Applied Computing and Informatics (2017) 13, 1–9

Saudi Computer Society, King Saud University

Applied Computing and Informatics

(http://computer.org.sa)
www.ksu.edu.sa
www.sciencedirect.com

REVIEW ARTICLE

Real-time detection of MAC layer misbehavior in mobile ad hoc networks

Abdessadek Aaroud [a,*], **Mohammed-Alamine El Houssaini** [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*

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 introduces 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 ûcontrol chartý 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.

* Corresponding author.
E-mail addresses: aaroud.a@ucd.ac.ma (A. Aaroud), elhoussaini.m@ucd.ac.ma (M.-A. El Houssaini), elhore.a@ucd.ac.ma (A. El Hore), 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

Contents

1. Introduction

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 scheme of the IEEE 802.11 MAC layer misbehavior (greedy node). In the fifth section, the authors evaluate the performance of their approach using the NS2 simulator. Conclusions and perspectives are presented in the last section.

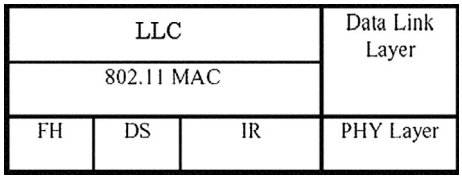

Figure 1 IEEE 802.11 layers description.

2. IEEE 802.11 layers

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 listens 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 mechanism of channel reservation Request To Send (RTS)/Clear To Send (CTS) [1].

The CSMA/CA access method defines the Binary Exponential Backoff (Fig. 2) in order to resolve the access medium problem when several stations want to transmit data simultaneously. This method requires that each station chooses a random 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.

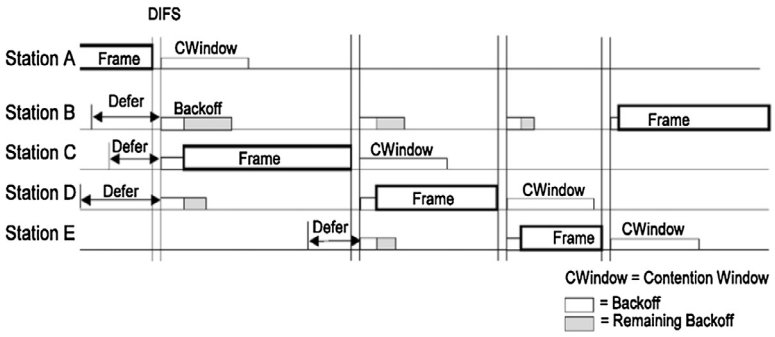

Figure 2 Backoff procedure.

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

- α misbehavior: The greedy node chooses the value of BEB in the interval [0 α(CW − 1)], where CW is the contention window, and $0 < \alpha < 1$.
- Deterministic BEB: The greedy node chooses a constant BEB independently of the contention window.
- β misbehavior: After a failed transmission, instead of putting a CW to be $\min\{2CW, CW_{max}\}$, greedy node sets its contention window as $CW = \max\{CW_{min}, \min\{\beta CW, CW_{max}\}\}$ where $0 < \beta < 2$.
- 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 statistical collection of all nodes RTS retransmission due to time out, packet retransmission due to ACK timeout and throughput 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 creates 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 engagement 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 in IEEE 802.11 Hotspots (DOMINO) deployed in the access point to detect misbehavior is exposed [6]. This method uses a modular architecture which comprises individual tests and a decision making component DMC. However, greedy nodes may exploit the knowledge of DOMINO in order to adapt its parameters to avoid the detection.

We propose in the following section a new detection strategy based on a statistical quality control approach (statistical 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 statistical process control has not been proposed before in the literature 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 $W_i = 2^i W$, where $i \in (0, m)$ is called "bachoff stage" and $W = CW_{min}$, $s(t)$ 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:

$$\begin{cases} P\{i,k|i,k+1\} = 1 & k \in (0, W_i - 2) \quad i \in (0,m) \\ P\{0,k|i,0\} = (1-p)/W_0 & k \in (0, W_0 - 1) \quad i \in (0,m) \\ P\{i,k|i-1,0\} = p/W_i & k \in (0, W_i - 1) \quad i \in (1,m) \\ P\{m,k|m,0\} = p/W_m & k \in (0, W_m - 1) \end{cases} \tag{1}$$

where

$$P\{i_1,k_1|i_0,k_0\} = P\{s(t+1) = i_1, b(t+1) = k_1 | s(t) = i_0, b(t) = k_0\} \tag{2}$$

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

$$\tau = \frac{2(1-2p)}{(1-2p)(W+1) + pW(1-(2p)^m)} \tag{3}$$

For n nodes using the shared medium,

$$P = 1 - (1-\tau)^{n-1} \tag{4}$$

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

The authors in [19] proposed a modeling of an 802.11 network with MAC layer misbehavior attacks. They consider n nodes in a network, with the presence of l greedy nodes modifying the backoff timer. The misbehaving nodes choose a random backoff interval in the range of $(0, g^a W - 1)$, where $(1 \leqslant a \leqslant l)$ and W is the current contention window (CW). The collision probability at the greedy node is p^a. Therefore they modified the stochastic process proposed in [18] to establish a simple modeling for the misbehaving nodes.

As a result they found the following equations with $2l + 2$ unknowns, $\tau^0, \tau^1, \ldots, \tau^l, p^0, p^1, \ldots, p^l$.

$$\begin{cases} \tau^0 = \frac{2(1-2p)^0}{(1-2p^0)(W+1)+p^0 W(1-(2p^0)^m)} \\ \tau^1 = \frac{2(1-2p)^1}{(1-2p^1)(g^1 W+1)+p^1 g^1 W(1-(2p^1)^m)} \\ \ldots \\ \tau^l = \frac{2(1-2p^l)^1}{(1-2p^l)(g^l W+1)+p^l g^l W(1-(2p^l)^m)} \\ P^0 = 1-(1-\tau^0)^{n-l-1}\prod_{1\leqslant i\leqslant l}(1-\tau^i) \\ P^1 = 1-(1-\tau^0)^{n-l}\prod_{2\leqslant i\leqslant l}(1-\tau^i) \\ \ldots \\ P^l = 1-(1-\tau^0)^{n-l}\prod_{1\leqslant i\leqslant l-1}(1-\tau^i) \end{cases} \quad (5)$$

The last equations can be solved to compute the unknown variables and also to define parameters adopted for the performance evaluation of the network. However, finding a closed form for each variable is not our goal, since our approach is based on simulation analysis.

4.2. Basic idea

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 between receptions (mean time between successive received packets) [3].

We showed that this misbehavior led to an increase of the average reception throughput and a decrease of times between receptions for the greedy nodes. On the other side it generates 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 by a control chart with two limits. These graphs are called control charts, following a statistical process control approach.

4.3. Statistical process control

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 detection. All variations on a system do not require modification. 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 dispersion [13].

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 ûcontrol chartý, 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 moving 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]

$$\mathrm{MR}_i = |x_i - x_{i-1}| \quad (6)$$

where the moving range number i is MR_i, and x_i is the range number i.

To establish a moving range control chart, the procedure is illustrated in the following section.

4.5. Development of the control chart

To calculate the control limits for individual values, we should use the below formulas [14]:

$$\mathrm{UCL} = \bar{x} + 3\frac{\overline{\mathrm{MR}}}{d_2} \quad (7)$$

$$\text{Center line} = \bar{x} \quad (8)$$

$$\mathrm{LCL} = \bar{x} - 3\frac{\overline{\mathrm{MR}}}{d_2} \quad (9)$$

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

$$\mathrm{UCL} = D_4\overline{\mathrm{MR}} \quad (10)$$

$$\text{Center line} = \overline{\mathrm{MR}} \quad (11)$$

$$\mathrm{LCL} = D_3\overline{\mathrm{MR}} \quad (12)$$

where UCL and LCL are the upper and lower control limits respectively, and $\overline{\mathrm{MR}}$ is the average of the moving ranges of two observations, x being the observation value.

The constants, d_2, D_3 and D_4 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].

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 $= \bar{x}$
Average moving range of observations (center line)	Center line $= \overline{\mathrm{MR}}$
Upper control limit of individual observations	$\mathrm{UCL} = \bar{x} + 3\frac{\overline{\mathrm{MR}}}{d_2}$
Lower control limit of individual observations	$\mathrm{LCL} = \bar{x} - 3\frac{\overline{\mathrm{MR}}}{d_2}$
Upper control limit of moving range observations	$\mathrm{UCL} = D_4\overline{\mathrm{MR}}$
Lower control limit of moving range observations	$\mathrm{LCL} = D_3\overline{\mathrm{MR}}$

4.6. Detection strategy

In this monitoring technique we propose supervising and plotting 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 detection scheme is performed at any receiving node for every transmitting 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.

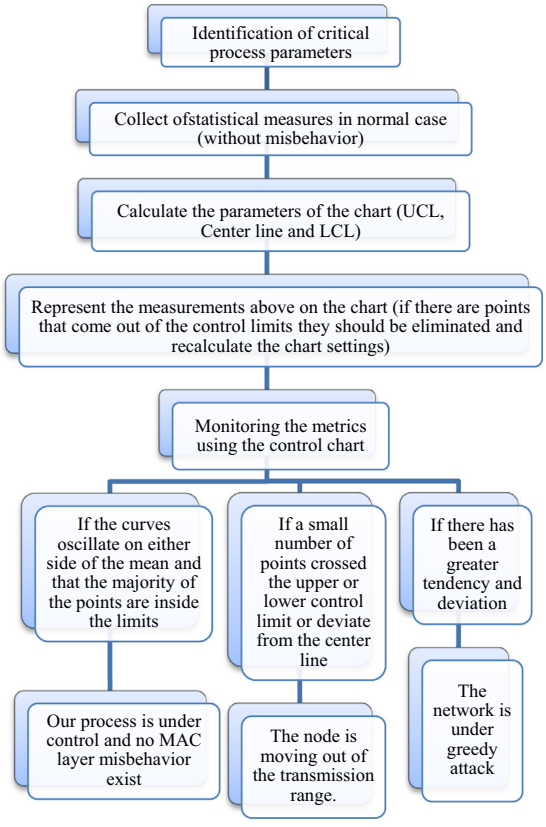

Figure 3 Block diagram of the detection scheme.

5. Performance evaluation

To achieve our detection method of the IEEE 802.11 MAC layer misbehavior [9], the simulator NS-2 can be used with some useful tools for processing traces files as explained by [8,11]. In our case we have chosen the simulator with the software 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).

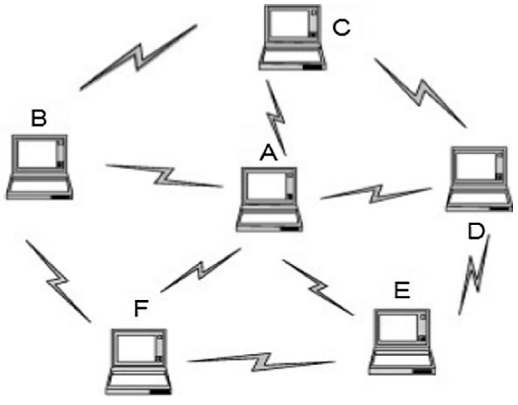

Figure 4 A mobile ad hoc network.

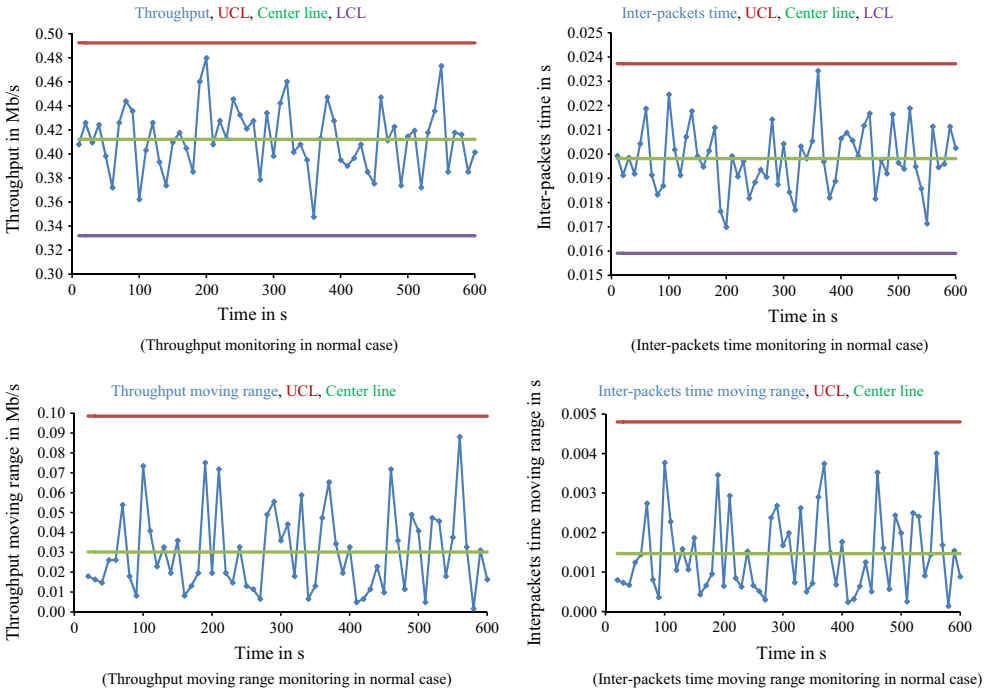

Figure 5 Control charts monitoring in normal case (without greedy attack).

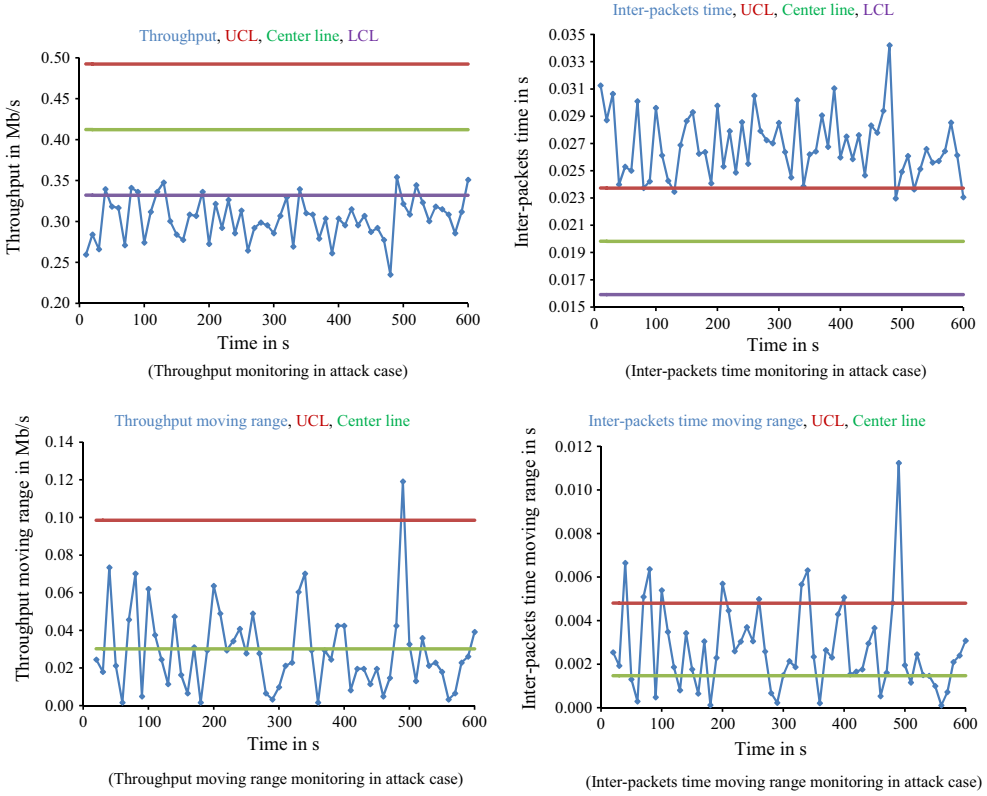

Figure 6 Control charts monitoring of the attacked.

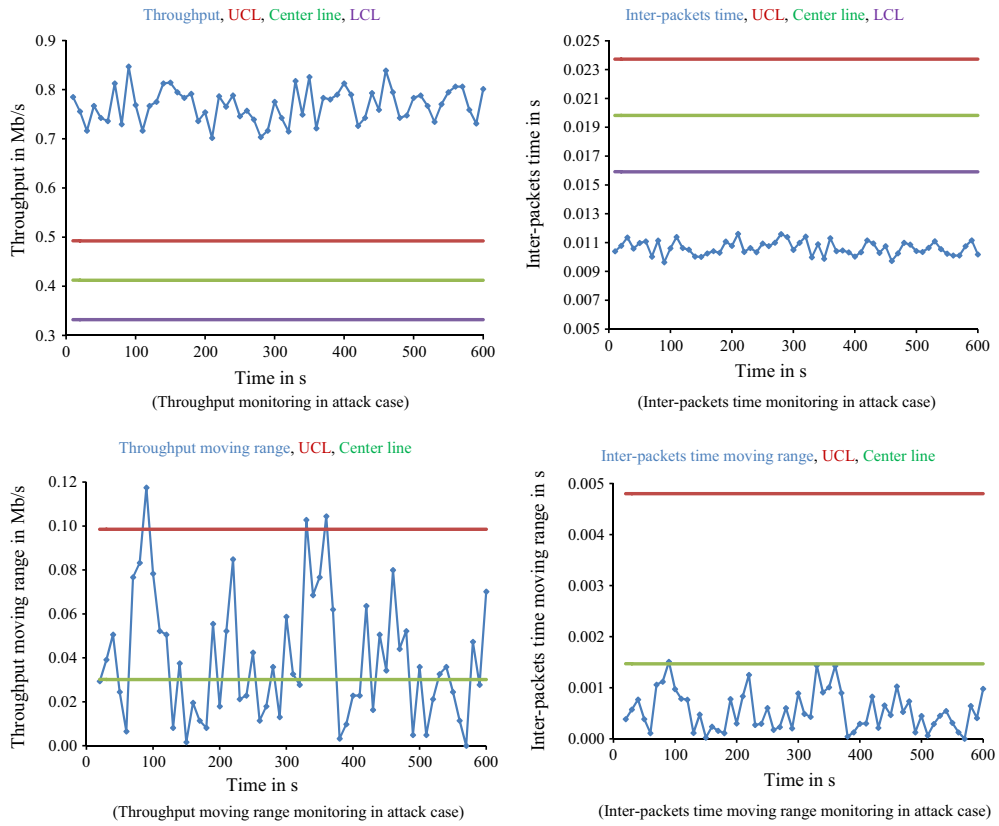

Figure 7 Control charts monitoring of the attacker.

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)	500 × 500
Transmission range (m)	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 monitoring	Shewhart control chart for inter-packets time monitoring
Individual measurement	UCL	0.49238	0.02372
	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

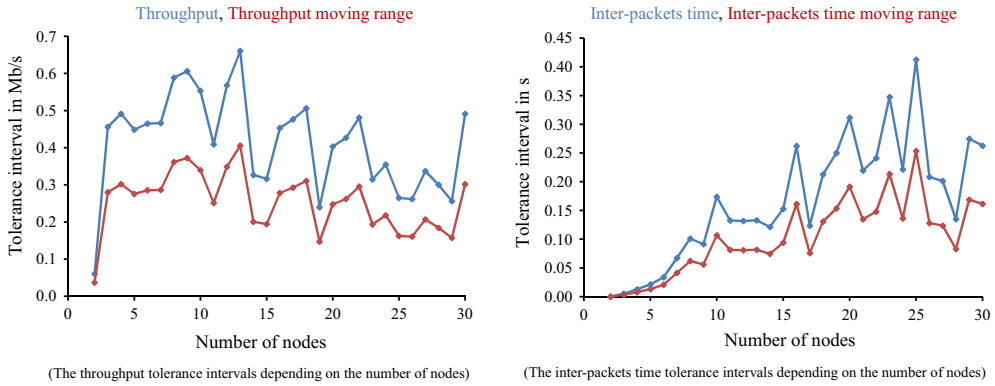

Figure 8 Tolerance intervals depending on the number of nodes.

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 (see Table 3).

5.3. Monitoring in the MAC layer misbehavior case

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 deviation. 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 curve crossed the lower control limit. There is a strong deviation, so we can decide that this node is a greedy one (this is the 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).

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.

6. Conclusion

The misbehavior at the MAC layer by changing the backoff mechanism can lead to performance degradation of the network. 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 presents 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.

References

[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/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.

[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. Naït-Abdesselam, Detecting greedy behaviors by linear correlation in wireless Ad 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.
[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 30 (2013) 90–110, January.
[9] P. Kyasanur, N.H. Vaidya, Selfish MAC layer misbehavior in wireless networks, IEEE Trans. Mob. Comput. 4 (5) (2005).
[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 analyzer for NS-2, in: 4th Student Conference on Research and 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 procédés 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.
[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 wireless networks, Int. J. Scient. Eng. Res. 3 (5) (2012) 909–912.
[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) (2000) 535–547.
[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) 364–387.