A Novel Solution for Minimum Cost Blocking Problem in Multi-path Wireless Mesh Network

M.Beema mehraj[1] **Sabari vasan.J** [2]

[1]Assistant Professor, Department of CSE, Bharath University, Chennai, beemamehraj@gmail.com.

[2]Dept. of CSE, Bharath University, Chennai, gjsvasan@gmail.com

ABSTRACT- ***This paper addresses the problem of multipath routing in wireless mesh networks. Here 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. (b) Low mobility for network nodes.***

Scenario (a) is proven to be NP-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 wireless network node mobility.

Keywords - :Attacks, Blocking, Multi-path routing, Max SNP problems (MAXSNP), Wireless networks,WMN, MCB, OPT.

1. 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 make WMNs ideal candidates for applying the full scope 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 NP-hard for the low/no node mobility scenario and NP-hard for networks with patterned node mobility

• Development of approximation algorithms for the best case scenario and the performance testing of these algorithms in different 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. BACKGROUND WORK

The initial goal of this work was to study and analyze techniques to support multi-path routing in wireless mesh networks. From the works surveyed, AODV-DM emerged as a protocol able to find non interfering routes with a reasonable signaling cost. Unfortunately, the latency in the discovery of the second route seemed very large. Our first idea was to modify the protocol in an attempt to speed up the route discovery process. Eventually, this effort leads to the design of a cluster-based algorithm for route discovery and maintenance. Existing System: 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. In wireless networks, even though the dynamic nature of networks and resource constraints entail additional overhead in maintaining and reconfiguring multiple routes, which could offset the benefits seen in wired networks, research has proven that multi-path routing provides better Quality of Service (QoS) guarantees. Disadvantages: Blocking, node-isolation and network-partitioning type attacks are easy to launch and are effective in the wireless networks domain due to channel constraints and dynamic network topologies Proposed System: • The identification of the Minimum Cost Blocking (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 NP-hard for the low/no node mobility scenario and NP-hard for networks with patterned node mobility. The reduction for no-mobility is derived from the basic Set Cover problem and for mobility scenario, from the 3SAT and #SAT problems. • Development of approximation algorithms for the best case scenario and the performance testing of these algorithms in different 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. Advantages: Our proposed system 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. Multi-path routing protocols unlike standard routing protocols intend to discover multiple paths between a source and a destination node. Their utility lies in compensating for the dynamic and unpredictable nature of networks. Specifically, the multiple paths provide load balancing, fault tolerance and higher aggregate bandwidth. It has been proven that using multi-path routing in dense networks enhances performance and result in better throughput than unipath routing. Traditionally, multi-path routing has been in the context of WMNs. But recently, there has been progress in adapting these protocols to other types of networks such as WSNs (Wireless Sensor Networks).The two main components of multi-path routing are discovering routes and then maintaining these routes based on certain metrics. Examples of such metrics include Estimated Transmission Count (ETX), Expected Transmission Time (ETT), etc.

III. ASSUMPTIONS AND THREAT MODEL

3.1 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.

3.2 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

IV. A MULTI-NODE MCB CASE IN WIRELESSNETWORKS

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 , $1 \leq i \leq n$, 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

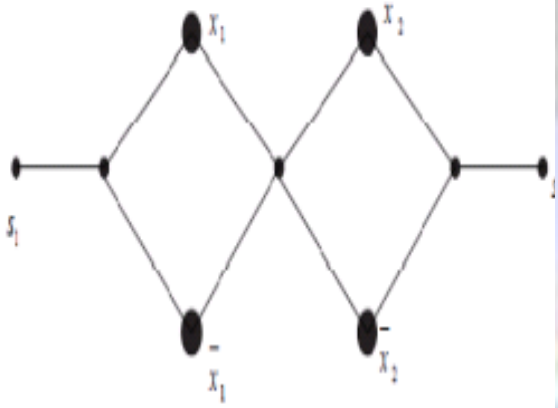

Fig. 1. The first layer of the constructed instanc

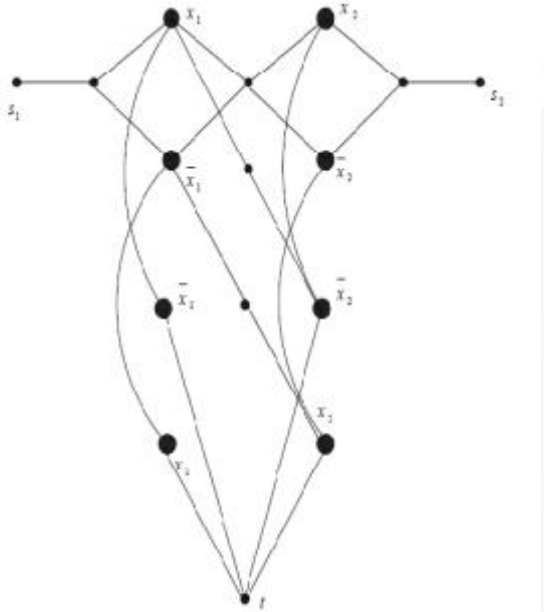

Fig. 2. The constructed instance of 3-node Induced Flow

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 NPhardness 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.

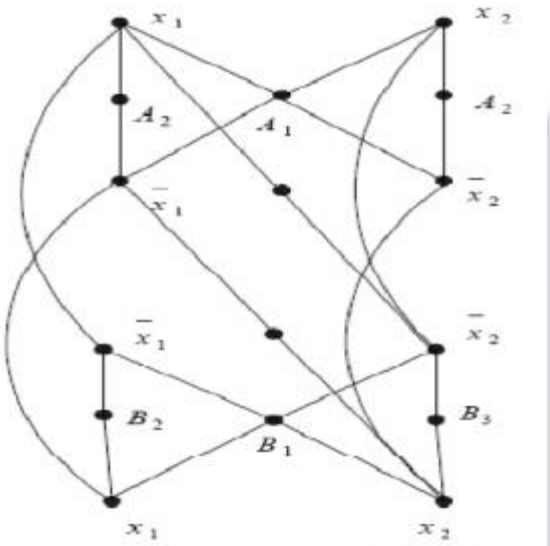

Fig. 3. The constructed instance of multi-node

Most of the routing protocols that have been proposed for mesh and ad hoc networks are unipath, which means only a single route is used between a source and a destination node. The main goal of multipath routing is to allow the use of several good paths to reach destinations, not just the best path. This should be achieved without imposing excessive control over head in maintaining such paths. The availability of multiple paths between a source and adestination can be used to achieve the following 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 mesh network,• some links can have limited bandwidth. Routing along a single path may not provide enough

bandwidth for a connection. Error resilience: multipath protocols can be• used to provide error resilience by distributing track (for instance, using data and error correction codes) over multiple paths. Security: with single-path routing protocols, it• is easy for an adversary to launch routing attacks, but multipath offers attack resilience We now present the Multi-path MCB problem for the stationary-nodes/low-mobility scenario. 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-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. 5.1 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 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 them in imum 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($0 \leq Ri \leq ni$) paths out of all paths belonging to thisnode (i.e., paths Pi1, . . . , Pini). This is a typical optimizationproblem. VI

V. 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 mathematical 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. Moreover, even though we do not necessarily consider insider attacks, we would like to point out that our analysis does allow for an attacker to possess topological information of the network, which is the case of an insider attack. Even in

this case, our analysis shows that staging a blocking attack is hard for the attacker, in a network of reasonable size. This paper also brings forth 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.

VI. 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. [6] C.-K. Chau, R. Gibbens, R. Hancock, and D. Towsley, " Robustmultipath routing in large wireless networks, " in INFOCOM, 2011Proceedings 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 IEEE73rd, May 2011, pp. 1

[8] M. Razzaque and C. Hong, " Analysis of energy-tax for multipath routing in wireless sensor networks," Annals of Telecommun-ications, 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, August2005. [10] C. Fragouli, J.-Y. Le Boudec, and J. Widmer, "Network coding: aninstant primer, "SIGCOMM Comput. Commun. Rev., vol. 36, no. 1,pp. 63–68, Jan. 2006. [11] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Networkinformation flow,"IEEE Trans. on Information Theory, vol. 46, pp.1204 – 1216, 2000. [12] S.-Y. R. Li, R. W. Yeung, and N. Cai, " Linear network coding, "IEEE Transactions on Information Theory, vol. 49, pp. 371–381, 2003.