DDoS Attack on WAVE-enabled VANET Through Synchronization

Subir Biswas  
Department of Computer Science  
University of Manitoba  
Winnipeg, Canada R3T 2N2  
Email: bigstan@cs.umanitoba.ca

Jelena Mišić  
Department of Computer Science  
Ryerson University  
Toronto ON, Canada M5B 2K3  
Email: jmisic@scs.ryerson.ca

Vojislav Mišić  
Department of Computer Science  
Ryerson University  
Toronto ON, Canada M5B 2K3  
Email: vmisic@scs.ryerson.ca

Abstract—A synchronization-based distributed denial of service (DDoS) attack can seriously affect the vehicular communications. IEEE 802.11p’s EDCA mechanism allows prioritization of outgoing frames from a VANET entity. However, small contention window size of EDCA access categories may expose a period transmission to malicious entities for launching a synchronization-based DDoS attack. Since broadcast communications in VANET do not have acknowledgements, both sender and receiver of the period broadcasts will be unaware of the attack. In this paper, we analyze the prospect of such an attack on vehicular communications. Our contribution includes different mitigation techniques to avoid synchronization-based DDoS attacks in VANETs.

I. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) have been introduced to achieve safer driving environment through intelligent vehicles, and smart roads. VANET consists of two major types of entities: road-side units (RSUs), and on-board units (OBUs). RSUs are typically installed at a road-side location to support the information exchange with vehicles, while OBUs are mounted in vehicles to enable the periodic exchange of safety information for a safe and comfortable driving environment. Also, a special kind of OBU named Public Safety On-board Unit (PSOBU) has been proposed to enable safety services (like emergency medical service or fire vehicles) to run certain public safety applications such as traffic signal prioritization for emergency vehicles.

Due to the ad hoc nature, communication types, and high-speed features, VANETs are challenged by several different security threats. Authentication and data integrity problems like identity/signature forging, repudiation, exculpability, and Sybil attacks are among the top VANET security issues addressed in recent years [1], [2], [3], [4], [5], [6]. Unfortunately, denial of service (DoS) attack on vehicular communications has not received much attention, although such attacks have been very commonly addressed in other ad hoc networks [7].

In a VANET, malicious entities might launch a denial of service (DoS) attack by overwhelming the communication channel so that crucial messages do not reach their destinations. The ideal intention of such an attack is to disable the whole network by continuously or selectively jamming the important transmissions. Since VANET is a real time communication system, consequences of losing regular transmissions could be fatal.

VANET providers offer multiple regular applications and services to the users through RSUs which can deliver road-safety information to the on-road vehicles. An RSU in a VANET serves as a gateway to the Internet backbone, several different road-safety applications and other services from the VANET providers. For example, an RSU may transmit periodic status for a parking assistance application [8], or traffic signal violation warning to the OBUs [9]; it can also broadcast traffic safety messages like ‘maximum curve turning speed’ or ‘construction ahead’ notifications to the vehicles in its communication range [10].

Presence of a long-term service or application is announced either in the context of a persistent WAVE Basic Service Set (WBSS [11]) using WAVE Service Announcements (WSA) on the control channel (CCH) at a regular interval, or through periodic WAVE Short Messages (WSMs [12]). A high-speed vehicle (OBU) may exchange information with neighboring entities by joining the nearest RSU’s WBSS. Also, a PSOBU may either form a persistent WBSS, or deliver periodic WSMs for transmitting its emergency public safety messages.

Since all these crucial service/application announcements or other important messages from providers (through RSUs, PSOBU, or even OBUs) are delivered in a periodic fashion, it is possible for a malicious node to launch a very straightforward but formidable attack on VANET by simply synchronizing to the corresponding provider’s periodic broadcast schedule.

A smart attacker may come in a disguise of an innocent OBU to broadcast the basic safety messages exactly at the same time as the periodic service announcements. Simultaneous frames would eventually collide, making a legitimate user unable to know about the offered service. The situation may get worse when multiple attackers collude for launching such an attack. Since broadcast communications are not accompanied by acknowledgements, the sending device would never come to know about the loss of the transmission.

In this paper, we analyze mathematically and through simulations synchronization-based distributed denial of service (DDoS) attack on a VANET by a small group of attackers. Also, we present different mitigation techniques to thwart...
the aforementioned DDoS attack in VANETs. Our solutions require modification of MAC layer’s Contention Window (CW) size and/or a re-arranging of the provider’s routine for broadcasting the periodic beacons.

We organize the rest of the paper as follows. DSRC and EDCA mechanism of IEEE 802.11p MAC are explored in Section II. Our attack model is presented in Section III. Configuration of the network simulator has been described in Section IV. Prevention methods to the synchronization-based DDoS attack in VANETs have been discussed in Section V while concluding remarks are posted in Section VI.

II. ON DSRC AND EDCA

IEEE’s Dedicated Short Range Communications or DSRC (IEEE 802.11p) [13] operates on a 75 MHz radio spectrum dedicated to a control channel (CCH), and 6 service channels (SCHs) in the range of 5.8/5.9 GHz.

A WAVE device in a VANET switches between the CCH and at least one of the SCHs as it is mandatory for a device to monitor the CCH on a regular interval. CCH is used for transmitting short, system control, and safety application messages while the SCH is usually picked for conducting ordinary data communications. Since WAVE entities are mostly assumed as single channel devices, they are essentially time synchronized using Coordinated Universal Time (UTC), commonly provided by Global Positioning System (GPS).

The concept of user priority in DSRC has been borrowed from the IEEE 802.11e EDCA mechanism to induce the prioritized access for data transmission on each DSRC channel. Access over each channel is ruled by four access categories as shown in Table I. Two channel access parameters, namely the Arbitration Inter-Frame Space (AIFS), and Contention Window (CW) jointly determine one of the four access categories for independent channel access function. Unlike a unicast operation, WAVE broadcast with EDCA uses only CWmin value to construct the backoff period.

We provide a brief outline on EDCA mechanism here with the help of Figure 1.

When the medium is idle, before transmitting a data frame, a station waits for $AIFS_k = SIFS + AIFSN_k \times t_{\text{slot}}$ where $t_{\text{slot}}$ is the duration of one time slot ($t_{\text{slot}} = 10\mu s$), and $AIFSN_k$ is determined by the priority class $k$.

If medium becomes busy during $AIFS_k$ period, the sender needs to wait for the end of busy period. As soon as the medium becomes idle, the sender restarts the $AIFS_k$ waiting process before being able to perform any action.

When there is a frame to broadcast, the sender selects a random number between 0 and $CW_{\text{min}}$ and counts down after every time slot while medium is idle. If the medium becomes busy, the station has to wait again for $AIFS_k$ before being able to decrement the backoff counter. The sender can broadcast the packet only when the backoff counter reaches the value of 0.

Hence, IEEE 802.11p’s EDCA mechanism at the MAC layer randomizes the time interval between two periodic announcements on a specific channel. EDCA not only prioritizes among the transmitted messages, but also reduces the chance of an external collision.

Broadcast communication in WAVE has no retransmission feature, meaning that the choice of CW values for a particular AC is limited. Therefore, due to the small CWmin of WAVE EDCA as shown in Table I, an attacker operating on the same AC can successfully synchronize to the RSU’s periodic broadcasts with a high probability. The greater the access category of an RSU is, the easier it is for attackers to launch the attack.

III. ATTACK MODEL

Our attack model consists of varying number of attackers which have the typical features of regular WAVE devices. An RSU broadcasts periodic frames either via Wireless Short Message Protocol (WCMP) on CCH, or transmits WAVE announcements at a regular interval for some service advertisement. The attackers in our model would attempt to synchronize to the RSU’s periodic transmissions and transmit the frame which will collide with RSU’s frame. In order to launch a successful attack, attackers need to achieve two kinds of synchronization: jitter, and backoff period.

a) Jitter estimation: In order to synchronize to the RSU’s periodic broadcasts, an attacker must estimate the slot boundary and backoff period for a frame in the first place. This can be accomplished by the following function of jitter estimation which takes into account multiple physical parameters of the attackers and the RSU.

$$jitter = f(t_{\text{prop}}, v_a, c_p, f_p)$$ (1)

where $t_{\text{prop}}$ is the propagation delay, $v_a$ is the ground speed of an attacker (attackers could be stationary too), $c_p$ is the clock precision indicator of an attacker with the corresponding RSU, and $f_p$ is the fading parameter of the network. An attacker can compute the RSU’s subsequent broadcast times by simply

![Figure 1. IEEE 802.11p’s EDCA mechanism](image-url)

**Table I**

<table>
<thead>
<tr>
<th>AC</th>
<th>AC</th>
<th>CWmin</th>
<th>CWmax</th>
<th>AIFSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>voice</td>
<td>3</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>video</td>
<td>3</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>best effort</td>
<td>7</td>
<td>15</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>background</td>
<td>15</td>
<td>511</td>
<td>9</td>
</tr>
</tbody>
</table>
adding on the known interval period to the estimated delivery time.

Since several different physical parameters contribute to the unexpected jitter between slot boundaries of the RSU and an attacker, the chances of an attacker start broadcasting within the same slot time as the RSU can be determined by approximating the offset or jitter using normal distribution with the mean equal to 0, and standard deviation equal to the half of unit backoff slot time \( t_{slot}/2 \approx 8\mu sec \). Thus, probability density function of slot synchronization yields:

\[
pr = \frac{1}{\sqrt{2\pi} \frac{t_{slot}}{4}} e^{-\frac{x^2}{2\left(\frac{t_{slot}}{4}\right)^2}} dx. \quad (2)
\]

(b) Estimation of backoff period : A successful attack would require an attacker not only to deliver the VANET frame simultaneously with the RSU, but also to have the same random CW size as RSU for a particular access category.

Let us consider that there are \( n \) attackers in a VANET trying to launch a DDoS attack by synchronizing the RSU’s periodic broadcasts. The probability of having \( r \) attackers with the same CW as RSU is given as:

\[
p_{cw}(r) = \binom{n}{r} \left( \frac{1}{CW} \right)^r \left(1 - \frac{1}{CW} \right)^{n-r} \quad (3)
\]

where \( CW \) is the size of the random contention window for a given access category.

Similarly, the probability of having \( l \) out of \( r \) attackers, who transmit within the same slot period as the RSU is:

\[
p_{slot}(r, l) = \binom{r}{l} (pr)^l (1-pr)^{r-l} \quad (4)
\]

where \( r \) is the number of attackers having same random CW as RSU.

Hence, the probability of a DDoS attack by \( n \) attackers is computed as:

\[
P_{DDoS} = \sum_{r=1}^{n} p_{cw}(r) \times \sum_{l=1}^{r} p_{slot}(r, l). \quad (5)
\]

From the equations above and the earlier discussions in Section II, we can claim that a successful synchronization to RSU’s periodic broadcast mostly depends on the length of the CW of the RSU and the attackers when both parties are operating on the same AC. In the following sections, we analyze the problem in more details with the help of simulation results of a practical VANET scenario.

IV. SIMULATION SETUP

We develop a simulation program to investigate the DDoS attack in VANET using the network simulator ns-2.34.

We assume a simple urban vehicular traffic scenario in a 200m \( \times \) 100m bidirectional road with 2 lanes in each direction. Individual vehicle’s speed follows following a Gaussian distribution with mean of 50 km/hr and standard deviation of 5 km/hr. We allow each OBU and the RSU to broadcast a WSMP packet every 100 ms for simulating OBU’s basic safety messages, and RSU’s periodic service announcements respectively.

Varying number of malicious attackers in the scenario pretend to be ordinary OBUs, but collude in a DDoS attack to synchronize to the RSU’s periodic broadcast schedule.

Times of the initial message broadcast for individual OBUs and the RSU have been chosen from a uniform distribution over 100 ms period. However, each attacker chooses the attack delay time to be the sum of the random backoff period and normally distributed jitter with mean value 0 and standard deviation of half of the unit backoff slot time (i.e. \( 8\mu sec \)).

We run the simulation for 30 seconds following a 10 seconds warmup period. Each experiment is run 10 times using different seeds, and individual results are averaged for the final outcome.

<table>
<thead>
<tr>
<th>TABLE II</th>
<th>SIMULATION PARAMETERS FOR MAC AND PHY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Values</td>
</tr>
<tr>
<td>Data Rate</td>
<td>6Mbps</td>
</tr>
<tr>
<td>Slot Time</td>
<td>16\mu sec</td>
</tr>
<tr>
<td>SIFS</td>
<td>32\mu sec</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>10MHz</td>
</tr>
<tr>
<td>Frequency</td>
<td>5.89GHz</td>
</tr>
<tr>
<td>Propagation Model</td>
<td>TwoRayGround</td>
</tr>
</tbody>
</table>

We implement the EDCA mechanism over IEEE Std 802.11p MAC and PHY provided by ns-2.34’s IEEE 802.11Ext package from Chen et al. [14]. We configure the EDCA parameters for individual access categories on the DSRC CCH. Other MAC and PHY parameters used in our simulation are listed in Table II.

IEEE 802.11p MAC allows four distinguished priority classes for best effort, background, video, and voice data traffic. The latter two categories are given higher priorities over the first two traffic classes as the related EDCA parameters for IEEE 802.11p control channel (CCH) are listed in Table I. Payloads for all the broadcasts are assumed to be the same. We follow the signed WAVE Short Message (WSM) protocol format (see C.6 of [15]) for the OBU, RSU, and the attacker payloads.

We plot the drop probability of RSU’s periodic frames from our analytical results, as well as from the simulation using different access categories and varying number of attackers. At this point, we ignore the presence of other legitimate OBUs in the network. As shown in Figure 2, the drop probability of a periodic broadcast from the RSU raises as the number of attackers increases.

Since the attackers are on the same access category, they have the same AIFS value as RSU. Therefore, the DDoS attack on RSU’s periodic broadcasts is mainly because of the CWmin values of the corresponding access categories. As both AC3 and AC2 have the same CWmin value of 3, the drop probability of RSU’s periodic frames on those ACs are overlapped with each other. As mentioned before, ACs with larger CWs performed better against the RSU synchronization.

In the next section, we do some further experiments using
Fig. 2. Probability of RSU’s periodic message drop on a DDoS attack.

our simulation tool to evaluate our proposed countermeasure options.

V. Mitigating the DDoS Attack

VI. Conclusion

REFERENCES


Fig. 3. Periodic message drop probability on a DDoS attack for different access categories and standard deviation values.

Fig. 4. Packet drop probability on DDoS Attack with extended contention window size in AC3.

- AC3
- AC2
- AC0
- AC1

![Graphs showing periodic message and packet drop probabilities for different access categories.](image-url)