Regular Article

Security for Multi-hop Communication of Two-tier Wireless Networks with Different Trust Degrees

Chan Dai Truyen Thai[1], Vo Nguyen Quoc Bao[2], Uyen Han Thuy Thai[3]

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

Correspondence: Chan Dai Truyen Thai, chan.ttd@vgu.edu.vn
Communication: received 10 July 2022, revised 11 October 2022, accepted 16 October 2022
Online publication: 26 October 2022, Digital Object Identifier: 10.21553/rev-jec.319
The associate editor coordinating the review of this article and recommending it for publication was Prof. Ngoc The Dang.

Abstract– **Many effective strategies for enhancing network performance have been put forth for wireless communications' physical-layer security. Up until now, wireless communications security and privacy have been optimized based on a set assumption on the reliability or network tiers of certain wireless nodes. Eavesdroppers, unreliable relays, and trustworthy cooperative nodes are just a few examples of the various sorts of nodes that are frequently categorized. When working or sharing information for one another, wireless nodes in various networks may not always have perfect trust in one another. Modern wireless networks' security and privacy may be enhanced in large part by optimizing the network based on trust levels. To determine the path with the shortest total transmission time between the source and the destination while still ensuring that the private messages are not routed through the untrusted network tier, we put forth a novel approach. To examine the effects of the transmit SNR, node density, and the percentage of the illegitimate nodes on various network performance components, simulation results are provided.**

Keywords– **Physical-layer security, two-tiered network, clustering, gateway, k-means, wireless sensor network.**

1 Introduction

Although wireless communications have advanced significantly, particularly in the last two decades, they are now beginning to encounter significant security and privacy issues [1–4]. A lot of effective ways to boost network performance have been developed recently thanks to physical-layer security for wireless communications [5]. However, a number of parameters, including energy [6], channel estimation [7, 8], and trust factors [9–11], play crucial roles in maximizing security in real-world situations.

As of now, wireless communications security and privacy are maximized based on a predetermined belief in the dependability of the wireless nodes. According to [12–14], they are frequently divided into several sorts, such as eavesdroppers, untrusted relays, and trusted cooperative nodes [15]. However, a node's trustworthiness or TD may not always be obvious and is heavily influenced by the social connections between its users and those of legitimate nodes (such as friendship in social networks) [16–18]. As a result, TD concerns have to be taken into account while enhancing network efficiency to really provide improved security and privacy. More and more wireless, particularly small, gadgets are being utilized throughout the globe today for communication as well as for monitoring security, health, education, and the environment. Wireless nodes in various networks serving various functions and/or belonging to various organizations do not fully trust one another while relaying information for the other, yet they still need to work together because of distant or inaccessible locations. The solution to this issue is crucial for enhancing the security and privacy of the current wireless network, particularly when taking into account novel factors [9, 19, 20].

Physical-layer security studies have largely concentrated on one-hop or two-hop wireless networks. Several studies have recently looked into multi-hop scenarios. For instance, a multi-hop network with decode-and-forward (DF) relays is presented with a physical layer security-aware routing method. Analytically, a number of outage probabilities in near forms are obtained. However, not every route selection step in the routing algorithm takes the security limitations into account. Only the final answer is used to calculate the security metrics using the well-known Bell-Ford technique [21]. Another study used the Bell-Ford method to determine the optimum path to the target [22], however unlike [21], it only takes into account fixed, obviously hostile nodes, commonly known as eavesdroppers. It is suggested to use a Dijkstra algorithm to randomize the routing in order to pick less predictable pathways. The model [23] concentrates on protocol features but ignores trust levels.

A few study groups have recently looked into the topic of two-tiered wireless networks [24]. However, to the best of our knowledge, this research is among the first to consider two tier networks with different trust

1859-378X–2022-3403 © 2022 REV

degrees. This work's originality may be summed up as follows:

- The route with the quickest total transmission time between the source and the destination that nonetheless ensures that the private messages are not routed through the untrusted network tier is what we suggest as our novel method.
- We consider clustering with inter-cluster links through gateways and analyze their corresponding computational complexity.
- We examine how transmit SNR, node density, and the percentage of the illegitimate nodes impact network performance indicators such the successful delivery rate, total transmission duration, and number of hops in a route.

The remainder 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 take into account a network of n nodes as in an example in Figure 1. To node n, node 1 wishes to deliver message s. Nodes 1 and n are legitimate nodes that are also referred to as the source and destination nodes, respectively. However, a trustworthy and reliable channel might not be what connects them directly. As a result, the other $n-2$ illegitimate nodes will assist by decoding and sending the message hop by hop. The directly connecting and available link between node i and node j is denoted by l_{ij}. If the distance between two nodes is larger than a threshold value of l_{T}, there is not a reliable channel between them. We assume that each node has no buffer and must transmit all of the information it has received and decoded.

Since every node employs the DF relaying mode, a relaying node must be able to receive the signal from the previous node in the relaying route with sufficient SNR, fully decode the message, and then re-encode it at a rate equal to the channel capacity between it and the next node in the route. It implies that a relay will have full knowledge of s. We consider two trustworthy models as follows.

- *Trust degree*: When seen from the valid nodes, each node has a unique TD of $t \in [0\ 1]$, $i = 1, ..., n$. It is the likelihood that a node does not exploit the data it obtains throughout the process of assisting with message decoding for nefarious purposes. Without a doubt, the TD of the legitimate nodes is always 1. The TDs of the relay set nodes that the message will pass through, indicated here by $\mathcal{R}$, determine the security level of s. The probability that the message is utilized maliciously by at least one node is determined by $p_{\mathrm{M}} = 1 - \prod_{i\in\mathcal{R}} t_i$. We presume that s is not a fully protected communication, which means we tolerate the possibility that the message is used maliciously with a probability below a threshold level p_{T}. If $p_{\mathrm{T}} = 0$, it requires that $p_{\mathrm{M}} \leq 0$, so $\prod_{i\in\mathcal{R}} t_i \geq 1$, $\prod_{i\in\mathcal{R}} t_i = 1$ or all relays have TDs of 1, the message is completely secured.
- *Network tiers*: The wireless nodes belong to different network tiers, e.g., wireless sensors of different owners installed in a common area. We consider public and private messages. The nodes of the same network tier are completely trustful to each other so they can freely share and relay both public and private messages for each other. However, only public messages are shareable to nodes of the other network tier. Therefore, different from the trust degree that the malicious probability is multiplicatively accumulated along the route, a private is forbidden to go through any node in the other network tier.

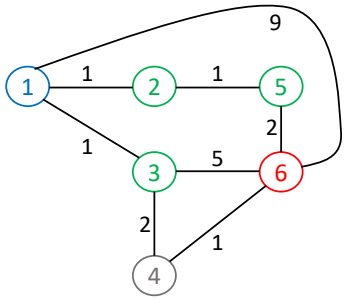

Figure 1. An example of the network with 6 nodes. The number next to a link shows its cost.

We also assume that only the next node in a route receives when a node in the route broadcasts. We only take into account the insecurity caused by the low trust degrees of the other network tiers' nodes and do not take into account the eavesdropping of specific eavesdroppers or other non-targeted illegitimate nodes. 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. A wireless network with accurate beamforming transmission between any two nodes and a wire network with copper or optical connections are two scenario examples with such a scenario.

Route $\mathcal{R}$ in the network has nodes renumbered from 1 (the source) to k (the destination, also node n in the network). The channel along the path between nodes i and $i+1$ is designated as h_i. The transmission's maximum achievable rate (MAR) from node i to node j is given by $c_{ij} = \log_2\left(1 + \frac{p|h_{ij}|^2}{\sigma^2}\right)$, $i \in \mathcal{R}$ where the transmit and noise powers, respectively, are denoted by p and σ^2. The same constellation can be used if all nodes along the path transmit at the same rate, and the rate is given by $r = \min_{i,j\in\mathcal{R}} c_i$ to guarantee that the message can be decoded by each receiver along the path. Each node along the route can re-encode the message with a new constellation, and as a result, a different rate of r_i (bits/s/Hz), in order to improve the routing and boost end-to-end transmission

rate. Assume that a 1-Hz bandwidth is used for all communications. It takes $\frac{f}{r_i}$ seconds to send f bits from node i to node $i+1$. When additional processing times are not taken into account, the amount of time it takes to send f bits over the selected route is provided 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

In a network, the shortest path between a source and a destination is found using the Dijkstra's method. Each possible link in the network has an additional cost, which is known in advance. The route from a source to a destination that incurs the least overall cost is called the shortest route. The method will progressively expand the known network to the target routing and move each node from the tentative list to the permanent list before checking every conceivable path [25].

The time it takes to transmit 1K bits from one node to the next is the cost in the Dijkstra's algorithm used in this study since we are looking for the path with the least delivery time. The cost of a connection is expressed as $\frac{f}{c_i}$. We denote the cost of link l_{ij} by d_{ij}. If $d_{ij} > c_{\max}$, where $c_{\max}$ is a very large number, node i and node j are not directly connected.

3.1 Clustering

For a large network with a huge number of nodes, it can be overloaded or impossible to put all links into a matrix. Moreover, some nodes are very far away from other nodes so there are no direct and reliable links between them. It is not necessary to consider all links in a common set. In addition, requiring the nodes to transmit to farther nodes will soon exhaust their energy. Due to all these reasons, separating the nodes into clusters has been considered for a long time.

For wireless sensor networks with data collection and aggregation purpose, a node in each cluster is selected as the cluster head. All nodes in a cluster report their sensed data to the cluster head which aggregates and forwards the aggregated value to the server of the cluster head of the upper-level cluster. However, this requires that the energy level of the cluster heads is high enough to transmit the signals to the far-away upper-level cluster head or server.

There several methods for clustering. In this paper, we consider two basic clustering methods with a predetermined number of clusters, n_{C}: grid-based clustering and K-means clustering as follows.

- *Grid-based clustering*: The network area is uniformly divided into n_{R} rows and n_{C} columns. There are $n_{\mathrm{C}} = n_{\mathrm{Ro}} n_{\mathrm{Co}}$ rectangular clusters. The advantage of this clustering method is that the clusters are uniformly distributed so the inter-cluster links are not physically long. In fact, as assumed in the system model, there is no reliable channel between any two nodes whose distance is larger than l_{T}. This means than grid-based clustering results in less isolated or separated clusters and increases the probability of successful data delivery from the source to the destination [26].
- *K-means clustering*: This method tries to optimally locate the centroids of n_{C} clusters. First n_{C} centroids are initially determined maybe randomly. Each node is associated to the cluster with the centroid closest to that node. The new centroid of each cluster is calculated based on all associated nodes of that cluster. The node association is redetermined and the centroids are re-calculated in an iterative way until the movements of the centroids are smaller than a threshold value [27].

We consider two basic clustering methods such as grid based clustering and k-means clustering because these methods are efficient in different scenarios and popularly used in many existing publications and have their own advantages. For grid-based clustering, we uniformly allocate equal area to all clusters so the inter-cluster head distances are not larger than a limit. For k-means clustering, the distance sum, for all cluster members to their heads, is minimized.

In a network without cluster heads, the data is routed inside a cluster from a data source to a gateway node. A gateway is an edge node of a cluster and directly connected to a gateway of the next cluster. There are probably several links connecting edge nodes of this cluster to edge nodes of an adjacent cluster. We can choose the best links which have the highest transmission capacities, to be inter-cluster links. The ends of those inter-cluster links become the corresponding gateways. There are two methods of choosing best links between a certain pair of clusters as follows.

- *Non-repeated gateways*: A node can be an end of more than one inter-cluster link. The gateways of the best inter-cluster link between clusters a and b is given by

$$\left(i_{ab}^{1}, i_{ba}^{1}\right) = \mathrm{argmin}_{i \in \mathcal{C}_a, j \in \mathcal{C}_b} c_{ij}. \tag{1}$$

  When the best link between clusters a and b is determined, it is removed out of the considered link set so that we can search for the second best link. In the k-th step, the best, the second best,..., and $(k-1)$-th best links are removed of the considered link set and we search for the k-th best link. The gateways of this link is given by

$$\left(i_{ab}^{k}, i_{ba}^{k}\right) = \mathrm{argmin}_{i \in \mathcal{C}_a^k, j \in \mathcal{C}_b^k} c_{ij}, \tag{2}$$

  where $\mathcal{C}_a^k = \mathcal{C}_a \setminus i_{ab}^{l}, l \in \{1, ..., k-1\}$ and $\mathcal{C}_b^k = \mathcal{C}_b \setminus i_{ba}^{l}, l \in \{1, ..., k-1\}$.
- *Repeated gateways*: A node can be an end of only one inter-cluster link. In step k, the link to be selected is given by

$$l_{ab}^{k} = \mathrm{argmax}_{l_{ij} \in \mathcal{L}_{ab}^{k}} c_{ij}, \tag{3}$$

  where $\mathcal{L}_{ab}^{k} = \mathcal{L}_{ab} \setminus l_{ab}^{l}, l \in \{1, ..., k-1\}$, $\mathcal{L}_{ab}$ is the set of all links between any node of cluster a and any node of cluster b. The gateways are selected correspondingly to link l_{ab}^{k}.

Algorithm 1: Finding the shortest path from node 1 to node n for a network without clusters.

Data: Link costs d_{ij}, $i, j \in \{1, ..., n\}$.
Result: The shortest path p_o.

Steps:

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 $\mathcal{S}$:
$$j = \arg\min_{m \in S'} D_{1m}. \quad (4)$$
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 $\mathcal{S}'$ as follows
$$\mathcal{N}_j = \{m | m \in \mathcal{S}', d_{jm} < c_{\max}\}. \quad (5)$$
6) Check for improvement in the minimum cost path from node 1 to each node in $\mathcal{N}_j$ as follows
$$D_{1m} = \min\{D_{1m}, D_{1j} + d_{jm}\}, \text{ for } m \in \mathcal{N}_j \cap \mathcal{S}'. \quad (6)$$
7) Go back to step (2) until $\mathcal{S}' = \emptyset$.

Algorithm 2: Finding the shortest path from node 1 to node n using grid-based inter-cluster routing through gateways such that all private messages do not go through any nodes of the second tier network.

Data: Link costs d_{ij}, $i, j \in \{1, ..., n\}$; message type t_{M} (0 = public, 1 = private); number of cluster n_{C}; node position p_i; number of gateway pairs between adjacent clusters n_{G}.
Result: The gateway-to-gateway cost matrix $\mathbf{G}$.

Steps:

1) Divide the nodes into grid of n_{G} clusters based on positions p_i.
2) If $t_{\mathrm{M}} = 0$, define black list $\mathcal{B} = \emptyset$. Otherwise, $\mathcal{B}$ includes all nodes in the second tier network.
3) Find n_{G} best links, with smallest costs, between any node of a cluster, except in the black list, and any node of an adjacent cluster, except in the black list:
$$\left(i_{ab}^k, i_{ba}^k\right) = \mathrm{argmin}_{i \in \mathcal{C}_a^k \backslash \mathcal{B}, j \in \mathcal{C}_b^k \backslash \mathcal{B}} c_{ij}. \quad (7)$$
4) Define gateway set $\mathcal{G}$ including the source ($\mathcal{G}(1)$), destination ($\mathcal{G}(|\mathcal{G}|)$) nodes and all gateways.
5) Find the shortest path between every gateway, including the source ($\mathcal{G}(1)$), of every cluster in $\mathcal{G}$ to any other gateway, including the destination ($\mathcal{G}(|\mathcal{G}|)$), of the same cluster in $\mathcal{G}$ using Algorithm 1.
6) Build the gateway-to-gateway cost matrix based on the cost of the shortest paths found in step 5.
7) Find the shortest path between the source and the destination through the gateway network based on the cost matrix achieved in step 6 using Algorithm 1.

The complexity of the Dijkstra algorithm for the unclustered network of n nodes can be represented by $\mathcal{O}(n^2)$. If the network is divided into n_{C} clusters, we need to run the algorithm in each cluster with complexity $\mathcal{O}\left(\left(\frac{n}{n_{\mathrm{C}}}\right)^2\right)$. We need to run for n_{C} clusters so the complexity is $\mathcal{O}\left(\frac{n^2}{n_{\mathrm{C}}}\right)$. With this complexity, we have the gateway-to-gateway cost matrix. If between any two adjacent clusters, there are two best n_{G} links which are equivalent to n_{G} gateway per cluster. If the network are clustered with $\sqrt{n_{\mathrm{C}}}$ rows and $\sqrt{n_{\mathrm{C}}}$ columns, there are 4 corners each with $2n_{\mathrm{G}}$ gateways; $(4\sqrt{n_{\mathrm{C}}} - 4)$ clusters each with $3n_{\mathrm{G}}$ gateways; and $(n_{\mathrm{C}} - 4\sqrt{n_{\mathrm{C}}})$ each with $4n_{\mathrm{G}}$ gateways. So the total equivalent complexity is given by[1]

$$c \sim \mathcal{O}\left(\frac{n^2}{n_{\mathrm{C}}} + (4 \times 2n_{\mathrm{G}} + (4\sqrt{n_{\mathrm{C}}} - 4)3n_{\mathrm{G}} + (n_{\mathrm{C}} - 4\sqrt{n_{\mathrm{C}}})4n_{\mathrm{G}})^2\right) \quad (8)$$

$$\sim \mathcal{O}\left(\frac{n^2}{n_{\mathrm{C}}} + 16(n_{\mathrm{C}} - \sqrt{n_{\mathrm{C}}} + 1)n_{\mathrm{G}}^2\right). \quad (9)$$

If n_{G} is small enough, this is smaller than the complexity of the routing algorithm without clusters. Certainly, with a higher n_{G}, the performance of the routing with clusters get closer to that of the routing with no clusters.

3.2 Trust Degree

In order to take the trust degree into account, we alter the method by include the TD restriction in the suggested routing strategy. We therefore modify the algorithm by adding the constraint regarding the TDs in the proposed routing algorithm. In the network example in Figure 1, six nodes with various TDs are displayed below the nodes in violet boxes. A related cost is displayed next to each link. The cumulative TD must exceed a predetermined TD threshold (α) in order for us to discover a path from node 1 to node 6 with the lowest accumulated cost. We identify the path in the network that has the lowest total cost between nodes i and j using the mathematical notation $\mathcal{P}_{ij}$ its corresponding cost by D_{ij}, and its corresponding accumulated TD by T_{ij}. By denoting the set of all nodes along path $\mathcal{P}_{ij}$ by $\mathcal{R}_{ij}$, we write $T_{ij} = \prod_{m \in \mathcal{R}_{ij}} t_m$. The routing algorithm is analogous to the following optimization problem for generic n. The optimization problem for the trust-degree routing is given by

$$\min_{\mathcal{P}_{1n}} D_{1n} \quad (10)$$

$$\text{subject to } T_{1n} \leq \alpha. \quad (11)$$

4 Simulation Results

We give the simulation results and examine the many factors impacting the performance of the network in this part. In the simulations, the placements of n nodes are uniformly distributed randomly in a 1m×1m square. Only when the separation between two nodes is less than a threshold of $d_{\mathrm{th}} = 0.4$ can they establish a stable wireless connection. A reliable wireless channel has a σ_{h}^2-variance and 0-mean complex distribution that are dispersed at random. In a Normal distribution, $\sigma_{\mathrm{h}}^2 = \left(\frac{c_{\mathrm{L}}}{4\pi f_{\mathrm{R}} d}\right)^2$, where c_{L} is the light velocity, f_{R} is the radio frequency, and d is the distance between the

[1] There are two special gateways which are the source and destination nodes. However, 2 becomes trivial when other variables tends to ∞ so we ignore 2 in the sum.

Table I
STEPS OF THE PROPOSED ROUTING ALGORITHM FOR THE TWO-TIER NETWORK IN FIGURE 1.
ONLY NODES IN THE FIRST-TIER NETWORK ARE CONSIDERED.

Iteration	$\mathcal{S}$	D_{12}	**Path**	D_{13}	**Path**	D_{15}	**Path**	D_{16}	**Path**
1	1	1	1-2	1	1-3	∞	-	9	1-6
2	1,2	1	1-2	1	1-3	2	1-2-5	9	1-6
3	1,2,3	1	1-2	1	1-3	2	1-2-5	6	1-3-6
4	1,2,3,5	1	1-2	1	1-3	2	1-2-5	4	1-2-5-6
5	1,2,3,5,6	1	1-2	1	1-3	2	1-2-5	4	1-2-5-6

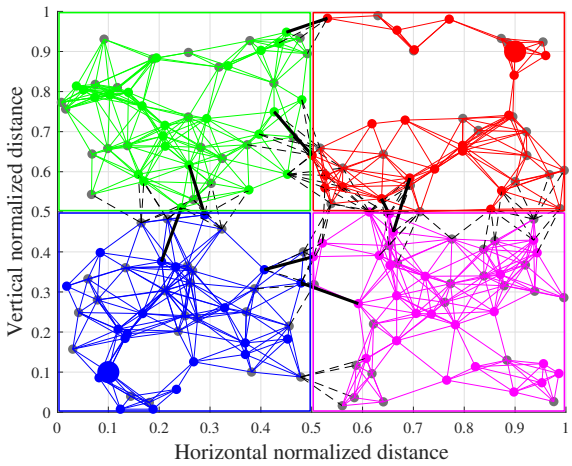

Figure 2. An example of the network with $n = 180$ nodes, $n_G = 2$ best links per cluster pair, distance threshold $d_{th} = 0.13$, and $n_C = 4$ clusters.

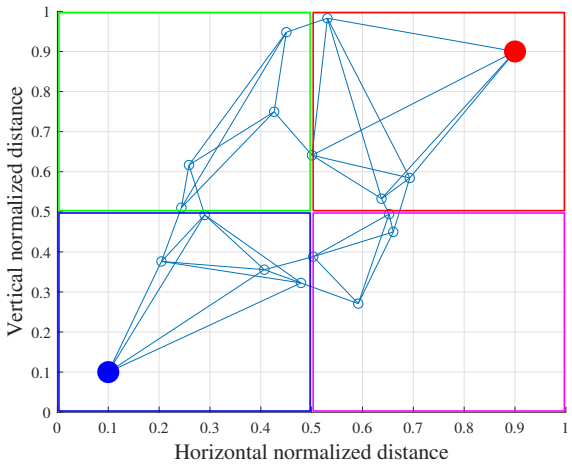

Figure 3. An example of the gateway network corresponding to the node network in Figure 2.

transmitter and receiver under consideration. One of the unlicensed frequency bands in the US is $f_R = 900$ MHz, which we use. The channel's variation represents the Friis's Transmission Formula [28].

The nodes are divided into n_C clusters using Grid-based clustering as shown in Figure 2. The nodes of the first tier network, the legitimate nodes, are marked with color of its cluster while the nodes of the second-tier network in the same cluser are marked with darker colors. Intra-cluster links are shown with the same color of that cluster. Normal inter-cluster links are shown with dashed, thin, and black lines while the n_G best links between any two adjacent clusters are shown with solid, think, and black lines. The data source and destination nodes are fixed at (0.1, 0.1) and (0.9, 0.9) in the first and last cluster, respectively, and shown with large circles.

After the best inter-cluster links are determined, their ends are defined as gateways. The data source and destination nodes are also (special) gateways. The Dijkstra routing algorithm is used to determine the shortest route, with the smallest total cost, from a gateway to any other gateways of the same cluster. The intra-cluster inter-gateway connections are now considered as a link with a cost obtained when running the routing algorithm above and shown as thin and blue lines in an example in Figure 3. Note that the intra-cluster links are not directly physical link but the inter-cluster links are. Now the best route from the data source node to the data destination node is determined by Dijkstra routing algorithm with the gateway-to-gateway cost matrix obtained. As presented in Algorithm 2, when considering a node to be a gateway, the nodes in second tier network are excluded so the final routing algorithm used is pure Dijkstra's. If the number of inter-cluster gateways increases, the best route to be found is better, however, the complexity is higher both for finding the best inter-cluster links and finding the best route in the gateway-to-gateway network. The number of inter-cluster gateways connected between any two clusters does not necessarily the same.

4.1 Two-Tier Networks

The average delivery time for 1 Kbits from node 1 to node n is shown in Figure 4. Since the receiver of each hop may receive a better signal and shorten the transmission time in each hop, it can be seen that all delivery times decrease with the transmit SNR of each hop. A no-cluster scheme will give a better routing solution as expected however it uses more signalling and computational resources due to higher complexity. A non-adaptive scheme always limits the considered nodes, for both selecting gateways in case of clustering and selecting intermediate nodes in intra-cluster routing, to the first tier network, known as legitimate nodes, only for both private and public data messages. An adaptive scheme considers nodes in the first tier network for a private message but all nodes in the network for a public message. Obviously, an adaptive scheme can find better routes in some cases. More

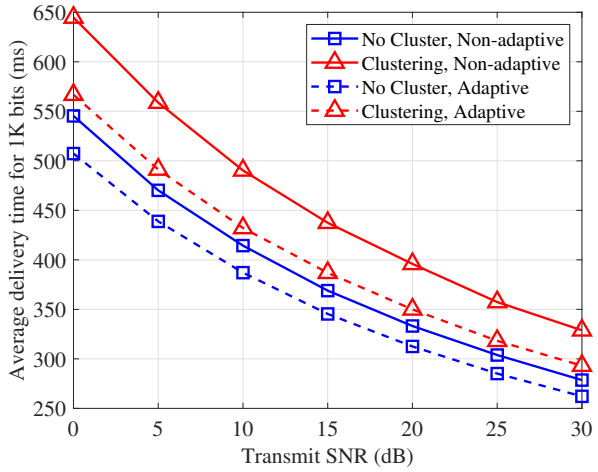

Figure 4. The effect of the transmit SNR on average delivery time for 1K bits in case $n = 60$, $n_G = 2$, and $d_{th} = 0.3$.

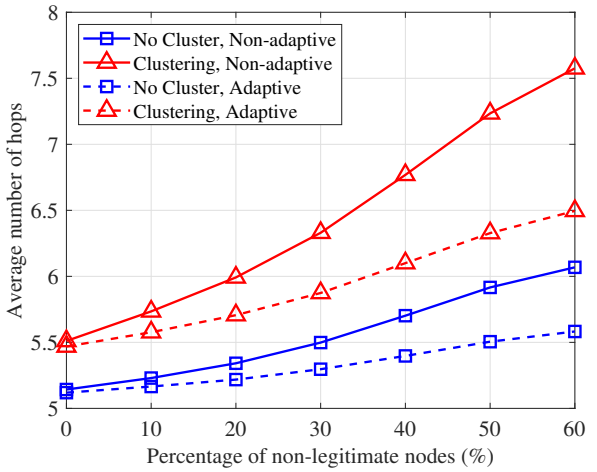

Figure 6. The effect of the percentage of illegitimate nodes on the average number of hops.

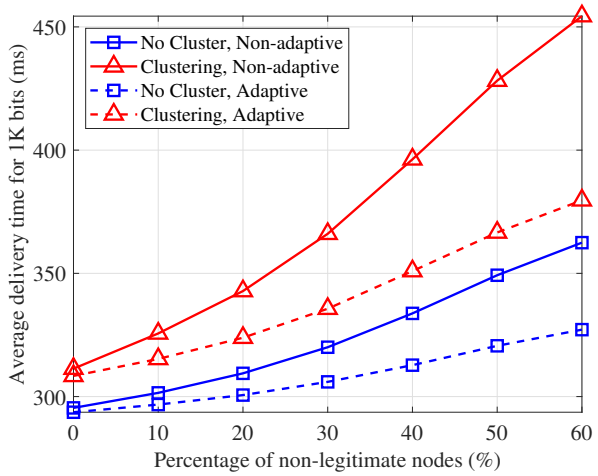

Figure 5. The effect of the percentage of illegitimate nodes on average delivery time for 1K bits in case $n = 60$, $n_G = 2$, SNR = 20dB and $d_{th} = 0.3$.

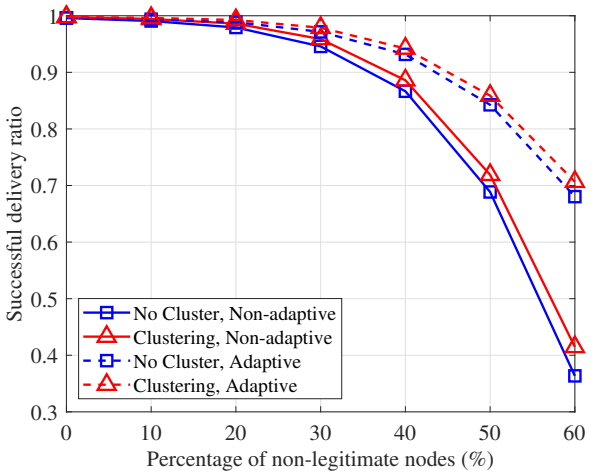

Figure 7. The effect of the percentage of illegitimate nodes on on the successful delivery ratio.

nodes in a network result in a faster transmission rate or shorter transmission times between any two nodes since there is typically a shorter distance between them. In all simulation with two-tier networks below, we public and private messages account for half of the occurrences. Due to the complexity of a network with more than two tiers in which trustful relation between any two tiers are considered and quantified, it will be considered in a future work.

Figure 5 shows the effect of the percentage of illegitimate nodes on average delivery time for 1K bits in case $n = 60$, $n_G = 2$, and $d_{th} = 0.3$. Certainly, there are more and more nodes of the second tier network and less nodes of the first tier network, there are less options for the best route for a private message's routing. Therefore, the delivery time increases correspondingly.

Figure 6 shows the effect of the percentage of illegitimate nodes on the average number of hops that the best route take from the source to the destination. When the illegitimate nodes occupy more, it is more difficult to find the best intermediate legitimate nodes which satisfy the tier-appropriate constraint for a private message. So in this case it may accept a detour with more hops.

Figure 7 shows the effect of the percentage of illegitimate nodes on on the successful delivery ratio. Not in all realizations of nodes' positions and channels, there is always a feasible route from the source to the destination. The source and the destination may be in two legitimately separated sub-networks. Therefore, when the illegitimate nodes occupy more, certainly the probability of a feasible route will decrease.

4.2 Trust Degree

A node's trust degree is randomly generated using a 1-mean and 0.4-variance.[2] If the random value is more than 1, the trust degree is set to 1; if it is lower than 0, the TD is set to 0. It is truncated in the value range

[2]The trust degree can be randomly generated accordingly to any appropriately modeled distribution. In this case the mean and variance are as such because with a lower mean, there is probably impossible to find a route from the source to the destination for both the conventional and proposed schemes. In a future work, more advanced model of trust degree will be considered.

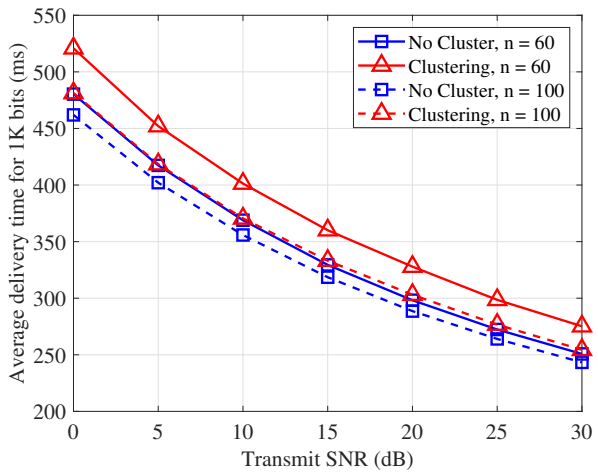

Figure 8. The average delivery time for 1K bits in case $\alpha = 0.7$.

of [0 1]. Figure 8 shows the effect of the transmit SNR on the average delivery time. The curves have a similar shape with those of the two-tier networks. The trust degree can be seen as the case with the number of tiers is infinity and each tier network has a different trust degree seen from the legitimate network.

5 Conclusion

Modern wireless networks' security and privacy may be enhanced in large part by optimizing the network based on network tiers' trust levels. To determine the path with the shortest total transmission time between the source and the destination while still ensuring that the messages with a certain privacy level do not pass nodes of the network tiers with trust level smaller than a corresponding threshold value, we put forth a novel approach. To examine the effects of the transmit SNR, node density, and the probability of other network tiers' nodes on various network performance components, simulation results are provided. In order to improve routing optimization, boost security, and improve network speed, it is crucial to have a clustering scheme with enough number of gateways between adjacent clusters and appropriate complexity.

Acknowledgment

This work was supported by NAFOSTED Grant 102.02-2018.318.

References

[1] X. Lu, L. Xiao, G. Niu, X. Ji, and Q. Wang, "Safe exploration in wireless security: A safe reinforcement learning algorithm with hierarchical structure," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 732–743, 2022.

[2] 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. 1–24, Feb. 2014.

[3] 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*, Dec. 2015.

[4] 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.

[5] 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, Mar. 2010.

[6] 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, Aug. 2016.

[7] X. Li, Q. Wang, M. Liu, J. Li, H. Peng, M. J. Piran, and L. Li, "Cooperative wireless-powered NOMA relaying for B5G IoT networks with hardware impairments and channel estimation errors," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5453–5467, 2021.

[8] 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, Oct 2018.

[9] 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, Aug 2017.

[10] 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.

[11] 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, April 2019.

[12] 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, March 2015.

[13] 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. 655, no. 9, pp. 7274–7284, 2015.

[14] 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, Feb. 2016.

[15] C. D. T. Thai, V. N. Q. Bao, T. Q. Nhu, N. T. Y. Linh, and H. V. Hoa, "Modified Dijkstra's routing algorithm for security with different trust degrees," *REV Journal on Electronics and Communications*, vol. 10, pp. 55–61, Jun. 2020.

[16] 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, Jun. 2014.

[17] 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.

[18] 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.

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

[20] 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.
[21] 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.
[22] 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, Feb. 2016.
[23] 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.
[24] X. Liao and J. Li, "Privacy-preserving and secure top-k query in two-tier wireless sensor network," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 335–341.
[25] D. Medhi and K. Ramasamy, "Network routing: Algorithms, protocols, and architectures," Elsevier, 2007.
[26] J. Zhang, X. Feng, and Z. Liu, "A grid-based clustering algorithm via load analysis for industrial internet of things," *IEEE Access*, vol. 6, pp. 13 117–13 128, 2018.
[27] T. M. Hoang, N. M. Nguyen, and T. Q. Duong, "Detection of eavesdropping attack in uav-aided wireless systems: Unsupervised learning with one-class svm and k-means clustering," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 139–142, 2020.
[28] J. R. C. and H. Jasik, "Antenna engineering handbook," (2nd ed.). New York, NY: McGraw-Hill, Inc., 1984, ISBN 0-07-032291-0.

Chan Dai Truyen Thai (S'10-M'14) 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; Singapore University of Technology and Design (SUTD); and is now with Vietnamese-German University (VGU). His research interests include cooperative communications, vehicle-to-vehicle communications, communication for high-speed vehicles, security in wireless communications, computer security, security in smart grid, and distributed networks.

Vo Nguyen Quoc Bao (Senior Member, IEEE) (M'11-SM'16) served as the Dean of the Faculty of Telecommunications and the Director of the Wireless Communication Laboratory. He is currently an Associate Professor of wireless communications with the Posts and Telecommunications Institute of Technology, Vietnam. He has authored over 200 journal and conference articles that have over 2700 citations and H-index of 25. 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 a member of the Executive Board of the Radio-Electronics Association of Vietnam and the Electronics Information and Communications Association Ho Chi Minh City. He served as the Technical Program Co-Chair of ATC (2013 and 2014), NAFOSTED, NICS (2014, 2015, and 2016), REV-ECIT 2015, ComManTel (2014 and 2015), and SigTelCom 2017. He is currently serving as a Scientific Secretary of the Vietnam National Foundation for Science and Technology Development Scientific Committee in Information Technology and Computer Science. He is a Technical Editor-in-Chief of REV Journal on Electronics and Communications since 2017, an Associate Editor of the EURASIP Journal on Wireless Communications and Networking, an Editor of the Transactions on Emerging Telecommunications Technologies (Wiley ETT), the VNU Journal of Computer Science and Communication Engineering, and the REV Journal on Electronics and Communications. Mr. Bao's awards and honors include IEEE Exemplary Reviewer for IEEE Wireless Communications in 2013, best paper award at the 9th International Conference on Communications and Networking in China (ChinaCom) in 2014, best paper award at the International Conference on Computing, Management and Telecommunications (ComManTel) in 2013, and outstanding paper award at the 14th International Conference on Advanced Communication Technology (ICACT) in 2012.

Uyen Han Thuy Thai received her B.S. degree in Information Technology from University of Science, Vietnam, in 2008 and her M.S. degree from Dept. of Computer Engineering, Kyung Hee University, Korea, in 2012. Her research interests include database systems and data mining.