INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 3, Issue 4 OCT 2014

AN APPROACH TO MODEL THE THEORETICAL HARDNESS OF ATTACKS ON MULTI-PATH ROUTING PROTOCOLS

[1] K. RUPA , [2] G. LAKSHMI KANTH

[1]M.Tech Student, Department of CSE, Sree Rama Engineering College, Tirupathi, Chittoor District, A.P, India.

[2]Associate Professor, Department of CSE, Sree Rama Engineering College, Tirupathi, Chittoor District, A.P, India.

ABSTRACT— We put forward a group of Minimum Cost Blocking (MCB) quandaries in Wireless Mesh Networks (WMNs) with multi-path wireless routing protocols. We set up the attestable preponderating of multi-path routing protocols over traditional protocols against blocking, node-isolation and network-partitioning kind of attacks. In our assailment model, an adversary is considered prosperous 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 circumstances, viz. (i) low mobility for network nodes, and (ii) lofty extent of node mobility, are evaluated. Situation (i) is proven to be NP-hard and situation (ii) is proven to be #P-hard for the adversary to understand the goal. Additionally, 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 prosper in such blocking-type attacks. These outcomes are verified through simulations which demonstrate the robustness of multi-path routing protocols against such attacks. To the best of our cognizance, this is the first work that theoretically evaluates the assailment-resiliency and performance of multi-path protocols with network node mobility.

Index Terms— Network- partitioning, Wireless Networks, Attacks, Security, Network Protocol.

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. In wireless networks, albeit the dynamic nature of networks and resource constraints entail supplemental overhead in maintaining and reconfiguring multiple routes, which could offset the benefits visually perceived in wired networks, research has proven that multi-path routing provides more preponderant Quality of Service (QoS) guarantees. 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) [1] 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 through multiple available network gateways. Primary traffic in WMNs is between the backbone network and stationary/mobile nodes. This architecture has led to WMNs emerging as a key component in the networking and communications domain due to their design

which sanction numerous diverse commercial and military applications [2], [3], [4], [5]. This uniqueness of WMNs has resulted in consequential research effort being placed on designing sundry protocols for it. The main focus, however, is on 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. This makes WMNs ideal candidates for applying the full scope of any wireless multi-path protocols and study the impact of these attack scenarios. Though the underlying representative network model considered for this study is WMN, the assailment scenarios and results in this paper are plenarily portable to other types of wireless data networks which use multipath routing protocols [6], [7], [8].

The scope of this paper is the dependability of interconnection networks, their performance, and fault tolerance under sundry attack scenarios. The research reported here is largely theoretical 1 and establishes the preponderation of multi-path routing protocols in the face of malevolent attacks. The impact and pertinence pertain to building confidence on subsisting schemes which primarily rely on the robustness of multi-path protocols. The impacted areas would include load balancing [9], network coding [10], [11], [12] and threshold cryptography [13], [14], in the wireless domain.

(a) Active Attack Scenarios for Recovery and Resiliency:

This work is highly pertinent for scenarios where it may be more facile (or harder) for the adversary to compromise some nodes in the network, as compared to compromising the rest of the nodes. For example, it would conventionally be more arduous (in terms of cost) to block nodes more proximate to the gateways or Base Stations (BS) due to reasons of physical proximity (physically more preponderant sentineled), or signal vigor (nodes more proximate to BS may have more preponderant received signal vigor).

Similarly, it is highly desirable for protocols to perpetuate to execute correctly without information compromise, even in the presence of a few maleficent nodes. Currently, most security protocols do not address instauration from malevolent demeanor. Protocols simply abort execution and restart if any malignant comportment is detected. This is detrimental especially in applications where authentic-time replication and high caliber security are paramount as information may have already been lost in the partial execution and frequent restart of the protocols.

(b) Relevance and Impact on Existing Protocols:

Multipath routing protocols can naturally elongate threshold cryptography concepts to the wireless domain. Demonstrated robustness of multi-path protocols against such blocking-type assailments would increment confidence in utilizing threshold cryptography schemes [15], [16]. In threshold cryptography, a node splits a secret into several portions, routes them along independent paths, and a threshold number of shares have to be compromised (at least) for an adversary to instaurate the secret. Our results implicatively insinuate 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 recuperates the secret, or equipollently, the secret is not recuperated felicitously at the destination. Network coding, where nodes perspicaciously send redundant information along multiple paths to ascertain security and reliability and to detect any quandaries with a route would additionally benefit from such demonstrated robustness of multi-path routing. Again, it would be at least exponentially hard for the adversary to optimally compromise more than a threshold number of these paths to render such network coding schemes ineffective.

While there has been some work on integrating the benefits provided by multi-path routing protocols with security mechanisms [17], [18], [19], there subsists a gap 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 mobilewireless networks multi-path protocols under different attack scenarios, and (b) Comparison with traditional single-path protocols under such circumstances. This paper endeavors to achieve the above two desirable goals. To the best of our erudition, 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 Minimum Cost Blocking (MCB) quandary. Though we consider MCB in the WMN setting, the quandary is applicable to other wireless or wired networks.
- Evaluating the hardness of the quandary. MCB is NPhard for the low/no node mobility scenario and #P-hard for networks with patternednode mobility. The reduction for no-mobility is derived from the rudimentary Set Cover quandary [20] and for mobility scenario, from the 3SAT and #SAT quandaries.
- Development of approximation algorithms for the best case scenario and the performance testing of these algorithms in different settings through arbitrary graphs predicated experiments.
- Laying direction for future research to evaluate the performance of multi-path protocols against sophisticated attacks in mobile wireless networks.

RELATED WORK

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 capricious nature of networks. Specifically, the multiple paths provide

link between two paths), making them least abundant and thus, hardest to find. Due to these practical considerations, in most multipath routing, more often than not non-disjoint routes are culled. This causes an astronomically immense security jeopardy, since the compromise of such paths could efficaciously partition the network. While such a quandary does arise with even unipath routing because of the aggregate nature of metrics in multi-path routing, it is more astringent in multi-path routing. Another fascinating point of multi-path routing is that while it might ascertain failure independence, nodes belonging to different paths might still be in the transmission range of each other causing interference with each other. 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 assailer who can utilize such nodes to partition a network. Even though most routing protocols endeavor to cull paths that are as transmission independent as possible to ascertain the least interference between routes, it is not always possible to do so due to network topologies and mobility. Thus, despite their intrinsical advantages, the innate natural disadvantages make multi-path routing protocols a captivating target for attacks. This has led to a fixate on security in multipath routing protocols. Much of this focus is on either information eavesdropping or optimizing security mechanisms for multi-path routing. Some of these assailments can be averted or contravened through cryptographic techniques. For example, OSPF uses MD5 to sentinel against mendacious packet injection. Digitally signed verbalizations can withal be utilized in OSPF to avert mendacious advertisement by legitimate users. In the wireless network domain, such cryptographic schemes for secure broadcast and erroneous data injection obviation are described. Recently, frameworks have been designed to insulate against information eavesdropping in routing protocols, without compromising on performance

[19]. This work presents a formulation of a game that integrates metrics of multi-path routing with security, predicated on which a system administration can incorporate one or more metrics of multi-path routing protocols. Other works present routing protocol predicated on secret sharing over multiple paths. The authors of [18] present a routing protocol that is designed to avert adversaries from overhearing information and fixates on node-anonymity to obviate identification of end nodes, by forwarding nodes. However, there are other attacks that cannot be contravened through cryptographic techniques. Link cut attacks in wired networks, first investigated in detail one such type of assailment. In wireless networks, link cuts can be achieved through jamming or interference. In authenticity, blocking a certain link in a wireless network conventionally denotes blocking all signals from a certain node or compromising the node consummately. As mentioned above this may be relatively facile to achieve for wireless nodes deployed in automated, unattended or bellicose scenarios, accentuating the desideratum for research on blocking attacks – an aspect that has been ignored by the aforementioned works. We adopt some computation intricacy cognate techniques to analyze this particular aspect in multi-path routing security. Specifically, we utilize techniques cognate to the fundamental set cover and partial set cover quandaries. The rudimentary set cover quandary is NP-hard and extensive research has been done on its approximation algorithms.

ASSUMPTIONS AND THREAT MODEL

Assumptions

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

1) We consider managed networks where each node has a unique identity. In other words, the mapping between 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 assailant while having the resources cannot deploy his own contrivances (nodes) to the network.
3) The adversary is a global adversary in the sense that the adversary wants to rigorous the network and can optate the way the network is to be severed. By this we betoken that he is not circumscribed to any particular localized area in the network.
4) Physical capture of nodes is sanctioned; there subsists a cost for each capture/compromise of nodes which is postulated to be computable for the sake of simplicity.
5) An assailer can withal compromise nodes, however, he does not control certain elements such as mobility of the nodes or modification/integration of the hardware of the captured nodes. This postulation is impeccably legitimate since our model considers that the assailer does not ken all the details of the network and it will exponentially increase the cost of amassing these details.
6) Although the assailant may have a fair cognizance of the workings of any system especially in wireless mesh networks, we do not explicitly consider insider attacks. Insider assailments are possible in any organization's system or networks. However, they are additionally involute in the sense that there are possibly many ways an insider attack can be staged. Consideration of insider attacks and its analysis will be quite involved, since there will be an inordinate quantity of parameters to consider and hence is outside the scope of this paper.

Threat Model

Blocking, node-isolation and network-partitioning type assailments are facile to launch and are efficacious in the wireless networks domain due to channel constraints and dynamic network topologies. We emulate adversarial demeanor by assailing the multi-path schemes through keenly intellective blocking and node-isolation type attacks

and study the impact. We additionally endeavor to design best-case scenarios for these assailments to prosper. Both low node-mobility and high node-mobility scenarios are considered. For comparison purposes, we additionally launch kindred attacks on conventional single-path protocols and quantify their impact. The minimum cost blocking (MCB) quandary can be verbally expressed as a special case of node blocking in a network at minimum cost to the assailant. Here the assailant 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. As we consider multipath routing protocols, the assailant has to consider the operation of multi-path routing since multiple paths will subsist from the source to the destination. While a nontrivial but facile solution is to launch a blackhole [45] or wormhole [46] attack, this would coerce the assailer to deploy his own nodes or capture a node proximate to the destination/source which would increment his assailment cost due to the nodes' close proximity to base stations.

In a blackhole attack, a particular node in a network erroneously advertises a route (predicated on metrics concrete to the protocol) to the destination node so as to coerce the route revelation algorithm to cull a route through it. The genuine blackhole attack occurs when the malignant node drops packets and hence blocks paths to the destination. Similarly, in a wormhole attack, an assailant records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them into the network. However, it has to be additionally noted that multi-path routing is not compulsorily affected by wormhole attacks [47]. For these reasons and for verbally expressed posits in Sec. 3.1, we do not consider blackhole and wormhole attacks explicitly in this paper. Further, sybil attack [48], [49] 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.

CONCLUSION

This paper demonstrates the preponderation 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 profoundly hard for an adversary to efficiently launch such attacks. This manuscript is an endeavor 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 additionally 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, albeit we do not obligatorily consider insider attacks, we would relish to point out that our analysis does sanction for an assailant 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 assailment is hard for the assailant, in a network of plausible size.

REFERENCES

[1] R. Coltun, D. Ferguson, and J. Moy, "Ospf for ipv6," Tech. Rep.,1999.

[2] S. Murphy, M. Badger, and B. Wellington, "OSPF with Digital Signatures," RFC 2154 (Experimental), Internet Engineering Task Force, Jun. 1997.

[3] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321 (Informational), Internet Engineering Task Force, Apr. 1992.

[4] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE NETWORK MAGAZINE, vol. 13, pp. 24–30, 1999.

[5] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop by-hop authentication scheme for filtering of injected false data in sensor networks," in IEEE Symposium on Security and Privacy, 2004, pp. 259–271.

[6] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," vol. 8, no. 5. Hingham, MA, USA: Kluwer Academic Publishers, Sep. 2002, pp. 521–534.

[7] S. Chen and M. Wu, "Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks,"Systems Engineering and Electronics, Journal of, vol. 22, no. 3, pp. 519 –527, June 2011.

[8] S. M. Bellovin and E. R. Gansner, "Using link cuts to attack internet routing," inTech. Rep., ATT Research, 2004, Work in Progress 2003 USENIX, 2003.

[9] "IEEE Standard for Information Technology: Wireless LAN Medium Access Control (MAC) and physical layer (PHY) Specifications,"IEEE Std 802.11-2007 - Revision of IEEE Std 802.11-1999, 2007.

[10] D. S. Johnson, "Approximation algorithms for combinatorial problems," in STOC '73: Proceedings of the fifth annual ACM symposium on Theory of computing. New York, NY, USA: ACM,1973, pp. 38–49.

[11] L. Lovasz, "On the ratio of optimal integral and fractional covers," Discrete Math., vol. 13, pp. 383–390, 1975. http://wire.less.dk/wiki/index.php/meshlinks.

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

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

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

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

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.