International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Minimum Cost Blocking Problem In Wireless Routing Protocols

Dipali M. Dhaskat[1], P. L. Ramteke[2]

[1]*Student, Department of CSIT, HVPM COET, Maharashtra, INDIA*
[2]*HOD, Department of CSIT, HVPM COET, Maharashtra, INDIA*

Abstract - *This paper addresses the problem of multipath routing in wireless networks. Here we present a class of MCB problems in Wireless Mesh Networks (WMNs) with multi-path wireless routing protocols. Malicious nodes can attack the network by jamming, selectively forwarding packets, black-hole attack and spoofing. In the case of statically deployed, dense Wireless Sensor Networks which use flat routing, alternate path for secure transmission on packets across such malicious nodes have to be found. We establish the provable superiority of multi-path routing protocols over conventional protocols against blocking, node-isolation and network-partitioning 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.*

Key Words: *Attacks, Blocking, Multi-path routing, Wireless networks, WMN*

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 network. This paper adopts a unique approach to further assay their utility by investigating the security and robustness offered by such protocols. Specifically, we study the feasibility and impact of blocking type attacks on these protocols. In our study, Wireless Mesh Networks (WMNs) [5] 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.

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 multipath routing attacks. 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, 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.

1.1 Scope, Impact and Relevance

The scope of this paper is the dependability of interconnection networks, their performance, and fault tolerance under various attack scenarios. The research reported here is largely theoretical1 and establishes the superiority of multi-path routing protocols in the face of malicious attacks. The impact and relevance pertain to building confidence on existing schemes which primarily rely on the robustness of multi-path protocols. The impacted areas would include load balancing, network coding and threshold cryptography in the wireless domain. Multipath 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. In threshold cryptography, a node splits a secret into several shares, routes them along independent paths, and a threshold number of shares have to be compromised (at least) 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 such demonstrated robustness of multi-path routing.

1.2 Contributions

The technical contributions of this paper are:

[1] 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.
[2] 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
[3] Development of approximation algorithms for the best case scenario and the performance testing of these algorithms in different settings through random graphs based experiments.
[4]Laying direction for future research to evaluate the performance of multi-path protocols against sophisticated attacks in mobile wireless networks.

2. MOTIVATION AND RELATED WORK

Quality security and privacy are important issues in any communication network have worked on these two areas as compared to MANETs and wireless sensor networks have received very attention. 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. a new multi-path routing protocol for heterogeneous networks where they choose QoS as a routing metric. However, it is important to note that unlike unipath routing, 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. To reiterate, since multi-path routing protocols are intended to increase (decrease) say aggregate bandwidth (end to end delay, for instance), the routes selected by these protocols need to facilitate it. This implies that such routes need to be disjoint (not have any common nodes or links) to increase fault tolerance, since the failure of a single node/link can cripple the entire network and be detrimental to the multi-path routing philosophy. Other works such as present routing protocol based on secret sharing over multiple paths. The authors of present a routing protocol that is designed to prevent adversaries from overhearing information and focuses on node-anonymity to prevent identification of end nodes, by forwarding nodes.

2.1 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.

3. TYPES OF ROUTING

3.1 Multipath Routing

Multipath routing protocols for wireless networks are unipath means only single route is used between a source and destination node. Multipath routing is to allow the use of several good paths to reach destinations achieved without imposing excessive control overhead in maintaining multiple paths between a source and a destination. Redundancy in the network or providing backup routes to be used when there is a failure are forms of introducing fault tolerance at the routing level in wireless networks which consists in modifying the route of a packet if the actual route broken. Bandwidth routing along single path may not provide enough bandwidth for a connection using simultaneously multiple paths to route data can be good approach to satisfy the bandwidth requirement of some applications. Suppose traffic distribution is not equal in all links in the network spreading the traffic along multiple resources can alleviate congestion in some links. Multipath protocols can be used to provide error resilience by distributing traffic over multiple paths, security routing protocols is easy for an adversary to launch routing attacks but multipath offers attack resilience.

3.2 Protocol

Protocol defines rules and conventions for communication between network devices for computer networking all generally use packet switching techniques to send and receive messages in the form packets include mechanisms for devices to identify and make connections with each other as well formatting rules that specify how data is packaged into messages sent and received. Uses of network sharing and transferring files within networks are very rapid while maintaining integrity of the file. Individually licensed copies of many popular software programs can be costly shared programs on a network version allows for easier upgrading of the program on one single file server instead of upgrading individual workstation. Sensitive files and programs on a network are passwords protected as copy inhibit. Software can be loaded on one computer eliminating that need to spend time and energy installing updates and tracking files on independent computers throughout the building. E-mail aids in personal and professional communication electronic mail on a LAN can enable staff to communicate within the building.

3.3 Selection of Route

To develop multipath routes nodes execute a special designed route which results path are guaranteed not to interface with each other and path is executed whenever path disrupted. Operation of the reactive component of the protocol is described the requirements protocol needs to accomplish its characteristics, the first and last nodes of the path all have to be in the range of the sender receiver which means that first and last hops of the path and no link is used

in two different location of paths means node disjoint and link disjoint at the same time. To reduce the overhead the multipath routing protocol maintained in each node for each route should be minimal, each node maintain a link state database of the overlay defined by the cluster heads that result from the clustering. Cluster heads do not interfere with each in the worst case nodes will be needed to link two cluster heads so that the information forms the topology table and refers to the cluster head nodes and the gateway nodes that link two clusters. To support this operation clustering terminates cluster head nodes broadcast link state message containing the identifier of their next hop cluster heads as well as gateway node to reach the advertised cluster heads. Link state messages are flooded on the network and stored by each node in a local link state database using this database each node is able to maintain information about the topology of the overlay defined by the cluster heads. Node can always find the available low coupling routes between itself and given target cluster ID all paths that do not share cluster heads other than the destination cluster head of the source node

4. ASSUMPTIONS AND THREAT MODEL

4.1 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 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.

4.2 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. 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.

5. A 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 5.1: (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 5.2: 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.

6. MULTI-PATH MCB PROBLEM

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 a destination can be used to achieve the following benefits:
[1] Fault tolerance: introducing redundancy in the network (Amir, Danilova, Kaplan, Musaloiu- Elefteri, & 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.
[2] 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.
[3]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.
[4]Security: with single-path routing protocols, it is easy for an adversary to launch routing attacks, but multipath offers attack resilience

7. CONCLUSIONS

Our paper presents blocking of attacks in wireless network in secure manner which evaluate the normal or abnormal activities and also the comparison of proposed solution. Multi-path protocols for WMNs make it extremely hard for an adversary to efficiently launch such attacks. Cryptography only protect the message in the packet our analysis NP hard problem is routing protocol that blocks the abnormal activities such as Network partitioning Node isolation in routing discovery which compromise the system from critical condition. Our future work extends more on implementation of secure computing. 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.

REFERENCES

[1] M. Wu, S. Chen, and J. Liao, "Data security in MANETs by integrating multipath routing and secret sharing," in Informatics in Control, Automation and Robotics (CAR), 2010 2nd International Asia Conference on, vol. 1, March 2010.

[2] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol. 40, no. 10, pp. 70 – 75, October 2002.

[3] J. Kong and X. Hong, "ANODR: Anonymous on demand routing withuntraceable routes for mobile ad-hoc networks," in Proc. 4th ACM Int.Symp. Mobile Ad Hoc Netw. Comput. 2003.

[4] M. A. Moustafa, M. A. Youssef, and M. N. El-Derini, "MSR: A multipath secure reliable routing protocol for WSNs," in Computer Systems and Applications (AICCSA), 2011 9th IEEE/ACS International Conference on, December 2011.

[5] F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," Computer Networks Journal.

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

[7] Qi Duan, Mohit Virendra, Shambhu Upadhyaya "Minimum Cost Blocking Problem in Multi-Path Wireless Routing Protocols," IEEE TRANSACTIONS ON COMPUTERS, vol. 63, no. 7, july 2014