Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 58 – 65

Procedia Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)

Multivariate control chart for the detection of MAC layer misbehavior in mobile ad hoc networks

Mohammed-Alamine El Houssaini[a,*], Abdessadek Aaroud[a], Ali El Hore[a], Jalel Ben-Othman[b]

[a] *Department of Computer Science, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco*
[b] *Department of Computer Science, Galilee Institute, Paris 13 University,* Paris, France

Abstract

The share nature of the transmission channel in IEEE 802.11 makes the network vulnerable to several attacks like the MAC layer misbehavior which can be similar to denial of service attack. In this way cheating node by choosing smaller backoff timer attempts to increase its resources at the expense to other stations which respect the protocol.
In this paper, we suggest a novel detection scheme of such attack using a multivariate control chart currently exist in industrial management with a large success. Our proposed strategy comes to replace the univariate Shewhart control chart which already exists in the literature research for the detection of greedy nodes, because it reduces the number of control chart. As we will prove by NS-2 simulations, the proposed mechanism doesn't require any modification to the 802.11 standard, it works in real time and very easy in implementation though it appears somewhat complicated because of the computation of the mean and the covariance matrix in the absence of the MAC layer misbehavior attack.

Peer-review under responsibility of the Conference Program Chairs

Keywords:Mobile ad hoc network; IEEE 802.11; MAC layer misbehavior; Statistical process control.

* Corresponding author.
E-mail address: elhoussaini.m@ucd.ac.ma

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.099

1. Introduction

The Distributed Coordination Function (DCF) of the 802.11[1] protocol is based on distributed algorithm, executed topically in every node in order to define the transmission instant. Cheating stations (called greedy stations)[2] may exploit this knowledge by modifying the backoff rules with the intention of increasing their throughput and then have more access to the transmission channel. This MAC layer misbehavior can be performed easily in network cards which integrates the MAC protocol in the software rather than in the hardware.

A greedy node can intentionally modify its backoff rules to increase its throughput and then enhance its bandwidth at the detriment of other honest nodes those respecting the 802.11 standard. In this way, the network may be conducted to the performance degradation. This performance deterioration can be like a denial of service attack[3]. Furthermore, the need of a detection scheme becomes an emergency.

Several attempts were proposed in the literature research to detect such attack. The most stressed detection methods do not require changes in the 802.11.

In this convergence, we try to propose in our present work, a novel detection method based on the statistical process control (SPC)[4]. The SPC has shown more success in industrial management context. Our new detection strategy has not been presented previously in the stat of the art in the context of the MAC layer misbehavior.

This paper is organized as follows: The next section presents a stat of the art on the research work related to the MAC layer misbehavior attacks. Secondly, the Hotelling control chart was highlighted. The fourth section is dedicated of the presentation of our novel detection method of greedy nodes. The fifth one tries to measure the performance of the so-called detection scheme. Finally, we summarise our work and give perspectives for the future plan.

2. Related work

Multiple studies in the literature review have addressed the subject of MAC layer misbehavior in 802.11 environments, we cite for example:

In[5], authors simulated the MAC layer misbehavior in mobile ad hoc networks through NS-2 and defined new metrics which can be adopted for the detection/reaction of such attacks. They also analysed the network's performance upon several metrics in the presence/absence of greedy behaviors. Generally, their work distinguished the impact of malicious attacks on their predefined metrics.

In[6], authors have addressed the problem of the Contention Widow (CW) cheating in 802.11b. They demonstrated by NS-2 simulator the impact of greedy nodes on the throughput and the packet delay as a function of the constant bit rate. Their work showed that greedy nodes dominate the network use by increasing the throughput and decreasing the packet delay.

Authors in[7], proposed a new detecting scheme for cheating nodes in the backoff rules. This novel scheme is based on the sequential analysis. They also proposed a new analytical model for the 802.11 networks with cheating stations.

The authors in[8] presented a multi-criteria analysis of MAC layer misbehavior, based on the reception throughput and inter-packets time. This analysis takes into consideration the Random Way Point mobility model. They also introduced a new metrics for measuring the process capability of communications in mobile ad hoc networks, borrowed from industrial fields. The work generally is a comparison between greedy behaviour case and honest case in term of performance and capability.

Several schemes have been proposed for the detection of greedy behavior, here are some solutions which are based on statistical approach:

Authors in[9] proposed a new statistical algorithm to detect greedy nodes. First, it compares probability distributions of transmission intervals among all nodes using Kolmogorov-Smirnov test and then it separates nodes into categories by test results. Second, the algorithm seeks to pick out the greedy node groups through comparing characteristics among groups.

Another approach[10] applied the statistical process control (SPC) to detect greedy behaviors in mobile ad hoc networks based on the reception throughput and inter-packets time. In this scheme, the Shewhart control chart was used for individual measurements of metrics (throughput and inter-packets) to detect the MAC layer misbehavior in a real time by visual graphs. The proposed method did not require any modifications to the 802.11 protocol, although it is based on SPC approach to define tolerance intervals.