On the Hardness of Minimum Cost Blocking Attacks on Multi-path Wireless Routing Protocols

Qi Duan, Mohit Virendra, Shambhu Upadhyaya
Department of Computer Science and Engineering
State University of New York at Buffalo
{qiduan, virendra, shambhu}@cse.buffalo.edu

***Abstract*: This paper demonstrates the provable superiority of multi-path routing protocols over other conventional protocols against blocking, node-isolation and network-partitioning type-attacks in Wireless Mesh Networks (WMNs) by emulating adversarial behavior. Though the underlying network model is of a WMN with mobile nodes, the results in this paper are equally applicable to other types of wireless data networks. The adversarial objective is to isolate a subset of network nodes through minimal cost optimal blocking of certain number of paths in the network (or partitioning the network). If less than a certain threshold of traffic from such node(s) reaches the routers, the adversary is successful. Two scenarios viz.: (a) low mobility for network nodes, and (b) high degree of node mobility, are evaluated. Scenario (a) is proven to be NP-hard and scenario (b) is proven to be #P-hard for the adversary to achieve the goal. Further, several approximation algorithms are presented which show that even in the best case scenario it is at least exponentially hard for the adversary to optimally succeed in such blocking-type attacks. These results are verified through simulations which demonstrate the robustness of multi-path protocols against such attacks. The objective of this paper is not to aid the adversary in succeeding in these attacks or to devise security measures for routing protocols; rather the aim is to study the performance and feasibility of multi-path protocols over conventional single-path protocols from a security angle in the wireless domain. To the best of our knowledge, this is the first paper to theoretically evaluate the attack-resiliency and performance of multi-path protocols with network node mobility.**

***Keywords:* Attacks; Blocking; Multi-path routing; Wireless networks;**

I. INTRODUCTION AND MOTIVATION

Multi-path traffic scheduling and routing protocols are deemed superior over conventional single path protocols in terms of enhanced throughput and robustness in wired networks. However, network dynamicity and resource constraints entail additional overhead in maintaining and reconfiguring multiple routes in wireless networks, and these overheads may offset the benefits mentioned above. Existing literature for wireless networks multi-path protocols [16, 17] only evaluates their performance in terms of throughput. This paper adopts a unique approach to assay their utility by investigating the additional security and robustness provided by these protocols. This paper emulates adversarial behavior and launches attacks on these protocols, and then studies the impact of such attacks.

Wireless Mesh Networks (WMNs) [13] are considered as the underlying representative network model. WMNs have emerged as a key component in the networking and communications domain due to their design which allows numerous diverse commercial and military applications [27, 28]. Significant research effort is being placed on designing protocols for WMNs [29]. WMNs have mobile nodes communicate wirelessly over multiple hops to the backbone network through multiple available network routers. Primary traffic in WMNs is between nodes and the backbone network. Efficient multi-path traffic scheduling schemes can split a node's traffic into multiple flows along several accessible routers and eventually reassemble this traffic at the backbone network at low cost. This makes WMNs ideal candidates for enumerating the full scope of any wireless multi-path protocols, especially to evaluate attack scenarios. Though the underlying representative network model is WMNs, the attack scenarios and results in this paper are completely portable to other types of wireless data networks.

A. Threat Model and Attack Scenarios

Blocking, node-isolation and network-partitioning type attacks are easy to launch and effective in the wireless networks domain due to channel constraints and dynamic network topology. We emulate adversarial behavior by attacking multi-path schemes through intelligent blocking and node-isolation type attacks for maximal impact. We also try to design best-case scenarios for these attacks to succeed. Both low node-mobility and high node-mobility situations are considered. For comparison purposes, we also launch similar attacks on conventional single-path protocols and measure their impact.

B. Impact, Scope, and Relevance

The scope of this work is to study active attack scenarios from recovery and resiliency point of view. The impact and relevance pertain to building confidence on existing schemes which rely on robustness of multi-path protocols. The impacted areas would include load balancing [18], network coding [19, 20, 21], and threshold cryptography [22, 23], in the wireless networks domain.

(a) Active Attack Scenarios for Recovery and Resiliency: This work is highly relevant for scenarios where it may be easier or harder for the adversary to compromise some nodes in the network, as compared with compromising the rest of the nodes. For example, it would usually be more difficult to block nodes closer to the routers or Base Stations (BSs) due to reasons of physical proximity (better physically guarded), or signal strength (nodes closer to BS may receive better signal strength).

It would be highly desirable for protocols to continue executing correctly without information compromise, even in the presence of a few malicious nodes. Most current security pro-

tocols do not address recovery from malicious behavior. These protocols simply abort execution and restart if any malicious behavior is detected. This is detrimental in applications where real-time response and high level security are important as information may already have been lost in the partial execution and frequent restart of the protocols.

(b) Relevance and Impact on Existing Protocols: Multi-path routing protocols can naturally extend threshold cryptography concepts to the wireless domain. Demonstrated robustness of multi-path protocols against such blocking-type attacks would increase confidence in utilizing threshold cryptography schemes. Here a node splits a secret into several shares, routes them along independent paths, and at least a threshold number of shares have to be compromised for an adversary to recover the secret. Our results imply that it would be at least exponentially hard for an adversary to optimally compromise or block certain threshold number of shares such that either the adversary recovers the secret, or equivalently, the secret is not recovered properly at the destination.

Network coding, where nodes intelligently send redundant information along multiple paths to ensure security and reliability and to detect any problems with a route would also benefit from demonstrated robustness of multi-path routing. Again, it would be at least exponentially hard for the adversary to optimally compromise more than a threshold number of these paths to render such network coding schemes ineffective.

C. Paper Organization

The rest of this paper is organized as follows. Section 2 presents problem statement with a summary of contributions and related work. Section 3 introduces the Minimum Cost Blocking (MCB) problem and proves its NP-hardness. Section 4 provides approximation algorithms for the MCB problem. Section 5 introduces the #P-Hard Blocking problem for WMNs with patterned node mobility. Section 6 presents simulation results. Section 7 concludes the paper with a discussion on its limitations and future research directions.

II. Summary of Contributions and Related Work

A. Problem Statement and Summary of Contributions

Clearly, there is lack of: (a) Performance investigation of mobile wireless networks multi-path protocols in terms of security and resiliency under even basic attack scenarios, and (b) Comparison with traditional single-path protocols under such circumstances. This paper attempts to achieve the above two desired goals. To the best of our knowledge, this is the first paper to theoretically evaluate the performance of wireless networks multi-path protocols with node mobility under simple attacks. The technical contributions can be summarized as:

- The identification of the Minimum Cost Blocking (MCB) problem. Though we consider MCB in WMN setting, the problem is applicable to other wireless or wired networks.
- Evaluating the hardness of the problem: MCB is NP-Hard for the low/no node mobility scenario and #P-Hard for networks with patterned node mobility. The reduction for no-mobility is derived from the basic Set Cover problem [6] and the mobility scenario from the 3-SAT [30] and #SAT [11].
- Development of approximation algorithms for best case scenarios and the performance testing of these algorithms in different practical experimental settings through simulations.
- Laying direction for future research to evaluate the performance of multi-path protocols against other well known and more sophisticated attacks in mobile wireless networks.

B. Related Work

(a) Pertaining to Attacks and Security: Attacks on routing system are widely explored in wired networks. Some of the attacks can be prevented or countered through cryptographic techniques. For example, OSPF [1, 3] uses MD5 [2] to guard against false packet injection. Digitally signed statements can also be used in OSPF to prevent false advertisement by legitimate users. In wireless networks such cryptographic schemes for secure broadcast and false data injection prevention are described in [25, 26]. However, there are other attacks that cannot be countered through cryptographic techniques. Link cut attacks in wired networks, first investigated in detail in [4], are one such type of attacks. In wireless networks, link cuts can be achieved through jamming or interference [24]. In reality, blocking a certain link in a wireless network usually means blocking all signals from a certain node or compromising the node completely. This may be relatively easy to achieve for wireless nodes deployed in automated, unattended or hostile scenarios, accentuating the need for research on blocking attacks.

(b)Pertaining to Network Model and Theoretical Hardness: Wireless mesh networks are comprehensively described in [13]. The basic set cover problem is NP-hard and extensive research has been done on its approximation algorithms [7, 8]. A generalization of the set cover problem is partial set cover problem [9, 10]. Complexity class #P was first introduced in [11]. Sociological orbits in wireless networks, utilized in describing the node-mobility scenario, were introduced in [12].

III. Minimum Cost Blocking: No/Low Mobility

This section presents the MCB problem for the stationary-nodes/low-mobility scenario from the adversary's perspective. The network is modeled as an undirected graph G, with vertex set V and edge set E. Here every vertex represents a node in the network and a link between two vertices implies that corresponding nodes are within each other's radio range. A directed graph may better represent the network for real life situations since nodes may have different radio ranges, signal strength may be different in each direction, and links may not be completely bidirectional. However for simplifying the problem description we assume an undirected graph, emphasizing that all our results are equally applicable to the general case of directed graphs.

A. MCB Optimization Problem

Suppose in the graph $G(V, E)$, $|V| = k$.

Every node v_i in V has a cost c_i to be compromised.

There are $m = \sum_{i=1}^{k} n_i$ paths,

$P_{11}, P_{12}, \cdots, P_{1n_1}, P_{21}, P_{22}, \cdots, P_{2n_2}, \cdots, P_{k1}, P_{k2}, \cdots, P_{kn_k}$.

Here, $P_{i1}, P_{i2}, \cdots, P_{in_i}$ ($i = 1, 2, ..., k$), are paths originating from node i (or equivalently, paths belonging to node i). What is the minimum cost to compromise a subset of the nodes such that a certain percentage of paths belonging to a node are compromised? That is, for every node i ($i = 1, 2, \cdots, k$), what is the minimum cost to compromise at least R_i ($0 \le R_i \le n_i$), out of all paths belonging to this node (i.e., paths $P_{i1}, P_{i2}, \cdots, P_{in_i}$)? This is a typical optimization problem. The corresponding decision problem is described below.

B. MCB Decision Problem

Given: Graph *G (V, E)*, where every node v_i in *V* has a cost c_i to be compromised, the set of nodes in $m = \sum_{i=1}^{k} n_i$ paths $(P_{11}, P_{12}, ..., P_{1n_1}, P_{21}, P_{22}, ..., P_{2n_2}, ..., P_{k1}, P_{k2}, ...P_{kn_k})$, and integers C and R_i ($0 \le R_i \le n_i$).

Statement: Is there a subset *V'* of *V* such that compromising *V'* will block at least R_i out of the paths $P_{i1}, P_{i2}, \cdots, P_{in_i}$, for every node v_i ($i = 1, 2, ..., k$), and the total cost of nodes in *V'* is no greater than *C*?

In reality, the adversary may not need to block all the nodes in a network. However, since our description and algorithms apply to the general case of blocking traffic from a subset of nodes, we can simply let all paths related to nodes not in the target subset to be empty. It is easy to show that the problem is NP-complete.

Theorem 3.1: The MCB decision problem is NP-complete.

Proof: The problem is a general case for the partial set cover problem [5], which is a well known NP-complete problem. So MCB is NP-complete.

IV. Approximation Algorithms: MCB No Mobility

In this section we propose two algorithms for the stationary-nodes MCB problem. The first one is a greedy algorithm and the second one is an LP-based algorithm. We prove the approximation ratio for both of them. We first define the notation of "cover" which will be frequently used later and then list some notations used in the description of the algorithms.

Definition 3.1: When a node (or a node within a subset of nodes) is on a path, we say that the node (or the subset of nodes) covers that path. When R_i paths belonging to a node i are covered, we say that node i is covered.

A. Notations

- T: The set of nodes that have been chosen at the beginning of an iteration (An iteration includes all sub-steps of step 2 in Algorithm 1).
- E_i: Effective number of node *i*, or the number of effective paths the node *i* will cover in the current iteration of the algorithm. An effective path means that the path has not been covered yet and the corresponding target node to which that path belongs has not been blocked yet.
- W_{ij}: Number of paths that belong to node *j* and are covered by node *i*.
- Y_j: Number of already covered paths that belong to node *j*.
- α_i: Cost-effective index of node *i*.
- D: Set of currently covered nodes (used in Algorithm 2).
- O_i: Number of paths belonging to node *i* covered by the set of nodes returned by the function call *SetCover* (used in Algorithm 2).
- c_i: Cost function associated with every node *i*, i.e., cost to compromise node *i*.

B. Algorithm1 and Approximation Ratio

Algorithm 1 selects the most cost-effective node iteratively and at the same time removes the covered paths and the paths unusable in future. Unusable paths are those originating from a node *i* with at least R_i paths already blocked, as covering these paths would be inconsequential.

Algorithm 1:

1. $T \leftarrow \phi$, and mark all paths and nodes as uncovered.
2. While not done (Done means nodes in *T* have already covered the required paths for all the nodes, i.e., *T* covers at least R_i paths for node *i*; $i = 1, 2, ..., k$), iterate the following sub-steps:
   2.1. For every remaining node *i* in $V \setminus T$ in the current iteration, compute its effective number E_i as follows:

   $E_i \leftarrow 0$

   2.1.1. For every node *j* not covered yet, compute $\min(\max((R_j - Y_j), 0), W_{ij})$, where W_{ij} is the number of paths that belong to node *j* and are covered by node *i* and Y_j is the number of already covered paths that belong to node *j*. Thus $\min(\max((R_j - Y_j), 0), W_{ij})$ is essentially the number of effective (or useful) uncovered paths that belong to node *j* and are covered by node *i*. Update E_i,

   $E_i = E_i + \min(\max((R_j - Y_j), 0), W_{ij})$

   2.2. Compute the cost-effective index α_i:

   $$\alpha_i = \frac{c_i}{E_i}$$

   2.3. Choosing the node *u* with lowest α_u: Mark as covered each path covered by node *u*. For every effective path *p* that *u* covers, set $price(p) = \alpha_u$. Check all currently uncovered nodes: mark as covered any node has already covered in this iteration.

$T \leftarrow T \cup u$

3. Output *T*.

End

Next we show that Algorithm 1 achieves an approximation ratio of $\ln R$, where $R = \sum_{i=1}^{k} R_i$.

Theorem 4.1: Algorithm 1 achieves an approximation ratio of $\ln R$.

Proof: Our method is similar to the *Proof* for the Greedy Algorithm ratio for the Set Cover problem in [14]. Suppose the optimum solution has a cost *OPT*. We number the covered effective paths in the algorithm in the order they are covered and name them as $P_1, P_2, \cdots, P_R$. In each iteration of the algorithm the new optimal solution (selected from $V \setminus T$) covering the remaining uncovered nodes, has a cost at most *OPT*. Amongst these nodes there must be one node that has cost-effective index at most *OPT/U*, where *U* is the number of uncovered effective paths (otherwise the optimum solution will have a cost greater than *OPT*). In the iteration that path P_j is covered, there are at least $R - j + 1$ paths not covered yet. Because we choose the node with lowest cost-effective index, we have $price(P_j) \le \frac{OPT}{R - j + 1}$. The total cost of our algorithm will be

$$\sum_{j=1}^{R} price(P_j) \le (1 + \frac{1}{2} + \cdots + \frac{1}{R}) \cdot OPT \le OPT \cdot \ln R$$

C. Algorithm2 and Approximation Ratio

Adopting the LP-relaxation based algorithm SetCover for partial set cover in [5], we develop Algorithm 2. For ease of reference, we include an Appendix with the details of SetCover and PrimalDual (partial set cover) algorithms from [5].

Algorithm 2

1. $T \leftarrow \phi$, $D \leftarrow \phi$
2. While *D* does not contain all nodes in the graph, iterate the following sub-steps:
   2.1. Choose node j with the highest value R_j. Then call SetCover$(P, V \setminus T, c, R_j)$
   Here *P* is the set of all uncovered paths belonging to node *j* and *c* is the array of cost values for nodes in $V \setminus T$ (i.e., $c_j, \forall j \in V \setminus T$). The function SetCover returns the selected sets (nodes) that cover at least R_j paths in *P*.
   2.2. $D \leftarrow D \cup j$.
   2.3. For every node *i* returned by the function, $T \leftarrow T \cup i$.
   2.4. Remove from *P*, every path *p* that is covered by the nodes returned by the function call SetCover: $P \leftarrow P \setminus p$
   2.5. For every $i \in V \setminus D$, adjust R_i as follows: $R_i = \max(0, R_i - O_i)$
   Here O_i is the number of paths belonging to node *i* that were covered by the set of nodes returned by the function call SetCover. If R_i becomes 0, which means node *i* is blocked, then $D \leftarrow D \cup i$.
3. Output T.

End

Algorithm 2 repeatedly blocks a node in every iteration (step 2) until all nodes are blocked.

Theorem 4.2: Algorithm 2 achieves an approximation ratio of $h \cdot k$, where *h* is the number of nodes in the longest path.

Proof: The approximation ratio of algorithm SetCover [5] is *h*. Obviously at every iteration the sum of the cost of selected nodes $\le h \cdot OPT$, so the total cost of the solution returned by Algorithm 2 will be $\le h \cdot k \cdot OPT$.

D. Approximation Ratios: Practical Significance

The high approximation ratios of these two algorithms signify the high level of difficulty for the adversary to achieve the optimal solution. It seems that Algorithm 2 is worse than Algorithm 1 in terms of the approximation ratio. However, the ratios obtained in this paper are a coarse performance measure and it is an open research issue to determine if any better algorithms (algorithms with guaranteed better ratios) exist. We further evaluate the performance of these algorithms through simulations in Section 6.

In a practical setting, if the graph (network) is sparse and the topology is known to the adversary, it would be easier for the adversary to successfully launch such blocking attacks. If the graph (network) is dense, then launching an effective attack would be more difficult. From a protocol security and resiliency point of view, it would be ideal if the network topology information is hidden from the adversary, making it extremely hard to launch such attacks. However, in real life setting, complete topology obfuscation is not necessary. If the adversary has partial topological information, the above algorithms cannot be executed correctly. Thus, even partial topology obfuscation can be a significant deterrent against the full scope of such attacks. This provides motivation for introducing the network node mobility scenario where exact network topology is never accurately known.

V. MESH NETWORKS WITH PATTERNED NODE MOBILITY

So far we considered limited/no network node mobility. If network nodes are mobile then the analysis of the MCB problem becomes more complicated. We first provide a brief motivation on graph theoretic modeling of node mobility and then present Stochastic Blocking, the MCB problem for networks with mobile nodes.

Nodes in real-life wireless networks have some form of patterned mobility (demonstrated in [12] and the references therein). In WMNs, the mobility pattern of the nodes is predictable [12, 13]. The nodes move within mobility orbits and the position of a given node has a probability distribution over the

positions of the orbit. Our analysis of the node-mobility blocking problem assumes that movement of the WMN nodes follows such a probabilistic patterned mobility model. We introduce the concept of Node-based Stochastic Graphs to characterize such patterned node mobility.

Definition 5.1: Node-based Stochastic Graph: It is an undirected graph with a subset of nodes that are dynamic, i.e., every such node is associated with a probability of existence. Formally, let *S = (V, E)* be an undirected graph with *n* nodes, where $V = \{v_{11},..,v_{1t_1},v_{21},..v_{2t_2},..,v_{h1},..v_{ht_h},v_{h+1},..,v_n\}$. *V* contains two types of nodes: fixed nodes and dynamic nodes[1]. Nodes $v_{h+1},\cdots,v_n$ are fixed nodes. Nodes $v_{i1},\cdots,v_{it_i}$ $(1 \le i \le h)$ are possible positions of node v_i $(1 \le i \le h)$. There is an associated probability p_{ij} for every v_{ij} $(1 \le i \le h, 1 \le j \le t_i)$, which means node v_i has probability p_{ij} in position v_{ij} of *G*.

A. The Stochastic Blocking Problem

Since the network is dynamic, the adversarial goal would be to choose such a set of target nodes, whereby blocking them would result in the blocking probability being higher than some desired value. The formal description of the Stochastic Blocking is as follows.

Given: (1) A Stochastic Graph *S (V, E)*, where every node v_i in *V* has a cost c_i to be compromised.

(2) The set of nodes in $m = \sum_{i=1}^{k} n_i$ paths $(P_{11},P_{12},...,P_{1n_1},P_{21},P_{22},...,P_{2n_2},...,P_{k1},P_{k2},...P_{kn_k})$. All source and destination nodes in these paths are fixed nodes.

(3) Integers R_i $(0 \le R_i \le n_i)$ and a value *p* $(0 \le p \le 1)$

Statement 1 (Optimization)**:** Is there a subset *V'* of *V* such that compromising *V'* will block with a probability *p* at least R_i out of the paths $P_{i1},P_{i2},\cdots,P_{in_i}$ $(1 \le i \le k)$, for every node v_i $(i = 1,2,...,k)$, and the total cost of nodes in V' is minimized? This is an optimization problem; the corresponding decision problem (with same conditions) is stated below.

Statement 2 (Decision)**:** Is there a subset *V'* of *V* such that, compromising *V'* will block with a probability *p* at least R_i out of the paths $P_{i1},P_{i2},\cdots,P_{in_i}$ $(1 \le i \le k)$, for every node v_i $(i = 1,2,...,k)$, and the total cost of nodes in *V'* is no greater than *C*? Here *C* is some pre-specified number.

Next we demonstrate that even determining the blocking probability of a given dynamic graph is #P-hard. For that we first define a problem called #Blocking, evaluate the hardness of #Blocking, and show that Stochastic Blocking is harder than #Blocking.

[1] Our definition of Node-based Stochastic Graphs is in line with the WMN architecture. WMN routers have no/low mobility and WMN nodes are mobile.

B. #Blocking: Evaluating Hardness of Stochastic Blocking

Definition 5.2: #Blocking**:** Given the above graph model, the computational problem #Blocking is to determine the probability that at least R_i out of the paths $P_{i1},P_{i2},\cdots,P_{in_i}$ $(1 \le i \le k)$ will be blocked.

It is evident that to an efficient solution of #Blocking is a necessary precursor to solving Stochastic Blocking efficiently: it is required to determine the blocking probability before finding the optimal subset of nodes for blocking. That is, stochastic MCB should be at least as hard as #Blocking. Next we show that #Blocking is #P-hard.

Theorem 5.1: #Blocking is #P-hard.

Proof: #SAT is reducible to #Blocking. Given a 3SAT instance, a stochastic graph can be created as follows. For every variable in 3SAT, create a dynamic node which has two possible positions in the stochastic graph, and every position has probability 1/2. Also create a source node and a destination node for every clause. The source and destination nodes are connected with three paths through the three dynamic nodes corresponding to the three variables in the clause. If at least one of these three paths is blocked for every such source destination pair, then it is evident that the blocking probability is exactly the probability that the 3SAT instance is satisfied. Thus, #Blocking is #P-hard. Fig. 5.1 shows the #Blocking instance constructed through this procedure for the following instance of #SAT:

$$(\bar{x}_1 \vee x_2 \vee \bar{x}_3) \wedge (\bar{x}_2 \vee \bar{x}_3 \vee x_4)$$

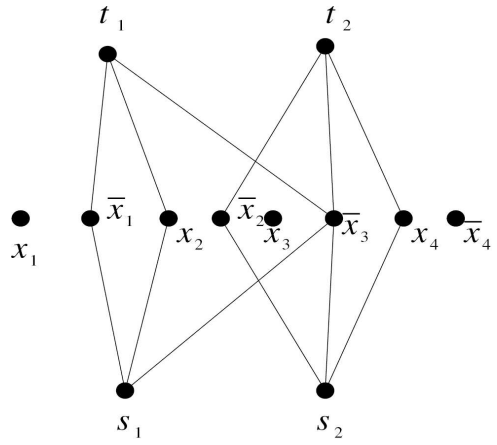

Figure 5.1

The above result demonstrates that even determining the blocking probability is very hard[2] in the patterned mobility model. So the task of blocking would be even harder for the adversary. Additionally, the adversary may not know the actual mobility patterns and the possible orbits of the network nodes, further enhancing the degree of hardness. Thus, it would be extremely hard for the adversary to efficiently launch such blocking-type attacks against multi-path protocols with node mobility. The degree of hardness prevents designing of approximation algorithms for efficient blocking in the node mobility sce-

[2] The actual position of #P in the complexity hierarchy is unknown, but it is generally assumed to be harder than NP

nario and this is an open research problem. Our continuing research focuses on further investigation of the blocking attacks for various mobility models and efficiency evaluation through simulations (see Sec VII).

VI. Simulation Results

We evaluated the performance of the two low/no mobility multi-path MCB algorithms using some random graphs. For comparison purposes, we also evaluated the performance of a greedy algorithm for MCB in single-path schemes. The single-path algorithm is similar to the multi-path MCB except that every node has only one path to the nearest (fewest number of hops in the path) router.

The goal of the attacker is to block the traffic of some target nodes. We test two scenarios. In the first case each node has cost 1, which means that the same effort is required to compromise every node. In the second scenario, every node has a basic cost 10, plus an additional cost inversely proportional to the distance between the node and the center of the whole square region, the maximum value of additional cost being 10. The second scenario is based on the assumption that it is more difficult to compromise nodes which are closer the routers (applicable in some practical settings).

The random graphs are generated as follows. All nodes in the graph are randomly distributed in a 500m by 500m square region, and if two nodes are within each other's radio range, they have a link in the graph. There are four routers that are located in the four corners of the square region. Every node has one route to each router, and the routing is based on Dijkstra's algorithm [15].

The total number of nodes in the region is denoted by n, the radio range of a single node is r and the possibility that a node is selected as target node is denoted by u. All selected target nodes are at least one hop away from any router. Here n, r and u are adjustable parameters. When at least 3 out of the 4 paths from a node to the routers (here a path does not include the router and the node itself) are blocked, we assume the node is blocked. We use our algorithms to determine the subset of nodes with minimum total cost in order to block paths from some randomly selected nodes in the square region.

The results of simulation are demonstrated in Figures 6.1 to 6.6. In all these figures the x-axis represents the r values and y-axis denotes the total cost of the subset found by the algorithm. All data points are the average of 100 runs. The value of r ranges from 100 to 180.

Figures 6.1 to 6.4 are results for the scenario where every node has cost value 1. Figure 6.1 corresponds to u = 1/20 and n = 120. Figure 6.2 has results with u = 1/10 and n =120. Figure 6.3 corresponds to u = 1/20 and n = 100. Figure 6.4 shows the results for = 1/10 and n = 100.

Figures 6.5 and 6.6 illustrate the results obtained when the second method to generate cost value of nodes is used. Figure 6.5 represents the results for u = 1/20 and n = 120, and Figure 6.6 represents u = 1/20 and n = 100.

The following conclusions can be drawn from these simulation results:

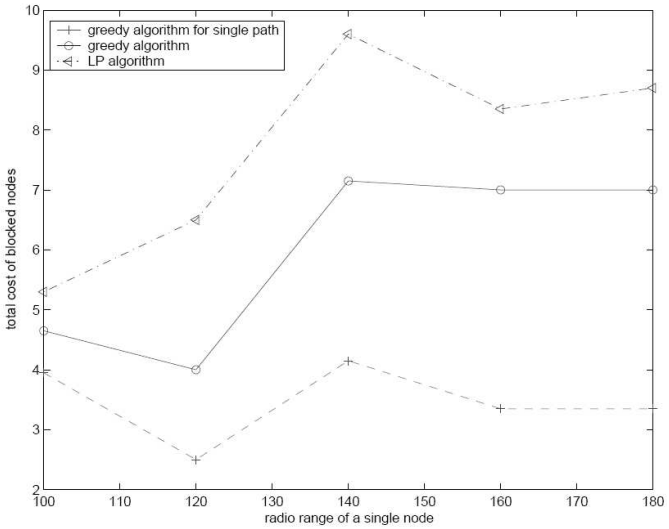

Figure 6.1

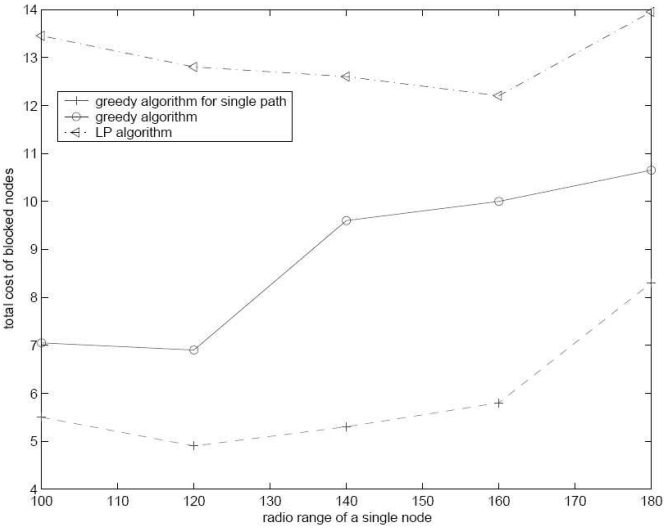

Figure 6.2

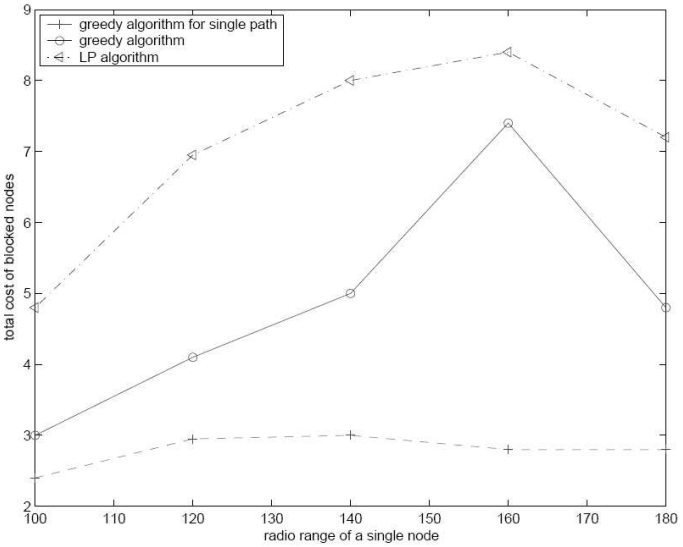

Figure 6.3

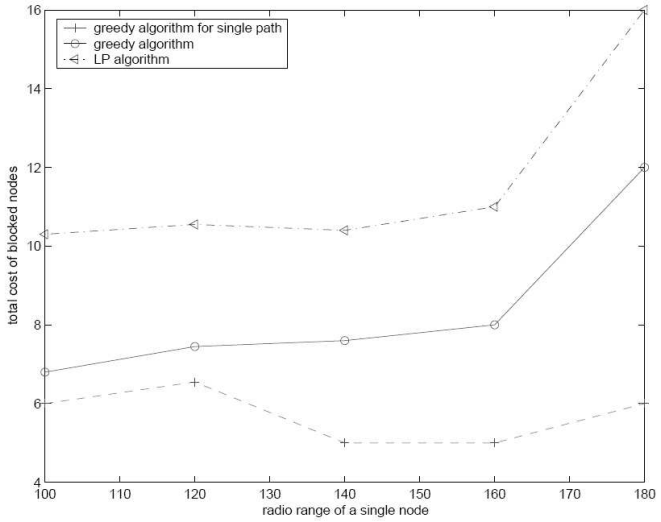

Figure 6.4

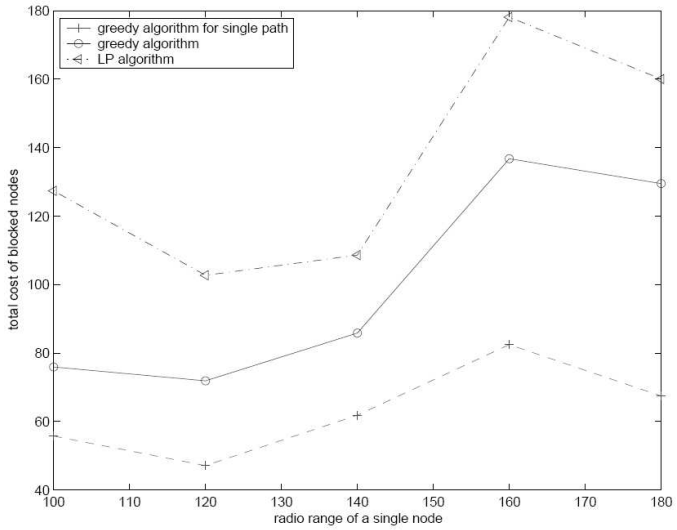

Figure 6.5

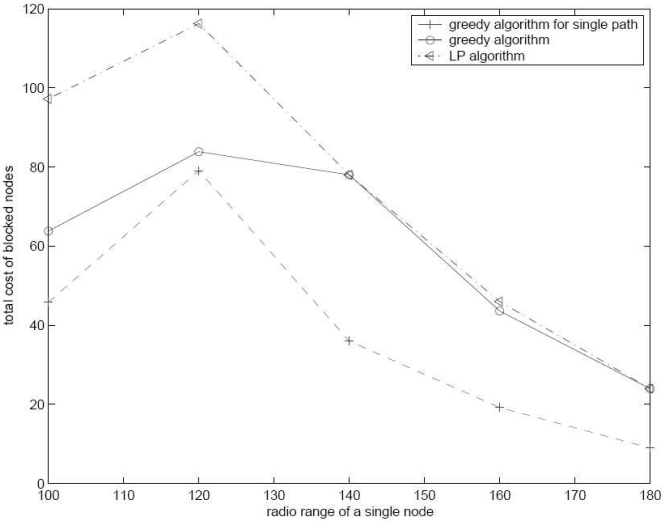

Figure 6.6

- The performance of Algorithm 1 (greedy algorithm) is better than Algorithm 2(LP-based algorithm) in most of the cases. Intuitively, this is attributable to the "global" nature of the first algorithm, whereas the second algorithm considers every node separately.
- In all the test cases, the cost of the single-path-blocking greedy algorithm is lower than the two multi-path algorithms. This is obvious and reasonable since it requires more effort to block more paths. But when the number of target nodes increases, the difference between the cost of single-path blocking and multi-path blocking decreases. Now there will be more paths in the graph and some nodes may become bottlenecks for several paths. These nodes would be easy targets for attacks.
- When the number of nodes increases, the cost for both single-path blocking and multi-path blocking increases. This is also reasonable since the graph become denser, and the target paths become increasingly disjoint.
- When the radio range of nodes increases, the trend of blocking-cost for target paths is not very obvious. In some cases, increasing the radio range results in a "peak" for the blocking-cost. Intuitively, increase in radio range also increases the number of edges in the graph, making the target paths more disjoint. But when the number of edges reaches a threshold, it ceases to have significant affect in the disjointedness of the paths.

VII. Discussion and Continuing Research

This paper demonstrates the superiority of multi-path protocols over traditional single-path protocols in terms of resiliency against blocking and node isolation-type attacks, especially in the wireless networks domain. Multi-path protocols for WMNs make it extremely hard for an adversary to efficiently launch such attacks. This paper is an initial attempt to model the theoretical hardness of attacking protocols for mobile nodes.

As a part of our continuing research, we plan to further investigate the approximation algorithms for the MCB problem. We also plan to investigate the problem in the settings related to ID-based key update protocols, which is very promising in wireless networks. In our discussions we assumed that the adversary has topological information of the network. It would be an interesting problem to study the additional difficulty associated with blocking when the topological information is effectively hidden from the adversary. This paper also brings forward some interesting related problems. For example, if link-cut and node-compromising are combined together (i.e., one can either cut some links or compromise some nodes), then what is the minimum total cost to block traffic from specific nodes?

References

[1] J. Moy, "OSPF version 2", RFC 2328, Internet Engineering Task Force, Apr. 1998.
[2] R. Rivest, "The MD5 message-digest algorithm", RFC 1321, Internet Engineering Task Force, Apr.1992
[3] S. Murphy, M. Badger and B. Wellington, "OSPF with digital signatures", RFC 2154, Internet Engineering Task Force, June 1997.

[4] S. Bellovin, E. Gansner, "Using Link Cuts to Attack Internet Routing", Tech. Rep., ATT Research, 2004, Work in Progress 2003 USENIX.
[5] R. Gandhi, S. Khuller, A. Srinivasan, “Approximation Algorithms for Partial Covering Problems”, Lecture Notes in Computer Science, Springer-Verlag GmbH, ISSN: 0302-9743, Vol. 2076, pp. 225-236.
[6] V.Chvatal. A greedy heuristic for the set-covering problem. Math. of Oper. Res. Vol. 4, 3, 233-235, 1979.
[7] D. S. Johnson. Approximation algorithms for combinatorial problems. J. Comput. System Sci., 9:256-278, 1974.
[8] L. Lovasz. On the ratio of optimal integral and fractional covers. Discrete Math. 13:383-390, 1975.
[9] M. Kearns. The computational complexity of machine learning. M.I.T. Press, 1990.
[10] E. Petrank. The hardness of approximation: Gap location. Computational Complexity 4:133-157, 1994.
[11] Christos Papadimitriou, Computational Complexity, 1st edition, Addison Wesley. ISBN 0201530821,1993.
[12] Joy Ghosh, "Sociological Orbit based Mobility Profiling and Routing for Wireless Networks", Ph.D. Dissertation, August, 2006, Buffalo, NY.
[13] Ian F. Akyildiz, Xudong Wang and Weilin Wang, “Wireless Mesh Networks: A Survey”, Computer Networks Journal (Elsevier), Vol. 47, pp. 445-487, Mar 2005.
[14] Vijay V. Vazirani, approximation algorithms, 15-17, Springer, 2004.
[15] E. W. Dijkstra: A note on two problems in connexion with graphs. In: Numerische Mathematik. 1, S. 269-201, 1959.
[16] W.H. Liao, Y.C. Tseng, S.L. Wang and J.P. Sheu, A multi-path QoS routing protocol in a wireless mobile ad hoc network, in: Proceedings of IEEE ICN , July 2001.
[17] Ying-Hong Wang, Hung-Zu Lin and Shu-Min Chang, Interfering-aware QoS Multipath Routing for Ad Hoc Wireless Network, 18th International Conference on Advanced Information Networking and Applications (AINA'04), Volume 1, p. 29.
[18] Jungmin So, Nitin H. Vaidya, "Load Balancing Routing in Multi-Channel HybridWireless Networks with Single Network Interface," qshine, p. 14, Second International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QSHINE'05), 2005.
[19] Christina Fragouli, et-al, Network Coding: An Instant Primer, ACM SIGCOMM, Vol 36, Number 1,Jan 2006.
[20] R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung, "Network information flow," IEEE Trans. on Information Theory. Vol. 46, pp 1204-1216, 2000.
[21] S.-Y. R. Li, R. W. Yeung, and N. Cai. "Linear network coding". IEEE Transactions on Information Theory , Februray, 2003.
[22] Ivan Damgård, Mads Jurik: A Length-Flexible Threshold Cryptosystem with Applications. ACISP 2003: 350-364.
[23] Ivan Damgård, Mats Jurik: A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. Public Key Cryptography 2001: 119-136.
[24] 802.11 Timelines. IEEE 802.11: Working Group for WLAN standards , May 2006.
[25] S. Zhu, S. Setia, S. Jajodia, P. Ning, “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks”, IEEE Symposium on Security and Privacy 2004, pp. 259-271.
[26] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, "SPINS: Security Protocols for Sensor Networks", Seventh Annual ACM International Conference on Mobile Computing and Networks (Mobicom 2001), Rome, July 2001.
[27] http://wire.less.dk/wiki/index.php/MeshLinks
[28] http://www.communitywireless.org/
[29] http://research.microsoft.com/mesh/
[30] S. A. Cook, “The Complexity of Theorem Proving Procedures”, Third Annual ACM Symposium on the Theory of Computing, New York, 1971, pp. 151-158.

Appendix: Algorithm for partial set-cover in [5].

PRIMAL_DUAL($\mathsf{T}', S^j, c', k_j$)

// Returns a subset C of S' that is feasible
// i.e, C covers $\geq k'$ elements of T'
// z is maitained implicitly in the algorithm, at all times
$z = \max_i u_i$
$C \leftarrow \phi$
$E \leftarrow \mathsf{T}'$
Initialize all u_i to 0
while C is not feasible
// increase the dual variables u_i for $t_i \in E$
// when selecting S_a, sum $\sum_{a:t_i \in S_a} u_i$
// is taken over all the $t_i \in S_a$ before the while loop
do increase u_i uniformly for all $t_i \in E$ until $\exists$ a
set S_a s.t. $\sum_{a:t_i \in S_a} u_i = c'(S_a)$
$E \leftarrow E \setminus S_a$
$C \leftarrow C \cup \{S_a\}$
return C

SetCover(T, S, c, k)
if ($k \leq 0$) return ϕ
sort the sets in increasing order of their cost
for $j \leftarrow 1$ to m
do $c'(S_j) \leftarrow \infty$
for $j \leftarrow 1$ to m
// create a modified instance $I_j = (\mathsf{T}', S^j, c', k_j)$
// run PRIMAL_DUAL on this instance.
// SC_j is the cover obtained in iteration j.
do $c'(S_j) \leftarrow c(S_j)$
// S_j is the highest cost set in OPT
$S^j \leftarrow S \setminus \{S_j\}$ // S_j is removed from the instance
$\mathsf{T}' \leftarrow \mathsf{T} \setminus S_j$ // all elements of S_j are removed
$k_j \leftarrow k - |S_j|$
cost(SC_j) = ∞
if ($|S_1 \cup S_2 \cup \cdots \cup S_j| \geq k$)
then $SC_j \leftarrow \{S_j\} \cup$ PRIMAL_
DUAL($\mathsf{T}', S^j, c', k_j$)
cost(SC_j) = $\sum_{S_x \in SC_j} c(S_x)$
SC = min{cost(SC_1), cost(SC_2), . . ., cost(SC_m) }
return SC