ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Enhanced Multipath Routing for Wireless Network

P. Vinod Kumar
PG Scholar,
Computer Science & Engineering,
Aditya Institute of Technology and Management, AP, India

K. Prasada Rao
Sr. Asst. Professor,
Computer Science & Engineering,
Aditya Institute of Technology and Management, AP, India

Abstract

We present a class of Minimum Cost Blocking (MCB) problems in Wireless Mesh Networks (WMNs) with multi-path wireless routing proto cols. We establish the provable superiority of multi-path routing protocols over conventional protocols against blocking, node-isolation and network-partitioning type attacks. In our att ack model, an adversary is considered succ essful if he is able to capture/isolate a subset of nodes such that no more than a certain amount of traffic from source nodes reaches the gateways. 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 realize 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 bloc king-type attacks. These results are verified through simulations which demonstrate the robustness of multi-path routing protocols against such attacks. To the best of our knowledge, this is the first work that theoretically evaluates the attack-resiliency and performance of multi-path protocols with network node mobility.

Index Terms - Attacks, Blocking, Multi-path routing, Max SNP problems (MAXSNP), Wireless networks.

1. INTRODUCTION

Multi-Path traffic programming and routing protocols in wired networks area unit deemed superior over standard single path protocols in terms of each incre ased out turn and strength. This might offset the advantages seen in wired networks, analysis has proved that multi-path routing provides higher Quality of Service guarantees. This paper adopts a novel approach to additional assay their utility by the work the protection and strength area unit offered by such protocols. Specifically, we tend tostudy the feasibleness and impact of obstruction kind attacks area unit on these protocols. In our study, Wireless Mesh Networks area unit thought-about because the underlying representative network model. WMNshave anovel system design wherever theyneed nodes communicationwirelessly over multiple hops to a back bone work to multiple offered network gateways. Primary traffic within the WMNs is between the backbone network and mobile nodes/stationary. These makes WMNs ideal candidates for applying the complete cope of any wireless multi-path protocols and study the impact of those attack eventualities. The underlying representative network model thought-about for this study is WMN, the attack eventualities and ends up in this paper area unit absolutely moveable in to alternative kinds of wireless know ledge networks during which use multipath routing protocols. Whereas there has been some work on integration to the advantages to supply 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 network smulti-path proto cols beneath totally different attack eventualities.

(b)Comparisonwith ancient single-way protocols beneath such circumstances.

The technical contributions of this paper are:

•The identification of the MCB drawback. We tend to take into account MCB within the WMN setting, the matter is applicable to alternative wireless or wired networks.

• Evaluating the hardness of the matter. MCB is NP-hard for the low/no node quality situation and NP -hard for networks with laced node quality.

• Development of approximation algorithms for the simplest case situation and therefore the performance testing of those algorithms in numerous settings through random graphs based mostly experiments.

• Laying direction for future analysis to gauge the performance of multi-path protocols against subtle attacks in mobile wireless networks.

2. EXISTING SYSTEM

In our Existing System, the two main elements of multi-path routing square measure discovering routes and so maintaining these routes supported sure metrics. This means that such routes ought to be disjoint (not have any common nodes or links) to extend fault tolerance, since the failure of one node/link will cripple the whole network and be prejudices to the multi-path routing philosophy. However, the price for locating such routes is pricey in terms of each time and resources. Further, due to the character of networks, non-disjoint routes square measure additional easy. In addition, node-disjointness could be a stricter demand than even link-disjointness, creating them least easy and so, hardest to seek out. Owing to these sensible concerns, in most multipaths routing, additional typically than not non-disjoint routes square measure designated. Whereas such a haul will arise with even unipath routing due to the mixture nature of metrics in Multi-path routing, it's additional severe in multi-path routing. Another attention-grabbing purpose of multi-path routing is that whereas it would guarantee failure independence, nodes happiness to completely different methods would possibly still be within the transmission vary of every alternative inflicting interference with one another.

DISADVANTAGES:

Blocking, node-isolation and network-partitioning sort attacks square measure straightforward to launch and square measure effective within the wireless networks domain owing to channel constraints and dynamic network topologies.

3. PROPOSED SYSTEM

In our proposed system, we have a tendency to take into account managed networks wherever every node encompasses a distinctive identity. In alternative words, the mapping between network nodes and their identities remains matched, a property that may be verified in any managed network. This may preclude node replication attacks. The assailant whereas having the resources cannot deploy his own devices (nodes) to the network.

The individual could be an international individual within the sense that the individual desires to severe the network and might opt for the manner the network is to be cut off. Physical capture of nodes is allowed; there exists a value for every capture/comp romise of nodes that is assumed to be estimable for the sake of simplicity. Associate degree assailant also can compromise nodes, however, he doesn't management sure components like quality of the nodes or modification/addition of the hardware of the captured nodes. This assumption is utterly legitimate since our model considers that the assailant doesn't grasp all the main points of the network and it'll exponentially increase the price of gathering these details.

ADVANTAGES:

Our projected system demonstrates the prevalence of multi-path protocols over ancient single-path protocols in terms of resiliency against interference and node isolation-type attacks, particularly within the wireless networks domain. Multi-path protocols for WMNs create it very laborious for associate degree individual to expeditiously launch such attacks.

4. THREAT MODEL

Blocking, node-isolation and network-partitioning sort attacks square measure straightforward to launch and square measure effective within the wireless networks domain owing to channel constraints and dynamic network topologies. We have a tendency to emulate adversarial behavior by assaultive the multi-path schemes through intelligent interference and node-isolation sort attacks and study the impact. We have a tendency to additionally try and style best-case situations for these attacks to succeed. Each low node-mobility and high node-mobility situations square measure thought-about. For comparison functions, we have a tendency to additionally launch similar attacks on standard single-path protocols and live their impact. The minimum value interference (MCB) downside are often explicit as a special case of node interference in a very network at minimum value to the assailant. Here the assailant desires to partition the network, so ceasing flow of information, by either capturing or interference a key node or by routing all knowledge through a selected node. As we have a tendency to take into account multipath routing protocols, the assailant must take into account the operation of multi-path routing since multiple methods can exist from the supply to the destination. whereas a nontrivial however straightforward answer is to launch a blackhole or hole attack, this may force the assailant to deploy his own nodes or capture a node near the destination/source which might increase his attack value owing to the nodes' shut proximity to base stations. In a very blackhole attack, a selected node in a very network incorrectly advertises a route (based on metrics specific to the protocol) to the destination node thus on force the route discovery formula to decide on a route through it. The particular blackhole attack happens once the malicious node drops packets and therefore blocks methods to the destination. Similarly, in a very hole attack, associate degree assailant records packets (or bits) at one location within the network, tunnels them (Possibly selectively) to a different location, and retransmits them into the network. However, it's to be additionally noted that multi-path routing isn't essentially suffering from whole attacks.

5. MULTI-NODE MCB CASE IN WIRELESS NETWORKS

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 for every variable has, one must choose it or it's 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

assignment can be found according to the cut to satisfy at least k clauses.

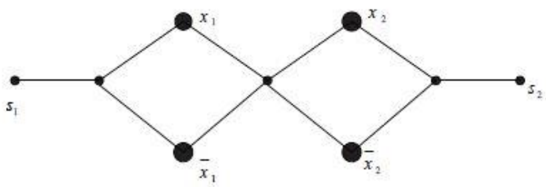

Fig1: The first layer of the constructed instance

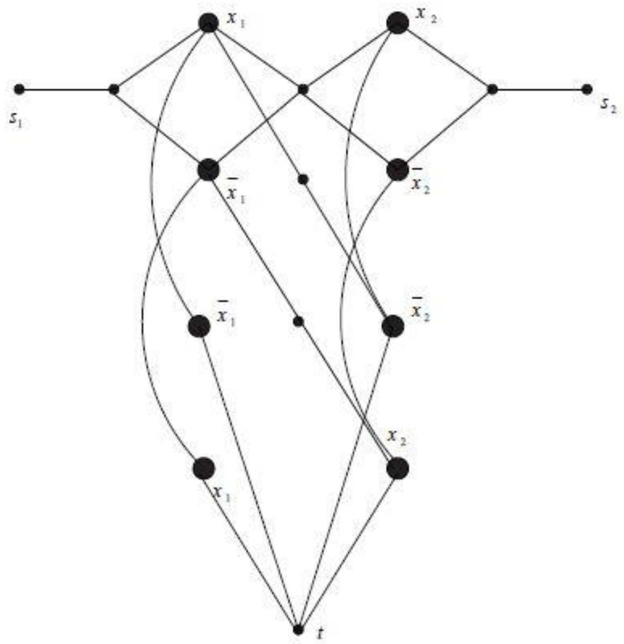

Fig1: The constructed instance of 3-node Induced Flow MCB

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 would Like 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, 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 s1 to s2 is 1. Inequalities guarantee that in every path from s1 (or s2) 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 L1 has integer solution, this can be guaranteed.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

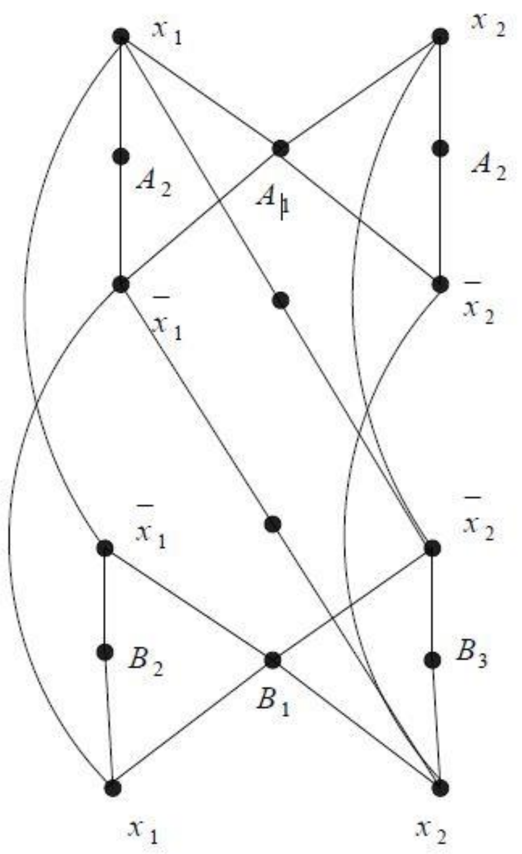

Fig3: The constructed instance of multi-node Induced Flow MCB

(2) Find a path from s1 to s2, 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 s1 to s2.

(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 s1 and s2. Then, find a minimum cut from s to t, and take this cut as the solution of the problem.

6. MULTI-PATH MCB PROBLEM:

Most of the routing protocols that are planned for mesh and circumstantial networks are unipath, which suggests solely one route is employed between a supply and a destination node. The most goal of multipath routing is to permit the utilization of many smart methods to succeed in destinations, not simply the simplest path. This could be achieved while not imposing excessive management overhead in maintaining such methods. The supply of multiple methods between a supply and a destination will be accustomed deliver the goods the subsequent benefits:

- Fault tolerance: introducing redundancy in the Network (Amir, Danilova, Kaplan, MusaloiuElefteri, & Rivera 2008) or providing backup routes to be used when there is a failure (Lee &Gerla 2000), are forms of introducing fault tolerance at the routing level in mesh networks.
- Throughput enhancement: in a very mesh network, some links will have restricted information measure. Routing on one path might not give enough information measure for an association.
- Error resilience: multipath protocols will be accustomed give error resilience by distributing track (for instance, victimization information and error correction codes) over multiple methods.
- Security: with single-path routing protocols, it's simple for AN mortal to launch routing attacks, however multipath offers attack resilience

We now present the Multi-path MCB drawback for the stationary-nodes/low-mobility state of affairs. The network is sculptural as AN afloat graph G, with vertex set V and edge set E. Here, each vertex represents a node within the network and a link between 2 vertices implies that corresponding nodes inside every other's radio vary. A directed graph could higher represent the network for real-world things since nodes could have totally different radio ranges, signal strength could also be totally different in every direction, and links might not be utterly duplex. But for simplifying the matter description we tend to assume AN afloat graph, accentuation that each one our results are equally applicable to the final case of directed graphs.

Multi-path MCB Optimization Problem

Suppose that in the graph G (V, E), |V | = k.Every node viin V is associated with a cost ci which is the cost of compromising the node. There are m =ki=1nipaths P11, . . . , P1n1, . . . , Pk1, . . . , Pknk. Here, Pi1, . . . ,Pini(i = 1, . . . , k), are paths originating from node i (or equivalently, paths belonging to node i). What is the minimum cost to compromise a subset of nodes such that a certain percentage of paths belonging to a node are compromised? That is, for every node i (i = 1 . . . k), what is the minimum cost to compromise at least Ri(0≤Ri≤ni) paths out of all paths belonging to this node (i.e., paths Pi1, . . . , Pini). This is a typical optimization problem.

6. CONCLUSION:

This paper demonstrates the prevalence of multipath protocols over ancient single-path protocols in terms of resiliency against obstruction and node isolation-type attacks, particularly within the wireless networks domain. Multi-path protocols for WMNs create it extraordinarily exhausting to expeditiously launch such attacks. This paper is an effort to model the theoretical hardness of attacks on multi-path routing protocols for mobile nodes and quantify it in mathematical terms. At now, it's conjointly worthy to say concerning the impact of this study. We tend to believe that the results of our analysis can impact variety of areas together with the safety and hardiness of routing protocols in mesh networks, threshold cryptography and network secret writing. Moreover, even supposing we tend to don't essentially take into account corporate executive attacks, we'd prefer to entails that our Analysis will allow an assaulter to possess topological info of the network that is that the case of a corporate executive attack. Even during this case, our analysis shows that staging an obstruction attack is difficult for the assaulter, in a very network of affordable size. This paper conjointly brings forth some fascinating connected issues. For instance, if link-cut and node compromising are combined along (i.e., one will either cut some links or compromise some nodes), then what's the minimum total price to dam traffic from specific nodes.

REFERENCES

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

[2]http://wire.less.dk/wiki/index.php/meshlinks

[3]http://www.communitywireless.org/.

[4] http://www.open-mesh.com/.

[5]http://pdos.csail.mit.edu/roofnet/design/.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] C. Fragouli, J.-Y. Le Boudec, and J. Widmer, “Network coding: an instant primer,” SIGCOMM Comput. Commun. Rev., vol. 36, no. 1, pp. 63–68, Jan. 2006.