

[Applied Computing and Informatics (2017) 13, 1](http://dx.doi.org/10.1016/j.aci.2015.11.001)–[9](http://dx.doi.org/10.1016/j.aci.2015.11.001)

|  |  |
| --- | --- |
|  | Saudi Computer Society, King Saud University  Applied Computing and Informatics  (http://computer.org.sa)  www.ksu.edu.sa  [www.sciencedirect.com](http://www.sciencedirect.com/science/journal/22108327) |

REVIEW ARTICLE

Real-time detection of MAC layer misbehavior in

mobile ad hoc networks

Abdessadek Aarouda,\*, Mohammed-Alamine El Houssainia, Ali El Horea, Jalel Ben-Othmanb

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

Received 13 July 2015; revised 3 November 2015; accepted 22 November 2015 Available online 2 December 2015

|  |  |  |
| --- | --- | --- |
| KEYWORDS  Mobile ad hoc Network; MAC IEEE 802.11;  Misbehavior detection;  NS2 simulation;  Statistical process control | Abstract | The MAC layer misbehavior of the IEEE 802.11 standard can have a negative impact on |
| the wireless network’s performance, similar to the effects of denial of service attacks. The goal of this misbehavior was handling the protocol to increase the greedy nodes transmission rate at the expense of the other honest nodes. In fact, nodes in IEEE 802.11 standard should wait for a random backoff interval time to access to the channel before initiating any transmission. Greedy nodes use a malicious technique to reduce the channel waiting time and occupy the channel. This paper intro- | |

duces a new scheme to detect such malicious behavior, which is based on statistical process control (SPC) borrowed from the industrial field in a quality management context. To the best of our knowledge, this approach has not been proposed in state of the art, reports concerning the detection of greedy behaviors in mobile ad hoc networks. The approach has the power to identify greedy nodes in real time by using a graphical tool called uˆ control charty´ that measures the throughput and the inter-packet interval time for each node, and raises an alert if this measure is over a defined threshold. The validation of all obtained results is performed in the network simulator NS2.� 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

\* Corresponding author.

E-mail addresses: [aaroud.a@ucd.ac.ma](mailto:aaroud.a@ucd.ac.ma) (A. Aaroud), [elhoussaini.m@ucd.ac.ma](mailto:elhoussaini.m@ucd.ac.ma) (M.-A. El Houssaini), [elhore.a@ucd.ac.ma](mailto:elhore.a@ucd.ac.ma) (A. El Hore), [jalel.ben-othman@univ-paris13.fr](mailto:jalel.ben-othman@univ-paris13.fr) (J. Ben-Othman).

Peer review under responsibility of King Saud University.

**Production and hosting by Elsevier**

<http://dx.doi.org/10.1016/j.aci.2015.11.001>  
2210-8327 [�](http://dx.doi.org/10.1016/j.aci.2015.11.001) 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

|  |  |
| --- | --- |
| 2 | A. Aaroud et al. |

Contents

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | | 2 |
| 2. | IEEE 802.11 layers . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | | 2 |
| 3. | Related work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | | 2 |
| 4. | Proposed detection system . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | | 3 |
| 4.1. | | Modeling 802.11 networks with greedy nodes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3 | | |
| 4.2. | | Basic idea. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4 | | |
| 4.3. | | Statistical process control . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4 | | |
| 4.4. | | The Shewhart control chart for individual measurements . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4 | | |
| 4.5. | | Development of the control chart. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4 | | |
| 4.6. | | Detection strategy. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5 | | |
| 5. | Performance evaluation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | | 5 |
| 5.1. | | Computation of control limits . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5 | | |
| 5.2. | | Monitoring in normal case . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8 | | |
| 5.3. | | Monitoring in the MAC layer misbehavior case. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8 | | |
| 5.3.1. | | | First scenario (detection of the attacked) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8 | |
| 5.3.2. | | | Second scenario (detection of the attacker) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8 | |
| 5.4. | | Generalization of the detection method. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8 | | |
| 6. | Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | | 8 |
| References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | | | 8 |
| 1. Introduction | | | 2. IEEE 802.11 layers | |

One of the most significant advantages of the IEEE 802.11 standard is the fair access to the medium. However sharing the transmission channel makes the networks vulnerable to several attacks such as jamming, black holes, and greedy behavior (MAC layer misbehavior) [12].

A greedy node intentionally modifies the MAC IEEE 802.11 protocol to get more network resources than honest nodes [10]. By this channel-access misbehavior a greedy node can benefit from several advantages such as:

� Increasing its throughput.

� Reducing its power consumption.

This work aimed to apply a statistical process control (SPC) scheme to detect the IEEE 802.11 MAC layer misbehavior.

Our paper is organized as follows. The second section is dedicated to presenting the architecture of the IEEE 802.11 with all its layers. An overview of the research works related to the IEEE 802.11 MAC layer misbehavior is shown in the third section. The fourth section proposes our detection

The IEEE 802.11 protocol covers the physical layer and the Medium Access Control (MAC) layer as described in Fig. 1. The MAC layer is the same for all IEEE 802.11 standards. However, the physical layer is divided into three categories: FH (Frequency Hopping Spread Spectrum), DS (Direct Sequence Spread Spectrum) and IR (Infrared).

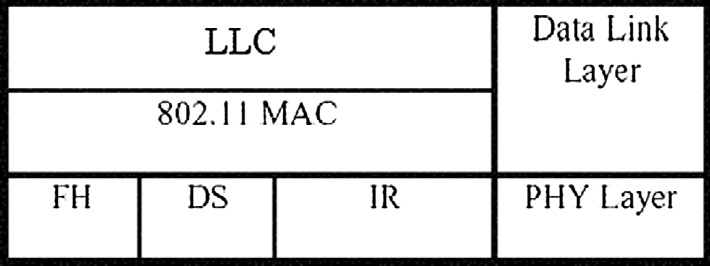
The IEEE 802.11 MAC layer defines the access method Carrier Sense Multiple Access/Collision Avoidance (CSMA/ CA) working as follows. Before transmitting, a node first lis-tens to the shared medium (such as listening for wireless signals in a wireless network) to determine whether another node is transmitting or not. If the channel is free for a DCF Inter-Frame Space (DIFS) time, then the station transmits a frame which is acknowledged after a Short Inter-Frame Space (SIFS) interval time with an ACK frame.

The transaction time (DATA + SIFS + ACK) is noted as a Network Allocation Vector (NAV) and blocks other stations from accessing channel till total NAV decrement.

Additionally the CSMA/CA method has an optional mech-anism of channel reservation Request To Send (RTS)/Clear To

scheme of the IEEE 802.11 MAC layer misbehavior (greedy Send (CTS) [1].

node). In the fifth section, the authors evaluate the perfor-mance of their approach using the NS2 simulator. Conclusions and perspectives are presented in the last section.



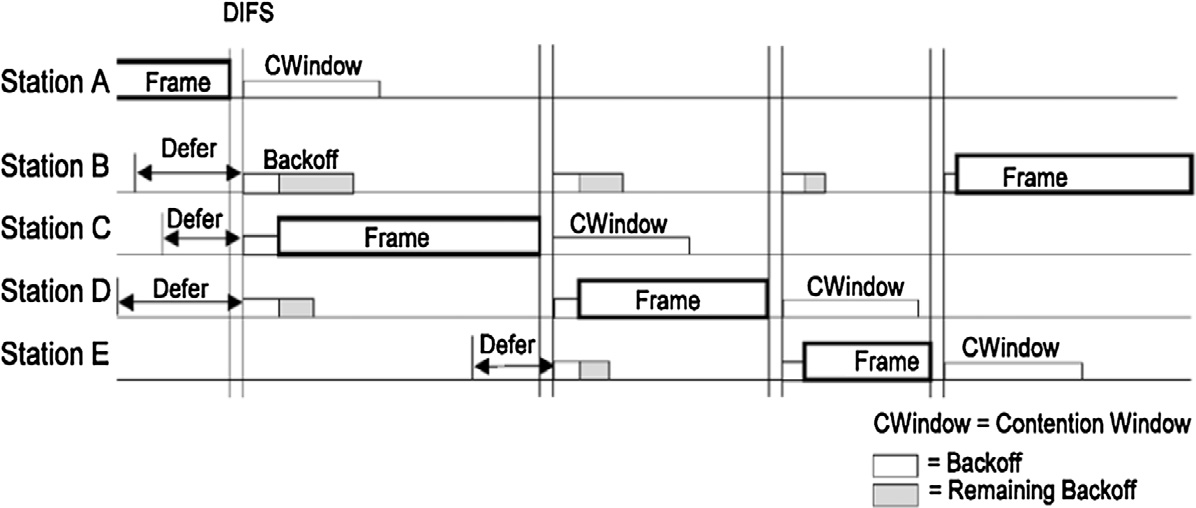
|  |  |
| --- | --- |
| Figure 1 | IEEE 802.11 layers description. |

The CSMA/CA access method defines the Binary Exponen-tial Backoff (Fig. 2) in order to resolve the access medium problem when several stations want to transmit data simulta-neously. This method requires that each station chooses a ran-dom waiting time between 0 and the size of a contention window CW (value equals to a number of time slots), and expects the number of slots before transmission [1].

3. Related work

The BEB algorithm provides a fair access to the medium. Greedy nodes change their BEB to increase their throughput at the expense of other honest nodes. This greedy behavior is considered as misbehavior of the IEEE 802.11 MAC layer.

|  |  |
| --- | --- |
| Detection of MAC layer misbehavior | 3 |



|  |  |
| --- | --- |
| Figure 2 | Backoff procedure. |

The classification of the MAC layer misbehavior, given in [4], is categorized as follows:

� a misbehavior: The greedy node chooses the value of BEB in the interval [0 a(CW � 1)], where CW is the contention window, and 0 < a < 1.

� Deterministic BEB: The greedy node chooses a constant BEB independently of the contention window.

� b misbehavior: After a failed transmission, instead of put-ting a CW to be min{2CW,CWmax}, greedy node sets its

|  |  |  |  |
| --- | --- | --- | --- |
| contention | window | as | CW = max{CWmin,min{bCW, |

CWmax}} where 0 < b < 2.

� Fixed maximum contention window.� Fixed contention window.

Several approaches have been proposed in the literature for the detection of the IEEE 802.11 MAC layer misbehavior.

Tiwary [16] proposed a detection scheme based on the sta-tistical collection of all nodes RTS retransmission due to time out, packet retransmission due to ACK timeout and through-put at receiver, then compared these results with the threshold values to decide whether a selfish attack is occurring. This method does not require any changes in protocols but it cre-ates computation overhead.

Other authors [17] also proposed an extension to the 802.11 standard that ensures a uniformly distributed random backoff through the protocol of coin flipping by telephone. The main idea is to let both the sender and receiver agree on a random value of backoff through a public exchange using an engage-ment method inspired by the protocol of applying flipping coins over the telephone. However, it is still unable to detect collision between sender and receiver.

An approach of greedy nodes detection in IEEE 802.11 was proposed [5] based upon the linear regression between instants of transmission to calculate a detection threshold and without requiring modifications to the standard. This idea results from the strong linear correlation noticed between nodes in terms of transmission instants.

The strategy called Detecting MAC Layer Greedy Behavior

process control). We use the Shewhart chart for individual value, applied to the receiving throughput and the average time between receptions.

Our new detection strategy can be implemented on any receiving node to monitor the network in real time. As we will demonstrate by the simulation, the proposed detection scheme does not require modifications of the IEEE 802.11 standard.

To the best of our knowledge our approach based on statis-tical process control has not been proposed before in the liter-ature to detect greedy behavior in mobile ad hoc networks.

4. Proposed detection system

4.1. Modeling 802.11 networks with greedy nodes

Bianchi [18] developed a Markov chain model for IEEE 802.11 protocol in a normal case and without any attacks, assuming that the network is saturated and the collision probability p is constant. The author adopted the notation Wi ¼ 2iW, where i 2 ð0; mÞ is called ‘‘bachoff stage” and W ¼ CWmin, s(t) and b (t) denote the stochastic process referring to the backoff stage and the backoff time counter of the node at time t respectively.

The stochastic process is defined as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 >  > | Pfi; kji; k þ 1g ¼ 1  Pf0; kji; 0g ¼ ð1 � pÞ=W0 Pfi; kji � 1; 0g ¼ p=Wi  Pfm; kjm; 0g ¼ p=Wm | k 2 ð0; Wi � 2Þ k 2 ð0; W0 � 1Þ k 2 ð0; Wi � 1Þ k 2 ð0; Wm � 1Þ | i 2 ð0; mÞ i 2 ð0; mÞ i 2 ð1; mÞ | ð1Þ |

where

|  |  |  |
| --- | --- | --- |
| P i1;k1ji0;k0 | g ¼ P sðtþ1Þ ¼ i1;bðtþ1Þ ¼ k1jsðtÞ ¼ i0;bðtÞ ¼ k0 | g |
| ð2Þ | |

The probability that a node in the network transmits a packet in a randomly chosen slot is denoted as s. Its computation can be done as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| in IEEE 802.11 Hotspots (DOMINO) deployed in the access | s | 2ð1 � 2pÞ | 3 |
| point to detect misbehavior is exposed [6]. This method uses | ¼ | ð1 � 2pÞðW þ 1Þ þ pWð1 � ð2pÞmÞ | ðÞ |
| a modular architecture which comprises individual tests and |
| For n nodes using the shared medium, | | ð4Þ |
| a decision making component DMC. However, greedy nodes |
| may exploit the knowledge of DOMINO in order to adapt | P ¼ 1 � ð1 � sÞn�1 | |
| its parameters to avoid the detection. |

We propose in the following section a new detection strat-egy based on a statistical quality control approach (statistical

The last two equations can be solved to compute the two unknowns variables n and p.

|  |  |
| --- | --- |
| 4 | A. Aaroud et al. |

The authors in [19] proposed a modeling of an 802.11 net-work with MAC layer misbehavior attacks. They consider n nodes in a network, with the presence of l greedy nodes mod-

Indeed, two processes are never exactly similar. There are many sources of variation in low amplitude that cannot be removed, all of them representing the common causes of dis-

ifying the backoff timer. The misbehaving nodes choose a ran- persion [13].

dom backoff interval in the range of ð0; gaW � 1Þ, where ð1 6 a 6 lÞ and W is the current contention window (CW). The collision probability at the greedy node is pa. Therefore they modified the stochastic process proposed in [18] to estab-lish a simple modeling for the misbehaving nodes.

As a result they found the following equations with 2l þ 2 unknowns, s0; s1; . . . ; sl; p0; p1; . . . ; pl.

|  |
| --- |
| 8 s0¼  s1¼   ð1�2p0ÞðWþ1Þþp0Wð1�ð2p0ÞmÞ  ð1�2p1Þðg1Wþ1Þþp1g1Wð1�ð2p1ÞmÞ   2ð1�2pÞ0  2ð1�2pÞ1  > . . .  sl¼ ð1�2plÞðglWþ1ÞþplglWð1�ð2plÞmÞ  2ð1�2plÞ1  ð5Þ  P0¼ 1 � ð1 � s0Þ  P1¼ 1 � ð1 � s0Þ  . . .  n�l�1Q  n�lQ 26i6lð1 � siÞ   16i6lð1 � siÞ  The last equations can be solved to compute the unknown > Pl¼ 1 � ð1 � s0Þ n�lQ 16i6l�1ð1 � siÞ |

variables and also to define parameters adopted for the perfor-mance evaluation of the network. However, finding a closed form for each variable is not our goal, since our approach is based on simulation analysis.

However, there are major causes of variation that require change. These cases are called special causes. The process becomes out of control, and thus we must look for the cause.

The SPC method provides an effective and proper tool to separate the ordinary from the extraordinary by creating a powerful graphic called uˆ control charty´ , among these charts are: The Shewhart control chart for individual measurements [13].

4.4. The Shewhart control chart for individual measurements

The Shewhart control chart for individual measurements should be used when we want to monitor a process on the basis of a periodically measured quantity [14].

In such situations, the control chart for individual units is useful. (The cumulative sum and exponentially weighted mov-ing average control charts will be a better alternative when the magnitude of the shift in process means that what is of interest is small.) In many applications of the individual control chart we use the moving range of two successive observations as the basis of estimating the process variability [14].

The moving range is defined as [14]

MRi ¼ jxi � xi�1j ð6Þ where the moving range number i is MRi, and xi is the range number i.

|  |  |
| --- | --- |
| 4.2. Basic idea | To establish a moving range control chart, the procedure is illustrated in the following section. |

The basic idea of our strategy for detecting IEEE 802.11 MAC

layer misbehavior emerges from the difference and the shift observed on the two previously defined metrics, namely throughput [7], which is defined as a measure of how many successful packets were received correctly in a given amount of time and the inter-packets time defined as the mean time

4.5. Development of the control chart

To calculate the control limits for individual values, we should

use the below formulas [14]:

|  |  |  |
| --- | --- | --- |
| between receptions (mean time between successive received | UCL ¼ �x þ 3 MR | ð7Þ |
| packets) [3]. |
| We showed that this misbehavior led to an increase of the | Center line ¼ �x | ð8Þ |
| average reception throughput and a decrease of times between |
| receptions for the greedy nodes. On the other side it generates | LCL ¼ �x � 3 MR |
| ð9Þ |
| a reverse effect for honest nodes [3]. |

Our detection method is based on the supervision of the two metrics defined in our previous work [3] and its dispersion

For the moving range, we find the equations [14] as follows:

|  |  |  |
| --- | --- | --- |
| by a control chart with two limits. These graphs are called con- | UCL ¼ D4MR | ð10Þ |
| trol charts, following a statistical process control approach. |
| 4.3. Statistical process control | Center line ¼ MR | ð11Þ |
| LCL ¼ D3MR | ð12Þ |

The SPC ensures optimum quality based on statistical tools. It aims to the following:

– Give a tool to monitoring process.

– Formalize the notion of capability.

– Distinguish between ordinary and extraordinary situations.

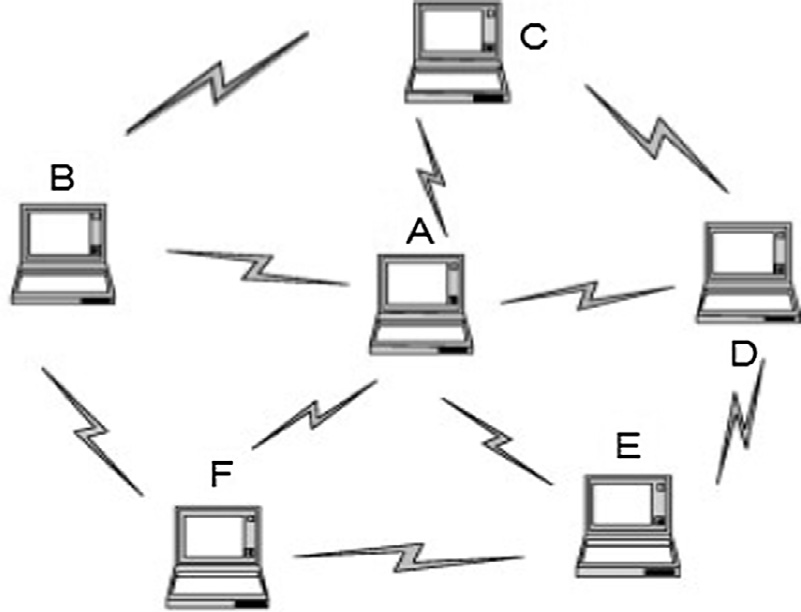
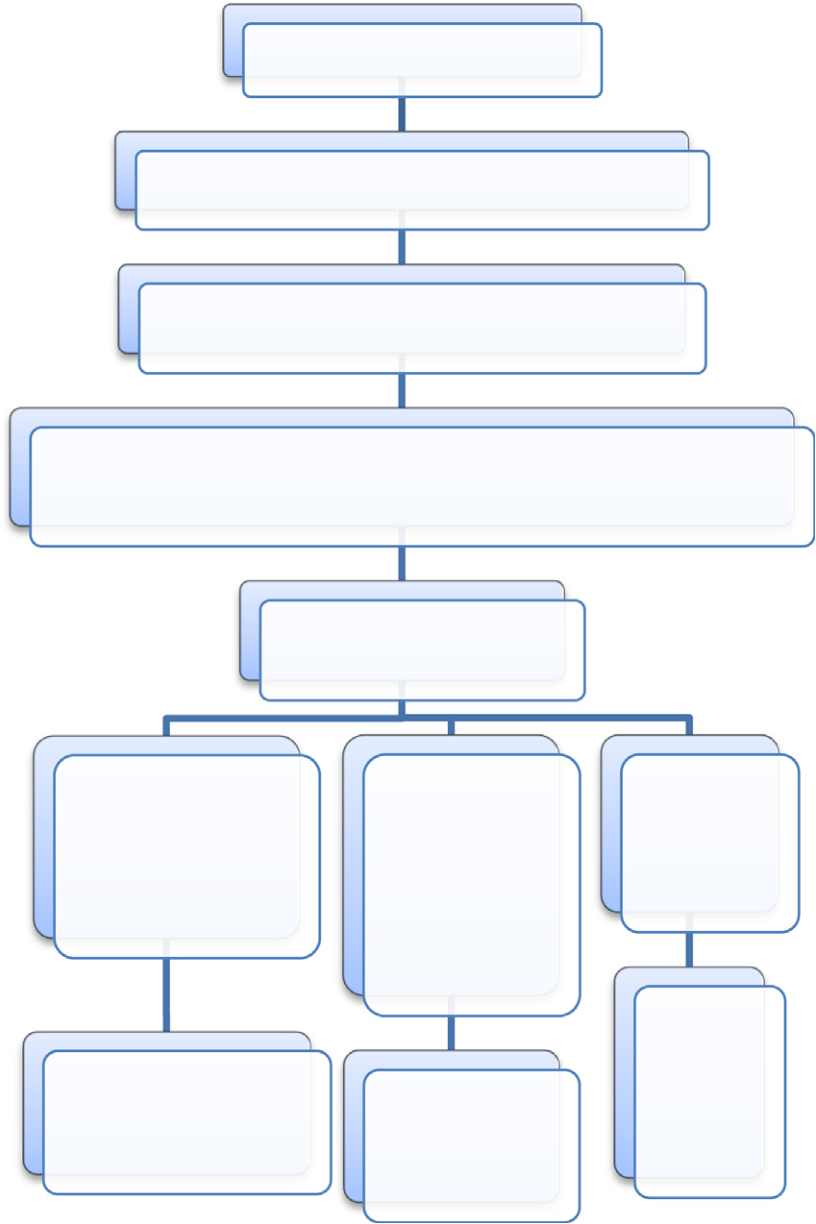
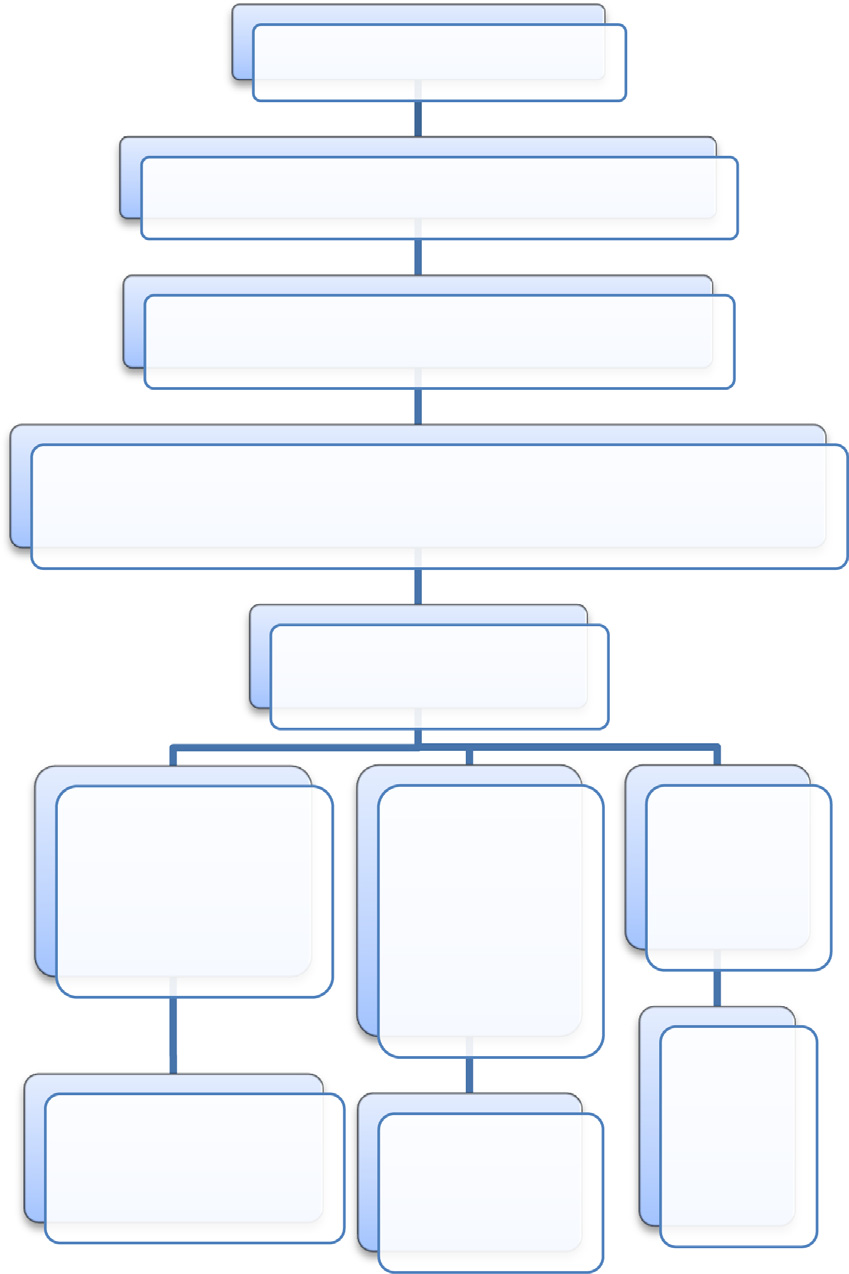
One of the basic principles of this control is deviation detec-tion. All variations on a system do not require modification.

where UCL and LCL are the upper and lower control limits

respectively, and MR is the average of the moving ranges of two observations, x being the observation value.

The constants, d2; D3 and D4 are tabulated for various sample sizes [14]. Its mathematical origins are shown in [20].

The control chart for the individual measurements includes two graphs, the first is for individual value monitoring used for detecting the slip of the system and the second is for moving range used for monitoring the quality [14].



|  |  |  |  |
| --- | --- | --- | --- |
| Detection of MAC layer misbehavior | |  | 5 |
| Table 1 | Lookup table of the chart parameters. |  |  |
| Parameter | | Value |  |
| The observation X | | Throughput or inter-packets time |  |
| Average of observations (center line) | | Center line ¼ �x  Center line ¼ MR  UCL ¼ �x þ 3MR |
| Average moving range of observations (center line) | |  |
| Upper control limit of individual observations | |
| Lower control limit of individual observations | |
| LCL ¼ �x � 3MR |
| Upper control limit of moving range observations | |
| UCL ¼ D4MR  LCL ¼ D3MR |
| Lower control limit of moving range observations | |

4.6. Detection strategy

In this monitoring technique we propose supervising and plot-ting the average reception throughput and the mean inter-packets time by control charts (Table 1).

The judgment and interpretations of the novel detection strategy can be summarized in the following block diagram (Fig. 3):   
 To illustrate our novel detection scheme, station A depicted in Fig. 4 for instance, receives packets from the set defined by {B, C, D, E, F}. The purpose is to identify which among this set of stations is a greedy one. Therefore, this detection scheme is implemented at every station to designate the cheater station through the supervision of the average reception throughput and the mean inter-packets time by control charts. The control is performed automatically for every node belonging to this set

of transmitters ({B, C, D, E, F} is the transmitters’ set of the station A).

For the computation of the thresholds (control chart parameters), we need a minimum of 20 values [13], but for the network monitoring, we draw every calculated value (for the throughput and for the inter-packets time). This is the real-time detection that we highlight in our paper. The detec-tion scheme is performed at any receiving node for every trans-mitting station (as in Fig. 4). In fact every node has the right to explore its received packets. We can emphasize that one honest node in the state of transmission is sufficient to calculate the control chart parameters (see Figs. 5–7).

The next section is dedicated to the performance analysis of the proposed detection scheme through NS-2 simulations. In our simulation parameters we used the shadowing model as a radio propagation model which is very near to the realistic radio propagation, taking into account the energy losses.

5. Performance evaluation

|  |  |
| --- | --- |
| Identification of critical  process parameters | To achieve our detection method of the IEEE 802.11 MAC layer misbehavior [9], the simulator NS-2 can be used with |

Collect ofstatistical measures in normal case (without misbehavior)

Calculate the parameters of the chart (UCL, Center line and LCL)

Represent the measurements above on the chart (if there are points that come out of the control limits they should be eliminated and recalculate the chart settings)

Monitoring the metrics   
using the control chart

If the curves If a small If there has oscillate on either number of been a side of the mean and points crossed   
 greater that the majority of the upper or tendency and the points are inside lower control deviation the limits   
 limit or deviate from the center   
 line

The

control and no MAC   
Our process is under

layer misbehavior exist the transmission   
 moving out of   
 The node is   
 network is

greedy   
attack   
under

range.

Figure 3 Block diagram of the detection scheme.

some useful tools for processing traces files as explained by [8,11]. In our case we have chosen the simulator with the soft-ware platform and parameters depicted in Table 2.

5.1. Computation of control limits

First, we calculated the control limits and center lines based on the results of the simulation in normal cases (without IEEE 802.11 MAC Layer Misbehavior) through equations from (6)–(12).

|  |  |
| --- | --- |
| Figure 4 | A mobile ad hoc network. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 |  |  | A. Aaroud et al. | | | | | | | | | | | | | | | | | | | | | | |
|  | Throughput in Mb/s | 0.50 | Throughput, UCL, Center line, LCL | | | | | | | | | Inter-packets time, UCL, Center line, LCL | | | | | | | | | | | | | |
|  | | | | | | | | | | Inter-packets time in s | | 0.025 | |  | | | | | | | | |
| 0.48 | 0.024 | |
| 0.46 | 0.023 | |
| 0.44 | 0.022 | |
| 0.42 | 0.021 | |
| 0.40 | 0.020 | |
| 0.38 | 0.019 | |
| 0.36 | 0.018 | |
| 0.34 | 0.017 | |
| Throughput moving range in Mb/s | 0.32 | 0.016 | |
| 0.30 | 0.015 | |
| 0 | 100 | | 200 | 300 | 400 | | 500 | | 600 | 0 | 100 | 200 | 300 | 400 | 500 | | 600 | |
| Time in s | | | | | | | | | Time in s | | | | | | | | | | | | | |
| (Throughput monitoring in normal case) | | | | | | | | | (Inter-packets time monitoring in normal case) | | | | | | | | | | | | | |
| Throughput moving range, UCL, Center line | | | | | | | | | | Interpackets time moving range in s | 0.005 | | Inter-packets time moving range, UCL, Center line | | | | | | | | | |
| 0.10 |  | | | | | | | | | |  | | | | | | | | | |
| 0.09 | 0.004 | |
| 0.08 |
| 0.07 |
| 0.003 | |
| 0.06 |
| 0.05 |
| 0.002 | |
| 0.04 |
| 0.03 | 0.001 | |
| 0.02 |
| 0.01 | 0.000 | |
| 0.00 |
| 0 | | 100 | 200 | 300 | | 400 | | 500 | 600 | 0 | | 100 | 200 | 300 | 400 | | 500 | | 600 |
| Time in s | | | | | | | | | | Time in s | | | | | | | | | |
| (Throughput moving range monitoring in normal case) | | | | | | | | | (Inter-packets time moving range monitoring in normal case) | | | | | | | | | | | | | |
| Figure 5 | | | Control charts monitoring in normal case (without greedy attack). | | | | | | | | | | | | | | | | | | | |

Inter-packets time, UCL, Center line, LCL

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Throughput in Mb/s Throughput moving range in Mb/s | 0.50 | Throughput, UCL, Center line, LCL | | | | | | | | | | | | Inter-packets time in s | 0.035 | |  | | | | | | | | | |
|  | | | | | | | | | | | | 0.033 | |
| 0.45 |
| 0.031 | |
| 0.40 | 0.029 | |
| 0.027 | |
| 0.35 | 0.025 | |
| 0.023 | |
| 0.30 |
| 0.021 | |
| 0.25 |
| 0.019 | |
| 0.017 | |
| 0.20 |
| 0.015 | |
| 0 | | 100 | | 200 | | 300 | | 400 | 500 | 600 | | 0 | | 100 | 200 | 300 | | 400 | | 500 | 600 |
| Time in s | | | | | | | | | | | | Time in s | | | | | | | | | |
| (Throughput monitoring in attack case) | | | | | | | | | | | | | (Inter-packets time monitoring in attack case) | | | | | | | | | | | | |
| 0.14 | | Throughput moving range, UCL, Center line | | | | | | | | | | | Inter-packets time moving range in s | | Inter-packets time moving range, UCL, Center line | | | | | | | | | | |
|  | | | | | | | | | | | 0.012 0.010 0.008 0.006 0.004 0.002 0.000 | |  | | | | | | | | |
| 0.12 | |
| 0.10 | |
| 0.08 | |
| 0.06 | |
| 0.04 | |
| 0.02 | |
| 0.00 | |
| 0 | | 100 | | 200 | | 300 | 400 | 500 | | 600 | 0 | 100 | 200 | | 300 | | 400 | 500 | 600 |
| Time in s | | | | | | | | | | | Time in s | | | | | | | | | | |
| (Throughput moving range monitoring in attack case) | | | | | | | | | | | | | (Inter-packets time moving range monitoring in attack case) | | | | | | | | | | | | |
| Figure 6 | | | | | | | | | Control charts monitoring of the attacked. | | | | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Detection of MAC layer misbehavior | | | | | | | | |  |  | Inter-packets time, UCL, Center line, LCL | | | | | | | 7 |
| Throughput, UCL, Center line, LCL | | | | | | | | | Inter-packets time in s | 0.025 |  |
| Throughput in Mb/s | 0.9 |  | | | | | | |  | | | | | | |
| 0.8 | 0.023 |
| 0.021 |
| 0.7 | 0.019 |
| 0.017 |
| 0.6 |
| 0.015 |
| 0.013 |
| 0.5 |
| 0.011 |
| 0.4 |
| 0.009 |
| 0.007 |
| 0.3 | 0.005 |
| 0 | 100 | 200 | 300 | 400 | 500 | 600 | 0 | 100 | 200 | 300 | 400 | 500 | 600 |
| Time in s | | | | | | |
| Time in s | | | | | | | | |

(Throughput monitoring in attack case)   
Throughput moving range, UCL, Center line

(Inter-packets time monitoring in attack case)

Inter-packets time moving range, UCL, Center line

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Throughput moving range in Mb/s | | | 0.12 |  | | | | | | | | | Inter-packets time moving range in s | 0.005 |  | | | | | | | |
| 0.10 | 0.004 |
| 0.08 | 0.003 |
| 0.06 | 0.002 |
| 0.04 | 0.001 |
| 0.02 |
| 0.00 | 0.000 |
| 0 | 100 | 200 | | 300 | 400 | | 500 | 600 | 0 | 100 | | 200 | 300 | 400 | 500 | 600 |
| Time in s | | | | | | | | | Time in s | | | | | | | |
| (Throughput moving range monitoring in attack case) | | | | | | | | | | | | (Inter-packets time moving range monitoring in attack case) | | | | | | | | | | |
| Figure 7 | | | | | | | | | | Control charts monitoring of the attacker. | | | | | | | | | | | | |
| Table 2 | | | | Platform and parameters. | | | | | | | | | | | | | | | | | | |
| Parameters | | | | | | | | | | | | Values | | | | | | | | | | |
| Computer | | | | | | | | | | | | HP Compaq 6730s | | | | | | | | | | |
| Operating system | | | | | | | | | | | | Ubuntu 10.10 | | | | | | | | | | |
| Version of the simulator | | | | | | | | | | | | ns-2.34 [2] | | | | | | | | | | |
| Trace file processing language | | | | | | | | | | | | Perl | | | | | | | | | | |
| Graph construction tool | | | | | | | | | | | | Microsoft Excel 2007 | | | | | | | | | | |
| Transmission rate (Mb/s) | | | | | | | | | | | | 2 | | | | | | | | | | |
| MAC layer | | | | | | | | | | | | 802.11 | | | | | | | | | | |
| Physical layer | | | | | | | | | | | | Direct Sequence Spread Spectrum | | | | | | | | | | |
| Simulation surface (m)  Transmission range (m) | | | | | | | | | | | | 500 � 500  250 | | | | | | | | | | |
| Radio propagation model | | | | | | | | | | | | Shadowing | | | | | | | | | | |
| Traffic generator | | | | | | | | | | | | CBR Constant bit rate | | | | | | | | | | |
| Simulation time (s) | | | | | | | | | | | | 600 | | | | | | | | | | |
| Packet size (byte) | | | | | | | | | | | | 1000 | | | | | | | | | | |
| Routing protocol | | | | | | | | | | | | AODV | | | | | | | | | | |
| Node speed (m/s) | | | | | | | | | | | | Randomly selected between 0 and 15 | | | | | | | | | | |
| Mobility model | | | | | | | | | | | | Random Way Point [15] | | | | | | | | | | |
| Table 3 | Control charts parameters for throughput and inter-packets time. | | | | | | | | | | | | | | | | | | | | | |
| Chart type | | Chart parameters | | | | | Shewhart control chart for throughput | | | | | | | | | | Shewhart control chart for inter-packets time | | | | | |
| monitoring | | | | | | | | | | | | monitoring | | | | | | | | | | |
| Individual | | UCL | | | | 0.49238 | | | | | | 0.02372 | | | | | | | | | | |
| measurement | | CENTER LINE | | | | | 0.41219 | | | | | 0.01982 | | | | | | | | | | |
| LCL | | | | | | 0.33200 | | | | | | 0.01591 | | | | | | | | | | |
| Moving range | | UCL | | | | 0.09850 | | | | | | 0.00480 | | | | | | | | | | |
| CENTER LINE | | | | | | | 0.03015 | | | | | 0.00147 | | | | | | | | | | |
| LCL | | | | | | 0 | | | | | | 0 | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | Tolerance interval in Mb/s | Throughput, Throughput moving range | | | | | | | | Inter-packets time, Inter-packets time moving range | | | | | | | | | A. Aaroud et al. |
| 0.7 |  | | | | | | | Tolerance interval in s | 0.45 |  | | | | | | |
| 0.6 | 0.40 |
| 0.5 | 0.35 |
| 0.30 |
| 0.4 | 0.25 |
| 0.3 |
| 0.20 |
| 0.2 | 0.15 |
| 0.10 |
| 0.1 |
| 0.05 |
| 0.0 | 0.00 |
| 0 | 5 | 10 | 15 | 20 | 25 | 30 | 0 | 5 | 10 | 15 | 20 | 25 | 30 |
| Number of nodes | | | | | | | | Number of nodes | | | | | | | | |
| (The throughput tolerance intervals depending on the number of nodes) | | | | | | | | (The inter-packets time tolerance intervals depending on the number of nodes) | | | | | | | | |
| Figure 8 | | | | Tolerance intervals depending on the number of nodes. | | | | | | | | | | | | |

5.2. Monitoring in normal case

In this case the two metrics (throughput and inter-packets time) are supervised in the control chart below composed by the control limits that we computed in the last section for a node in the network.

As we can see in the control chart for throughput and the inter-packets time, curves oscillate on either side of the mean and the majority of the points are inside the limits. Obviously we can decide that this node communicates in an environment without greedy attack.

If few points come out of the control limits, we can explain this fact by the movement outside of the transmission range

Small and random variations in curves are detected. We should compute the chart parameters for every number of nodes to obtain a better supervision of the network.

The detection thresholds and the tolerance interval depend on the number of nodes; therefore, each receiver updates these parameters for each number of transmitters. In our work we tested the detection scheme in an ideal environment which depends on the number of nodes with constant bit rate traffic. The statistical process control is a useful and strong tool for supervising and detecting strong derivations in any type of environment (realistic or theoretical). Thus, the purpose is

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| the | separation | of | the | extraordinary | from | the | ordinary |

situations.

|  |  |
| --- | --- |
| (see Table 3). | 6. Conclusion |

5.3. Monitoring in the MAC layer misbehavior case   
 The misbehavior at the MAC layer by changing the backoff

5.3.1. First scenario (detection of the attacked)

In this monitoring case we note that when the throughput curve crossed the lower control limit and the inter-packets time curve crossed the upper control limit, there is a strong devia-tion. Consequently we can decide that this node is under a MAC layer misbehavior attack.

We can also lay emphasis on the absence of any great change for the moving range curves related to the deviations for the mean but not for the amplitude, due to the greedy behavior.

5.3.2. Second scenario (detection of the attacker)

In this monitoring case we reveal that the throughput curve crossed the upper control limit and the inter-packets time

mechanism can lead to performance degradation of the net-work. In this paper we tried to propose a novel detection scheme for this misbehavior based on the supervision of two metrics (reception throughput and inter-packets time) through statistical process control charts. Our detection scheme pre-sents several advantages. It does not require any changes in the IEEE 802.11 protocol and it can be implemented at any receiving node. Its most significant advantage is the detection of such attack in real time by visual graphs.

In the perspective, we will try to extend the proposed scheme by introducing other performance measurements in order to develop other detection systems that are easier than the previous ones. We also plan an implementation of the so-called detection strategy in a realistic environment.

|  |  |
| --- | --- |
| curve crossed the lower control limit. There is a strong devia-tion, so we can decide that this node is a greedy one (this is the | References |

MAC layer misbehavior attack).

We can also focus on a change in the moving range curve of the inter-packets time resulting from an improvement of the transmission time for the attacker due to the greedy behavior.

5.4. Generalization of the detection method

We plot the tolerance interval (the difference between the upper and lower control limits) as a function of the number of nodes. Our results are represented in the graphics below (Fig. 8).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| [1] IEEE | Standards | Association, | IEEE | 802.11 | Standard | for |

Wireless LAN Medium Access Control (MAC) and Physical

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Layer | (PHY) | Specifications, | IEEE | Standards | Association |

(March), 2012, pp. 818–840.

[2] Information Sciences Institute, The Network Simulator – ns-2,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information | Sciences | Institute, | 1995 | <[http://www.isi.edu/](http://www.isi.edu/nsnam/ns/) |

[nsnam/ns/](http://www.isi.edu/nsnam/ns/)> (accessed July 10, 2015).

[3] M. El Houssaini, A. Aaroud, A. Elhore, J. Ben-Othman, Analysis and simulation of MAC layer misbehavior in mobile ad-hoc networks, in: Proceedings of the 5th International

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Workshop | on | Codes, | Cryptography | and | Communication |

Systems, 2014, pp. 50–54.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Detection of MAC layer misbehavior | | | | | | | | | | | | | | | 9 |
| [4] V.R. Giri, N. Jaggi, MAC layer misbehavior effectiveness and collective aggressive reaction approach, in: Proceeding 33rd IEEE Sarnoff Symposium, Princeton, NJ, April 2010, pp. 1–5.  [5] A. Hamieh, J. Ben-Othman, A. Gueroui, F. Naı¨t-Abdesselam, Detecting greedy behaviors by linear correlation in wireless Ad | | | | | | | | | | | | | | | Development (SCOReD 2006), Shah Alam, Selangor, Malaysia, 27–28 June, 2006.  [12] V. Gupta, S. Krishnamurthy, M. Faloutsos, Denial of service attacks at the MAC layer in wireless ad hoc networks, in: Presented at IEEE MILCOM, Anaheim, California, 2002.  [13] M. Pillet, Appliquer la maitrise statistique des proce´ de´ s MSP/ SPC, forth ed., Edition d’Organisation, Paris, France, 2005.  [14] [C. Douglas Montgomery, Introduction to Statistical Quality Control, sixth ed., John Wiley & Sons Inc, United States of America, 2008](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0070).  [15] F. Bai, A. Helmy, A Survey of mobility modeling and analysis in wireless ad-hoc networks, in: Wireless Ad-Hoc and Sensor Networks, 2004.  [16] [O.N. Tiwary, Detection of misbehaviour at MAC layer in](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0080) wireless networks, Int. J. Scient. Eng. Res. 3 (5) (2012) 909–912. |
| Hoc | networks, | | | in: | | Presented | | at | the | IEEE | | International | | |
| Conference | | on | | | Communications | | | | (IEEE | | ICC), | | Dresden, | |
| Germany, 2009.  [6] [M. Raya, J.P. Hubaux, I. Aad, DOMINO: detecting MAC layer greedy behavior in IEEE 802.11 hotspots, IEEE Trans. Mob. Comput. 5 (12) (2006) 1691–1705](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0030).  [7] S. Szott, M. Natkaniec, R. Canonico, A.R. Pach, Misbehaviour analysis of 802.11 mobile ad-hoc networks – contention window | | | | | | | | | | | | | | |
| cheating, | | in: | Med-Hoc-Net | | | | 2007, | | 12 | June | | 2007, | | Ionian |

Academy, Corfu, Greece.

[8] [C. Bouras, S. Charalambides, M. Drakoulelis, G. Kioumourtzis, K. Stamos, A tool for automating network simulation and processing tracing data files, Simul. Model. Pract. Theory 3](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0040)0 [(2013) 90–110, January](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0040).

[9] [P. Kyasanur, N.H. Vaidya, Selfish MAC layer misbehavior i](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0045)n

[17] A.A. Cardenas, S. Radosavac, J.S. Baras, Detection and prevention of MAC layer misbehavior in ad hoc networks, in: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, 2004, pp. 17–22.

[18] [G. Bianchi, Performance analysis of the IEEE 802.11 distributed coordination function, IEEE J. Select. Areas Commun. 18 (3)](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0090)

[wireless networks, IEEE Trans. Mob. Comput. 4 (5) (2005)](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0045). [(2000) 535–547](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0090).

[10] S. Szott, M. Natkaniec, A. Banchs, Impact of misbehaviour on QoS in wireless mesh networks, in: Proceeding NETWORKING‘09 Proceedings of the 8th International IFIP-TC 6 Networking Conference, P639-650, 2009.

[11] A.U. Salleh, Z. Ishak, N.M. Din, M.Z. Jamaludin, Trace

[19] Y. Rong, S.-K. Lee, H.-A. Choi, Detecting stations cheating on backoff rules in 80211 networks using sequential analysis, in: Proceedings of IEEE INFOCOM, 2005.

[20] [L.H.C. Tippett, On the extreme individuals and the range of samples taken from a normal population, Biometrika 17 (1925)](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0100)

analyzer for NS-2, in: 4th Student Conference on Research and [364–387](http://refhub.elsevier.com/S2210-8327(15)00023-X/h0100).