, 2014.

[14] M. Zhang, X. Chen, and J. Zhang, "Social-aware relay selection for cooperative networking: An optimal stopping approach," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Jun. 2014, pp. 2257–2262.

[15] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Exploiting social ties for cooperative D2D communications: A mobile social networking case," *IEEE/ACM Transactions on Networking*, vol. 23, no. 5, pp. 1471–1484, 2014.

[16] J. P. Coon, "Modelling trust in random wireless networks," in *Proceedings of the 11th International Symposium on Wireless Communications Systems (ISWCS)*, Aug. 2014, pp. 976–981.

[17] W. She, Q. Liu, Z. Tian, J. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38 947–38 956, 2019.

[18] Y. Xu, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Physical layer security-aware routing and performance tradeoffs in ad hoc networks," *Computer Networks*, vol. 123, pp. 77 – 87, 2017.

[19] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Transactions on Communications*, vol. 64, no. 2, pp. 753–764, 2016.

[20] M. Pagan, A. Hession, and S. Yuan, "A security-enhanced routing algorithm with path randomization," in *Proceedings of the International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2015, pp. 1137–1141.

[21] D. Medhi and K. Ramasamy, *Network Routing: Algorithms, Protocols, and Architectures*. Elsevier, 2007.

[22] R. C. Johnson and H. Jasik, *Antenna Engineering Handbook*, 2nd ed. New York, NY: McGraw-Hill, Inc., 1984.

Chan Dai Truyen Thai received the B.S. degree from Posts and Telecommunications Institute of Technology (PTIT), Ho Chi Minh City, Vietnam; the M.Sc. degree from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea; and the Ph.D. degree from Aalborg University, Denmark, in 2003, 2008, and 2012, respectively. He was with IFSTTAR, LEOST, Villeneuve d'Ascq, France; with Singapore University of Technology and Design (SUTD); and is now the Academic Coordinator cum Senior Lecturer of the Electrical and Computer Engineering (ECE) Study Program, Vietnamese-German University (VGU). His research interests include cooperative communications, vehicle-to-vehicle communications, communication for high-speed vehicles, security in wireless communications, and security in smart grid.

Vo Nguyen Quoc Bao received the B.E. and M.Eng. degree in electrical engineering from Ho Chi Minh City University of Technology (HCMUT), Vietnam, in 2002 and 2005, respectively, and Ph.D. degree in Electrical Engineering from University of Ulsan, South Korea, in 2009. In 2002, he joined the Department of Electrical Engineering, Posts and Telecommunications Institute of Technology (PTIT), as a lecturer. Since February 2010, he has been with the Faculty of Telecommunications, PTIT, where he is currently an Associate Professor. He is a Senior Member of IEEE. His research interests include wireless communications and information theory with current emphasis on MIMO systems, cooperative and cognitive communications, physical layer security, and energy harvesting. He is currently serving as the Editor of Transactions on Emerging Telecommunications Technologies (Wiley ETT) and VNU Journal of Computer Science and Communication Engineering. He is also a Guest Editor of EURASIP Journal on Wireless Communications and Networking, special issue on "Cooperative Cognitive Networks" and IET Communications, special issue on "Secure Physical Layer Communications". He served as a Technical Program co-chair for ATC (2013,2014), NAFOSTED-NICS (2014, 2015, 2016), REV-ECIT 2015 and ComManTel (2014, 2015), and SigComTel (2017, 2018). He is a Member of the Executive Board of the Radio-Electronics Association of Vietnam (REV) and the Electronics Information and Communications Association Ho Chi Minh City (EIC). He is currently serving as vice chair of the Vietnam National Foundation for Science and Technology Development (NAFOSTED) scientific Committee in Information Technology and Computer Science (2017-2019).

Tran Quang Nhu received the B. S. degree in electronics and telecommunications engineering and the M. S. degree in telecommunications engineering from the University of Transport and Communication (UTC), Vietnam, in 2008 and 2012, respectively. From 2008 to 2009, he joined Global Telecommunications Corporation (GTEL), and from 2009 to 2012, VNPT-NEC Telecommunication Systems Company. He is now the Team Leader of lab engineers, ECE study program, Vietnamese-German University (VGU). His major research interests are wireless communications, radio frequency engineering, IP networking.

Nguyen Thi Yen Linh was born in Tien Giang province, Viet Nam in 1982. She received the B.Sc. and M.Sc. degrees in applied physics from Vietnam National University, Ho Chi Minh (VNUHCM) in 2004 and 2008, respectively. In 2009, she joined the Department of Foundation, Posts and Telecommunications Institute of Technology (PTIT), as a lecturer. She is now a research member of Wireless Communication Laboratory (WCOMM), PTIT, Vietnam. Her major research interests are random wireless network, short packet communication, cooperative communications, cognitive radio and physical layer security.

Huynh Van Hoa received the B. S. degree in electronics and telecommunications engineering and the M. S. degree in telecommunications engineering from Posts and Telecommunications Institute of Technology (PTIT), Vietnam, in 2013 and 2018, respectively. In 2018, he joined the Department of Telecommunications, PTIT, as a lecturer. His major research interests are wireless communications, cooperative and cognitive communications, physical-layer security, NOMA and Short-packet communications.