Routing for Information Leakage Reduction in Multi-channel Multi-hop Ad-Hoc Social Networks

Wei Cheng[1], Dengyuan Wu[2], Xiuzhen Cheng[2], and Dechang Chen[3]

[1] Department of Computer Science,
University of California, Davis, Davis CA, USA
[2] Department of Computer Science,
The George Washington University, Washington DC, USA
[3] Department of Preventive Medicine and Biometrics,
Uniformed Services University of the Health Sciences
weicheng@ucdavis.edu
{andrewwu,cheng}@gwu.edu
dchen@usuhs.mil

Abstract. This paper investigates the routing problem for information leakage reduction in multi-channel ad-hoc networks. In particular, we focus on two routing models: Trusted Group Multicast (TGM) and Confidential Unicast (CU). In TGM, a group member shares the information with all other group members; while in CU, a group member may only want to share the information with a few selected group members. In both cases, the sender would like to transmit the information through a route with a minimal probability of being overheard by non-destination users. To achieve this objective, we propose a routing algorithm to reduce the information leakage. The performance of our design is evaluated through simulation studies.

1 Introduction

The routing problem in wireless networks has been extensively studied with the objectives of improving either the networking performance such as end-to-end delay and throughput, or robustness, reliability, and security. However, a fundamental problem of preventing information leakage to unwelcome users, who should not but can overhear the transmissions over the air, has never been addressed in literature. Although wireless transmissions can be secured by cryptographic primitives, reducing the probability of being overheard by unwelcome users is still critical as security mechanisms could be broken and the exposure of the information to malicious users may cause wreak havoc to certain applications (such as military applications). We therefore target on studying the routing problem to reduce the probability of information leakage in wireless networks.

This problem can be generally defined as follows. Given an information source and the corresponding sets of destinations and unwelcome users, computing a

X. Wang et al. (Eds.): WASA 2012, LNCS 7405, pp. 31–42, 2012.

routing path satisfying the following three requirements with decreasing priorities: i) the information can successfully reach all destinations; ii) the probability of information leakage to unwelcome users is minimized; and ii) the probability of information leakage to non-destination users is minimized. This problem is NP-hard as a special case, the well-known Steiner tree problem which asks for the minimum number of non-destination nodes in forming a routing path, is NP-Complete.

Instead of considering the general problem defined above, this paper investigates two special instances focusing on reducing the information leakage in social networking applications, in which users share their information with others who may also be interested through ad-hoc multi-hop transmissions. There are two types of users in a social network: the members of a common interest group and the non-group users. The two instances of the general routing problem for information leakage reduction respectively adopt the following two routing models: the *Trusted Group Multicast* (*TGM*) model and the *Confidential Unicast* (*CU*) model. In TGM, a user is willing to share its information with all members in its common interest group; thus the objective of TGM is to minimize the non-group user's probability of overhearing the information. In CU, a user may only want to share its information with a certain subset of members. As non-destination group members may even be more harmful than non-group users since the former may have more interests in and more knowledge about the information, the objectives of CU must first minimize the non-destination group member's overhearing probability and then minimize the probability of information leakage to non-group users. In such a case, the non-destination group members are unwelcome users.

We assume that the multi-hop ad hoc social network under our consideration can make use of multiple channels for wireless transmissions. We further assume that each user is aware of its available channels and the network topology, which can be obtained during the common interest group construction. Our intention is to design a routing algorithm that can select a path satisfying the design objectives of TGM and CU. The contributions of the paper are quad-fold:

- We propose a general problem, the routing problem for information leakage reduction in wireless networks. This problem has never been addressed in literature.
- We analyze the objectives of two novel routing models (TGM and CU), which defines two special instances of the general problem in social networks, and propose a general graph model that can cover both TGM and CU.
- We propose a routing algorithm for information leakage reduction in social networks based on the general graph model.
- Simulation studies demonstrate that our proposed algorithm outperforms the Breadth-First Search (BFS) based routing algorithm in terms of the information leakage probability.

In the rest of the paper, we briefly summarize the related work in the area of ad-hoc networks in Section 2. Our general graph model for both TGM and CU is presented in Section 3. A routing algorithm for information leakage reduction, denoted by RILR, is proposed in Section 4. A simulation study to validate the performance of the RILR algorithm is reported in Section 5. Finally, we conclude the paper and discuss our future research in Section 6.

2 Related Work

Routing problems have been extensively studied in wireless ad-hoc networks and sensor networks. The objectives of the prior research are either to improve the transmission performance such as delay, throughput, and energy consumption, or to enhance the robustness of the network when malicious attacks targeting on the transmissions exist. Various routing schemes have been proposed in the literature, including the classic AODV algorithm [1], the secure routing mechanism [2], and the recent cooperative relay selection algorithm [3], just to name a few. But none of them takes into account the objective of reducing the information leakage to non-destination users, which is the focus of this paper.

Existing multicast routing algorithms for information sharing [4–7] are studied mainly based on graph theory. Steiner tree based routing is considered in [4] and [5] with different objectives: [4] aims to minimize the path length and the energy consumption while [5] intends to reduce the computation overhead and the number of transmissions. On the other hand, Spanning trees are also exploited for multicast routing algorithm design [6, 7]. In particular, [6] selects the relays from a minimal spanning tree that is constructed based on an energy consumption metric while [7] targets on reducing the retransmissions caused by interference during the spanning tree construction.

Inspired by the opportunity of utilizing multiple channels for highly crowded wireless transmissions, a number of routing algorithms have been proposed to achieve the traditional routing objectives [9–13]. In [9], a shortest path routing algorithm is developed based on a weighted graph, where the assigned weights are utilized to avoid the interference among adjacent links. In [10], the links with the highest channel availability are selected to relay the data to the destination. A cross-layer opportunistic spectrum access and dynamic routing algorithm is proposed in [11] to maximize the network throughput by performing joint routing, dynamic spectrum allocation, scheduling, and transmit power control. Routing algorithms for route robustness enhancement in terms of the degree of connectivity are studied in [12, 13].

In this paper, we study the routing problem to reduce the information leakage for information sharing among common interest group members in social networks. This problem has never been addressed in any type of wireless networks. Two novel routing models are proposed and a routing algorithm that can reduce the information leakage for both models is investigated.

3 Problem Formulation

In order to model the routing problem for information leakage reduction in social networks, we first analyze the objectives of TGM and CU in this section.

Then, a general mathematical model that can realize all the objectives of both TGM and CU is proposed. At the end of this section, we discuss the metrics for evaluating the performance of a routing algorithm in terms of the information leakage probability.

3.1 Objectives

In social networks, Trusted Group Multicast and Confidential Unicast both involve three types of users: *destinations*, *unwelcome users*, and *outsiders*. In TGM, all the members within the common interest group are destinations and the set of unwelcome users contains the unauthorized users that are interested in the group information but do not have the right to joint the group. In CU, the destination(s) is (are) one (a few) of the members within the common interest group and the unwelcome users include both the unauthorized non-group users and the non-destination group members. The outsiders for both TGM and CU include users in the network that are neither destinations nor unwelcome users. Generally speaking, a user needs to deliver the information to its destinations, parry the unwelcome users, and minimize the probability of information being overheard by unwelcome users and outsiders in both models. Correspondingly, we can employ the following common objectives to summarize those of TGM and CU in descending order of priorities.

1. Ensure successful information deliveries to the destinations.
2. If possible, do not employ unwelcome users as information relays.
3. Minimize the probability of being overheard by unwelcome users.
4. Minimize the number of outsiders as information relays.
5. Minimize the probability of being overheard by outsiders.
6. Minimize the transmission time in terms of the number of hops to reach all the destinations.

We model these six objectives by a graph, in which the destinations, the unwelcome users, and the outsiders are the vertices. Since TGM and CU both have the same three types of nodes and the same design objectives for information leakage reduction, a common graph model suffices.

If only considering the objective of successful and fast information delivery, we can construct a routing topology by employing the Breadth-First Search algorithm (BFS). However, BFS does not consider information leakage reduction, which is addressed by the 2nd-5th objectives. The problem of information leakage reduction is non-trivial when all the six objectives are considered. In the rest of this section, we formally present the graph model along with the performance evaluation metrics.

3.2 A General Graph Model for Information Leakage Reduction

We assume that an information source is aware of the network topology that contains all the common interest group members and the set of unwelcome users for a specific information sharing session. We also assume that the source and all its destinations are connected, which can be ensured during the common interest group construction procedure. We model the network topology by a weighted graph $G(V, E)$, where V is the set of users, and E is the set of edges. There exists an edge between two users if they can overhear each other. We assign a weight $w_{i,j}$ to each edge $e_{i,j} \in E$, where $w_{i,j}$ denotes the probability for v_j to detect v_i's transmissions. The value of $w_{i,j}$ is set according to the network topology and the available channels. Note that edges can be directed, and that $w_{i,j} = 0$ if the edge $e_{i,j}$ does not exist. Without loss of generality, we denote by v_0 the information source itself. The set of destinations, the set of unwelcome users, and the set of outsiders are denoted as V_D, V_A, and V_O, respectively. Note that $V_D \bigcup V_A \bigcup V_O = V$ and $|V_D| + |V_A| + |V_O| = |V|$. Let V_R be the set of users that are on v_0's information sharing routes and can actively relay the information. Thus $v_0 \in V_D$ and $v_0 \in V_R$. Let $I(v_i) = \{v_j | (v_i, v_j) \in E\}$ represent the set of users that are within v_i's transmission range, where $0 \leq i, j \leq |V|$ and $i \neq j$. Denote by $G_R(V', E')$ the derived graph of V_R such that $V' = \{v_i | v_i \in V_R$ or $v_i \in I(v_j)$, where $v_j \in V_R\}$ and $E' = \{e_{j,i} | v_j \in V_R$ and $v_i \in I(v_j)\}$. Note that G_R is a subgraph of G that includes all the users who may overhear or obtain the information, and that there is no edge between any two non-relay users in G_R. For each user $v_i \in V'$, we calculate its probability of overhearing the interested information, denoted as $P'_{ro}(v_i)$, according to the following formula.

$$P'_{ro}(v_i) = \begin{cases} 0, V_R = \Phi \\ 1, v_i \in V_R \bigcup V_D \\ 1 - \prod\limits_{v_j \in V_R} (1 - w_{j,i}), \text{otherwise} \end{cases} \tag{1}$$

Note that $P'_{ro}(v_i) \in [0, 1]$ increases with the increase of the number of relays that include v_i in their communication ranges. We utilize $P'_{ro}(v_i)$ as v_i's weight.

Let $D(v_0, V_D)$ represent the maximum hop distance from v_0 to the destinations in G_R. Note that $D(v_0, V_D) = +\infty$ if V_D is not connected in G_R. The notations used in this model are summarized in Table 1. Also note that we use '*node*' to substitute '*source*', '*outsider*', '*relay*' and '*destination*' in the following graph-based modeling and analysis.

Given a graph G, v_0, V_D, V_A, and V_O, our goal is to find a V_R, such that the following six objectives can be achieved in a descending order of priorities:

1. $G_R \supseteq V_D$ and V_D is connected in G_R: all the nodes in V_D are in G_R, and they are connected.
2. $V_R \bigcap V_A = \Phi$: V_R does not include any node in V_A.
3. $min(\max\{P'_{ro}(v_i) | v_i \in V_A\})$: the maximum node weight in V_A is minimized.
4. $min(|V_O \bigcap V_R|)$: the number of nodes in the intersection of V_R and V_O is minimized.
5. $min(\max\{P'_{ro}(v_i) | v_i \in V_O \setminus V_R\})$: the maximum node weight in $V_O \setminus V_R$ is minimized.
6. $min(D(v_0, V_D))$: the maximum hop distance from v_0 to the nodes in V_D is minimized.

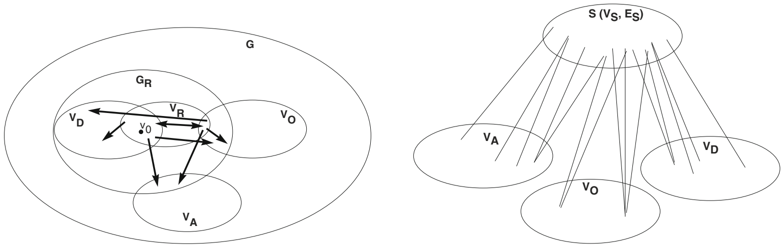
Table 1. Notations and their semantic meanings

Notations	Meanings
V_D	The set of destinations
V_A	The set of unwelcome users
V_O	The set of outsiders
V_R	The set of relays
G_R	The derived graph of V_R
$I(v_i)$	v_i's one-hop directed neighbors
$w_{i,j}$	v_j's probability of detecting v_i's transmissions
$P'_{ro}(v_i)$	v_i's probability of overhearing the information
$D(v_0, V_D)$	Maximum hop distance from the source to the destinations

3.3 Performance Metrics

The layout of the proposed graph model is illustrated in Fig. 1(a). According to the objectives, the performance of a feasible V_R should be evaluated based on the following criteria in descending order of priorities:

1. $\boldsymbol{max} P'_{ro}(A)$: the maximum node weight in V_A.
2. $\mathbf{N}_{ro}$= $|V_O \bigcap V_R|$: the number of outsider relays.
3. $\boldsymbol{max} P'_{ro}(O \setminus R)$: the maximum node weight in $V_O \setminus V_R$.
4. $\boldsymbol{max}\mathbf{D}$: the maximum hop distance between v_0 and the nodes in V_D.



(a) General model

(b) Optimization model, where $V_S = V \setminus V_A$ and $E_S = E \setminus \{e_{i,j} | \forall v_i \in V_A \textit{ or } \forall v_j \in V_A\}$

Fig. 1. The graph model for Information leakage reduction

4 Routing Algorithm for Information Leakage Reduction

In this section, we present a routing algorithm for information leakage reduction in social networks based on the proposed general graph model shown in Fig. 1(a). In order to check the existence of feasible solutions to achieve the first two objectives, we first remove the nodes in V_A from the graph G. We then check whether there exists a connected subgraph that contains all the nodes in V_D in the residual graph. This checking process can be finished in a polynomial time by employing the BFS algorithm starting from the node v_0.

In the rest of this section, we assume there always exist feasible solutions so that we can focus on the optimization problem of achieving the last four objectives. In order to solve the problem, we construct a graph shown in Fig. 1(b), where S is the residual graph constructed by removing V_A and all the edges associated with the nodes in V_A from G, based on the general model in Fig. 1(a). The edges that connect two nodes in V_A and V_S, in V_O and V_S, and in V_D and V_S, represent the edges in E. Note that all the nodes in V_O and V_D are also in V_S, and that each pair of these duplicated nodes is connected by an edge.

During the routing algorithm design, we assume that the channel availability information is known, that the selected relays only broadcast the information once, and that all the selected receivers can receive the information successfully from the relays. The $w_{i,j}$ is set as the reciprocal of the number of available channels.

In Fig. 1(b), to achieve the third objective, we need to find a connected subgraph S' of S such that all the nodes in V_D can be dominated by the nodes in S', and that the maximum P'_{ro} value among the dominated nodes in V_A is minimized. Note that $V_R = V_{S'}$ is a candidate solution, and that there may exist multiple candidate solutions. As the objectives are listed in descending priority orders, the next step is to choose a candidate solution that should satisfy the following conditions with decreasing order of priorities: i) it should include the minimum number of outsiders, ii) it should minimize the maximum P'_{ro} value, which is less than 1, among the dominated nodes in V_O, and iii) it should minimize the maximum hop distance from v_0 to the destination nodes.

According to the above analysis, we propose a greedy routing algorithm, which is illustrated in Algorithm 1, to find a feasible solution based on the graph model shown in Fig. 1(b). The notations used in the algorithm are summarized in Table 2.

In the algorithm, we select the relay nodes and add them to V_R one by one. The algorithm consists of three phases. In the first phase, we set $\{v_0\}$ as V_R, and calculate P'_{ro} for all the nodes (line 4). We then construct a set of dominating relays from V_S in the second phase, so that all the nodes in V_D can be dominated.

Table 2. Algorithm notations

Notations	**Meanings**
$Info(v_i)$	Whether v_i can obtain the information
w_i^A	v_i's aggregated probability of being overheard by unwelcome users (3)
w_i^O	v_i's aggregated probability of being overheard by outsiders (4)
$\overline{V_D}$	The set of nodes that can directly reach V_D (2)
V_R^E	The set of dominating relays

Finally, we add nodes from V_S to the set of selected dominating relays so that all the relays can be connected in the third phase.

In the dominating relay selection process, we first construct a set of nodes, denoted by $\overline{V_D}$, which can directly send information to at least one of the destinations according to (2).

$$\overline{V_D} = V_D \bigcup \{v_j \in V \setminus V_A | e_{j,i} \in E \ and \ v_i \in V_D\} \tag{2}$$

We iteratively select nodes from $\overline{V_D}$ one by one to construct the dominating relay set until all the destinations are dominated by the selected nodes. At each selection iteration, we first remove the unnecessary nodes, which can not send information to more destinations, from $\overline{V_D}$ (*Line 10-14*). Then, we find a set of nodes in $\overline{V_D}$, which can minimize the accumulated probability of being overheard by the unwelcome users if they are selected as relays (*Line 15-16*). The accumulated probability is calculated according to (3).

$$w_i^A = \max\{1 - (1 - P'_{ro}(v_j))(1 - w_{i,j}) | v_j \in V_A\} \tag{3}$$

Similarly, we define a node v_i's impact on the accumulated probability of being overheard by the outsiders in (4).

$$w_i^O = \max\{1 - (1 - P'_{ro}(v_j))(1 - w_{i,j}) | v_j \in V_O \setminus V_R\} \tag{4}$$

Based on the priority order of the 4th and the 5th objectives, we select a node from the smallest w_i^A node set according to *Line 17-22*. Then, we add the selected node to V_R. It follows from (1) that $P'_{ro}(v_i)$ depends on the nodes in V_R. Thus, it should be recalculated at each iteration (*Line 24*).

As the constructed dominating relay set (*Line 27*) may not be connected, we iteratively add nodes to V_R until it is connected (*Line 30-34*). In order to achieve the 3rd-5th objectives, the connecting node selection process is in a way similar to the process of dominating relay selection, and the selection is not based on the nodes' connectivity. As a result, there may exist redundant nodes in V_R. Therefore, jointly considering the last objective, the final route is calculated by employing the BFS algorithm on the selected V_R with the branch cut procedure (*Line 35-36*), which can remove the branches that do not contain any destination node.

Note that the algorithm's complexity is polynomial as the selection process, the BFS algorithm, the connectivity checking, and the branch cut procedure, can all be finished in a polynomial time.

5 Simulations

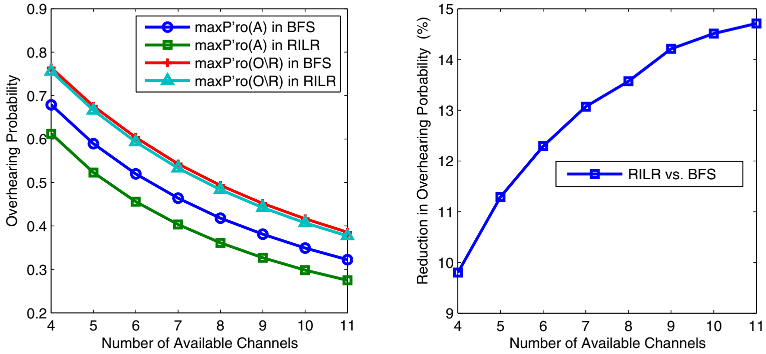
In this section, we use Matlab to evaluate the performance of the proposed algorithm (denoted as RILR) by comparing its performance with that of the BFS based algorithm. For fairness, we revise the BFS algorithm by skipping the unwelcome users and giving priority to the destinations during the route

Algorithm 1. Routing for Information Leakage Reduction

```
 1: **Phase I: Initialization**
 2: $V_R = \{v_0\}$, $Info(v_0) = 1$;
 3: $Info(v_i) = 1$, for $\forall v_i \in I(v_0) \bigcap V_D$;
 4: Calculate $P'_{ro}(v_i)$ for $\forall v_i \in V$ according to Eq. (1);
 5: $\forall v_i \in V_D \setminus I(v_0)$, $Info(v_i) = 0$;
 6:
 7: **Phase II: Relay Selection**
 8: Construct $\overline{V_D}$ according to Eq. (2);
 9: **while** $\exists v_i \in V_D$ s.t. $Info(v_i) == 0$ **do**
10:     **for** $\forall v_j \in \overline{V_D}$ **do**
11:         **if** $\forall v_k \in I(v_j) \bigcap V_D$, s.t. $Info(v_k) == 1$ **then**
12:             Remove $v_j$ from $\overline{V_D}$;
13:         **end if**
14:     **end for**
15:     Calculate $w_j^A$ for $\forall v_j \in \overline{V_D}$ according to Eq. (3);
16:     Find a set of nodes with the smallest $w_j^A$ in $\overline{V_D}$;
17:     Calculate $w_j^O$ for all the nodes in the set according to Eq. (4);
18:     **if** the set includes nodes in $V_D$ **then**
19:         Pick a node $v_j$, which has the smallest $w_j^O$, from the intersection of the set
    and $V_D$;
20:     **else**
21:         Pick a node $v_j$, which has the smallest $w_j^O$, from the set;
22:     **end if**
23:     Add $v_j$ to $V_R$;
24:     Recalculate $P'_{ro}(v_i)$ for $\forall v_i \in V$ according to Eq. (1);
25:     $\forall v_k \in I(v_j) \bigcap V_D$, set $Info(v_k) = 1$;
26: **end while**
27: $V_R^E = V_R$;
28:
29: **Phase III: Connected Rout Construction**
30: **while** $V_R^E$ is not connected **do**
31:     Calculate $w_j^A$ for $\forall v_j \in V_S \setminus V_R$ according to Eq. (3);
32:     Find a set of nodes with the smallest $w_j^A$ in $V_S \setminus V_R$;
33:     Repeat *Line 17-24*;
34: **end while**
35: Construct a BFS tree in $V_R$ starting from $v_0$;
36: Remove the subtrees that do not contain the nodes in $V_R^E$, from $V_R$;
37: Recalculate $P'_{ro}(v_i)$ for $\forall v_i \in V$ according to Eq. (1);
38:
39: **Outputs:**
40: Output the smallest BFS tree containing $V_R^E$, $\boldsymbol{max}P'_{ro}(A)$, $\mathbf{N}_{ro}$, $\boldsymbol{max}P'_{ro}(O \setminus R)$,
    and $\boldsymbol{max}\mathbf{D}$;
```

construction. This means that the revised BFS algorithm does not choose unwelcome users as relays but selects the destinations as relays when destinations and outsiders are in the same level.

In the simulation study, 100 nodes are randomly deployed in a 100 × 100 area. The source node v_0 are deployed in the center of the area. 10 nodes are randomly selected as the destinations, and another set of 10 nodes are randomly selected as the unwelcome users. We assume that all the nodes have the same communication range and the same set of available channels. The number of available channels varies between 4 and 11. We set the edge weight $w_{i,j}$ as the reciprocal of the number of available channels. The average node degree is controlled by the communication range, which is set as 20. As a result, the average node degree varies between $9.8 - 12.5$ in the simulations. Note that we only consider the simulated networks containing routes that can connect the sources and the destinations without the help of the unwelcome users, during the performance evaluation. Each reported result in Fig. 2(a), Fig. 2(b), and Fig. 3 is the mean of $100,000$ instances.



(a) Overhearing probability (b) RILR's outperformance

Fig. 2. Simulation results

Fig. 2(a) reports the performance of RILR in terms of the maximum overhearing probabilities of the unwelcome users and the outsiders. We can conclude that increasing the number of available channels can help to reduce the overhearing probabilities. This indicates that we can effectively reduce the probability of information leakage to non-destination users by take the advantage of multi available channels. Moreover, the proposed routing algorithm always outperforms the revised BFS algorithm in terms of overhearing probability. Regarding the unwelcome users' overhearing probability, which is the most important concern in confidential information sharing, RILR can achieve an average of 12% reduction in information leakage compared with the revised BFS algorithm as shown in Fig. 2(b). Note that the outperformance of RILR increases along with the increase of the number of available channels. The costs of the reduction include the increase in route length and the increase of the number of outsider relays as shown in Fig. 3.

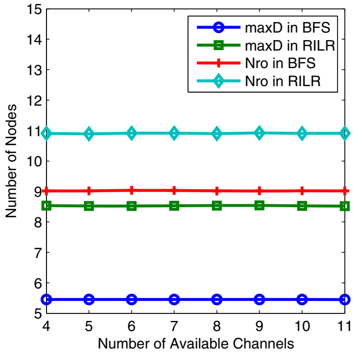


Fig. 3. Number of nodes in the route

6 Conclusion and Future Research

In this paper, we propose a routing algorithm to reduce the probability of information leakage during the wireless transmissions in social networks. Two routing models, Trusted Group Multicast and Confidential Unicast, are considered in this paper. Through the simulations, the proposed RILR routing algorithm always yields a lower overhearing probability compared with the BFS based routing algorithm.

In our future work, we will study the routing problem of information leakage reduction in more complex environments. For example, retransmissions, which can increase the overhearing probability and can affect the values of $w_{i,j}$, w_i^A, and w_i^O, will be considered during the algorithm design. We will also add thresholds to w_i^A and w_i^O during the relay selection so that the maximum overhearing probability can be controlled. Moreover, the scheme that can handle the case with dynamic available channels will be proposed for the routing algorithm design.

Acknowledgments. The research was partially supported by the US NSF under grants CNS-0963957 and CNS-0964060.

References

1. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100 (1997)
2. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. In: Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113–127 (May 2003)
3. Li, Y., Wang, P., Niyato, D., Zhuang, W.: A dynamic relay selection scheme for mobile users in wireless relay networks. In: INFOCOM, 2011 Proceedings IEEE, pp. 256–260 (April 2011)

4. Wu, S., Candan, K.S.: Gmp: Distributed geographic multicast routing in wireless sensor networks. In: Proceedings of the 26th IEEE International Conference on Distributed Computing Systems, ICDCS 2006. IEEE Computer Society, Washington, DC (2006)
5. Sanchez, J., Ruiz, P., Stojmnenovic, I.: Gmr: Geographic multicast routing for wireless sensor networks. In: 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, SECON 2006, vol. 1, pp. 20–29 (September 2006)
6. Frey, H., Ingelrest, F., Simplot-Ryl, D.: Localized minimum spanning tree based multicast routing with energy-efficient guaranteed delivery in ad hoc and sensor networks. In: Proceedings of the 2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks, WOWMOM 2008, pp. 1–8. IEEE Computer Society, Washington, DC (2008)
7. Johansson, T., Osipov, E., Carr-Motyčkovà, L.: Interference Aware Construction of Multi- and Convergecast Trees in Wireless Sensor Networks. In: Balandin, S., Moltchanov, D., Koucheryavy, Y. (eds.) NEW2AN 2008. LNCS, vol. 5174, pp. 72–87. Springer, Heidelberg (2008)
8. Liu, Y., Liang, W.: Energy-Efficient Multiple Routing Trees for Aggregate Query Evaluation in Sensor Networks. In: Harju, J., Heijenk, G., Langendörfer, P., Siris, V.A. (eds.) WWIC 2008. LNCS, vol. 5031, pp. 201–212. Springer, Heidelberg (2008)
9. Xin, C., Xie, B., Shen, C.C.: A novel layered graph model for topology formation and routing in dynamic spectrum access networks. In: 2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005, pp. 308–317 (November 2005)
10. Pefkianakis, I., Wong, S., Lu, S.: Samer: spectrum aware mesh routing in cognitive radio networks. In: Cognitive Radio Networks, 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2008, pp. 1–5 (2008)
11. Ding, L., Melodia, T., Batalama, S., Matyjas, J., Medley, M.: Cross-layer routing and dynamic spectrum allocation in Cognitive Radio Ad hoc Networks. IEEE Transactions on Vehicular Technology 59(4), 1969–1979 (2010)
12. Shih, C.F., Liao, W., Chao, H.L.: Joint routing and spectrum allocation for multihop cognitive radio networks with route robustness consideration. IEEE Transactions on Wireless Communications 10(9), 2940–2949 (2011)
13. Abbagnale, A., Cuomo, F.: Gymkhana: A connectivity-based routing scheme for cognitive radio ad hoc networks. In: INFOCOM IEEE Conference on Computer Communications Workshops, pp. 1–5 (March 2010)