Volume 4, Issue 8, August 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

MCB Problem in Routing Protocols

O. Hogla
M.Tech, CSE, LBRCE,
Mylavaram, India

A. Sri Rama Chandra Murthy
Assistant Professor, CSE, LBRCE,
Mylavaram, India

Dr. S. Sai Satyanarayana Reddy
Professor, CSE, LBRCE,
Mylavaram, India

Abstract: ***We present a class of MCB problems in Wireless Mesh Networks (WMNs) with multi-path wireless routing protocols. We establish the provable superiority of multi-path routing protocols over conventional protocols against blocking, node-isolation and network-partitioning type attacks. In our attack model, an adversary is considered successful if it is able to isolate/capture of a subset of nodes such that no more than a certain amount of traffic from source nodes reaches the gateways. In that Two scenarios, (a) nodes high degree of node mobility, are evaluated. Scenario, and (b) low mobility for network nodes. Scenario (a) is proven to be #P-hard for the adversary (b) is proven to be NP-hard and scenario to realize the goal. Several approximation algorithms are presented which show that in the best case scenario and it is 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 routing protocols against such attacks. The best of our knowledge, it is the first work that evaluates theoretically and the attack-resiliency and performance of multi-path protocols with wire-less network node mobility.***

Keywords: WMN, MCB, OPT,

I. INTRODUCTION

Multi-Path traffic scheduling and routing protocols in wired networks are deemed superior over conventional single path protocols in terms of both enhanced throughput and robustness**.** This could offset the benefits seen in wired networks, research has proven that multi-path routing provides better Quality of Service guarantees. This paper adopts a unique approach to further assay their utility by the investigating the security and robustness are offered by such that protocols. Specifically, we study the feasibility and impact of blocking type attacks are on these protocols. In our study, Wireless Mesh Networks are considered as the underlying representative network model. WMNs have a unique system architecture where they have nodes communicating wirelessly over multiple hops to a backbone network though multiple available network gateways. Primary traffic in the WMNs is between the backbone network and mobile nodes/stationary. These makes WMNs ideal candidates for applying the full cope of any wireless multi-path protocols and study the impact of these attack scenarios.The underlying representative network model considered for this study is WMN, the attack scenarios and results in this paper are fully portable in to other types of wireless data networks in which use multipath routing protocols.While there has been some work on integrating to the benefits to provide by the multi-path routing protocols with in security mechanisms there exists in analyzing multi-path routing attacks. Specifically two areas that need to be analyzed are: (a) The performance in terms of security and resiliency of mobile wireless networks multi-path protocols under different attack scenarios, and (b) Comparison with traditional single-path protocols under such circumstances. This paper attempts to achieve the above two desirable goals. To the best of our knowledge, this is the first paper to theoretically evaluate the performance of wireless network multipath protocols considering node mobility under attack scenarios. The technical contributions of this paper are:

- The identification of the MCB problem. Though we consider MCB in the WMN setting, the problem is applicable to other wireless or wired networks.
- Evaluating the hardness of the problem. MCB is NPhard for the low/no node mobility scenario and #P-hard for networks with patterned node mobility.
- Development of approximation algorithms for the best case scenario and the performance testing of these algorithms in dif erent settings through random graphs based experiments.
- Laying direction for future research to evaluate the performance of multi-path protocols against sophisticated attacks in mobile wireless networks.

II. ASSUMPTIONS AND THREAT MODEL

2.1 ASSUMPTIONS:

The network and the threat model in this paper conform to the following conditions:

1) We consider managed networks where each node has a unique identity. In other words, the mapping between the network nodes and their identities remains one-to-one, a property that can be verified in any managed network. This will preclude node replication attacks.
2) The attacker while having the resources cannot be deploys his own devices to the network.
3) The adversary is a global adversary in the sense of that the adversary wants to severe the network and can choose the way of the network is to be severed.
4) Physical capture of the nodes is allowed; there exists a cost for each compromise of nodes which is assumed to be the computable for the sake of simplicity.
5) An attacker can also compromise nodes; however, he does not control certain elements such as mobility of the nodes modification/addition of the hardware of the captured nodes. This assumption is perfectly legitimate since our model considers that the attacker does not know all the details of the network.
6) Although the attacker may have a fair knowledge of the workings of any system especially in wireless mesh networks, we do not explicitly consider insider attacks. We Insider the attacks are possible in any organization's networks. Consideration of insider attacks and its analysis will be quite involved, since there and hence is outside of the scope of this paper.

2.2 THREAT MODEL:

Blocking, node-isolation and network-will be too many parameters to the consider Partitioning type attacks are easy to launch and there are effective in the wireless networks domain due to the channel constraints and dynamic network topologies. We also try to design best-case scenarios for these attacks to succeed. Both low node-mobility and high node-mobility scenarios are considered. For comparison purposes, we also launch similar attacks on conventional single-path protocols and measure their impact. As we consider multipath routing protocols, the attacker has to consider the operation of multi-path routing since multiple paths will exist from the source to the destination. this attack cost due to the nodes' close proximity to base stations. In a black hole attack, a particular node in a network falsely advertises a route based on metrics specific to the protocol to the destination node so as to force the route discovery algorithm to choose a route through in it. The actual black hole attack occurs when the malicious node drops packets and hence blocks paths to the destination. Similarly, in a wormhole attack, an attacker records at packets at one location in the network, tunnels them to another location, and retransmits them into the network. However, it has to be also noted that multi-path routing is not necessarily affected by wormhole attacks. we do not consider black hole and wormhole attacks explicitly in this paper. Further, Sybil attack where a node can be assigned multiple identities is precluded from our threat model since the focus of this paper is primarily the blocking attack.

III. EXISTING METHOD

Multi-path routing protocols unlike standard routing protocols intend to discover multiple paths between a source and in to a destination node. Specifically, the multiple paths provide load balancing, fault tolerance and higher aggregate bandwidth. It has been proven that using multipath routing in dense networks enhances performance and result in better throughput than uni path routing traditionally, multi-path routing has been in the context of WMNs.

But the recently, there has been progress to adapting these protocols in to other types of networks such as WSNs .The two main components of multi-path routing protocols are is overing the routes and then maintaining these routes based on the certain metrics. However, it is the important to note that unlike uni path routing and, multi-path routing metrics are aggregate in the nature. Further, because of the nature of networks, non-disjoint routes are more abundant. Additionally, node-disjointness is a stricter requirement than even link-disjointness making them least abundant and thus, hardest to be find. Due to these practical considerations, is in most multipaths routing, more than not non-disjoint routes are to be selected.

While such a problem does arise with even the Unipart routing, because of the aggregate nature of the ethics in the multi-path routing, it is more than severe with in multi-path routing. Such routes would then cause more harm than benefit as they would have to wait for the transmission medium to be free and thus be unable to perform concurrent transmissions.

This presents a unique opportunity to an attacker who can use such Nodes to partition a network. Even though most routing protocols try to choose paths that are as transmission independent as possible to ensure the least interference between routes, it is not always possible to do so due to network topologies and mobility. This has led to a focus on security in multipath routing protocols. Some of these attacks can be prevented or countered through cryptographic techniques to guard against false packet injection. In the wireless network domain, such cryptographic schemes for secure broadcast and false data injection prevention are described .This work presents a that integrates metrics of a multi-path routing with security, based on the which system administration can incorporate one or more metrics of multi-path routing protocols.

IV. PROPOSED METHOD

The general problem of blocking possible traffic flow between a pair of the vertices in a connected graph is known as the max-flow min-cut problem. In this section, we first consider to a particular case of blocking between a pair of nodes in wireless networks. The adversary can now stage an attack by blocking some nodes in the network such that all traffic between a certain pair of nodes will pass through at least one of the compromised nodes. Though this is conceivable, we

show that it is NP-hard to find the minimum cost set of nodes so that all traffic between the source destination pair will pass through the one of the compromised nodes. The minimum cut has the following property: it will separate node t from nodes s1 and s2, at the same time, keep nodes s1 and s2 connected. In this case, the cut will cause all traffic flow from s1 to t to pass through C. The formal problem definition is as follows:Definition 4.1: (3-node Induced Flow MCB).

Suppose we have an undirected graph G = (V,E), where |V | = n, and every node vi ∈ V , 1 ≤ i ≤ n, has an associated positive integer cost ci.3 Given three nodes s1, s2, t, and an integer b can we find a set of nodes in V , such that the total cost of nodes in V is no more than b, and removal of all nodes in this set will separate t from s2 and s1, at the same time.

definition 4.2: The 3-node Induced Flow MCB is np complete even if every node has a unit cost. All the nodes represented in thick dots in the figure are cliques. In the first layer, every thick node is a clique of size (m+ r). In the second layer, every thick node is a clique of size (m + r) 2 and any neighboring node of the thick node is connected to every node in the clique. The two layers are connected as follows: the two variable nodes corresponding to a variable and its negation in another layer are connected, and for every clause is connect the first variable in the first layer to the second variable in the second layer through an intermediate node.

We have the following observations:

1) Since s1 and s2 must be connected, for every variable node pair in the first layer, a variable and its negation cannot be chosen in the cut simultaneously.
2) Since s1 and s2 must be separated from t, one of the two appearances (in the two layers) of every variable must be chosen in the cut.
3) Since the variable node in the second layer has clique size (m + r)2, then for every variable and its negation in the second layer, only one of them can be chosen in the cut.we can conclude that the for every variable has, one must choose it or its the negation but not both in both layers. So, the cost of the chosen variable nodes will be m(m+r)2 +m(m+r). If the original has an assignment that can satisfy k clauses, then we can choose the intermediate node of the unsatisfied clause edges, and the variables in the truth assignment in both layers. if a cut of no more than m(m+r)2 +m(m+r)+r−k can be found it ,then an assignment can be found according to the cut to satisfy at least k clauses.

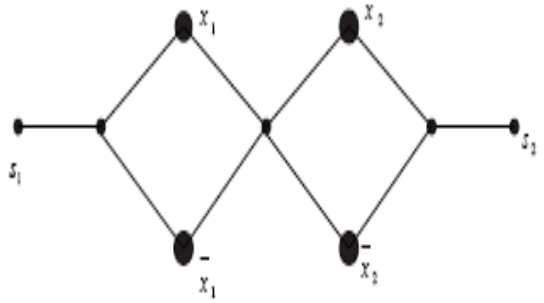

Fig. 1. The first layer of the constructed instance

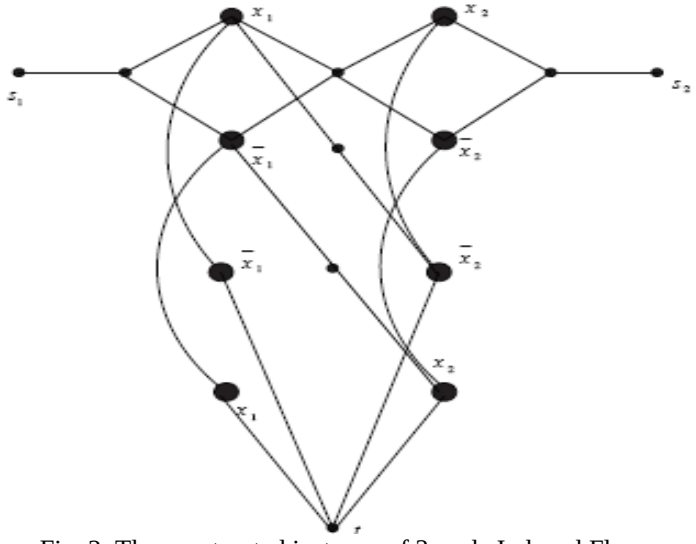

Fig. 2. The constructed instance of 3-node Induced Flow

Similarly, we can define a multi-node induced Flow MCB, in which we have u + v nodes A1. . . Au,B1, . . . , Bv in the graph, and we wouldLike to find the minimum cut that can separate A1, . . . , Au from B1, . . . , Bv, and at the same time, keep A1, . . . , Au connected and B1, . . . , Bv also connected.

Proof: We can use a similar reduction as in the proof of the NP-hardness of 3-node Induced Flow MCB. Given an instance of MAX2SAT with m variables, we construct an instance of multi-node Induced Flow MCB, which is similar to the instance constructed in the proof of the NP-hardness of 3-node Induced Flow MCB. In the constructed instance of multi-node Induced Flow MCB, we have nodes A1, . . . , Au, and B1, . . . , Bv, where we need to find a cut to separate A1, . . . , Au from B1, . . . , Bv, at the same time, keep all nodes in A1, . . . , Au connected and all nodes in B1, . . . , Bv connected. In the constructed graph, we also have two layers, but every layer is similar to the first layer in our construction in the proof of NP hardness of the 3-node Induced Flow MCBWe set the bound b to be 2m + r − k. Figure 3 is the graph constructed for the instance (x1 ∨ x2) ∧ (x1 ∨ x2). It is easy to see, since we need to keep A1, . . . , Au connected and B1, . . . , Bv connected, that for every variable, one must choose to block the variable or its negation in both layers. So we can see that the instance denoted as I has an assignment which satisfies at least k clauses if and only if the constructed multi-node Induced Flow MCB instance denoted as I1 has a blocking cost at most b. Suppose the optimal solution of the MAX2SAT instance is OPT. Then the optimal solution of the corresponding multi-node Induced Flow MCB is (MCB). The cost of the solution found for the constructed multi-node Induced Flow MCB instance is c(I1). The cost of the corresponding solution of the original instance is c(I) and we have OPT ≥ 3r/4. We can also assume that every variable should appear in at least one of the clauses,

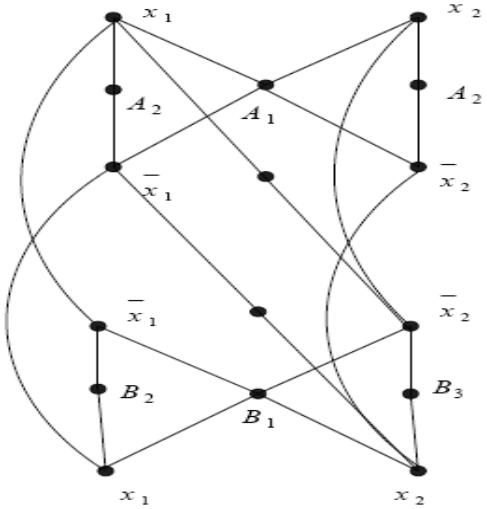

Fig. 3. The constructed instance of multi-node Induced Flow MCB then we has r ≥ m/2.

Now we have OPT (MCB) ≤ 2m +r\4 ≤17/3 OPT (2SAT) c(I1) − OPT(MCB) ≤ OPT(2SAT) − c(I) This means the reduction is an L-reduction, and consequently, multi-node Induced Flow MCB is np-hard.We also present an approximation algorithm for the3-node Induced Flow MCB. The idea is to use linear programming (LP) formulation.Here *qu* is a label we assign for every node *u*. Equation in this are three steps

(1) Guarantees that every node has a balanced flow, and the total flow from *s*1 to *s*2 is 1. Inequalities guarantee that in every path from *s*1 (or *s*2) to *t*, the summation of all labels *qu* along this path will be at least1. Inequalities mean that if a node is labeled, then no flow should pass through it if *L*1 has integer solution, this can be guaranteed.

(2) Find a path from *s*1 to *s*2, which satisfies the following condition: for every node *u* in the path, there is a flow of size at least 1*/*(*n*−3) passing through *u*. This can be done because in the above LP, we find a fractional flow of size 1 from *s*1 to *s*2.

(3) Change the cost of all nodes in the identified path in Step 2 to infinity, and add a new node *s*, which is connected only to *s*1 and *s*2. Then, find a minimum cut from *s* to *t*, and take this cut as the solution of the problem.

V. APPROXIMATION ALGORITHMS FOR MULTIPATH MCB, NO MOBILITY

In this we present two algorithms for the MCB problem with stationary nodes. The first one is a greedy algorithm and the second one LP-based. We derive the approximation ratio for both of them.

Definition 5.1: 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 Ri paths belonging to a node i are covered, we say that node i is covered.

5.1 Notations

T: The set of nodes that have been chosen at the beginning of iteration

Ei: 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.

Wij: Number of paths that belong to node j and are covered by node i.

Yj : Number of already covered paths that belong to node j.αi: Cost-effective index of node i.

D: Set of nodes currently covered

Oi: Number of paths belonging to node i covered by the set of nodes returned by the function call Set Cover

5.2 The Greedy Algorithm and Approximation Ratio

Our first algorithm, a greedy one, selects the most cost effective node iteratively and at the same time removes the covered paths and the paths unusable in the future. Unusable paths are those originating from a node i with at least Ri paths already blocked, as covering these paths would be inconsequential. The algorithm runs until the nodes in T have covered the required paths for all the nodes in V , i.e., T covers at least Ri paths for node i, where i = 1, . . . , k. This condition is termed as "Done."

Algorithm 5.2:

1. T ← φ, and mark all paths and nodes as uncovered;
2. While not done, iterate the following sub-steps:
   2.1. For every remaining node in V \T, say, node i, in the current iteration, compute its effective number Ei as follows:
   Ei ← 0
   2.1.1. For every node j that is not covered yet, compute min(max((Rj − Yj), 0),Wij).
   Update Ei as follows:
   Ei = Ei + min(max((Rj − Yj), 0),Wij)
   2.2. Compute the cost-effective index αi as follows:
   αi =ci/Ei
   2.3. Choose node u with the lowest cost effective index (αu); Mark every path node u covers as Covered; For every effective path p that node u covers, set the price of the effective path, i.e., price (p) = αu; Iterate through all the currently uncovered nodes; Mark those nodes that have been covered by node u in this iteration as covered; Add node u to T, i.e.,
   T ← T ∪ u
3. Output T;

Note that in Step 2.1.1 of Algorithm 5.2, Wij is the number of paths that belong to node j and are covered by node i, Yj is the number of already covered paths that belong to node j.

Theorem 5.3: Algorithm 5.2 Achieves an Approximation Ratio Of in R

Proof: The proof is similar to the proof for the ratio of the greedy algorithm for set cover problem in suppose the optimum solution has a cost OPT. We number the covered effective paths in the algorithm in the order in which they are covered, and name them as P1, . . . , PR. In

the iteration that covers path Pj , there are at least R−j+1 paths not yet covered. Because we choose the node with lowest cost-effective index, we have price (Pj) ≤ OPT R−j+1.

The total cost of our algorithm will be R _

j=1

price(Pj) ≤ (1 +12+ . . . +1R) × OPT≤ OPT × lnR If we adopt the algorithm Set Cover for partial set cover in [51], which is based on LP relaxation, then we get a new algorithm which is described next.

5.3 The LP Algorithm and Approximation Ratio

The LP Algorithm uses a function Set Cover (P, V \T, c,Rj), where P is the set of all uncovered paths belonging to node j, c is the array of cost values for nodes in V \T (i.e., cj , ∀j ∈ V \T). The function Set Cover returns the selected sets (nodes) that cover at least Rj paths in P.

Algorithm 6.4:

1. T ← φ, D ← φ
2. While D does not contain all nodes in the graph, iterate the following sub-steps:
   2.1. Choose node j with the highest Rj value; Call Set Cover(P, V \T, c,Rj);
   2.2. D ← D ∪ j
   2.3. For every node returned by the function, T ← T ∪ i
   2.4. Remove from P, every path that is covered by the nodes returned by the function call SetCover;P ← P\p
   2.5. For every i ∈ V \D, adjust Ri as follows:

Ri =max(0,Ri − Oi) ; If Ri becomes 0 (it means that node i is blocked); D ← D ∪ i

3. Output T.

Algorithm 5.4 repeatedly blocks a node in every iteration , until all nodes are blocked. Note that

in Step 2.5 of Algorithm5.4, Oi is the number of paths belonging to node i that were covered by the set of nodes returned by Set Cover.

Theorem 5.5: Algorithm 5.4 achieves an approximation ratio of h × k, where h is the length (number of nodes in the path) of the longest path.

Proof: The approximation ratio of algorithm Set-Cover is h. obviously at every iteration the sum of the cost of selected nodes < h×OPT, so the total cost of the solution returned by algorithm 5.4

VI. MULTI-PATH MCB PROBLEM

Now present the Multi-path MCB problem for the low-mobility scenario. The network is modeled as an undirected graph *G*, with vertex set 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-world 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

.

6.1 Multi-path MCB Optimization Problem

Suppose that in the graph $G(V,E)$, $|V| = k$. Every node *vi* in *V* is associated with a cost *ci* which is the cost of compromising the node. There are i=k, i=1ni paths *P*11. . . P1n1, . . . , Pk1, . . . , Pknk . Here, Pi1, . . . , Pini(i = 1, . . . , k), are paths originating from node. That is, for every node *i* (i = 1, . . . , k), what is the minimum cost to compromise at least Ri($0 \leq$ Ri $\leq$ ni) paths out of all paths belonging to this node (i.e., paths Pi1, . . . , Pini). This is a typical optimization problem. The corresponding decision problem is described below.

6.2 Multi-path MCB Decision Problem

Given: Graph $G(V,E)$, where every node *vi* in *V* has a cost *ci* of compromise, the set of nodes in paths *P*11, . . . , *P*1*n*1, . . . , *Pk*1, . . . , *Pknk* and integers *C* and *Ri*($0 \leq Ri \leq ni$).

Statement: Is there a subset *V* _ of *V* such that compromising *V* _ will block at least *Ri* paths out of *Pi*1, . . . , *Pini* , for every node *vi* (*i* = 1, . . . , *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. 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 6.1: The MCB decision problem is NPcomplete.

Proof: The problem is a general case of the partial set cover problem [20], which is a well known NP-complete problem. So multi-path MCB is NP-complete.

VII. CONCLUSIONS

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 attempt to model the theoretical hardness of attacks on multi-path routing protocols for mobile nodes and quantify it in arithmetical terms. At this point, it is also worthwhile to mention about the impact of this study. We believe that the results of our research will impact a number of areas including the security and robustness of routing protocols in mesh networks, threshold cryptography and network coding.As a part of our ongoing research, we plan to further investigate the approximation algorithms for the MCB problem. It would be an interesting problem to study the additional difficulty associated with blocking when the topological information is effectively hidden from the adversary. Further, we would also like to evaluate our algorithms by running them on a real wireless mesh network and validate the results obtained by the C++ based experiments on random graphs. This paper also brings forth some interesting related problems. For example, if link-cut and node compromising are combined together then what is the minimum total cost to block traffic from specific nodes.

REFERENCES

[1] C.-K. Chau, R. Gibbens, R. Hancock, and D. Towsley, "Robust multipath routing in large wireless networks," in INFOCOM, 2011 Proceedings IEEE, April 2011, pp. 271 –275.

[2] Y. Kato and F. Ono, "Node centrality on disjoint multipath routing," in Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd, May 2011, pp. 1 –5.

[3] M. Razzaque and C. Hong, "Analysis of energy-tax for multipath routing in wireless sensor networks," Annals of Telecommunications, vol. 65, pp. 117–127, 2010.

[4] J. So and N. H. Vaidya, "Load balancing routing in multi-channel hybrid wireless networks with single network interface," in Second International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QSHINE'05), Washington, DC, USA, August 2005.

[5] F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Computer Networks Journal*, vol. 47, pp. 445–487, 2005.

