Ad Hoc Networks 20 (2014) 119–131

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Network coding versus traditional routing in adversarial wireless networks

Donghai Zhu [a], Xinyu Yang [a,*], Wei Yu [b], Xinwen Fu [c]

[a] Dept. of Computer Science and Technology, Xi'an Jiaotong University, Xi'an, China
[b] Towson University, Towson, MD 21252, USA
[c] University of Massachusetts Lowell, Lowell, MA 01854, USA

ARTICLE INFO

Article history:
Received 2 November 2013
Received in revised form 15 February 2014
Accepted 2 April 2014
Available online 16 April 2014

Keywords:
Network coding
Pollution attack
Wireless network
Performance evaluation

ABSTRACT

When network coding is used in wireless mesh networks (WMNs), the epidemic effect of pollution attacks can reduce network throughput dramatically. Nevertheless, little attention has been directed toward the performance gain of network coding versus traditional routing in adversarial wireless mesh networks. To address this critical issue, in this paper, we formally model and analyze the impact of pollution attacks on traditional routing and network coding in both unicast and multicast scenarios. With the combination of both numerical and simulation studies, we evaluate the performance of traditional routing and network coding in adversarial wireless networks. Our data is consistent with the theoretical findings. Our results show that network coding is not absolutely better than traditional routing and its performance gain largely depends on various factors. Most importantly, given a network, the threshold of these factors can be derived from numerical solutions given by our developed closed-form formulae. Thus, we can determine whether network coding should be used in the network. Our results contribute to the foundation, providing guidelines for designing and applying network coding into hostile wireless networks.

1. Introduction

In this paper, we tend to investigate the performance gain of network coding versus traditional routing in adversarial wireless mesh networks (WMNs). Network coding [1] is a mechanism that integrates coding and routing schemes, enabling relay nodes to combine information content in packets before forwarding them. Existing research efforts such as [2,3] demonstrated that network coding could improve network throughput and be extended to numerous applications [4,5].

Although network coding can improve network performance, network coding is vulnerable to pollution attacks. Through such attacks, malicious nodes can alter or forge some corrupted packets and inject them into the network. Through the epidemic propagation, corrupted packets can pollute the whole network quickly and network throughput can be impacted significantly [6]. Note that in traditional routing, because downstream nodes only receive packets from their direct last hop, such epidemic effect will not occur.

To deal with pollution attacks in network coding, a large number of defense schemes have been proposed in the past [7–22]. In addition, a number of research efforts have been conducted to secure routing through authentication in traditional routing [23]. Although the performance gain of network coding in non-adversarial networks has been

* Corresponding author. Tel.: +86 18629053812; fax: +86 2982668098.
E-mail addresses: Dr.zhudonghai@stu.xjtu.edu.cn (D. Zhu), yxyphd@mail.xjtu.edu.cn (X. Yang), wyu@towson.edu (W. Yu), xinwenfu@cs.uml.edu (X. Fu).

http://dx.doi.org/10.1016/j.adhoc.2014.04.002
1570-8705/

well established, it is uncertain whether the conclusion still holds in adversarial wireless networks. Hence, before deploying network coding, the following urgent and fundamental issue must be addressed: *with a defensive scheme in place to detect and mitigate pollution attacks to some extent (in the condition where some nodes cannot be trusted and may launch a pollution attack), can network coding still achieve a higher performance than traditional routing?*

To answer this question, in this paper, we consider and generalize key factors of defensive schemes and inherent networks in traditional routing and network coding rather than focusing on individual defense schemes. We use the Expected Transmission Count (ETX) [24] for successful packet delivery to evaluate the effectiveness of network coding and traditional routing. We consider the abilities of the defender, the adversary, and the network. The ability of the network includes the compromised ratio of nodes in the network to measure its hostile degree, the detection probability of defense schemes deployed in well-behaved nodes, the attack ability of malicious nodes, and the generation size of network coding.

To understand the insightful relationship between metrics and parameters, we then model and analyze pollution attacks on traditional routing and network coding in both unicast and multicast scenarios, according to their fundamental principles (i.e., hop-by-hop in routing and then adding network coding) and the effect of pollution attacks. We derive closed-form formulae to analyze the performance of traditional routing and network coding in adversarial wireless networks. Through comprehensive and realistic modeling, we also obtain the quantitative threshold of parameters. We develop algorithms to compute the ETX of successful packet delivery in pollution attacks in both unicast and multicast scenarios. Through the combination of both numerical and simulation studies, we evaluate the performance of traditional routing and network coding in an adversarial Roofnet [25] network. Our data is consistent with our theoretical findings.

To the best of our knowledge, our work is the first to study and compare the performance of network coding and traditional routing in adversarial wireless mesh networks. The main findings from this research are listed as follows: (i) Network coding is not absolutely better than traditional routing in adversarial networks; (ii) If defense schemes in network coding can achieve a high enough detection probability, network coding can consistently perform better than traditional routing; (iii) Network coding is more suitable than traditional routing for the network in which the adversary's attack ability is limited to a certain level; and (iv) Network coding is more suitable than traditional routing for the network in which the compromised ratio of nodes is smaller than a certain level. *Most importantly, given a network, the threshold of the aforementioned parameters can be obtained through numerical solutions given by our derived closed-form formulae. Then, we can determine whether network coding should be used in the network based on the derived thresholds.*

For example, as shown in our results based on Roofnet [25], if the compromised nodes can corrupt all the packets forwarded and the detection probability of the authentication scheme is 0.99, the coding gain varies from 2.01 to 4.53 as the node compromised ratio varies from 0 to 0.5. If the detection probability is only 0.8, the coding gain varies from 2.06 to 0.58. This means that network coding is not always better and it only holds in some conditions. To achieve better performance in this scenario, the detection probability of the well-behaved nodes should be at least 0.847. This means if the detection probability in both network coding and traditional routing is higher than 0.847, network coding performs better. Our work is fundamental and among the first to formally model and compare the effect of pollution attacks in network coding and traditional routing. Our results contribute to the foundation, providing guidelines for designing and applying network coding into hostile wireless networks.

The rest of this paper is organized as follows. In Section 2, we introduce the system and threat models, along with key factors and assumptions. In Sections 3 and 4, we carry out the modeling and analysis of pollution attacks on network coding and traditional routing in unicast and multicast scenarios, respectively. In Section 5, we present our numerical and simulation results. In Section 6, we briefly introduce related work. Finally, in Section 7, we conclude the paper.

2. Preliminary

In this section, we first present the system and threat models and then review key factors and assumptions.

2.1. System model

In this paper, we consider the reliable unicast and multicast communications, which are supported by traditional routing and random linear network coding [2]. In traditional routing, source S transmits packets hop-by-hop through a predetermined single path in the unicast scenario or through a multicast tree to a group of receivers in the multicast scenario. We also assume that the ETX metric [24] is used to conduct a routing decision. Note that the ETX metric can effectively measure the expected count of transmissions required to successfully deliver a packet over a lossy wireless link. It can also be easily obtained by pinging other neighbor nodes periodically and estimating the delivery probability on each link. More importantly, the ETX of a route is the sum of the link metrics, which can be easily computed in both traditional routing and network coding. However, other metrics do not have all these benefits. The advantages of ETX compared with hop-count is shown in [24] and there are also several extended metrics (e.g., METX [26]), aiming to improve the throughput of multicast.

Based on the principle of network coding, a source generates a message stream and splits it into generations. Assume that each generation consists of m messages. After prefixing every message with a unit vector of dimension m, the source randomly selects the coefficients and sends the linear combination of messages to nodes downstream. Hence, the first m symbols of a coded message, denoted as the global coding vector, will be further used for decoding. In a similar way, forwarders overhear the