An Enhanced Active Sybil Detection Algorithm and its Impact on the Reliability of Safety Applications in VANET

Mohamed S. Mohamed
Department of Computer Engineering
Military Technical College
Cairo, Egypt
mohamedms@mtc.edu.eg

Axel Krings
Department of Computer Science
University of Idaho
Moscow ID, USA
krings@uidaho.edu

***Abstract*—Safety applications as a part of modern Intelligent Transportation Systems (ITS) play an important role in reducing vehicle accidents. These applications rely on Vehicular Ad Hoc Networks (VANET) for communication and need to be secure to provide reliable services. A particularly severe attack in VANET is the so-called Sybil attack, in which a malicious node pretends to be one or more fake nodes. Several methods have been suggested to counter this type of attack, however these methods were based on some assumptions that may be not realistic. This research proposes an enhanced active Sybil attack detection algorithm that can be used in both static and dynamic power environments. It uses short detection packets to analyze medium access behavior of nodes. The algorithm can control how often detection packets are sent and it can tune packet duration to minimize overhead. The algorithm's impact on the reliability of safety application is presented. The results from field experiments show that the proposed algorithm can improve the reliability of safety applications against Sybil attacks.**

***Index Terms*—VANET, Safety Applications, Sybil Attack**

I. Introduction

Connected vehicle technology uses wireless communication to share information between vehicles and the infrastructure. This requires that vehicles are equipped with an On Board Unit (OBU) for Vehicle-to-Vehicle (V2V) communication, and the infrastructure to be equipped with a Road Side Unit (RSU) for Vehicle-to-Infrastructure (V2I) communication. These devices together can establish a Vehicular Ad Hoc Network (VANET). Vehicles in this network are broadcasting beacon messages at fixed intervals containing vehicle information, such as speed, location, and brake status. The messages are used by Dedicated Short Range Communications (DSRC) safety applications, which are considered to be the most critical applications, aiming at reducing traffic accidents. Securing these messages is crucial, as false or absent information could lead to safety application failure, potentially resulting in accidents causing injuries and death. A severe threat in VANETs is the so-called Sybil attack, in which a malicious vehicle acts as multiple vehicles by using fake or stolen IDs. The main purpose of such attacks is to give the illusion of a traffic jam or more importantly, to fool the DSRC safety applications to use values of fake vehicles, called Sybil vehicles (Sybil nodes), in order to manipulate their decision process.

As security is perhaps the greatest challenge facing the deployment of VANET [1], this research focuses on developing solutions to increase reliability of safety applications in the presence of faults and attacks. It is based on the work in [2], where an active detection algorithm was presented that is capable of detecting different attack scenarios using so called detection packets, which in turn helped improve the resilience of safety applications to Sybil attacks launched by rouge nodes. Extending the approach in [2], the main contributions of this paper are: 1) The impact of the frequency and duration of detection packets on Sybil node detection is analyzed. 2) An enhanced algorithm using these two metrics is presented, and its impact on DSRC safety application reliability is shown.

II. Background and Related Work

V2V and V2I communication uses DSRC, with an allocated bandwidth of 75 MHz at 5.9 GHz, divided into seven channels [3]. There is one Control Channel (CCH) (CCH178), and six Service Channel (SCH) (CH172, 174, 176, 180, 182, and 184). CH172 is the most important channel and is reserved for V2V public safety communications. A beacon message called Basic Safety Message (BSM), is broadcast periodically with a rate of 10 BSMs per second on this channel. It is the most critical message and is used in a variety of DSRC safety applications to exchange information about the status of the vehicle [4]. A BSM has two parts. The first part is mandatory and contains data such as message ID, GPS coordinates, speed, heading, and brake system status. The second part is optional, transmitted less frequently, and may include additional information for certain applications.

A number of DSRC safety applications, such as Forward Collision Warning (FCW), Intersection Movement Assist (IMA), and Emergency Electronic Brake Lights (EEBL), have been proposed in [5]. These applications use the information contained in BSMs received from surrounding vehicles to alert drivers about impending dangers. The EEBL application is considered for this research. It enables a Remote Vehicle (RV)

to broadcast an emergency brake event to surrounding RVs. Upon receiving such event, a Host Vehicle (HV) determines the relevance of the event and provides a warning to the driver, if appropriate. EEBL is helpful in situations where the line of sight is blocked, e.g., due to adverse weather conditions, or another vehicle. Figure 1 shows the EEBL timing model. Assume the driver of the RV brakes hard at time t_{brake}, e.g., due to an observed hazard. The time interval T_{brake} defines

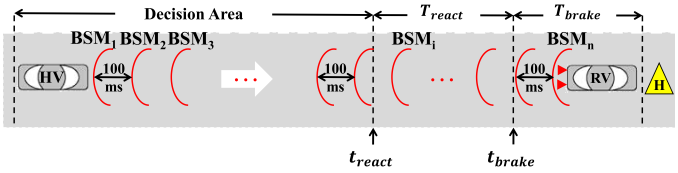

Fig. 1. Timing model of EEBL safety application

the time during which the RV sends BSMs indicating this braking event e to all vehicles in its transmission range. It should be noted that a lower case t denotes an instance of time, whereas an upper case T denotes a time interval. The EEBL application, installed in the OBU of the HV, checks received BSMs for event e, and warns the driver accordingly. This warning has to be issued early enough to allow the driver to react, i.e., before time t_{react}. The typical reaction time T_{react} is within 0.9 to 1.2 seconds [6].

The OBU implements the networking protocol stack. After a packet to be sent is created, it is placed in the First-in First-out (FIFO) transmission queue [7], [8]. Once the medium is free for an Arbitration Interframe Space (AIFS), the node selects a random backoff time to delay the transmission, before the packet is taken from the queue to be transmitted. However, if the node does not get a chance to send its packets, newly arriving packets will be added to the transmission queue. This could go on until the queue overflows. Depending on the queue size and the scheduling strategy used, queuing may result in packet delays or even worse, drops.

The literature on detecting Sybil attacks in VANET will be presented by their respected approaches, as introduced in [2].

A. Resources Testing

The objective of resource testing is to detect inconsistencies in the amount of resources used by a number of nodes, e.g., including Sybil nodes. This method falls into three categories. The first category is *Radio Resource Testing*, presented in [9]. In this method, the node that wants to detect a Sybil nodes assigns a channel to each neighboring node to broadcast messages and randomly chooses a channel to listen. If it is a legitimate node, it should receive the message and response on the same channel. Otherwise, the malicious node can not send a response message for its Sybil nodes simultaneously on different channels. The second category is *Computational Resource Testing*. When a node wants to detect Sybil nodes it sends a puzzle to be solved to all nodes. As the malicious node and its Sybil nodes share resources, nodes failing to solve a puzzle are marked as Sybil nodes [10]. Finally, *Identification Resource Testing* is discussed in [11]. Here a node can detect Sybil attacks by saving the Medium Access Control (MAC) addresses of neighbor nodes in a list. If a node is detected with a MAC address not recorded in this list, it is identified as a Sybil node. None of these methods are applicable in VANET.

B. Ranging Methods

Two categories of ranging methods were proposed to calculate the distance between a transmitter and a receiver:

1) Received Signal Strength Indicator (RSSI): The authors in [12] [13] proposed a Sybil attack detection approach based on the Received Signal Strength Indicator (RSSI) propagation model. The receiving nodes rely on the received signal strength to estimate the distance of the sending node. If this estimated distance appears to be inconsistent with the distance implied by the nodes' GPS coordinates, the sending node is considered suspicious. A method consisting of two complementary techniques, assuming all nodes use identical transmission power, is described in [14]. In this method, first RSSI is used to calculate the distance between the sending and receiving nodes using the Friis model. If incoherent signal strengths are observed, the second technique, which uses what so-called "distinguishability degree metric", is invoked. This metric is computed based on tracking the differences of two nodes over a certain time.

However, these approaches can be fooled by an intelligent attacker who can manipulate the transmission power level to appear consistent with the GPS coordinates.

2) Time-Based Methods: Time-based methods such as Time Of Arrival (TOA) and Time Difference Of Arrival (TDOA) are presented in [15], [16]. Here the estimated distance between two nodes is based on the signal propagation time. However, this requires an accurate real-time clock synchronization between the transmitter and the receiver, which may not be a realistic assumption in VANET [17].

C. RSU-Based Methods

The "Robust method of Sybil Attack Detection" (RobSAD) for urban VANETs is introduced in [18]. This approach assumes that authorized RSUs are distributed over the area. If RSUs see sybil vehicles in the same group (location and direction) all the time, it is considered abnormal behavior. Each RSU broadcasts timestamped digital signatures. Honest vehicles that move independently will have unlike trajectories. These trajectories are calculated based on signatures collected from authorized RSUs. Detection of Sybil nodes is done by analysis of the neighboring vehicles' signatures.

In [19] Sybil attack detection is presented based on timestamps using the RSU, under the assumption that it is improbable that two vehicles pass by different faraway RSUs at same time. Messages sent from Sybil nodes will contain similar series of timestamps. This suspicious behavior triggers Sybil attack detection. However, Sybil attack detection might be difficult or even impossible, if too few RSUs are installed that could observe abnormal behavior.

D. Collaboration-Based Techniques

A collaboration technique is proposed in [20] based on periodic exchanges of information between nodes. Specifically, nodes exchange data about their neighbors with other nodes. The intersection of these sets of neighbors is computed by each node. The assumption is made that it is unlikely for two nodes to have the same set of neighbors for a time exceeding a specific threshold. Accordingly, if similar neighbors are observed by a node over a long time, the matching neighbors are marked as Sybil nodes. However, this approach adds more communication overhead by sending extra messages and it has limited detection capabilities.

E. Cryptography and Authentication-Based Mechanisms

Mechanisms to prevent Sybil attacks using public key cryptography and authentication are proposed in [22] and [23]. This asymmetric cryptography is based on a combination of signatures and digital certificates, issued by a Certification Authority (CA). Secure communications between CAs is established to keep track of issued digital certificates. Any message with invalid certificate is rejected and only valid messages are considered. However, this mechanism introduces time delays and it is required that each vehicle be assigned only one certificate at a time. The latter could raise privacy concerns as certificates should be changed frequently.

III. Attack Model

The attack model for this research will be described using the scenario shown in Figure 2, which shows two honest RVs, an HV, and a malicious vehicle M simulating four Sybil vehicles. Each RV sends a BSM every 100ms. The malicious

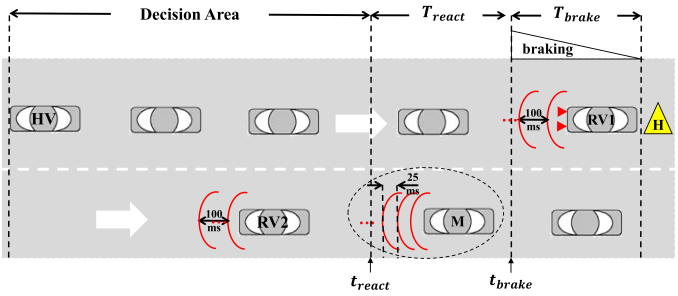

Fig. 2. Attack scenario [2]

vehicle sends with transmission rate of 4 BSMs/100ms, as it is impersonating four (non-existing) vehicles. The attacker gives each Sybil vehicle different IDs and manipulates their real transmission power to be consistent with the GPS coordinates of the spoofed positions. Suppose that the driver of RV1 brakes hard due to a hazard. This event e is included in it's subsequent BSM "brake flag". As in [26], [27] assume the HV executes an EEBL safety application using a voting scheme. The main idea of these voting schemes is to see if a certain threshold of vehicles in the area of RV1 react consistently with the event. The danger is that the HV's vote can be manipulated by the malicious vehicle, e.g., by having its Sybil vehicles inject BSMs opposing the event. Almost all Sybil detection algorithms, especially those which are based on RSSI, fail to resolve this situation.

IV. Proposed Algorithm

We now propose a probabilistic Enhanced Active Sybil Detection Algorithm (EASDA), based on the ability to detect a BSM delay induced by a Detection Packet (DP) [2]. The objective of this DP, which is a bogus packet of predefined duration τ, is to examine if targeted vehicles delay sending their BSMs due to queuing. Queuing is due to the vehicle not being able to access the medium during the DP's emission. The time between two consecutive DPs is specified as period T. Detection is based on the observation in the targeted vehicle's queue, i.e., if it queues its BSMs or not. In this algorithm Sybil attacks can be detected based on two cases. In the first case the Sybil vehicles are assumed to be placed between the HV and the malicious vehicle, while in the second case the malicious vehicle is placed between the HV and any Sybil vehicles. From these two cases we can deduce all other cases. Thus, if the malicious vehicle is in-between Sybil vehicles, we can divide the Sybil vehicles into two groups, those between the HV and malicious vehicle, as in the first case, and the rest form the scenario of the second case. These scenarios will be further discussed later.

Algorithm 1 Probabilistic EASDA

```
Initialize BL= ∅; ϵ = 1;
START: Receive BSM from a suspecting vehicle
Mark vehicle as "potential Sybil";
Calculate distance d;
Determine τ and T;
Calculate P_snd and send DP(P_snd);
if (BSM delay <δ_t) then
    Is Sybil with prob q or Honest with prob 1 − q;
else
    Calculate P'_snd and send DP(P'_snd);
    if (BSM delay < δ_t) then
        // Not helpful to determine if Honest/Sybil;
    else
        Mark vehicle "Sybil" and set ϵ = 0;
        Add vehicle to blacklist BL;
    end if
end if
ϵ = ϵ(1 − q); // consider prob. that DP did not overlap
if Detection uncertainty ϵ > specified value then
    Goto: START;
else
    Stop Algorithm;
end if
```

The detection algorithm is shown in Algorithm 1. In order to keep track of illegitimate (Sybil) vehicles, a Blacklist (BL) is defined locally, which is initially empty. BL stores the vehicle IDs of detected Sybil nodes. Once a BSM from a

suspecting vehicle is received, the algorithm calculates the distance, d, between the HV and the suspected vehicle. The GPS coordinates included in the received BSM, which may be spoofed, is used to calculate d. The variables τ and T need to be determined next. The values of the variables are affected by the number of vehicles in the neighborhood and d. As large values of τ are highly disruptive and can result in a self-induced DoS, it is desirable to have shorter durations, which however reduce the probability of detection. This can be compensated by increasing the frequency of sending a DP, i.e., a reduction in T. How τ and T are determined and the trade off associated with their values will be discussed later in Section V. The time available for the algorithm to detection a Sybil node will be the time it takes the HV to reach the suspected node, minus the reaction time, i.e., $T_{detect} = d/V_{HV} - T_{react}$. Any detection after that duration will be too late. The transmission power P_{snd} of DP is computed using

$$P_{snd} = S \times d^2/G \tag{1}$$

where S is the receiver sensitivity of the suspected vehicle, which is assumed to be known, and G is the gain. This gain is calculated as in [28] to be

$$G = G_{snd} \times G_{rcv} \times \lambda^2/(16\pi^2) \tag{2}$$

where λ is the wavelength, and G_{snd}, G_{rcv} are the send and receive gains, which are assumed to be known. The DP is sent with transmission power P_{snd} and for duration τ.

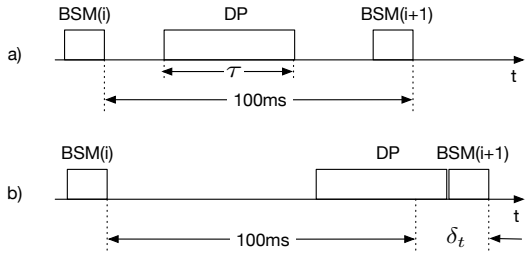

Fig. 3. BSM delay due to DP

The following two scenarios can occur. 1) DP does not interfere with the timing of BSM transmission, as shown in Figure 3a), or 2) the DP causes BSMs from vehicles that intend to send during the time that overlaps with the transmission of DP to be queued, as the medium is blocked. This scenario can be seen in Figure 3b), where BSM(i+1) is delayed. The queuing delay is the sum of the BSM's delayed medium access due to the DP and possible delay due to contention of other BSMs. Contention delay cannot be estimated precisely as it is nondeterministic and may increase with traffic density. We therefore declare a *Delay Sensitivity threshold* δ_t to be a tunable minimum time threshold for a considered delay, i.e., a delay less than δ_t is interpreted as no delay. Parameter δ_t is used to adjust the sensitivity of the detection algorithm. For the sake of simplicity we will consider it constant in the discussion to follow.

In the scenario shown in Figure 3a) DP has no impact on messages. Therefore, lets consider the scenario in Figure 3b), which can be used for Sybil detection. If the DP delays less the δ_t, or if no delay occurred, then this vehicle is marked as *Sybil* and its position must be between the malicious node and the HV. Otherwise, a new P'_{snd} is computed that will cause the suspected vehicle to be out of range. Thus, the DP sent with that power would not be received by the suspected vehicle. If the delay caused by the DP is less than δ_t or no delay occurred, then this vehicle must be *Honest*. Otherwise it is a Sybil node, and the malicious node is positioned between this Sybil and the HV. Based on the status of a vehicle, i.e., Honest or Sybil, the HV can accept or reject BSMs from this vehicle respectively. In the latter case the Sybil is added to the blacklist. Algorithm 1 terminates when a specified detection probability is achieved, i.e., if detection uncertainty ϵ is below a certain threshold, as will be describe in detail in Subsection V-B.

The impact of τ and T on safety application reliability will now be discussed in the context of the fault model in [29]. Two fault scenarios are considered.

The first assumes undetected Sybil attacks. As a result of non-detection falsified BSMs are used, which constitute value faults for the safety application. In [29] such fault type is called *transmissive symmetric*, which is a value fault in which a false BSM is received by all vehicles. If however the false BSM was not received by some vehicles, then this constitutes a *Single Error Omissive Asymmetric* fault, described in [30].

The second scenario addresses the case where BSMs are delayed by DPs to the point where the information is deemed outdated. According to [31] this time-to-live of a BSM should be no more than 500ms. BSMs that exceed the time-to-live should be discarded. In the context of the fault model in [29], this timing fault effectively causes an *omissive symmetric* fault. Specifically, in [29] an omissive symmetric fault implies that no value was received by any node. In our case the result is that no value is used by any node, as it is discarded due to being outdated.

The safety application will fail in either of the following two scenarios: 1) the Sybil detection algorithm fails to detect the attack or 2) BSMs containing crucial information, such as an event, are discarded due to the second scenario. In reliability analysis this can be represented by a series reliability block diagram [32], and thus the safety application reliability, $R_{app}(t)$, can be expressed as $R_{app}(t) = R_1(t)R_2(t)$, where $R_1(t)$ is the detection probability, and $R_2(t)$ is the probability of receiving at least one BSM containing an event before it is too late to react.

V. Field tests and analysis

A. Field Tests

The feasibility of the EASDA and its impact on the reliability of DSRC safety applications were examined using field experiments. Four vehicles were equipped with LocoMate Classic OBUs from Arada Systems [25], one serving as the HV, two as RVs, and one as a malicious node acting as

four Sybil nodes with different GPS locations and message IDs. The EASDA was installed on the OBU in the HV, allowing it to send DPs with different transmission powers, durations, and periods. All OBUs were sending BSMs using a transmission power of 23 dBm, a data rate of 3 Mbps, and the standard BSMs transmission rate of 10 BSMs/s on safety channel CH172. After extensive experimentation with the setup above, a sensible value for the delay sensitivity threshold δ_t was determined as 25ms. The position of vehicles can be seen in Figure 4 for the two aforementioned extreme locations of the malicious node. It should be noted that all nodes were stationary in a controlled configuration. The reason behind conducting the experiments with stationary rather than moving nodes was to isolate the experiment from any external influences, including changes in elevation, unrelated traffic or road layout, as no dedicated filed site was available. The experiment parameters are summarized in Table I.

TABLE I
FIELD TEST PARAMETERS

OBU Model	Arada LocoMate Classic
Number of OBUs	4 (1 HV, 2 RV, 1 Malicious)
Test road range	Straight two-lane road
Distance: HV to RV	80 m
Vehicles speed	0 m/s (Fixed)
Tx power & Data rate	23 dBm, 3 Mbps
BSM generation rate	10 BSM/s
Channel	CH 172
DP power & Data rate	1 dBm, 3Mbps
DP durations τ	25, 50, 75 and 100ms
Delay sensitivity δ_t	25ms

In the scenario of Figure 4a) all Sybil nodes are positioned between the malicious vehicle and the HV. Figure 4b) shows the other scenario, where the malicious vehicle is the closest to the HV. The closest suspected Sybil vehicle is located 80m from the HV in both scenarios. The DP transmission power was computed using Equation 1, resulting in a coverage distance of 100m.

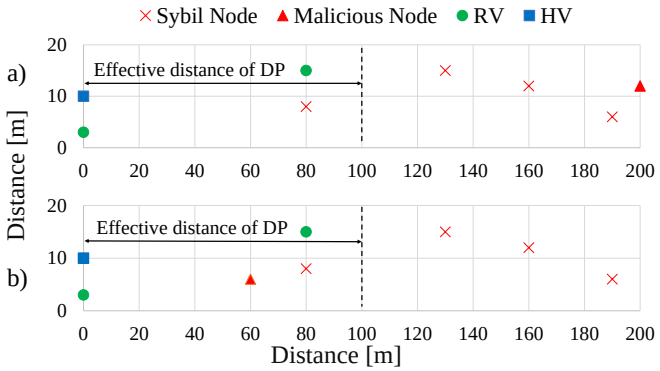

Fig. 4. Position of malicious vehicles

Recall that EASDA relies on the ability to cause the suspected vehicle to delay its BSMs as a result of the DP, and any BSM delay time shorter than δ_t, in our case $\delta_t = 25$ms, will not be considered delayed. The DP can overlap with the time interval of an intended BSM transmission, which in turn will cause a delay of that BSM. If it does not overlap, then no delay will occur. However, collisions may occur if a node located outside the range of the DP broadcasts a BSM. Such scenario constitutes the *hidden terminal* or *hidden node* problem [33]. Field tests were conducted consisting of 10 experiments, each consisting of 20 DPs for different τ and T to study the impact of the durations on delay detection. The trade-off for the choice of values for τ will be discussed below. Obviously, a long DP duration has a high probability of delay detection, especially if τ exceeds the BSM spacing by more than δ_t. However, such long DP may be too invasive, suggesting the investigation of shorter DP durations, although those may not lead to recognized delays for that specific DP. Thus, one should look at detection using shorter τ over multiple BSMs with DP rate T.

The actual values of T will have an impact of the delay detection probability. For example, increasing the frequency of sending short DPs will also increase the probability of detection. As indicated before, T_{detect} is the maximum time available to EASDA for Sybil detection. Thus the values for τ and T should be analyzed in the context of T_{detect}, the duration of time left before t_{react}. The safety application reliability is therefore directly linked to this detection probability.

B. Detection Probability

Let q be the probability that DP overlaps with the intended transmission time of a suspected BSM in such a way as to cause a delay greater than or equal to the minimum recognition delay δ_t. Figure 3b) depicts such case. Assume δ_t =25ms, and $\tau = 25, 50, 75$, and 100ms, denoted by $\tau_{25}, \tau_{50}, \tau_{75}$ and τ_{100} respectively. If DPs are sent without precise time placement, i.e., their transmission times are random, then detection probability q for a single DP sent out to target a BSM from a specific vehicle can be calculated as $q = 0.2, 0.4, 0.6$, and 0.8 for $\tau_{25}, \tau_{50}, \tau_{75}$ and τ_{100} respectively. This is calculated using the parameters given and relating them to Figure 3b), i.e., for a given τ_x the detection probability $q(\tau_x) = \tau_x/(100ms + \delta_t)$.

Assume vehicles are separated by 3s. With an assumed reaction time of 1s a driver has 2s left to react to a safety application alert. At the standard rate of 10 BSM/s this leaves 20 BSMs for potential detection. Detection probabilities are shown in Figure 5, where the calculated q can be compared with the minimum, maximum and average values as derived from 7 experiments of 20 DPs for each τ. Whereas we conducted a total of 120 experiments, we intentionally did not average over a large number of experiments, as we are interested in seeing the impact of small samples when calculating q. Inspecting individual experiments we could not observe any obvious patterns for delay detection as the result of DPs. This was even the case when sending DPs periodically for specific T. As expected, shorter τ result in lower delay detection probabilities q than longer τ, e.g., the average q for $\tau = 25ms$ and $100ms$ increased from 0.17 to 0.83 respectively.

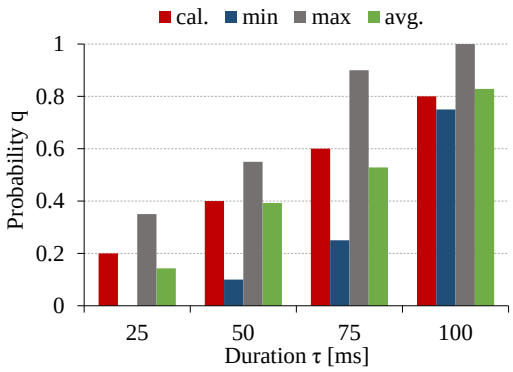

Fig. 5. Probability of delay detection for different τ

Sybil detection of EASDA is based on detecting at least one BSM delayed by at least δ_t. Since q is the probability of detecting a delay as the result of one DP, $1-q$ is the probability that either the DP does not overlap with the BSM, as shown in Figure 3a), or it overlaps, but not enough to cause a delay of δ_t. Every time a DP is sent, there is a chance for delay detection. Let N be the number of BSMs considered for delay detection. Thus N DPs need to be sent. The probability of not detecting a BSM delay with any of those N DPs, denoted by ϵ, is

$$\epsilon = (1-q)^N \tag{3}$$

Probability ϵ is the unreliability of the Sybil detection algorithm. Thus detection probability $R_1(t)$, defined in Section IV, is equal to $1-\epsilon$. As N increases the probability of not observing at least one delay decreases exponentially.

The following questions arise: 1) Is it better to send longer DPs less frequently or shorter ones more often? 2) What is the DP-related overhead (medium blocking) for different τ and T to achieve a required reliability?

The answer to question 1 can be found in Figure 6, which displays graphs showing the probability of not detecting a delay for specific DP durations and periods. The values for τ were the same as used in Figure 5, and the values for q were their corresponding average value. The notation T_{100}, T_{500} and T_{1000} was used to denote periods of T = 100, 500 and 1000ms respectively. The x-axis considers the algorithm's execution time and the y-axis the probability of non-detection. The plots are stepping functions where ϵ decreased with each additional DP considered. The objective of the Sybil detection algorithm should be to have a reasonably high detection probability in the shortest time. As is obvious from comparing the graphs in Figure 6a), b) and c), smaller T result in shorter times to improve ϵ. This however comes at the cost of higher medium blocking.

Let's consider the detection interval $T_{detect} = 2s$, as in the discussion above. This cutoff time is indicated by a vertical dashed line in Figure 6. For a given time, period T dictates how many DPs are sent. In our case of 2 seconds, T_{100} results in 20 DPs, T_{500} in 4, and T_{1000} in 2 DPs. For long T this poses a problem for achieving a low ϵ, as there are only few

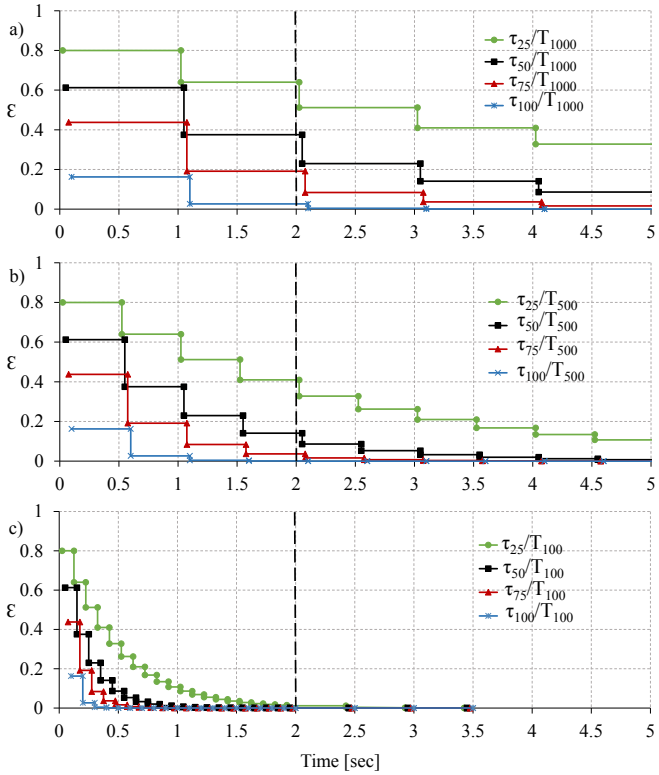

Fig. 6. Probability of not detecting a delay for DPs with different τ and T

DPs contributing to Equation 3. For example, in the case of T_{1000}, the algorithm has only two chances to detect a delay. In the case of Figure 6a) with T_{1000}, only τ_{100} was able to achieve a low uncertainty, below 0.03 in plot τ_{100}/T_{1000}, thus achieving a reliability of greater than 0.97. All other τ resulted in unacceptable ϵ, and thus reliabilities.

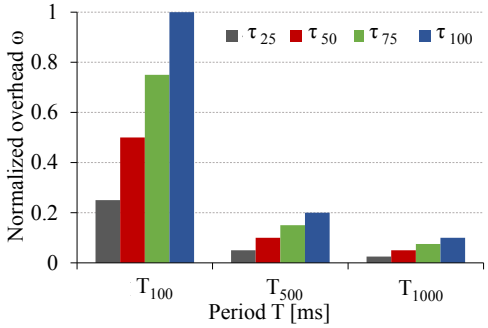

Fig. 7. Normalized DP overhead ω for different τ and T

Question 2 addressed the overhead, i.e., medium blocking, for detecting delays. Figure 7 shows the DP overhead normalized over the detection interval T_{detect}. This ratio for medium blocking is denoted by ω. Obviously, for a given τ, overhead ratio ω for longer periods, e.g., T_{1000}, is lower than that of shorter periods, e.g., T_{100}, since fewer DPs are sent. Furthermore, for a given T, longer durations τ result in higher overhead ratios than short τ. Overhead was calculated based

on the assumption that one sends DPs during the entire interval T_{detect}. This however is not necessary, as one only needs to run detection until a specified ϵ is reached.

Figure 8 shows the overhead ratio ω during the 2 seconds to achieve 90% detection probability, i.e., for $\epsilon = 0.1$. Recall that Algorithm 1 terminates once a specified ϵ has been reached. It should be noted that a zero entry in the graph indicates that the specified ϵ could not be achieved in the given time, and thus for T_{500} only $\tau = 75$ and 100 resulted in detection, whereas for T_{1000} only $\tau = 100$ could achieve the specified detection probability. To answer question 2) above, from a medium blocking point of view, it is best to select the largest T with the τ producing the smallest ω. Preference is given to the largest T, in order to spread the DPs as wide as possible, thereby minimizing monopolization of the medium by DPs and allowing BSMs, including those from other vehicles, to be transmitted.

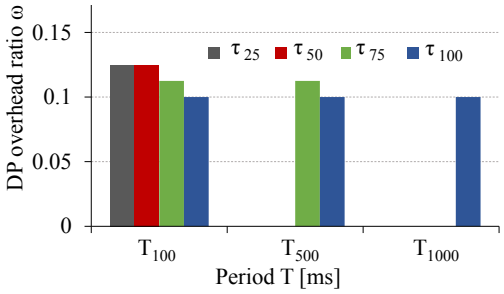

Fig. 8. Overhead Ratio ω to achieve $\epsilon = 0.1$ during 2s

VI. Conclusion

This research investigated Sybil attack detection in VANETs operating in dynamic power environments. A Sybil detection algorithm for such challenging environment was presented that is based on detecting queuing delays of nodes subjected to Detection Packets to determine if a BSM is valid or has been spoofed. In order to minimize the impact of these overhead packets on medium usage, delay detection should be spread over time. Analysis and field experiments on the impact of detection packet duration τ period T on Sybil node detection showed that it is best to use the largest periods with the lowest overhead ratio ω that can achieve a predefined detection probability.

References

[1] Rashmi Mishra, Akhilesh Singh, Rakesh Kumar, *VANET Security: Issues, Challenges and Solutions*, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016.

[2] Mohamed S. Mohamed, P. Dandekhya and Axel Krings, *Beyond Passive Detection of Sybil Attacks in VANET*, 6th IEEE International Conference on Reliability, Infocom Technologies and Optimization, 2017.

[3] *Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band)*, Federal Communications Commission FCC 03-324, 2004.

[4] *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, Society of Automotive Engineers, SAE J2735, November 2009.

[5] *Vehicle safety communications-applications (VSC-A) final report*, DOT HS 811 492 A. U.S. Department of Transportation, NHTSA, 2011.

[6] G. Johansson, K. Rumar, *Drivers' brake reaction times - Human Factors*, The Journal of the Human Factors and Ergonomics Society 13, 1971.

[7] *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 Amendment 6: Wireless Access in Vehicular Environments*, IEEE Std 802.11p, 2010.

[8] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation*, IEEE Std 1609.4TM, 2010.

[9] J. Newsome, E. Shi, D. Song, and A. Perrig, *The Sybil Attack in Sensor Networks: Analysis & Defenses*, In International symposium on information processing in sensor networks, pages 259268, 2004.

[10] J. Douceur *The Sybil Attack*, In First International Workshop on Peer-to-Peer Systems, pages 251-260, March 2002.

[11] C. Piro, C. Shields, B. N. Levine, *Detecting the Sybil attack in mobile ad hoc network*, in proceedings of the International Conference on Security and Privacy in Communication Networks, pp. 111, 2006.

[12] M. Demirbas and Y. Song, *An RSSI-based scheme for Sybil attack detection in wireless sensor networks*, Proc. IEEE Int. Symp. on a World of Wireless Mobile and Multimedia Networks, 2006.

[13] B. Xiao, B. Yu, and C. Gao, *Detection and localization of Sybil nodes in VANETs*, Proc. of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS '06), USA, 2006.

[14] Mohamed S. Bouassida, et. al., *Sybil Nodes Detection Based on Received Signal Strength Variations within VANET*, International Journal of Network Security, Vol.9, No.1, PP.22-33, 2009.

[15] Caffery J, Ster GL., *Overview of radio location in CDMA cellular systems*, IEEE Transactions on Vehicular Technology, Apr. 1998.

[16] Alam MS.,Alsharif S.,Haq N., *Efficient CDMA wireless,position,location system using TDOA method*, International Journal of Communication Systems, 24(9):12301242, 2011.

[17] S. Hussein, Axel Krings, and Azad Azadmanesh, *VANET Clock Synchronization for Resilient DSRC Safety Applications*, in Proc. 7th Resilience Week Symposia, USA, 2017.

[18] Chen Chen, et. al., *A Robust Detection of the Sybil Attack in Urban VANETs*, 29th IEEE International Conference on Distributed Computing Systems Workshops, 2009.

[19] Soyoung Park, et. al., *Defense against Sybil attack in vehicular ad hoc network based on roadside unit support*, MILCOM, pp. 1-7, 2009.

[20] Jyoti Grover, et. al., *A Sybil Attack Detection Approach using Neighboring Vehicles in VANET*, Proc. of the 4th Int. conference on Security of information and networks, 2011.

[21] Kamran Zaidi, et. al., *Host Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection*, IEEE Transactions on Vehicular Technology, 2015.

[22] M. Raya and J.P. Hubaux, *Securing vehicular ad hoc networks*, Journal of Computer Security, 15(1), 39-68, 2007.

[23] A. Khalili, J. Katz, and W. Arbaugh, *Toward secure key distribution in truly ad-hoc networks*, in Proceedings of IEEE Workshop on Security and Assurance in Ad hoc Networks, 2003.

[24] M. Rahbari, M. Ali and J. Jamali, *Efficient detection of Sybil attack based on cryptography in VANET*, International Journal of Network Security and Its Applications IJNSA, Vol.3, No.6, November 2011.

[25] Arada Systems, *www.aradasystems.com*

[26] Hani Alturkostani and Axel Krings, *The Impact of Jamming on Threshold-Based Agreement in VANET*, International Conference on Connected Vehicles and Expo (ICCVE), 2014.

[27] Z. Cao, et. al., *Proof-of-relevance: Filtering false data via authentic consensus in VANET*, in IEEE INFOCOM Workshops, 2008.

[28] D. M. Pozar, *Microwave Engineering 3rd Edition*, NY, Wiley, 2010.

[29] M. H. Azadmanesh and R. M. Kieckhafer, *Exploiting omissive faults in synchronous approximate agreement*, IEEE Transactions on Computers, vol.49, no.10, pp.1031,1042, Oct 2000.

[30] Paul J. Weber, *Dynamic Reduction Algorithms for Fault Tolerant Convergent Voting with Hybrid Faults*, Order No. 3209907, Michigan Technological University, Ann Arbor, 2006.

[31] X. Ma, et. al., *On the Reliability of Safety Applications in VANETs*, Invited paper, International Journal of Performability Engineering Special Issue on Dependability of Wireless Systems and Networks, 8(2), 2012.

[32] W. B. Johnson, *Design and Analysis of Fault-Tolerant Digital Systems*, Addison-Wesley Publishing Company, New York, 1989.

[33] K. Sjoberg, et. al., *How Severe Is the Hidden Terminal Problem in VANETs When Using CSMA and STDMA*, IEEE Vehicular Technology Conference (VTC Fall), San Francisco, 2011.