Beyond Passive Detection of Sybil Attacks in VANET

Mohamed S. Mohamed
Department of Computer Science
University of Idaho
Moscow, ID 83843
Email: moha3425@vandals.uidaho.edu

Prajjwol Dandekhya
Department of Computer Science
University of Idaho
Moscow, ID 83843
Email: dand6697@vandals.uidaho.edu

Axel Krings
Department of Computer Science
University of Idaho
Moscow, ID 83843
Email: krings@uidaho.edu

***Abstract*—Dedicated Short Range Communications Safety Applications play an important role in reducing road accidents. These applications rely on wireless communication between vehicles and thus inherit all of the associated security problems. Vehicular Ad Hoc Network security is crucial, since application reliability, and thus safety, must not be compromised. One of the most severe attacks in these networks is the Sybil attack, in which a malicious node forges many fake identities to fool Safety Applications. This research presents an active Sybil attack detection algorithm. It can locate Sybil nodes using short detection packets without adding special hardware or information exchanges. Unlike previous detection approaches, the algorithm is capable of Sybil detection even in dynamic power environments. The proposed algorithm was evaluated in the field using vehicles equipped with Arada LocoMate Classic on-board units.**

I. Introduction

In the last few years there has been growing interest in connected vehicles, where technologies, services, and applications allow wireless communication between vehicles and between vehicles and the roadside infrastructure using Dedicated Short Range Communications (DSRC) [1]. Each vehicle is equipped with an On Board Unit (OBU) and the infrastructure, such as a traffic intersection, has a Road Side Unit (RSU) to allow Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. A collection of these devices can form a Vehicular Ad Hoc Network (VANET), designed for quick message exchanges in a fast-changing topology. The most important applications in VANET are DSRC Safety Applications. The goal is to increase safety by alerting drivers of potential hazards or accidents. As safety applications use wireless communication, they are potentially subjected to all security challenges associated with this communication paradigm. Any compromise, such as malicious attacks attempting to cause safety applications to fail, may result in injury, death, and undermines the public's trust in these technologies. A serious threat to VANET is a Sybil attack, in which a rogue node pretends to be multiple nodes by impersonating their identities using stolen or fake IDs. This illusion could be used by an attacker to gain advantages, e.g., to fool traffic management systems to redirect traffic away from the attackers path, or more dangerously, to cause DSRC safety applications to fail.

This research focuses on detection of malicious act, specifically Sybil attacks in VANET. The remainder of this paper is organized as follows. Section II introduces important background information. Section III states the assumptions and attack model used. The Sybil detection algorithm is presented in Section IV, followed by experimental performance evaluation using field tests in Section V. Finally, Section VI concludes the paper.

II. Background and Related Work

Necessary background related to the key technologies used in this research will be introduced next.

A. DSRC and DSRC Safety Applications

DSRC provides communication for V2V and V2I, and uses 75MHz of bandwidth at 5.850-5.925GHz, as allocated by the Federal Communications Commission (FCC). There are seven 10Mhz channels, i.e., six Service Channels, CH172, 174, 176, 180, 182, and 184, one Control Channel, CH178, leaving the remaining 5Mhz for future use [2]. The most important channel for our research is Safety Channel CH172, which is reserved for DSRC safety applications. The Basic Safety Message (BSM), which is a beacon message broadcast periodically every 100ms on CH172, is the most important message to exchange information about the status of the vehicle. The information includes speed, heading, acceleration, GPS location, and brake status [3]. Various DSRC Safety Applications have been presented in [4]. They use information in BSMs received from surrounding vehicles to warn drivers about impending dangers. The Emergency Electronic Brake Lights (EEBL) is an example of such safety application. It alerts the driver of a vehicle called Host Vehicle (HV) of an impending rear-end collision with another vehicle, referred to as Remote Vehicle (RV), which is driving ahead in the same direction and lane.

B. Attackers and Attack Types

In [24] attackers are classified into four basic categories based on the scope and behavior of attacks. The categories are: Insiders vs. outsiders: insiders are authenticated members in a network, while outsiders are intruders with less capabilities. Malicious vs. rational: malicious attackers cause accidents but do not personally benefit from this attack, while rational attackers have specific goals. Active vs. passive: active attackers send fake or manipulated messages, whereas passive attackers sniff the network to collect information for future attacks. Local vs. extended: the scope of a local attacker is of limited range, whereas extended attackers target the larger network.

Several types of attacks have been identified and classified in [25]. In Denial of Service (DoS) the attacker is attempting to block the network from authentic users by flooding or jamming the signal. The attacker could be an insider or outsider. In GPS spoofing the attacker attempts to deceive a GPS receiver by broadcasting incorrect GPS signals, stronger than those generated by genuine satellites, to fool other drivers by providing false locations. The Sybil attack was described in [5], where one node, called the *Malicious* node, is sending multiple messages with multiple forged identities. In other words, the attacker simulates several nodes in the network. These simulated nodes are called *Sybil* nodes. The attacker is an insider, rational, and active. A Sybil attack might be launched with different goals. One of the goals is to give the illusion of a traffic jam, to convince other vehicles to take other roads to the benefit of the attacker. However, the attacker may be more harmful by trying to provoke fake events, e.g., a collision, to force safety applications that use voting schemes to make wrong decisions [6], [7], [8], [9]. The attacker attempts to stack wrong values, sent by Sybil nodes, in the voting sets of safety applications to out-vote the correct values, causing safety applications to fail. The misbehaving detection techniques presented in [10] [11] fail to detect Sybil nodes because they obey medium access rules.

The literature on detecting Sybil attacks in VANET shows a variety of approaches. These approaches can be classified as follows.

C. Received Signal Strength Indicator

Sybil attacks can be detected using the Received Signal Strength Indicator (RSSI) propagation model as described in [12] [13]. In this method, the receiving node uses the received signal strength as the basis for calculating the distance of the sending node. If the calculated distance differs from the distance implied by the two nodes' GPS coordinates, the sending node may be a Sybil node. The authors in [14] present an approach that is composed of two complementary techniques assuming all vehicles use the same transmission power. They first use RSSI to estimate the distance between two nodes using the Friis model. When incoherent signal strengths are observed, a second technique using a "distinguishability degree metric" is used, which is based on observing differences of two nodes over time. However, any intelligent attacker who can manipulate the GPS coordinates and power levels to appear consistent, will be able to fool these approaches.

D. Neighbor Information and Collaboration

The authors in [15] proposed a technique in which each node exchanges group information of its neighbors periodically with other nodes. Each node performs the intersection of these groups. If nodes observe very similar neighbors over a longer time, they flag these matching neighbors as Sybil nodes. The assumption is that it is unlikely that two nodes have the same set of neighbors for a time surpassing a certain threshold. However, this approach has limited detection capabilities and adds more communication/message overhead to the system.

An intrusion detection system approach to rogue node detection was introduced in [19]. Their anomaly-based detection approach uses node driving information to calculate metric such as average flow, density and location, which is then used as a base line shared with other nodes. This collaboration allows comparisons of traffic flow averages. Flow averages that appear extreme are rejected and reported. However, Sybil nodes, especially if there are many, could affect these computations. Furthermore, these nodes can behave normal, yet inject and broadcast false data, e.g., a brake status event indicating hard braking.

E. Road-Side Unit (RSU)

In [16] the authors introduced a so-called "Robust method of Sybil Attack Detection (RobSAD)" in urban VANETs. Because their Sybil nodes have the same location and direction all the time, their group behavior is assumed suspicious. The authors suppose that authorized RSUs are distributed over part of this area. These RSUs broadcast digital signatures with timestamps to vehicles in their range. Honest nodes have independent trajectories and collect the signatures received from authorized RSUs. Sybil detection is achieved by analysis of the neighboring nodes' signatures.

A timestamp-based approach using RSU support to detect a Sybil attack is presented in [17]. The authors assume that it would be unlikely for two vehicles to pass by two or more different non-proximate RSUs at similar times. Sybil attack detection is triggered when multiple messages from different vehicles (Sybil nodes) contain similar series of timestamps. However, if RSUs are located at intersections or in the absence of RSUs, it may make Sybil attack detection difficult or impossible.

F. Cryptography and Authentication

A mechanism using public key cryptography and authentication to prevent Sybil attacks is described in [18] [20]. Specifically, asymmetric cryptography is used. Signatures are combined with digital certificates, issued by a Certification Authority (CA), with one CA for each region. The CAs communicate through secure channels and keep track of issued certificates used for signed messages. Only messages with valid certificates are considered and invalid messages are ignored. However, this mechanism requires that each node is assigned one certificate at a time. On the other hand, these certificates should be changed frequently for privacy. It is unrealistic and difficult in VANETs to deploy Public Key Infrastructure as there is no guarantee that the appropriate infrastructure will be present and the approach is time consuming.

In [21] a scheme is proposed that uses encryption and four security aspects. 1) Authentication - before any message is transmitted, a vehicle should receive its public authentication key. 2) Non-repudiation - the vehicle uses a group authentication key and an encryption function, which it then sends along with the original message to other vehicles and RSUs. 3) Privacy - it is not mandatory for each member to have the private information of other members. 4) Data Integrity - receiving nodes verify the authenticity of members using the signature. The major drawback of this approach is that most operations are done in the CA and do not run at node itself, which may not be practical in all situations. Furthermore, it is not possible to discover the location of malicious nodes.

III. Assumptions and Attack Model

In this research the following assumptions will be made:

1) An attacker can have more computational power and flexibility than ordinary OBUs or RSUs. It may tune its transmission power to achieve certain signal strengths at a target vehicle's receiver. This assumption can be easily justified by the availability of devices satisfying such properties.

2) An attacker may inject false information or other fields into a BSM. This includes manipulation of GPS coordinates. Thus, there are no restrictions imposed on the attacker's conduct. We have experimented extensively with such manipulations using Arada LocoMate Classic [22] OBUs.

3) Attackers can use more than one certificate to send messages. The justification for this assumption is the possibility that any attacker could possess portable DSRC devices, such as the *Arada LocoMate Me* [22], or use stolen devices. Furthermore, sending a BSM does not require authentication if the goal is to reduce overhead, as may be the case in high traffic density situations.

4) Similar to the research presented in [14], we assume that honest vehicles are equipped with standard OBUs, where the antenna's properties and gains are fixed and known.

Figure 1 depicts an attack scenario with an HV, two honest RVs, and a malicious vehicle projecting four Sybil nodes. Whereas RV1 and RV2 send BSMs every 100ms, the malicious node sends one BSM each 25ms, alternately claiming to be another (non-existing) vehicle. Now assume that RV1 brakes hard due to an observed hazard. It consequently sends this "hard braking" event in its BSMs. Assume the HV runs a safety application using voting, such as presented in [7] or [8]. The goal of these voting algorithms is to collect BSMs from vehicles in the vicinity of the reported event to see if they also reacted. If a certain threshold of vehicles report the braking event, the HV assumes it is legitimate. However, the malicious node, with its Sybil nodes, can inject BSMs contradicting the event, thereby affecting HV's vote.

Sybil detection algorithms based on RSSI, such as described in Subsection II-C, are of little use to resolve this situation. The reason is that RSSI-based approaches may not be precise enough, and do not work at all in dynamic power environments, since the sending power is not known, but needed.

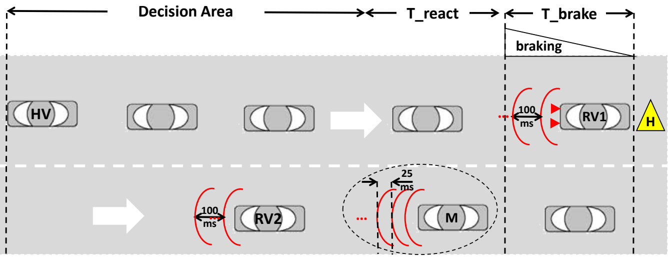


Fig. 1. Sample attack scenario

IV. Active Sybil Detection Algorithm

A. Impact of forced BSM queuing

The purpose of the Detection Packet (DP), which is a bogus packet of specified duration, is to check if selected nodes queue their BSMs. Queuing is the result of the node having no medium access at the Medium Access Control (MAC) layer. Figure 2 shows the impact of forcing BSMs to be queued for 500ms by means of a DP. The bars in Figure 2 represent the number of BSMs received by the HV from four nodes, each emitting BSMs every 100ms. Specifically, these four nodes were stationary, one node was positioned 80m from the HV, while the other three nodes were 150m from the HV. The figure can be divided into three intervals, the closed time interval $[0, 1.1]$, the open time interval $(1.1, 1.7)$, and interval $[1.7, 2.6]$. During the first interval the HV received 4 BSMs every 100ms, whereas no BSMs were received during the second interval, due to the DP. Note that this DP was sent with a power of 1 dbm to affect only the nearest node, i.e., RV1. As a result, RV1 queued 5 BSMs as it could not access the media, and obviously no BSM was received by the HV. In the third interval, the 5 queued BSMs of RV1 were sent in a burst. The investigation of the message IDs of the BSMs received by the HV confirmed that the bust of RV1 was among them. The other three nodes outside of the range of the DP sent their BSMs normally. However, these BSMs collided with the DP, and were thus not received.

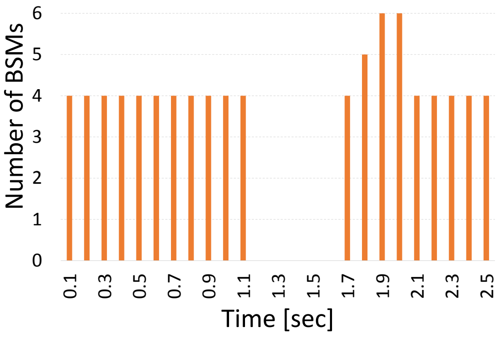


Fig. 2. Field experiment with a DP duration of 500ms

The above experiment shows that the HV could in fact tune the power level of the DP to affect and observe a specific node, in this case only RV1. However it should be noted that long detection packets are like an HV-induced DoS attack [26], which motivated the investigation of shorter DP durations.

Figure 3 shows the impact of forced queuing of BSMs with a 50ms DP, displaying the cumulative inter-arrival times of 10 BSMs. In this particular experiment the DP caused the 5^{th} BSM to be delayed by approximately 30ms.

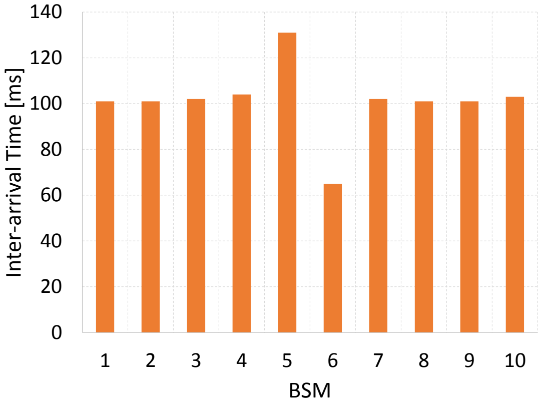


Fig. 3. Cumulative BSM inter-arrival times for a DP of 50ms

B. Active Sybil Detection Algorithm

The proposed algorithm shown in Figure 4 is capable of detecting sophisticated Sybil attacks by considering two cases. In the first case the Sybil nodes are assumed to be positioned between the HV and malicious node, whereas in the second case the malicious node is between the HV and any Sybil nodes. All other cases can be derived from these two cases. Thus, if the malicious node has Sybil nodes on either side, one can partition the Sybil nodes into two groups, i.e., those between the HV and malicious node, and those after the malicious node.

The detection algorithm works as follows. Upon receiving a message from a suspecting vehicle, the algorithm calculates the distance between the HV and the suspected vehicle, using the GPS coordinates, which may be correct, or spoofed, as in the case of a Sybil node. Next, the transmission power P_{snd} to be used for the DP is determined using

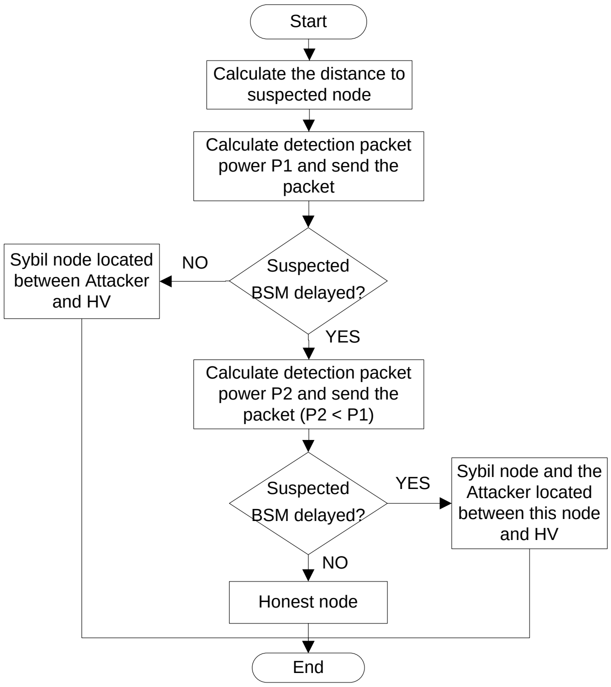
$$P_{snd} = S \times d^2/G \tag{1}$$

where S is the receiver sensitivity of the suspected vehicle, d is the distance between the HV and the suspected vehicle, and G is the gain, as computed by [23]

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

where λ denotes the wavelength of the radiation. Now the HV sends the DP of duration τ. The exact value to be used for τ will be discussed later. The DP forces nodes that expect to send a BSMs during the time that overlaps with the DP to be delayed, as their MAC layer access is blocked.

If the DP does not cause a delay, then this node is marked *Sybil*. Otherwise, a new P_{snd} is computed that will exclude the suspected node. Thus, the DP sent with that power will not interfere with the suspected node. If the DP does not cause a delay, then this node is marked *Honest*. Otherwise it is a Sybil, and the attacker is located between the HV and the Sybil. Based on the status of a node, *Honest* or *Sybil*, the HV can consider or reject BSMs from this node respectively.



Start
Calculate the distance to suspected node
Calculate detection packet power P1 and send the packet
Suspected BSM delayed?
NO
Sybil node located between Attacker and HV
YES
Calculate detection packet power P2 and send the packet (P2 < P1)
Suspected BSM delayed?
YES
Sybil node and the Attacker located between this node and HV
NO
Honest node
End

Fig. 4. Active Sybil detection algorithm

V. Field Experiments

The feasibility of the Sybil detection algorithm was tested using field experiments. One vehicle representing the HV and one vehicle representing a malicious node acting as four Sybil nodes were equipped with LocoMate Classic OBUs from Arada Systems [22]. The malicious OBU was configured to act as 4 different OBUs (4 Sybils) with different message IDs and GPS locations. All OBUs transmitted BSM every 100ms on safety channel CS172, using a transmission power of 23 dBm. The OBU in the HV executed the active detection algorithm capable of sending DPs with different transmission powers. The experiments were conducted in a controlled configuration, where the vehicles were stationary. The HV sent detection packets using a power of $P_{snd} = 1$ dBm for different DP durations $\tau = 25$, 50, 75 and 100ms. The HV was placed 80 meters from the malicious node. The rational for conducting the experiments with stationary, rather than moving vehicles, was to eliminate the impact of external influences, such as changing road geometry (e.g., curves), elevation changes, and unrelated road traffic, as no dedicated test site was available. Table I summaries the parameters used in the experiment.

As indicated above, of special interest is the position of the malicious node with respect to its Sybil nodes. Two scenarios are shown in Figure 5, in which the malicious nodes are at

TABLE I
FIELD EXPERIMENT PARAMETERS

OBU Model	Arada Systems LocoMate Classic
Number of OBUs	2 (1 HV and 1 malicious)
Test range	Straight two-lane road
Distance: HV to malicious	80 m
Vehicles speed	0 m/s (Fixed)
Tx power & Data rate	23 dBm, 3 Mbps
BSM generation	10 BSM/s
Channel	Safety Channel 172
DP power & data rate	1 dBm, 3Mbps
Delay sensitivity threshold δ_t	30ms

the extreme positions with respect to the Sybil nodes and the HV. Specifically, in the scenario of Figure 5 a) all Sybil nodes are positioned between the HV and the malicious node. The scenario in Figure 5 b) shows the other extreme, where the malicious node is closer to the HV than all Sybil nodes. Recall that scenarios where the malicious node is in-between Sybil nodes can be broken up into the previous two cases. In both cases the first Sybil node is at distance 80m and the DP transmission spans over a distance of 100m.

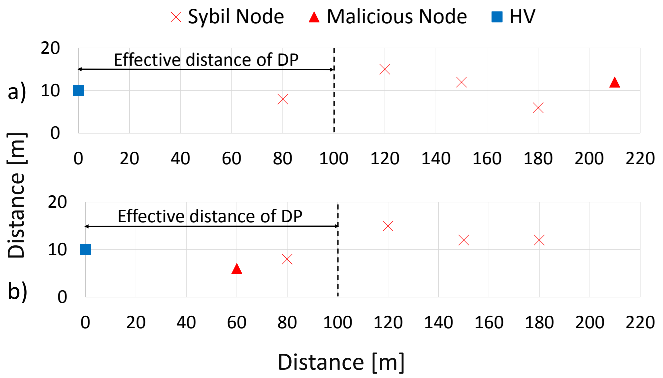


Fig. 5. Extreme position of malicious nodes

The Sybil detection algorithm is based on the capability of detecting a delayed BSM transmission of a suspected node as the result of a DP. Several scenarios are possible. Either the DP will overlap with the time interval of the intended BSM transmission or not. If it does not, the transmission time of a BSM is unaffected by the DP, and thus there is no delay. If however it does overlap, then it will result in a BSM delay or a collision. Collisions occur if the BSM was sent from a node outside of the range of the DP. Let δt be the minimum delay time that will constitute a recognized delay. δt is thus a parameter that allows tuning the sensitivity of delay detection, e.g., to account for MAC access delays due to other network activity. Any BSM delay shorter than δt is ignored. Let q be the probability that DP is sent in such fashion that it overlaps and results in a delay of at least δt. If the DP has a duration of τ = 100ms $+\delta t$, then a delay is recognized with high probability, approaching 1. However, such long DP may be too invasive. Thus, lower DP durations are desirable, but they may lead to unrecognized delays.

Figure 6 shows the probability q of delay detection for DPs with different τ for two DP transmission precisions F1 and F2. Precision relates to how precise one can time the transmission of the DP to delay a BSM. F1 was the precision of our DP generation and transmission mechanism, a jamming application developed by Arada for use in our jamming related research such as [26]. Imprecision was due to variable startup times of the jammer, as the result of process setup and switching times of the Arada LocoMate Classic's operating system. The precision of F2 was higher as the result of implicit timing manipulation. In either case shorter DP durations resulted in lower delay recognition probabilities, but delay recognition was significantly higher for F2.

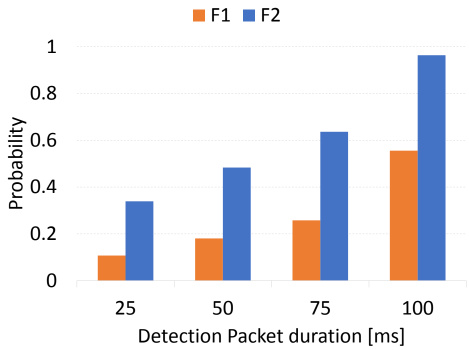


Fig. 6. Probability of delay detection

Effective delay detection in the context of DSRC Safety Applications implies that at least one BSM delay has to be detected. For each BSM there is a probability of $1-q$ that detection will fail. Every 100ms, the BSM transmission period, there is another chance to detect delay. Assume that N BSMs are considered for delay detection. Then the probability ϵ of not observing a delay of any of the N BSMs is

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

As N grows larger, i.e., as more BSMs are considered, the probability of missing all delays decreases exponential.

Field experiments were conducted, consisting of 10 repetitions with 20 DP for different τ durations. The results for precisions F1 and F2 are shown in Figures 7 and 8 respectively, which show the trade-off space between N, ϵ and τ. The observations were over 20 BSMs, implying time intervals of 2 seconds at the 10 BSM/s rate. This represents a scenario in which cars drive with 3 seconds separation, and assuming a reaction time of 1 second, thus leaving 2 seconds, or 20 BSMs, to detect at least one delay. Probabilities ϵ were considered for ϵ in $[0, 0.4]$. The figures show that shorter DPs result in larger probabilities of not observing any delay. More importantly, the figures show the impact of the DPs placement precision. Specifically, in Figure 8, where each DP was placed more precisely to delay a BSM, significantly fewer BSMs were required to detect delays with smaller error probability ϵ. Especially for F2 very high delay detection probabilities could be archieved with few BSMs, e.g., even in the case of $\tau = 25$ms, it took only 6 BSMs to achieve an ϵ of 0.1, or alternatively a delay recognition probability of 90%. Very high recognition probabilities could be achieved for all τ when N was larger. Specifically, close to 100% detection was achieved for $\tau = 25, 50, 75$ and 100ms for $N = 16, 10, 6$ and 2, respectively. This shows that even with shorter DP, Sybil detection is highly effective if one considers multiple BSMs in the detection algorithm.

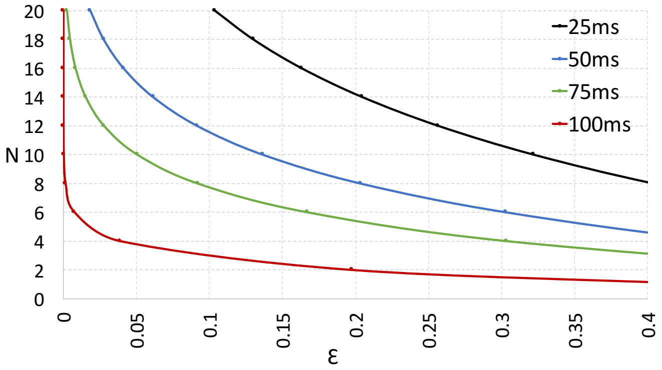


Fig. 7. Low-precision scenario F1

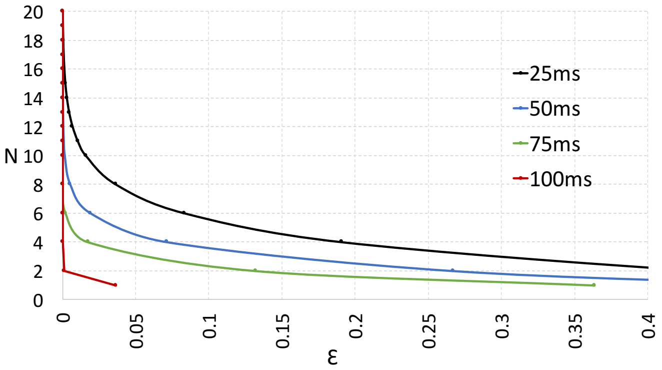


Fig. 8. High-precision scenario F2

VI. Conclusions

This paper presented an active approach to detect Sybil attacks, which can cause serious problems for DSRC Safety Applications using voting schemes. An algorithm was presented that, upon suspecting a Sybil node, used a Detection Packet to investigate queuing delays of nodes. In order to minimize the intrusiveness of these DPs, delay detection was spread over multiple BSM messages, increasing detection probability exponentially in the number of BSMs investigated. Analysis and field experiments on the effects of the number of BSMs and DP duration & time placement accuracy revealed that DP placement and duration have the largest impact on Sybil detection effectiveness.

References

[1] Kenney, J. B., *Dedicated short-range communications (DSRC) standards in the United States*, Proc. of the IEEE, vol.99, no.7, pp.1162-1182, 2011.

[2] *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.

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

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

[5] J. Douceur *The Sybil Attack*, In First International Workshop on Peer-to-Peer Systems, pages 251260, March 2002.

[6] J. Petit and Z. Mammeri, *Dynamic consensus for secured vehicular ad hoc networks*, in Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE 7th International Conference on. IEEE, 2011, pp. 18, 2011.

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

[8] Z. Cao, J. Kong, U. Lee, M. Gerla, and Z. Chen, *Proof-of-relevance: Filtering false data via authentic consensus in vehicle ad-hoc networks*, in INFOCOM Workshops, IEEE. IEEE, 2008, pp. 16, 2008.

[9] Yu-Chih Wei and Yi-Ming Chen, *Adaptive Decision Making for Improving Trust Establishment in VANET*, IEICE - Asia-Pacific Network Operation and Management Symposium (APNOMS), 2014.

[10] M. N. Mejri and J. Ben-Othman, *Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks*, Global Communications Conference (GLOBECOM), pp. 5032-5037, 2014.

[11] L. Toledo, and X. Wang, *Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks*, IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 347-358, Sep. 2008.

[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*, Proceedings of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS 06), Los Angeles, CA, USA, pp. 18., 2006.

[14] Mohamed S. Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, *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] Jyoti Grover, Manoj Singh Gaur and Vijay Laxmi, *A Sybil Attack Detection Approach using Neighboring Vehicles in VANET*, Proceedings of the 4th international conference on Security of information and networks, 2011.

[16] Chen Chen, Xin Wang, Weili Han, and Binyu Zang, *A Robust Detection of the Sybil Attack in Urban VANETs*, 29th IEEE International Conference on Distributed Computing Systems Workshops, 2009.

[17] Soyoung Park, Baber Aslam, Damla Turgut and Cliff C. Zou, *Defense against Sybil attack in vehicular ad hoc network based on roadside unit support*, MILCOM, pp. 1-7, 2009.

[18] 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.

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

[20] M. Raya and J.P. Hubaux, *Securing vehicular ad hoc networks*,Journal of Computer Security, 15(1), 3968, 2007.

[21] 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.

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

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

[24] M. Raya and J. Hubaux, *The security of vehicular ad hoc networks*, In Proceeding SASN, Alexandria, VA, USA, Nov. 2005, pp. 1121.

[25] A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M.Gerlach, R. Kroh, andT. Leinmuller, *Attacks on inter-vehicle communication systemsan analysis*, In Proceedings of the 3rd international Workshop on Intelligent Transportation (WIT), 2006.

[26] S. Hussein, M. S. Mohamed and Axel Krings, *A New Hybrid Jammer and its Impact on DSRC Safety Application Reliability*, The 7th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, Canada, 13-15 October, 2016.