GDVAN: A New Greedy Behavior Attack Detection Algorithm For VANETs

Mohamed Nidhal Mejri*† and Jalel Ben-Othman*
*L2TI – Université Paris13, Sorbonne Paris cité, France
Email: [mejri; jalel.ben-othman]@univ-paris13.fr
†Communication System Laboratory Sys'Com, National Engineering School Of Tunis
University Tunis El Manar

Abstract—Vehicular Ad hoc Networks (VANETs), whose main objective is to provide road safety and enhance the driving conditions, are exposed to several kinds of attacks such as Denial of Service (DoS) attacks which affect the availability of the underlying services for legitimate users. We focus especially on the greedy behavior which has been extensively addressed in the literature for Wireless LAN (WLAN) and for Mobile Ad hoc Networks (MANETs). However, this attack has been much less studied in the context of VANETs. This is mainly because the detection of a greedy behavior is much more difficult for high mobility networks such as VANETs. In this paper, we propose a new detection approach called *GDVAN* (Greedy Detection for VANETs) for greedy behavior attacks in VANETs. The process to conduct the proposed method mainly consists of two phases, which are namely the suspicion phase and the decision phase. The suspicion phase is based on linear regression mathematical concept while decision phase is based on a fuzzy logic decision scheme. The proposed algorithm not only detects the existence of a greedy behavior but also establishes a list of the potentially compromised nodes using three newly defined metrics. In addition to being passive, one of the major advantages of our technique is that it can be executed by any node of the network and does not require any modification of the IEEE 802.11p standard. Moreover, the practical effectiveness and efficiency of the proposed approach are corroborated through simulations and experiments.

Index Terms—Vehicular Ad hoc Networks (VANETs), Greedy behavior, DoS attacks, Linear Regression, Fuzzy logic, IEEE 802.11p.

1 Introduction

VANET is an important use case of mobile networks in ad hoc mode. In this type of architecture, nodes connect automatically without the need of a preexisting infrastructure. VANET networks were designed primarily to improve road safety and provide comfort services for road users [1]. The life of the passengers is one of the factors involved, hence the critical importance of securing VANETs against any kind of attacks they can undergo. Compared to MANETs, VANETs present many other constraints such as the high mobility of nodes, the network topology changing and the short times of connection. However, different types of conventional attacks to which they are exposed ad hoc mobile networks are valid for VANET but the behavior of VANETs against these attacks is not the same.

As proposed in [2], attacks and vulnerabilities against VANETs can be classified into attacks on availability, integrity and data trust, authenticity, confidentiality and non repudiation. Attacks on availability are mainly formed by the Denial of Service (DoS) attacks family [3]. These attacks have catastrophic effects since they can lead to the partial or total loss of vital information. Their impact is generally measured by the proportion of the needed time to recover the VANET system to its normal status. DoS attacks can be achieved by external or internal malicious nodes to the network [3], [4]. Generally, the attacker aims to interrupt services for legitimate users. Thus, these services will be more available to him. In other cases, the purpose of conducting a DoS attack is just a challenge. Detecting and avoiding DoS attacks is a critical security requirement for VANETs whose main objective is to ensure the live of drivers and road users.

Multiple techniques can be used by malicious users/drivers to make the VANET experience service interruptions. In this study, we focus on greedy behavior which is a common DoS attack. It targets the operation of the MAC layer and exploits the weaknesses of the access method to the medium. A greedy node aims to minimize its waiting time for a faster access to the channel and therefore penalize the other honest nodes [5]. Then, it does not respect restrictions of the channel access method and tries always to connect to the medium and maintains it for its own use. The major problem of such attacks is that they can be performed by an authenticated user which makes the detection more complicated.

Generally, attacks based on a greedy behavior in VANETs exploits the weakness of the MAC layer. There are several techniques to carry out such attacks in practice including backoff manipulation, RTS/CTS frames scrambling, oversized NAV and DATA frames manipulation. Due to the high mobility of VANETs and also to the short connection duration times, the manipulation of the backoff mechanism has often been considered as the most efficient attack technique based on greedy behavior [6]. It allows a considerable reduction of the waiting time for the attacker [2]. Therefore, it is necessary to overview in what follows the IEEE 802.11p standard and how it can be exploited to perform a greedy denial of service attack.

VANETs use the band 5.850 to 5.925 GHz (with 75 MHz band wide) known as DSRC band (Dedicated Short Range

Manuscript received May 21, 2015; revised month day, 2015.

Communications) [7]. The DSRC band is divided into seven channels of 10 MHz: One *CCH* channel (Control CHannel) and six *SCH* channels (Service CHannels). DSRC specifications cannot be considered as a standardization for VANETs but a strict rules of frequency usage. As VANET architecture, IEEE proposes WAVE (Wireless Access in Vehicular Environments) which is a complementary set of protocols that allow to vehicles to work together. The WAVE protocol list is given in ITS standards fact sheet of IEEE updated in [8]. For the PHY and MAC layers, IEEE has added the standard IEEE 802.11p [9] to its 802.11 family to accommodate VANETs with DSRC and WAVE requirements. IEEE 802.11p standard defines the adaptation of the PHY and MAC layers of IEEE 802.11 [10] to be used in a vehicular wireless environment.

The MAC layer of IEEE 802.11p [9] uses EDCA (Enhanced Distributed Channel Access) which is an improvement of the former distributed coordination function DCF (Distributed Coordination Function) used in most of the standard IEEE Std 802.11 [10]. To ensure more likely to highly relevant safety messages, so they can be transmitted within a reasonable time in a VANET, the EDCA introduces in [11] the concept of *QoS management* through the notion of *Access Categories (AC)*. Four categories are defined according to the type of traffic: Background traffic (or AC0 BK), Best Effort traffic (BE or AC1), Video traffic (VI or AC2) and Voice traffic (VO or AC3). AC3 is considered with the highest priority.

EDCA uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) method as access channel method. In EDCA [12], [13], if a node is ready to transmit, it senses the medium. If the latter is free during an $AIFS$ (Arbitration Inter-Frame Space) period, the node must defer transmission by selecting a random backoff time. The EDCA 802.11p backoff procedure consists of the following steps:

(i) The node that wants to transmit selects a backoff value uniformly distributed in the interval $[0, CW]$, where the initial value of CW (contention window) is equal to CW_{min},
(ii) The value of CW increases (double + 1), if the transmission attempt fails until the CW reaches CW_{max} value, the maximum number of retry attempts is set to 7 (Table 1),
(iii) The backoff value will be reduced when the channel is idle,
(iv) If the value of backoff reaches 0, the node will send immediately.

The waiting time $AIFS_k$ for a category of access k is calculated as follows:

$$AIFS_k = SIFS + AIFSN_k * t_{slot}$$

where $t_{slot} = 13\mu s$ represent the time slot and $SIFS = 32\mu s$ represent the Short Inter Frame Space for IEEE 802.11p PHY OFDM ($10MHz$) as defined in [9].

Different $AIFSN$ (Arbitration Inter-Frame Space Number) and CW values are selected for different types of access ACs for each use case with the CCH and SCH, respectively Control and services channels. Table 2 presents all of these values which are calculated with the formulas given in [14].

It is easy to understand now that a greedy node can greatly increase its chances of access to the channel by reducing its backoff time. This is done by manipulating the CW_{max}, CW_{min} and $AIFSN$ values. There are other techniques to achieve a greedy behavior but in a high mobility environment, manipulation of backoff parameters remains feasible but more difficult to detect.

Retry	BK	BE	VI	VO
0	15	7	3	3
1	31	15	7	7
2	63	15	7	7
3	127	15	7	7
4	255	15	7	7
5	511	15	7	7
6	511	15	7	7
7	511	15	7	7

TABLE 1: Contention Windows values used for CCH [11]

	CCH			SCH		
AC	CW_{min}	CW_{max}	AIFSN	CW_{min}	CW_{max}	AIFSN
BK	15	511	9	15	511	7
BE	7	15	6	15	511	3
VI	3	7	3	7	15	2
VO	3	7	2	3	7	2

TABLE 2: EDCA parameters set used on CCH and SCH WAVE channels

Obviously, handling backoff parameters allows easily a greedy attack. A malicious node can for example choose a low value of backoff instead of random one. It can even choose zero and increases considerably its chances to access to the medium. To detect this kind of attack, we have developed an algorithm based on linear regression concept [15] for the suspicion phase and on a watchdog supervision software using fuzzy logic design for the decision phase. The proposed algorithm is able to suspect a greedy behavior in a VANET and determine the responsible nodes.

The rest of the paper is organized as follows. Section 2 runs through related work. Our detection algorithm is described in Section 3. Section 4 presents the simulation environment and the simulations for each phase. Section 5 discuses the obtained results. Finally, Section 6 concludes the paper and gives directions for future works.

2 RELATED WORK

The problem addressed by this paper is related to several research axes such as DoS attacks, MAC layer misbehavior, accurate detection metrics, fuzzy logic design, ad hoc networks and also greedy behavior attack especially for VANETs characterized by their high mobility and the short connection durations of nodes. To the best of our knowledge there are no actual work for MAC greedy behavior detection in VANET based on the IEEE 802.11p protocol. Most of the existing approaches only focus on MANETs based on IEEE 802.11 protocol and do not extend to the 802.11p protocol. This is in spite of the numerous solutions that have been proposed for MAC greedy behavior in wireless networks, for MANETs and Wireless Mesh Networks (WMNs). The proposed solutions can be classified into three families:

- *New MAC design based solutions* (or backoff algorithm modification): for this category, a new MAC layer is proposed to avoid backoff algorithm weakness

against greedy attacks. Examples of this category can be found in [16] and [17].

- *Monitoring-based solutions*: an additional component is added to detect greedy nodes, without any modification of the MAC layer. The proposed solution in both [18] and [5] are significant examples of this category.
- *Game theory-based solutions*: in this category, honest and malicious nodes are supposed adversaries in a fictitious game. Detection and reaction solutions against attacks are based on game theory. Examples of this category can be found in [19] and [20].

Raya et al. proposed in [6] a greedy behavior detection scheme called DOMINO, for infrastructured networks (IEEE 802.11 hotspots). DOMINO is a software system for detection of greedy behavior in IEEE 802.11 MAC layer for public networks. It is to be installed in the Access Point (*AP*), it can identify and detect greedy stations without any required modification of the standard protocol at the *AP*. It has the advantage to be transparent to network users. Given the lack of mobility, DOMINO can detect many kinds of manipulation techniques such as the reduction of backoff time, CTS and ACK delay and increase the NAV (Network Allocation Vector) time. Some significant improvements and deficiencies of DOMINO have been sufficiently demonstrated in [21].

Buchegger and Le Boudec proposed CONFIDANT [22]: a protocol called CONFIDANT for mobile ad hoc networks (MANETs) which is based on selective altruism and utilitarianism. It detects and isolates misbehaving nodes which refuse to cooperate with the other honest nodes of the network. CONFIDENT built routing decisions and trust relationships based on observation, experience, and reports on behavior of the other cooperating nodes. The proposed system can detect several types of attacks and thus honest nodes have the possibility to isolate misbehaved one from the network. Decisions are based on a reputation system. In fact, nodes have reputation records for first-hand and trusted second-hand observations.

FLSAC (Fuzzy Logic based Scheme to Struggle Against Adaptative Cheaters) has been proposed by Djahel et al [23]. FLASAC is an Enhancement of DOMINO scheme [6] but adapted to wireless mesh networks (WMNs). FLSAC focus the detection of greedy behaving or selfish nodes which aim to violate the proper use of the CSMA/CA protocol rules in order to increase their bandwidth at the expense of the well-behaving nodes. The proposed scheme can be implemented in such gateways or Mesh Routers to supervise attached wireless nodes behavior and also report any deviation from the proper use of the MAC protocol.

As an example of monitoring-based solutions Toledo and Xiaodong proposed a method to detect selfish misbehavior of nodes that may deliberately manipulate their backoff window to gain unfair access to the network resources [18]. They provided non-parametric sequential detectors and batch based on Kolmogorov-Smirnov statistics. This proposal does not require any modification on the CSMA/CA MAC layer protocol. They simulate their method under ns-2 to detect misbehavior in DCF based IEEE 802.11 standard. They evaluate the performance of their proposed detectors with perfect information optimum detectors. They claimed that their proposed non-parametric detectors have a similar performance compared to optimum detectors and this for the majority of the more severe misbehavior. The attacker model in this proposal is similar to our model and the honest nodes have any prior knowledge of the misbehavior strategies.

In [24], Buchegger et al. have studied several misbehavior detection and reputation systems that were proposed for mobile ad-hoc networks and based on direct observation mechanisms of the network behavior so-called watchdogs. They were mainly interested in the capabilities of the watchdog detection component in a real network and they presented their test-bed implementation of misbehavior detection.

Hamieh et al. [5] used the linear regression mathematical concept to detect MAC greedy nodes in an IEEE 802.11 based-protocol network (MANET). This method is based on the observation that successive access times of nodes are highly correlated. It was possible to represent the behavior of nodes in a network linearly. The calculated slope of the linear regression straight is used to assess the presence or absence of a greedy behavior. This proposition does not require any modification of the MAC layer of the protocol IEEE 802.11. In our algorithm, we have adopted a similar concept to distinguish between a normal VANET and a VANET under attack.

A careful analysis of the existing approaches reveals the lack of a greedy behavior detection scheme that takes into consideration the particular features of VANET. This was our major motivation to tackle this issue. Henceforth, in this paper we propose a new detection algorithm which distinguishes the presence of a greedy behavior and identifies the nodes that are suspected to be compromised using as input a short periodic traffic traces. The design and the functional description of the proposed algorithm are described in the sequel.

3 Proposed detection algorithm

3.1 Algorithm overview

The main goal of our algorithm introduced in [25] and depicted in Fig. 1 is to supervise the VANET. If a greedy behavior is suspected, the watchdog software determines the responsible nodes using three newly defined metrics. We identify these metrics to be suitable to greedy behavior in VANETs and after a deep study of the 802.11p MAC layer. In fact, according to several studies related to MANETs (Mobile Ad hoc Networks) [6] and [5], the packet delivery ratio, the queue length, the throughput and the backoff supervision can be used as metrics. However, these metrics are only efficient in the case of infrastructured or low mobility networks. In the VANET context, due to the high mobility of nodes and their short connection periods, we have argued that it is not practical to use the aforementioned metrics. We have chosen to supervise the number of connection attempts, the node connection durations and the average of waiting times between connections. In fact, a VANET

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2016.2577035, IEEE Transactions on Mobile Computing

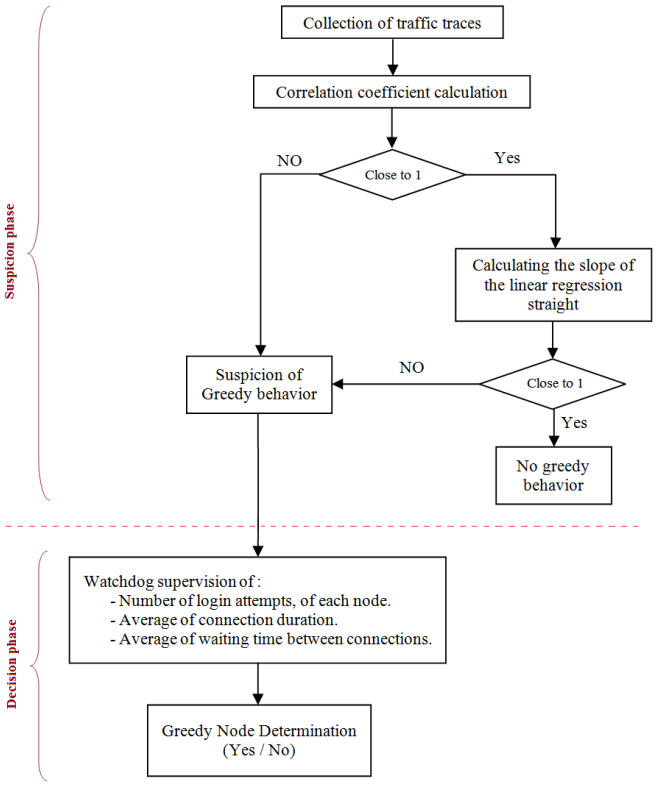

Fig. 1: The proposed detection algorithm.

greedy node has not enough time to perform adaptive manipulation of backoff parameters. Another characteristic is that it tries to connect to the network more often than honest nodes, also it maintains the medium much more time for its own profit and of course it has to reduce its waiting time between connections.

Thus, our main contribution is the design of *GDVAN*: a new greedy behavior detection algorithm for VANETs. *GDVAN* combines and enhances both linear regression and watchdog concepts to be suitable for VANETs. These two techniques have been used separately only for MANETs. Due to the high mobility in VANETs, we argue later that linear regression method is not totally suitable for VANETs. It can be only used for the distinction between a normal network behavior and a network under attack (suspicion phase). In *GDVAN*, the decision scheme uses the strength of design tools provided by the fuzzy logic theory to determine if a node is either greedy or it is honest. This way decrease the rates of both false positive and false negative. We detail in what follows the various components and the operation mode of respectively the suspicion and decision phases.

3.2 GDVAN suspicion phase

In a VANET, the nodes of the same WIBSS (Wave Independent Basic Service Set) share access to the transmission medium with respect to CSMA/CA access method managed by the MAC layer protocol which guaranteed a fairness access to all connected nodes. It was observed in [5] that for MANET the access times of active nodes are highly correlated. In a normal behavior of the network nodes (without greedy nodes), if the node N_1 connects to the support, the node N_2 has to wait and cannot connect until N_1 ends its transmission. Thus, the connection time of the node N_{i+1} linearly depends on connection time of the node N_i. The presence of one or more greedy nodes in the network violates this important access regulation rule.

To mathematically model the problem, we denote by t_i the connection time of the node N_i and by t_{i+1} the connection time of the node N_{i+1} that connects to the media just after N_i. We also denote by $\{ x_i \}$ the set of values taken by t_i and $\{ y_i \}$ the set of values taken by t_{i+1}.

The calculation of correlation coefficient is used to determine the dependence degree between the times of nodes connection. Statistically, this coefficient measures the dependence between two random variables [15]. In our case, we compute this coefficient for two random variables X and Y taking their values respectively in $\{ x_i \}$ and $\{ y_i \}$. The correlation coefficient takes values in the interval $[-1, 1]$. The values -1 and 1 indicate a strong correlation. Thus, more we move away from these two values more the dependency decreases. For MANET, it has been proved in [5] that in the case of existence of strong correlation, the relationship between the connection times can be expressed in a linear way for both normal or greedy behavior. However, the correlation coefficient is always close to 1. Also, the slope of the estimated linear regression straight is close to 1 for a normal network and higher in the case of greedy behavior. Thus, calculating the slope of the estimated linear regression straight can determine if we suspect the existence of a greedy behavior or not. Contrary for VANETs, we confirm the previous result only in the absence of greedy attack. Otherwise, this technique is no longer valid and the relationship between the connection times is rather random. In fact, due to their high mobility and short connection times, VANET greedy nodes have to access rapidly to support and maintain it as long as possible for their own use. Thus, connection times are never more correlated contrary to the case of MANETs. To solve this problem we have introduced the watchdog technique to monitor our newly defined metrics in order to report possible greedy attacks.

Thus, the *GDVAN* suspicion phase works as detailed in what follows in Algorithm 1:

As we need to compute the correlation coefficient in *GDVAN*, the method is detailed bellow.

3.2.1 Correlation coefficient

The correlation coefficient ρ measures statistical relationships between two random variables or observed data values [15]. It is defined as the covariance of the variables X and Y divided by the product of their standard deviations.

$$\rho = \frac{Cov(X,Y)}{\sigma_x \sigma_y} \qquad \rho \in [-1, 1]$$

To calculate ρ, and by definition, it is assumed that the values taken by connection times are random. Statistically, we define the two random variables X and Y as follows: If a node connects to the network at time t_n the next connects to time t_{n+1}. Thus X takes values in the set $\{ x_i \}$ of the connection times t_i of any network node, while Y in the set $\{ y_i \}$ of the connection times t_{i+1}. In the case of presence of correlation, the variables x_i and y_i represent respectively t_i and t_{i+1}, which can be connected by a linear relationship.

Algorithm 1: Suspicion phase

INPUT : T : Monitoring period, State_Greedy = FALSE.
OUTPUT: Annonce_Greedy(State_Greedy)

begin
  repeat
    1) Collect traffic traces during T,
    2) Calculate the correlation coefficient ρ
    if ρ *is close to* 1 **then**
      goto (3);
    else
      goto (4);
    end
    3) Calculate the slope of the linear regression straight,
    if *the slope is close to* 1 **then**
      State_Greedy = FALSE;
    else
      run (4);
    end
    4) A greedy behavior is suspected: Return and run the watchdog supervision tool.
    Return; Annonce_Greedy(State_Greedy)
  until *No existing communication*;
end

Therefore we have : $t_{i+1} = at_i + b$. The application of the method of linear regression can approach the values of the slope a and b.

If the calculated correlation coefficient is close 1, we need to calculate the slope a of the linear regression straight. An overview on the mathematical foundations and the method of calculating the linear regression parameters are detailed in the following.

3.2.2 The linear regression concept

The linear regression mathematical concept is a statistical method for finding functional linear relationship between two random variables X and Y. This functional relationship is a linear function of approximation.

Provided when X is given, Y is not completely determined; values scatter around a certain average value. When X varies, the values of Y describe a curve called the regression straight of Y with respect to X. Mathematically, the desired function is : $f(x) = E(Y/X = x)$.

Therefore, we have samples of n pairs of observations (x_i, y_i) that can be represented on a graph in the plane where each point i is a couple of observations with x_i on the x-axis and y_i on the y-axis. In practice, the samples formed a cloud of points (Fig.2(a)). We looked for a straight line $y^* = ax + b$ which describes well the trend of the observed cloud. We have: $y_i = ax_i + b + e_i$, where e_i is the error approximation called residues (Fig.2(b)), e_i is added to the value $y_i^* = ax_i + b$.

For a better approximation of the straight line $y* = ax + b$, we use the least squares method that consists to minimize the sum S of square residuals e_i:

$$S = \sum_{i=1}^{n} e_i^2 = \sum_{i=1}^{n} (y_i - ax_i - b)^2$$

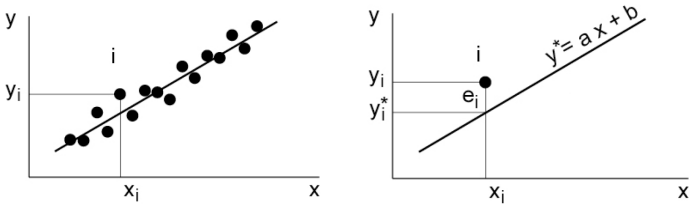

Fig. 2: (a) Cloud of linear regression points, (b) Approximated linear regression straight.

S is minimal if the partials derivatives with respect to a and b are zero:

$$\frac{\partial S}{\partial a} = -2\sum_{i=1}^{n} x_i(y_i - ax_i - b) = -2\sum_{i=1}^{n} x_i e_i = 0 \quad (1)$$

$$\frac{\partial S}{\partial b} = -2\sum_{i=1}^{n} (y_i - ax_i - b) = -2\sum_{i=1}^{n} e_i = 0 \quad (2)$$

The processing of equations (1) and (2) is used to calculate the values of a and b. In our algorithm, we are just interested in the calculation of the slope:

$$a = \frac{Cov(X, Y)}{Var(X)}$$

Whenever the calculated correlation coefficient or the slope of the linear regression straight is not close to 1 (with accurate authorized slight deviation), we run the watchdog monitoring tool based on fuzzy logic decision scheme which functioning is described below.

3.2.3 Watchdog supervision tool

In a network security context, and as defined in [24], watchdogs refer to several misbehavior detection and reputation tools that have been proposed for mobile ad-hoc networks and based on direct network observation mechanisms. In our case we supervise the greedy behavior in a VANET network. For this behavior, nodes do not respect MAC layer access method requirements by manipulating several parameters such as CW_{min}, CW_{max}, $AIFSN$ etc. Using these manipulations, an attacker is able to increase his chances of access to the support and penalize the other nodes.

In *GDVAN*, we suspect the existence of a greedy behavior in the two following cases:

1) The correlation coefficient is not close to 1.
2) The correlation coefficient is close to 1 and the slope of the linear regression straight is not close to 1.

VANETs are characterized by high mobility and relatively short connection times compared to ordinary ad hoc networks. Thus, the most effective way for a greedy behavior attacker is to disregard the backoff time and quickly try to connect before the other nodes. In addition, a greedy node tries to establish a high number of connections with an occupation time of the support higher than a normal node. Thus, our software monitors the following parameters:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2016.2577035, IEEE Transactions on Mobile Computing

1) The duration between two successive transmissions: The waiting time of a greedy node is almost close to zero.
2) Transmission time: a greedy node occupies the medium more than other normal nodes.
3) Connection attempts number of a node: a greedy node tries much more than the other nodes to connect to the network.

Other parameters can be monitored but for a high efficiency, rapidity and in order to simplify watchdog supervision tool, we have only maintained these parameters.

3.3 GDVAN decision phase

For decision making systems, where the membership of an element (node in our case) to a class (honest or greedy) remains proportional, fuzzy logic can be an efficient tool for design. In this work, we propose a new decision scheme for detecting greedy behavior suitable for VANETs. This scheme detects nodes which aim to violate the proper use of the CSMA/CA protocol rules in order to increase their bandwidth at the expense of the well-behaving nodes. As shown in Fig. 3, it used newly defined metrics which best convenient to highly mobile networks and can be used during short monitoring periods. Design details are given in the following.

As already explained, in our watchdog detection software, we have to supervise the following 3 newly defined metrics for each node in the VANET:

- The Number of connection attempts,
- The average of connection duration,
- The average of waiting times between connections.

From a fuzzy logic point of view, and for each parameter, we begin to suspect the existence of a greedy behavior from a certain value of the parameter (first threshold). Reaching a certain value of the parameter (second threshold) makes suspicion high enough. Between these two threshold values suspicion is gradual. So, our idea is based on the use of the tools provided by the fuzzy logic theory which help to solve this kind of problems.

Before detailing our scheme and the use of the three monitoring parameters, we introduce some basic facts about the fuzzy logic. It helps to understand some basics such as inputs, fuzzy sets, membership functions, inference and defuzzification (for more details refer to [26] and [27]).

3.3.1 Inputs, fuzzy sets and membership functions

As any system of data processing, our fuzzy logic-based scheme requires inputs to be processed to get results. We use the three inputs already described and supervised by the watchdog software after short collection periods. In a high mobility environment such as VANET, we have argued that these tree variables are the most accurate for suspecting a greedy behavior unlike other parameters used for MANET networks for example.

In the classical theory of sets, an element belongs or does not belong to a set. However, this basic concept does not satisfy some simple situations frequently encountered. By contrast, fuzzy set theory permits the gradual assessment of

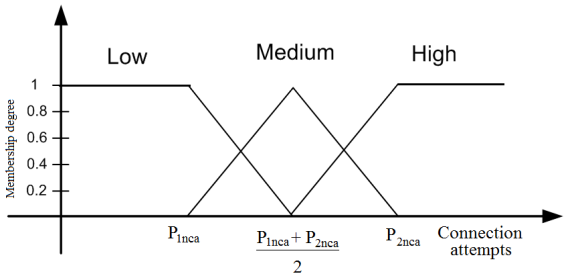

Fig. 4: Membership function of the number of connection attempts parameter.

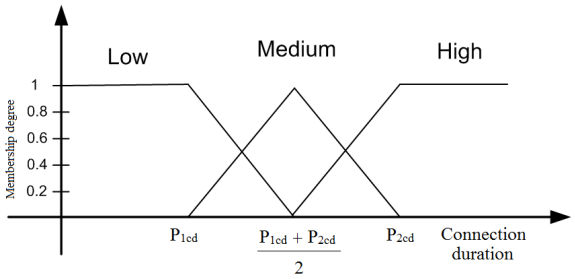

Fig. 5: Membership function of connection durations parameter.

the membership of elements in a set. In this theory, each element belongs partially and gradually to defined fuzzy sets. The contours of each fuzzy set are not "net", but "fuzzy" or "gradual". This can be described with membership function which takes values in the interval $[0, 1]$, while the indicator of classical function sets takes only 0 or 1. The fuzzy set theory is widely used in a domain where information is incomplete or imprecise.

The designer of a fuzzy logic based system has to clearly define his fuzzy sets. A fuzzy set is defined by its "membership function", which corresponds to the notion of "characteristic function" in classical logic theory.

3.3.2 Fuzzification and membership degree

Fuzzification step (or the determination of membership degree) is used to switch from real to fuzzy domain. It consists in determining the degree of membership of a input value (measured for example) to a fuzzy set. In our system, for each value of an input variable, we define its membership to one of the following chosen fuzzy sets "Low", "$Medium$" and "$High$", respectively denoted by L, M and H.

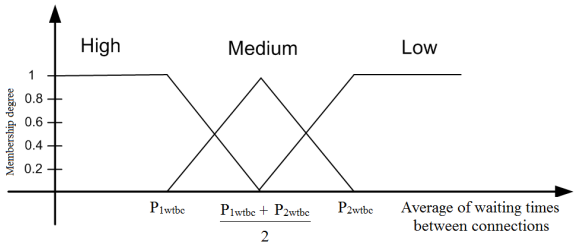

Fig. 6: Membership function of average of waiting times between connections parameter.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2016.2577035, IEEE Transactions on Mobile Computing

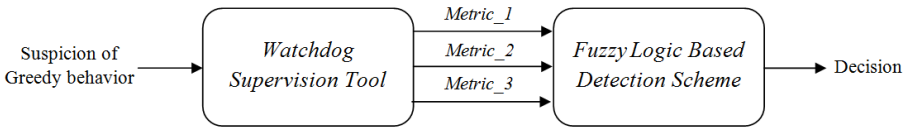

Fig. 3: Fuzzy logic based decision scheme

Mathematically, a fuzzy set S of an universe U can be defined by the membership function [28]:

$$M_S : U \longrightarrow [0, 1]$$

The degree of membership to the fuzzy set S is given by $M_S(e)$, for each element e of U. For our fuzzy scheme design, we choose the use of the trapezoidal method [27] for membership functions which is often used in such cases and is well appropriate for our conception, given that we use the three fuzzy sets "Low", "$Medium$" and "$High$". Our designed membership functions are given in Figures. 4, 5 and 6.

Parameter	Description
T	Monitoring period
N	Total number of vehicles. (we suppose that it is constant during the monitoring period).
T_{CA}	Number of total connections attempts during T.
T_{CD}	Total connections duration of all vehicles during T.
P_{1nca}	Threshold of connection attempts from which we begin to suspect greedy behavior.
P_{2nca}	Threshold of connection attempts from which we have a high suspected greedy behavior.
P_{1cd}	Threshold of connection duration from which we begin to suspect greedy behavior.
P_{2cd}	Threshold of connection duration from which we have a high suspected greedy behavior.
P_{1wtbc}	Threshold of waiting times between connections average from which we begin to suspect greedy behavior.
P_{2wtbc}	Threshold of waiting times between connections average from which have no suspected greedy behavior.
V_1	Number of connections attempts.
V_2	Connection duration.
V_3	Average of waiting times between connections.

TABLE 3: Description of the model parameters.

Furthermore, we need to define the parameters mentioned in Table 3 and used especially to specify the first and the second threshold for each supervised metric. More precisely, these parameters are defined as follows:

- $P_{1nca} = \frac{T_{CA}}{N}$: is the threshold from which we begin to suspect greedy behavior. If the number of connection attempts of a controlled node exceeds the average $\frac{T_{CA}}{N}$ then the node is suspected.
- $P_{2nca} = 0.7T_{CA}$: is the threshold from which we classify the controlled node as greedy. We determine statistically in our simulations that if a node reaches 70% of the total number of connections, then it is suspected as greedy.
- $P_{1cd} = \frac{T_{CD}}{N}$: is the threshold from which we begin to suspect greedy behavior. If the average of the total connections duration of a controlled node exceeds the total average of all nodes $\frac{T_{CD}}{N}$ then the node is suspected.
- $P_{2cd} = 0.6T_{CD}$: is the threshold from which we classify the controlled node as greedy. We determined statistically in our simulations that if a node reaches 60% of the total duration of connections, then it is suspected greedy.
- $P_{1wtbc} = min(AIFS_K)$: if the average of waiting times between connections of a controlled node is lower than $AIFS_K$ threshold, the node is greedy.
- $P_{2wtbc} = max(AIFS_K + CW_{max}.t_{slot})$: If the average of waiting times between connections of a controlled node reaches the maximum allowed waiting period for IEEE 802.11p which equal to $max(AIFS_K + CW_{max}.t_{slot})$, then the node is not suspected greedy.

3.3.3 Decision rules

In this step, we define the decision rules, what will determine the system outputs. A fuzzy rule allows to connect the inputs with the outputs. By the established rules, we classify the behavior of vehicles in one of the three classes: $Normal$, $Suspected$ and $Greedy$ respectively denoted by N, S and G.

The rules are formulated using the algorithmic formalism: $IF(condition), THEN(conclusion)$. The condition part uses the membership of each input to a fuzzy set and the conclusion part is the desired classification of vehicle behavior.

To compute the truth value of a condition (called also a predicate), of the form C is S, the membership function is used and the truth degree T_d of an attribute e is given by $T_d = M_S(e)$.

To better illustrate these concepts, we give the example shown in Fig. 7 which is similar to our membership functions (trapezoidal representation). The truth degrees of the values related to e_1 and e_2 are given in Table. 4. In this example, e_1 belongs to the class Low with a membership degree equal to 0.7 (70%), to the class

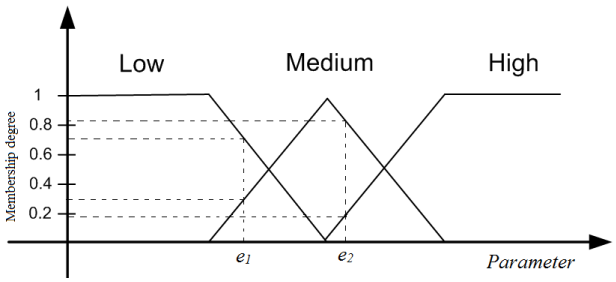

Fig. 7: Membership function illustration example.

$Medium$ with a membership degree equal to 0.3 (30%) and to the class $High$ with a membership degree equal to 0 (0%).

	L	M	H
e_1	0.7	0.3	0
e_2	0	0.81	0.19

TABLE 4: Degree of truth values of the illustration example

For two truth degrees T_{d1} and T_{d2}, Zadeh [26] has redefined the classical logical operators AND and OR to be suitable for fuzzy logic theory. Thus, the truth values can be calculated as following:

$$T_{d1}\ \ AND\ \ T_{d2} = min(T_{d1}, T_{d2})$$
$$T_{d1}\ \ OR\ \ T_{d2} = max(T_{d1}, T_{d2})$$

There are other definitions of AND and OR operators but Zadeh definition [26] is the most widely used one. In our case, at the end of each monitoring period, the three variables V_1, V_2 and V_3 mentioned above are selected for processing in order to define the final affiliation of a vehicle to one of the classes N, S and G. For each vehicle of the network, these variables are computed as follows:

$$CLASS = (V_1\ AND\ V_2)\ OR\ V_3$$

This gives:

$$CLASS = \max[\min(V_1, V_2), V_3]$$

The following tables summarize our classification rules. Table.5 summarizes the fuzzy rules of the formula: $CLASS1 = min(V_1, V_2)$ and Table.6 summarizes the fuzzy rules of the final formula $CLASS = max(CLASS1, V_3)$.

	V_1 :	L	M	H
V_2				
L		N	N	S
M		N	S	S
H		S	G	G

TABLE 5: Fuzzy rules of CLASS1 formula

	CLASS1:	N	S	G
V_3				
L		N	S	G
M		N	S	G
H		S	G	G

TABLE 6: Fuzzy rules of CLASS formula

3.3.4 Defuzzification

At the end of the inference, the fuzzy outputs are determined but they are not directly usable. It is necessary to move from "fuzzy world" to the "real world": It is the defuzzification step. Defuzzification is to provide an exact final value as a result of the end of treatment to help make a decision. This value is called *Crisp value* [27]. Several defuzzification techniques exist, the most used one is the method of center of gravity. With this method, the value of *Crisp* is calculated from the values of the area center of each fuzzy set. This value is given by the formula:

$$Crisp = \frac{\int cL(c)d_c}{\int L(c)d_c} \quad (3)$$

In the discrete domain and in the case of our system the formula (1) can be written as :

$$Crisp = \frac{\sum_{i=1}^{3} c_i L(c_i)}{\sum_{i=1}^{3} L(c_i)} \quad (4)$$

where:

- c_i: is the center of the area corresponding to the class i of node behavior (we have 3 nodes behavior classes).
- $L(c_i)$: is the node behavior membership level to the class i.

The development of the formula (2) gives:

$$Crisp = \frac{c_N L(c_N) + c_S L(c_S) + c_G L(c_G)}{L(c_N) + L(c_S) + L(c_G)}$$

Algorithm 2: Decision phase

INPUT : T: Monitoring period;
File: Collected_Trafic_File;
State_Class $\in \{N, S, G\}$
OUTPUT: Annonce_Decision(V_ID, State_Class)

```
begin
    Extract Vehicle_IDs existing in File during the T
    period,
    Extract N;
    Calculate: T_CD, P_1cd, P_2cd, P_1wtbc, P_2wtbc;
    foreach Vehicle ∈ {Vehicle_IDs} do
        Calculate: T_CA, P_1nca, P_1nca;
        Calculate: V_1, V_2, V_3;
        Calculate: Crisp;
        if Crisp > 50% for the class G then
            V_ID is G
        else
            if Crisp > 50% for the class S then
                V_ID is S
            else
                V_ID is N
            end
        end
        Return: Annonce_Decision(V_ID, State_Class)
    end
end
```

It is good to design new methods to solve problems as shown in both algorithm 1 and 2 respectively for the suspicion and decision phases, but it is better to test their effectiveness in realistic scenarios.

4 Performance Evaluation

4.1 Simulation environment

To evaluate the performance of both suspicion and decision phases which form the proposed algorithm, and for a maximum of reality, we used the ns-3 network simulator [29] as network simulator and *SUMO* [30] as a mobility

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2016.2577035, IEEE Transactions on Mobile Computing

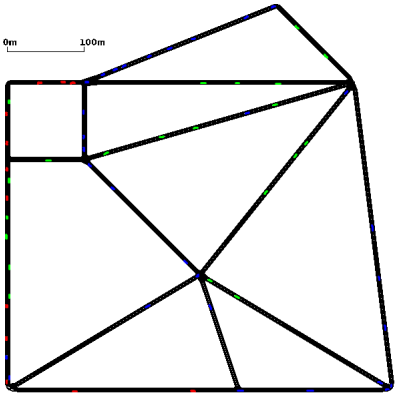

Fig. 8: The map of the urban area of simulation.

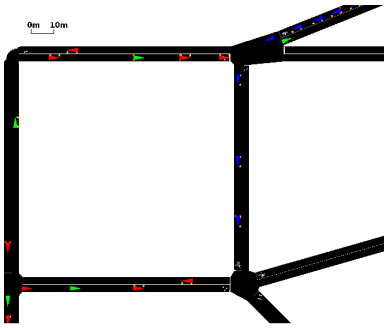

Fig. 9: Zoom on a part of the urban area of simulation.

simulator. We simulate a VANET composed of 40 nodes and the selected traffic model is *CBR* (Constant Bit Rate). Any node of the network can transmit at any time at a constant rate which is often the case in practice. The generated traffic is of type *WSMP* (Wave Short Message Protocol) and in accordance with the requirements of standards [31] and [11]. In fact, our algorithm is an executable code which can be executed by the On-Board Unit (OBU) of any node of the VANET. It is independent of the MAC layer and does not require any modification. Any honest node running *GDVAN* will be able to detect greedy nodes among VANET existing vehicles. For performance evaluation purposes, we simulate separately and respectively both suspicion and decision phases.

Parameter	Value
Environment	Dense urban
Network size	500m x 500 m
Node count	40
Average speed	36 Km/h ($\approx$ 10m/s)
Max speed	50 Km/h ($\approx$ 14m/s)
Execution time	From 10s to 40s
Sending capacity	6 Mbps
Packet size	Variable (max 1400 bytes)
Traffic model	CBR
Channel	CCH
Routing protocol	OLSR
Mobility simulator	SUMO
Traffic flow	40 $vehicles/s$
Traffic density	160 $vehicles/Km^2$
Correlation coefficient deviation	$\pm 10^{-4}$
Slope deviation	$\pm 10^{-1}$

TABLE 7: Simulation environment parameters.

The parameters of the simulation environment are described in Table 7. To ensure a maximum degree of efficiency of the statistical results we have repeated each simulation case about twenty times.

4.2 Mobility model

According to several studies [32], [33] and [34], the mobility model chosen for the simulation of a VANET network plays an important role in the accuracy of results. To the best of our knowledge and according to [32], there are no current open source simulator which can be used simultaneously to simulate IEEE 802.11p protocol with a real mobility model (using real vehicle motion and road map). However, there are combining solutions of simulators such as proposed in [35], where a mobility simulator such as SUMO and a protocol network simulator can be used together. In addition to the slowness, this kind of solution presents the drawback of the long procedure of data processing.

To avoid this disadvantage and for each simulated scenario, we generate our mobility traces file using SUMO simulator and we use them directly with ns-3. Based on a real city map with signs and traffic lights designed for this purpose shown in Figures 8 and 9, the mobility files contained the coordinates and the speeds of all the nodes at each instant. This technique is used instead of the predefined mobility model of ns-3 originally designed for MANETs, it allow of course a real simulation environment. The traffic flow expressed in $vehicles/s$ [36], which define the rate of vehicles insertion into the network is fixed to 40 vehicles, that mean all vehicles exist allover the simulation. The traffic density expressed in $vehicles/Km^2$ is 160 which is a normal value for a dense urban environment.

4.3 Simulation of the suspicion phase

First we have simulated a normal behavior of network nodes in a dense urban environment. We confirmed the application of the linear regression method for the detection of normal behavior (absence of greedy nodes). Fig.10 shows the correspondent obtained straight. The choice of the correlation coefficient and slope deviations are fixed respectively to 10^{-4} and 10^{-1}. These parameters have been chosen based on statistical observations of the different simulations cases. We showed in Fig.11 that nodes had almost the same chance to access the media and the maximum connection duration for one node connection has not exceeded $6ms$.

Among the several techniques developed to achieve greedy behavior in the MAC layer, the manipulation of backoff parameters is known as having the best effect [6] particularly for VANETs characterized by short connection duration where nodes have not enough time to perform adaptive manipulation. Then, in a second step, we have simulated the injection of respectively one, two, three and four greedy vehicles ($CW_{max} = CW_{min} = 0$). In fact, in a VANET and due to very short connection duration between nodes, it is not beneficial to perform a complicated attack. We suppose of course that normal nodes are majority, which is a realistic assumption in our case. Contrary to the network normal behavior, we observed that the connection times are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2016.2577035, IEEE Transactions on Mobile Computing

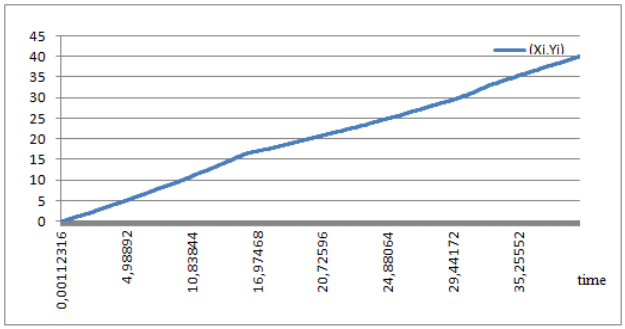

Fig. 10: Linear regression straight of a normal behavior without greedy nodes.

never more correlated. The correlation coefficient varies for all performed simulations in the interval $[-0.29; 0.29]$. Table 8 shown the effects of the greedy nodes injection for all the different simulated cases. These effects are characterized by the percentage of total occupied transmission time for each simulated scenarios. For example, one fully greedy vehicle uses approximately 66% of the total transmission time of the entire network, while four vehicles can reach together 75%. Figures 12 and 13 respectively for one and two injected greedy nodes show that the connections duration of these nodes were very high. For these suspected nodes and according to our proposed algorithm 1, if a greedy behavior is suspected, the algorithm 2 must be performed to determine the accuracy of suspicion and of course the responsible nodes.

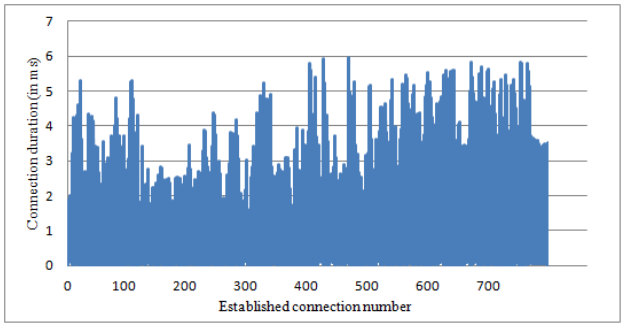

Fig. 11: Connection durations in a normal network (without greedy nodes)

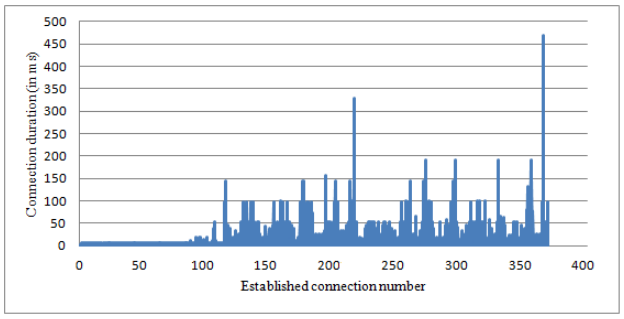

Fig. 12: Connection durations in a VANET with one greedy node.

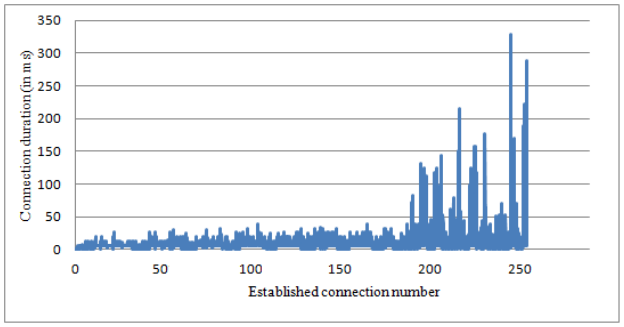

Fig. 13: Connection durations in a VANET with two greedy nodes.

Number of injected greedy nodes	Occupation percentage of the total transmission time
1	66%
2	69%
3	73%
4	75%

TABLE 8: Time occupation percentage and established connection number of greedy nodes.

4.4 Simulation of the decision phase

To evaluate the performance of the fuzzy logic based decision phase as detailed in the algorithm 2, we used also the same parameters and conditions as in the simulation of the suspicion phase. Using the collected traffic traces file and using our designed watchdog tool, which can be implemented in any network vehicle, we supervise the behavior of the other vehicles. Our fuzzy logic based decision scheme implementation is added to the watchdog tool and we supervised results for the effective injecting of respectively 1, 2, 3 and 4 greedy nodes. Simulation parameters are the same provided in Table 7. Obtained results are given and discussed in the following.

Our fuzzy logic based decision scheme for greedy behavior provided results as a percentage of belonging of a node to one of the Normal (N), Suspected (S) and Greedy (G) classes. In all performed simulations, the greedy nodes belong to the class G with a percentage greater than 95%. Fig. 14 shows the results of the distribution of the 40 vehicles to the classes N, S and G respectively for the four greedy injected nodes. Table 9 summarizes all the simulation

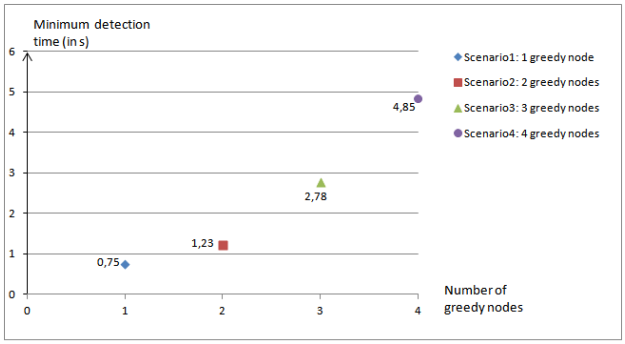

Fig. 15: Minimum detection times for the four simulation scenarios with 40 vehicles.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2016.2577035, IEEE Transactions on Mobile Computing

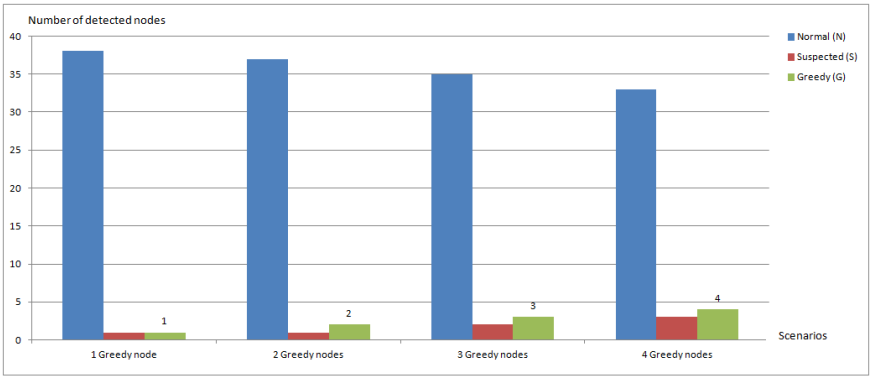

Fig. 14: Detection results for the four scenarios.

cases. For each scenario, figure 15 illustrates the minimum detection time required by the scheme to fully detect all the existing greedy nodes in the network.

Greedy nodes	Final decision: N	S	G
1	38	1	1
2	37	1	2
3	35	2	3
4	33	3	4

TABLE 9: Final decision results

5 Discussion

Compared to the normal operation, a VANET which contains one ore more greedy nodes can be distinguished using the proposed approach. At first, the suspicion scheme is able to state whether the global network behavior is normal or not. If a greedy behavior is suspected, the fuzzy logic decision scheme is able to confirm the assumption or deny it, and determine the compromised nodes using our monitoring metrics.

Through the realistic simulation scenarios described and discussed in the foregoing section, we demonstrated the feasibility, the effectiveness and the efficiency of our technique. In fact, we used the concept of linear regression to distinguish between a normal VANET, and a VANET under attack. Once the existence of a probable attack is confirmed, the three defined metrics are used to determine perfectly the nodes that exceeded the normal operating thresholds. Using our model in a dense urban environment, and for 40 vehicles for example, the minimum required detection times are $0.75s$, $1.23s$, $2.78s$ and $4.85s$, respectively for one, two, three and four greedy nodes.

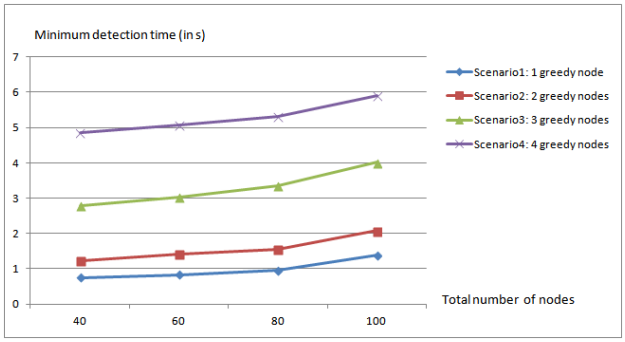

Fig. 16: Minimum detection times for the four simulation scenarios with 40, 60, 80 and 100 vehicles.

It can be observed from these four simulations scenarios that all the existing greedy nodes have been entirely detected. Furthermore, some other nodes have been classified in the intermediate class S. According to our decision rules, these nodes have momentarily exceed at least one of the fixed thresholds and they have to be supervised in the next monitoring period. Thus, it can be concluded from these results that for a VANET of 100 vehicles, a monitoring period of only 8 seconds is widely sufficient if we consider that most of nodes do not exhibit a greedy behavior, which is a realistic assumption. Moreover, the results confirm that our approach is very efficient and it was able to detect all greedy existing vehicles with a very high probability.

As it has been pointed out above, given the absence of existing models aiming at detecting and avoiding greedy attacks in VANETs, we have not been able to compare our experimental results (especially detection times) to a similar approach, but compared to the results of greedy behavior attack detection for MANETs obtained by [5], it turns out that our approach outperforms the existing detection algorithms.

Nonetheless, we draw the attention of the reader that the proposed approach has some limitations that are currently under study. In fact, the framework proposed in this paper is mainly directed towards the detection of greedy behavior based on the manipulation of the backoff mechanism. Our approach has to be extended in order to support other attack techniques including the scrambling of RTS/CTS frames and the manipulation of DATA frames. To this purpose, both phases of our detection process have to be slightly modified. For instance, a context-aware inspection scheme should be developed in order to detect the existence of RTC/CTS scrambling in the network. This can be implemented through a comparison of some key fields of these signaling messages with relevant information from the context, such as the neighborhood of the transmitting node, the average path length to the destination and the number of resource reservation requests per node. Such contextual information can lead to the detection of a greedy behavior in the network that can be more carefully analyzed

in the second step. Regarding the detection metrics and the corresponding thresholds, they should also be enriched and improved to support other greedy attack strategies. We are currently investigating the use of adaptive mechanisms (e.g., game theory, machine learning, control feedback loop) to make the decision thresholds adapt to the parameters of the context so that to support scenarios in which the attacker is aware of the parameters of the metrics and tries to evade the underlying detection scheme. These techniques can also be used to thwart cooperative attack scenarios.

6 Conclusion

Although the IEEE 802.11p MAC layer has been enhanced to fit VANETs requirements and despite all the advantages it offers, it remains vulnerable to many DoS attacks especially the greedy behavior. This attack is practically easy to achieve by simple manipulation of the backoff parameters. It can easily paralyzes a VANET and endangers the lives of road users. To deal with, we propose in this paper *GDVAN* (Greedy Detection for VANETs): A new algorithm for detecting greedy behavior in VANETs. *GDVAN* uses three newly defined metrics which were argued to be well appropriate for greedy detection in a high mobile environment such as VANET, where connections are short and nodes have not enough time to perform adaptive manipulation of backoff parameters. It is composed of both suspicion and decision phases respectively based on enhanced linear regression and fuzzy logic concepts. By monitoring network traffic traces, the algorithm is able to affirm the existence or not of a greedy nodes. In the affirmative case, it is able also to determine responsible nodes.

GDVAN has the advantages of being passive, non-resource-intensive and does not require changes in MAC layer. It has the advantage also to be transparent to users and it can be executed by any node of the network. The simulation results are quite promising and they confirmed the correctness of our choice of the metrics and the decision method design. Our objective in the future is the application of the proposed algorithm for the detection of other VANET denial of service attacks such as jamming. We aim also to develop a reaction method against greedy attacks in order to eliminate or mitigate their serious impacts.

References

[1] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[2] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET," *International Journal of Computer Science*, vol. 2, 2013.

[3] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[4] M. N. Mejri and M. Hamdi, "Recent advances in cryptographic solutions for vehicular networks," in *Networks, Computers and Communications (ISNCC), 2015 International Symposium on*. IEEE, 2015, pp. 1–7.

[5] A. Hamieh, J. Ben-Othman, A. Gueroui, and F. Naït-Abdesselam, "Detecting greedy behaviors by linear regression in wireless ad hoc networks," in *Communications, 2009. ICC'09. IEEE International Conference on*. IEEE, 2009, pp. 1–6.

[6] M. Raya, J.-P. Hubaux, and I. Aad, "Domino: a system to detect greedy behavior in IEEE 802.11 hotspots," in *Proceedings of the 2nd international conference on Mobile systems, applications, and services*. ACM, 2004, pp. 84–97.

[7] DSRC, "http://grouper.ieee.org/groups/scc32/dsrc/," 2013.

[8] ITS, "ITS standars fact sheets of IEEE, http://www.standards.its.dot.gov/factsheets/factsheet/80 seen in march 2014," 2013.

[9] "802.11p-2010 - IEEE standard for information technology - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (MAC) and physical layer (PHY) specifications amendment 6: Wireless access in vehicular environments," 11 June 2010.

[10] "802.11-2007 - IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (MAC) and physical layer (PHY) specifications." IEEE STANDARD, 12 June 2007.

[11] "1609.4-2010 - IEEE standard for wireless access in vehicular environments (wave)–multi-channel operation (revision of IEEE std 1609.4-2006)," 7 February 2011.

[12] Y. Wang, A. Ahmed, B. Krishnamachari, and K. Psounis, "IEEE 802.11 p performance evaluation and protocol enhancement," in *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on*. IEEE, 2008, pp. 317–322.

[13] S. Biswas, J. Misic, and V. Misic, "Ddos attack on wave-enabled vanet through synchronization," in *Global Communications Conference (GLOBECOM), 2012 IEEE*. IEEE, 2012, pp. 1079–1084.

[14] "1609.4-2006 - IEEE trial-use standard for wireless access in vehicular environments (wave)multi-channel operation," 29 November 2006.

[15] P.-a. Cornillon and É. Matzner-Løber, *Régression: théorie et applications*. Springer, 2006.

[16] P. Kyasanur and N. H. Vaidya, "Detection and handling of mac layer misbehavior in wireless networks." in *DSN*. Citeseer, 2003, pp. 173–182.

[17] A. A. Cardenas, S. Radosavac, and 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*. ACM, 2004, pp. 17–22.

[18] A. L. Toledo and X. Wang, "Robust detection of selfish misbehavior in wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 6, pp. 1124–1134, 2007.

[19] J. Konorski, "Multiple access in ad-hoc wireless lans with noncooperative stations," in *NETWORKING*. Springer, 2002, pp. 1141–1146.

[20] A. B. MacKenzie and S. B. Wicker, "Stability of multipacket slotted aloha with selfish users and perfect information," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3. IEEE, 2003, pp. 1583–1590.

[21] A. Cárdenas, S. Radosavac, J. S. Baras *et al.*, "Evaluation of detection algorithms for mac layer misbehavior: theory and experiments," *Networking, IEEE/ACM Transactions on*, vol. 17, no. 2, pp. 605–617, 2009.

[22] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2002, pp. 226–236.

[23] S. Djahel and F. Naït-Abdesselam, "Flsac: A new scheme to defend against greedy behavior in wireless mesh networks," *International Journal of Communication Systems*, vol. 22, no. 10, pp. 1245–1266, 2009.

[24] S. Buchegger, C. Tissieres, and J.-Y. Le Boudec, "A test-bed for misbehavior detection in mobile ad-hoc networks-how much can watchdogs really do?" in *Mobile Computing Systems and Applications, 2004. WMCSA 2004. Sixth IEEE Workshop on*. IEEE, 2004, pp. 102–111.

[25] M. N. Mejri and J. Ben-Othman, "Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks," in *Global Communications Conference (GLOBECOM)*. IEEE, 2014, pp. 4742–4747.

[26] L. A. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, no. 3, pp. 338–353, 1965.

[27] K. GEORGE J and Y. Bo, "Fuzzy sets and fuzzy logic, theory and applications," -, 2008.

[28] K. M. Passino and S. Yurkovich, *Fuzzy control*. Citeseer, 1998, vol. 42.

[29] NS-3, "ns-3, http:// www.nsnam.org/," 2013.

[30] "Simulation of urban mobility, http:// sumo.sourceforge.net/," 2013.

[31] "1609.3-2010 - IEEE standard for wireless access in vehicular environments (wave)networking services (revision of IEEE std 1609.3-2007)," 30 December 2010.

[32] F. J. Martinez, C. K. Toh, J.-C. Cano, C. T. Calafate, and P. Manzoni, "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)," *Wireless Communications and Mobile Computing*, vol. 11, no. 7, pp. 813–828, 2011.

[33] A. Mahajan, N. Potnis, K. Gopalan, and A. Wang, "Urban mobility models for VANETs," in *2nd IEEE International Workshop on Next Generation Wireless Networks*, 2006.

[34] A. K. Saha and D. B. Johnson, "Modeling mobility for vehicular ad-hoc networks," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004, pp. 91–92.

[35] F. K. Karnadi, Z. H. Mo, and K.-c. Lan, "Rapid generation of realistic mobility models for vanet," in *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*. IEEE, 2007, pp. 2506–2511.

[36] J. Luo and J.-P. Hubaux, "A survey of inter-vehicle communication," *EPFL, Lausanne, Switzerland, Tech. Rep*, 2004.

Mohamed Nidhal MEJRI Received his degree in Telecommunications Engineering in 2001 from the Tunisian aviation school "Borj El Amri". He obtained his DESS degree in security and cryptography in 2004 from the High School of Communications of Tunisia (Sup'Com). In 2012 he also obtained his Master in Electronic Systems and Telecommunication Networks from the Tunisian Polytechnic School. He passed prestigious the professional Cisco Certified Network Academy (all levels from 1 to 4), Cisco security and the Red Hat Certified Engineer. Since September 2001 he is a member of Tunisian army Crypto Lab. he directed several national software and hardware development projects in cryptography. On April 2013, he joined the L2TI laboratory of Paris 13 university as PhD student. He received his Ph.D. degree from the Sorbonne Paris cité (Paris 13 university), France, in 2016. His research interests are in the field of network security, cryptography, wireless ad hoc and vehicular networks.

Jalel BEN-OTHMAN Received his B.Sc. and M.Sc. degrees both in Computer Science from the University of Pierre et Marie Curie, (Paris 6) France in 1992, and 1994 respectively. He received his Ph.D. degree from the University of Versailles, France, in 1998. He was an Assistant Professor at the University of Orsay (Paris 11) and University of Pierre et Marie Curie (Paris 6), in 1998 and 1999 respectively. He was an Associate Professor at the University of Versailles from 2000 to 2011. He is currently full professor at the University of Paris 13 since 2011. Dr. Ben-Othmans research interests are in the area of wireless ad hoc and sensor networks, Broadband Wireless Networks, multi-services bandwidth management in WLAN (IEEE 802.11), WMAN (IEEE 802.16), WWAN (LTE), VANETS, Sensor and Ad Hoc Networks, security in wireless networks in general and wireless sensor and ad hoc networks in particular. His work appears in highly respected international journals and conferences, including, IEEE ICC, Globecom, LCN, MSWIM, VTC, PIMRC etc. He has supervised and co-supervised several graduate students in these areas. He is widely known for his work on wireless ad hoc and sensor Networks, in particular, security. He gave several talks on these topics, as Keynote in conferences Road Transportation System Strategy and Standardization (Korea), WCCCS13, NSERC DIVA Distinguished Lecture Series (Canada), P2MNET10, PEDISWESA09, and as invited talks in GIST (Korea), Seoul National University, KRRI (Korea), USTHB (Algieria), Fes University (Marocco), Hanoi Science and Technology University (Vietnam), Reims (France), Martinique (France), University of Ottawa (Canada), INRS (Canada), Gliwice (Pologne)...

He is an editorial board member of Wiley Wireless Communications and Mobile Computing (WCMC), Wiley Security and Communication Networks (SCN), Inderscience Int. J. of Satellite Communications Policy and Management, IEEE comsoc Journal of Communications and Networks (JCN) and International Journal On Advances in Networks and Services IJANS. He is also an Associate Editor of Wiley International Journal of Communication Systems (IJCS). He has served as a member of Technical Committees of more than 80 international IEEE/ACM conferences and workshops including ICC, Globecom, MSWIM, LCN. He is a member of IEEE and ACM.

He served as Local Arrangement Chair for the 13th IEEE International Symposium on Computer Communication (ISCC 09). He served as a TPC Co-Chair of IEEE Globecom Wireless Communications Symposium (Globecom 2010) and 9th international Workshop on Wireless local Networks (WLN09) and 10th international Workshop on Wireless local Networks (WLN10). He served as a publicity chair of several conferences such as the 12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 09), IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WOWMOM 2010), 25th Biennial Symposium on Communications. He has served as TPC Co-Chair for IEEE Globecom Ad hoc and Sensor and and Mesh Networking (Globecom 2011, 2014), 6th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2010, 2011, 2012), Wireless Networking Symposium of The 7th International Wireless Communications and Mobile Computing Conference (IWCMC 2011, 2012, 2013, 2014), IEEE International Conference on Communications Ad hoc and Sensor and and Mesh Networking (ICC 2012, ICC 2014). He has served for other conferences in ICNC, WSCP, CNIT. He has also served as Tutorial chair for Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS 2014). He was the secretary and he is currently Vice chair of the IEEE Ad Hoc and sensor networks technical committee since January 2012. He is an active member of IEEE CIS-TC, and WTC.