International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 9 Issue 3 –SEPTEMBER 2014.

MULTI PATH BLOCKING

SHAIK RESHMA [*1], and M.VENKATESH NAIK [#2]

[*]*Student M.Tech (CSE), CRIT- ANANTAPURAMU, Affiliated to JNTU University*

[#]*Assistant Professor (CSE), CRIT- ANANTAPURAMU, Affiliated to JNTU University*

[1]reshma047@gmail.com

[2]venkateshnaikm0@gmail.com

Abstract—Consider a point-to-point communication network on which a number of information sources are to be mulitcast to certain sets of destinations. We assume that the information sources are mutually independent. In this paper, 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 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.

The proposed work is implemented using two algorithms: greedy based and LP based. This algorithm can be successfully introduced to the domains that involve multi path routing.

Keywords: Multi-path routing, Max SNP problems (MAXSNP), Wireless networks, black hole attack.

I. INTRODUCTION

WMNs have a unique system architecture where they have nodes communicating wirelessly over multiple hops to a backbone network through multiple available network gateways. Primary traffic in WMNs is between the backbone network and stationary/mobile nodes. Quality of Service (QoS) based routing is defined in RFC 2386 as a "Routing mechanism under which paths for flows are determined based on some knowledge of resource availability in the network as well as the QoS requirement of flows." several routing protocols have been developed for

wireless Ad-hoc networks or sensor networks.

The existing reactive routing algorithms such as Ad-hoc on-demand distance vector (AODV) protocol and dynamic source routing protocol (DSR) maintain routing information for a small subset of possible destinations, namely those currently in use. Hierarchical routing protocols, such as low-energy adaptive clustering hierarchy (LEACH) , hybrid energy-efficient distributed clustering (HEED) , etc., are suitable for large-scale networks to monitor outdoor environments with periodical data transmissions. As because of the dynamic nature of the Wireless networks 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. WMNs have a unique system architecture where they have nodes communicating wirelessly over multiple hops to a backbone network through multiple available network gateways. multi-path routing schemes since efficient multi-path traffic scheduling schemes can split a node's traffic into multiple flows along several accessible gateways and eventually reassemble this traffic at the backbone network at low costs.

The underlying representative network model considered for this study in this paper is WMN, the attack scenarios and results in this paper are fully portable to other types of wireless data networks as well which use multipath routing protocols.

II. EXISTING SYSTEM

In existing computer networks, each node functions as a switch in the sense that it either relays information from an input link to an output link, or it replicates information received from an input link and sends it to a certain set of output links. A node can function as an encoder in the sense that it receives information from all the input links, encodes, and sends information to all the output links. From this point of view, a switch is a special case of an encoder. In the sequel, we will refer to coding at a node in a network as network coding.

The utility of multi-path routing protocols lies in compensating for the dynamic and unpredictable nature of networks. Specifically, the multiple paths provide load balancing, fault tolerance and higher aggregate bandwidth. 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). However, multi-path routing metrics are aggregate in

nature, i.e., paths at each hop are chosen to maximize/minimize the sum of the individual paths at each hop and not choose the best path each hop.

Since the failure of a single node/link can cripple the entire network, node-disjointness is a stricter requirement than even link-disjointness.

The existing routing protocols Traffic load and lifetime Deviation based Power-aware Routing protocol (TDPR), Cost-effective Lifetime Prediction based Routing (CLPR), Energy aware Node Disjoint Multipath Routing (ENDMR), QoS Aware Stable and Effective Lifetime Prediction Routing (QSEL), Collision Constrained Energy Algorithm (ECCA). Each of these protocols, attempt to provide QoS routing based on the factors of Mobility issue, energy factors, multiple paths and node-disjoint routes.

The ECCA provides for multiple node disjoint paths between source and destination. It calculates the total transmission power needed for transmission. Using this protocol, recalculating new paths in case of path failure becomes tedious and introduces delay. The QSEL selects the stable paths. It calculates the lifetime of the path by using the location predictions, Link Expiration Time and the communication cost. This protocol does not consider the issue of multiple paths if a node moves out of transmission range. The CLPR on the similar grounds calculates the predicted lifetime from the residual energy and rate of depletion of energy per packet at a particular node. This protocol does not consider the mobility factor. The TDPR protocol uses node lifetime prediction function. It considers not only residual battery capacity and transmission power but also the traffic load.

The ENDMR is a node disjoint multipath routing protocol. It assigns the cost to the node based on its residual energy. The routing process is such that it limits the route request packet broadcast and hence, prevents loop formation. The paths are selected which have minimum cost and maximum routing energy. 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. Hence, multi-path routing protocols an attractive target for attacks. Some of these attacks can be prevented or countered through cryptographic techniques. The existing cryptographic based routing protocols present routing protocol based on secret sharing over multiple paths. In wireless networks, link cuts can be achieved through jamming or interference.

III. PROPOSED SYSTEM

The basic problem of blocking possible traffic flow between a pair of vertices in a connected graph is known as the max-flow min-cut problem, which can be solved in polynomial time for both cases of minimum edge cut and minimum node cut. 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.

In this paper, we propose a Minimum Cost Blocking (MCB) problem, a special case of node blocking in a network at minimum cost to the attacker. Here the attacker wants to partition the network, thus ceasing flow of data, by either capturing and blocking a key node or by routing all data through a particular node.. In this paper, We emulate adversarial behavior by attacking the multi-path schemes through intelligent blocking and node-isolation type attacks. In a blackhole attack, a particular node in a network falsely advertises a route to the destination node so as to force the route discovery algorithm to choose a route through it. The actual blackhole attack occurs when the malicious node drops packets and hence blocks paths to the destination.

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. Consider a situation where the adversary has already compromised a set of nodes in the network.2 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. The compromised node C is assumed to have connectivity only to the destination node t and other node s2.

Theorem 4.1: The 3-node Induced Flow MCB is NP complete even if every node has a unit cost.

Proof: The result can be proved by reducing the MAX2SAT problem to this problem. Given an instance of MAX2SAT with m variables, r clauses, and integer value k, we can construct a two-layer graph as follows:

The first layer has two end points s1 and s2, between which are pairs of variable nodes . 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 in the MAX2SAT instance, we connect the first variable in the first layer to the second variable in the second layer through an intermediate node.

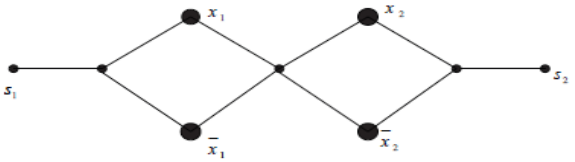

Fig. 1. The first layer of the constructed instance

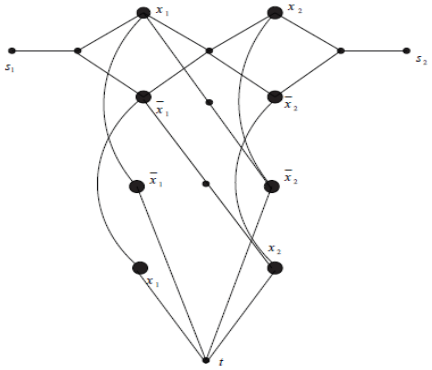

Fig. 2. The constructed instance of 3-node Induced Flow MCB

From the above Fig 1 and Fig 2, we have the following observations:

1) Since *s*1 and *s*2 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 *s*1 and *s*2 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.

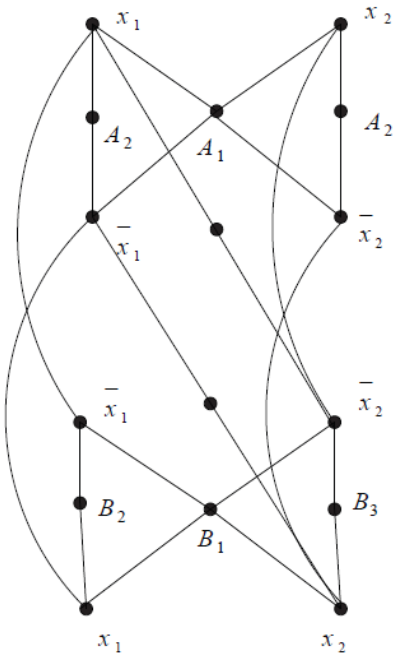

Fig. 3. The constructed instance of multi-node Induced Flow MCB

Multi Path MCB Optimization problem

Suppose that in the graph $G(V,E)$, $|V| = k$. Every node v_i in V is associated with a cost c_i which is the cost of compromising the node. There are $m = \sum_{i=1}^{k} n_i$ paths $P_{11},\ldots,P_{1n_1},\ldots,P_{k1},\ldots,P_{kn_k}$. Here, $P_{i1},\ldots,P_{in_i}$ $(i = 1,\ldots,k)$, 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 ($i = 1,\ldots,k$), what is the minimum cost to compromise at least R_i $(0 \le R_i \le n_i)$ paths out of all paths belonging to this node (i.e., paths $P_{i1},\ldots,P_{in_i}$).

Multi Path MCB Decision problem

Given: Graph $G(V,E)$, where every node v_i in V has a cost c_i of compromise, the set of nodes in paths $P_{11},\ldots,P_{1n_1},\ldots,P_{k1},\ldots,P_{kn_k}$ and integers C and R_i $(0 \le R_i \le n_i)$.

This decision problem is to prove that the MCB problem is NP-complete.

We propose two algorithms for the MCB problem with stationary nodes. The first one is a greedy algorithm and the second one LP-based.

The Greedy Algorithm and Approximation Ratio:

The greedy algorithm selects the most cost effective node iteratively and at the same time removes the covered paths and the paths unusable in the future. 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 1:

1. $T \leftarrow \phi$, and mark all paths and nodes as uncovered;
2. While not *Done*, iterate the following sub-steps:

2.1. For every remaining node in $V \backslash T$, say, node i, in the current iteration, compute its effective number E_i as follows:

$$E_i \leftarrow 0$$

2.1.1. For every node j that is not covered yet, compute $min(max((R_j - Y_j), 0), W_{ij})$. Update E_i as follows:

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

2.2. Compute the cost-effective index α_i as follows:

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

2.3. Choose node u with the lowest cost-effective index (α_u); 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) = α_u; 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.,

$$T \leftarrow T \cup u$$

3. Output T;

The LP Algorithm and Approximation Ratio

The LP Algorithm uses a function $SetCover(P, V \backslash T, c, R_j)$, where P is the set of all uncovered paths belonging to node j, c is the array of cost values for nodes in $V \backslash T$ (i.e., $c_j, \forall j \in V \backslash T$). The function *SetCover* returns the selected sets (nodes) that cover at least R_j paths in P.

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 R_j value; Call $SetCover(P, V \backslash T, c, R_j)$;

2.2. $D \leftarrow D \cup j$

2.3. For every node returned by the function, $T \leftarrow T \cup i$

2.4. Remove from P, every path that is covered by the nodes returned by the function call *SetCover*; $P \leftarrow P \backslash p$

2.5. For every $i \in V \backslash D$, adjust R_i as follows: $R_i = max(0, R_i - O_i)$; If R_i becomes 0 (it means that node i is blocked); $D \leftarrow D \cup i$

IV. CONCLUSION AND FUTURE WORK

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. 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. The results of the proposed work will have an significant impact in various areas which include the security and robustness of routing protocols in mesh networks, threshold cryptography and network coding.

The future scope of this work can be made to develop the approximation algorithms for MCB problem. Also, this problem can be investigated for settings related to ID-based key update protocols as well. We can also study the additional difficulty associated with blocking when the topological information is effectively hidden from the adversary.

REFERENCES

[1] Qi Duan, Mohit Virendra, Shambhu Upadhyaya, Senior Member, IEEE, Ameya Sanzgiri, Mi Wireless Routing Protocols , IEEE TRANSACTIONS ON COMPUTERS, VOL. X, NO. X, FEBRUARY 2013.

[2] 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.

[3] 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.

[4] 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.

[5] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," IEEE Transactions on Information Theory, vol. 49, pp. 371–381, 2003.

[6] I. Damg˚ard and M. Jurik, "A generalisation, a simplification and some applications of Paillier's probabilistic public-key system," in Public Key Cryptography 2001, 2001, pp. 119–136.

[7] "A length-flexible threshold cryptosystem with applications," in Proceedings of the 8th Australasian conference on Information security and privacy, ser. ACISP'03. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 350–364.

[8] L. Ertaul and W. Lu, "ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET (i)," 2005, pp. 102–113.