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 VANET that uses IEEE 802.11p EDCA mechanism is susceptible to a synchronization-based DDoS attack due to periodicity of transmissions and small contention window sizes. To make things worse, neither the sender nor receivers of periodic broadcasts will be aware of the attack since broadcast communications in VANET do not have acknowledgements. In this paper, we analyze the prospect of a synchronization-based DDoS attacks on vehicular communications and propose mitigation techniques to avoid such an attack.**

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 vehicles (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]. However, 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].

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.

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 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.

A straightforward attack of this kind might be launched by a malicious node that would simply synchronize to the corresponding providers broadcast schedule and broadcast false messages at the exact same time as the service announcement (which are delivered in a periodic fashion). Multiple attackers may focus on the same transmission, with increased chance of success. Simultaneous frames would eventually collide, making a legitimate user unaware of the real messages with potentially disastrous consequences. Worse yet, the device that sent the real message would never know that it has been lost, since broadcast communications are not accompanied by acknowledgements.

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 broadcast 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

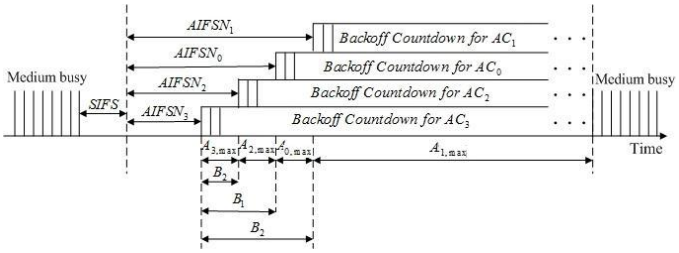


Fig. 1. IEEE 802.11p's EDCA mechanism

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 can be performed using four access categories AC_k, $k = 0..3$ as shown in Table 1. Priority of AC_k is regulated with two channel access parameters, namely the Arbitration Inter-Frame Space ($AIFS_k$), and Contention Window (CW_k). Unlike a unicast operation, WAVE broadcast using AC_k uses only $CWmin_k$ 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 $AIFS_k = SIFS + AIFSN_k \times t_{slot}$ where t_{slot} is the duration of one time slot ($t_{slot} = 16\mu sec.$), and $AIFSN_k$ is determined by the priority class k.

If the 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 CWmin 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,

TABLE I
EDCA Parameters used in CCH(values taken from [11]).

ACI	AC	CWmin	CWmax	AIFSN
3	voice	3	7	2
2	video	3	7	3
0	best effort	7	15	6
1	background	15	511	9

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_k values for a particular AC_k is limited. Therefore, due to the small CWmin of WAVE EDCA as shown in Table I, an attacker operating on the same AC_k 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 attempt to synchronize to the RSU's periodic transmissions and transmit frames to collide with RSU's frames. In order to launch a successful attack, attackers need to achieve two kinds of synchronization. First one is with respect to start of backoff slot, and the second one is with respect to the duration of backoff period.

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

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

where t_{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 between an attacker and RSU. An attacker can compute the RSU's subsequent broadcast times by simply adding on the known interval period to the estimated delivery time.

Since several different physical parameters contribute to the jitter between slot boundaries of the RSU and an attacker, the probability of an attacker starting to broadcast within the same slot time as the RSU can be determined by approximating the jitter using normal distribution with zero mean, and standard

deviation of half of unit backoff slot time $t_{slot}/2$= 8μsec. i.e.,

$$pr = \int_{-t_{slot}/2}^{t_{slot}/2} \frac{1}{\sqrt{2\pi(\frac{t_{slot}}{2})^2}} e^{\frac{-x^2}{2(\frac{t_{slot}}{2})^2}} dx. \quad (2)$$

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_k size as RSU for a particular access category k.

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

$$p_{cw}(r,k) = \binom{n}{r} (\frac{1}{CW_k})^r (1 - \frac{1}{CW_k})^{n-r} \quad (3)$$

where CW_k is the size of the random contention window for a given access category k.

Similarly, the probability of having l attackers that 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_k as RSU on class k.

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

$$P_{DDoS_k} = \sum_{r=1}^{n} p_{cw(r,k)}(r) \sum_{l=1}^{r} p_{slot}(r,l). \quad (5)$$

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_k of the RSU and the attackers when both parties are operating on the same AC_k. $AIFS_k$ values do not affect P_{DDoS_k} for attackers with the same access class k.

IV. Simulation Setup

We developed 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 $900m \times 100m$ bidirectional road with 2 lanes in each direction. Individual vehicle's speed varies following a Gausian 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.

A varying number of malicious attackers in the scenario pretend to be ordinary OBUs participate in a DDoS attack by synchronizing 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 uniformly distributed random backoff period and normally distributed jitter with mean value

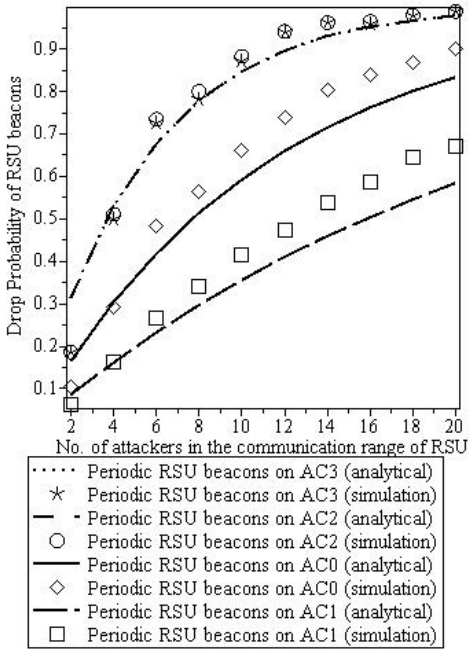


Fig. 2. Probability of RSU's periodic message drop on a DDoS attack.

0 and standard deviation of half of the unit backoff slot time (i.e. 8μsec).

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.

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.

TABLE II
Simulation Parameters for MAC and PHY

Parameters	Values
Data Rate	6Mbps
Slot Time	16μs
SIFS	32μs
Bandwidth	10MHz
Frequency	5.89GHz
Propagation Model	TwoRayGround

IEEE 1609.4 and 802.11p MAC access classes AC_k, $k = 0..3$ (with parameters listed in Table I) are mapped into best effort, background, video and voice classes respectively.

Payloads for all the broadcasts are assumed to be 254 Bytes long. 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, using analytical values obtained from expression 5 and simulation results obtained with the same access categories and

number of attackers. (At this point, we ignore the presence of other legitimate OBUs in the network.) As shown in Fig. 2, the drop probability of a periodic broadcast from the RSU increases with the number of simultaneous attackers. Since the attackers use the same access category as the RSU, their AIFS value is the same as well. In general, access categories with larger contention window value perform somewhat better because the corresponding contention windows are longer; as AC3 and AC2 have the same minimum contention window value of 3, the corresponding curves are very close to each other.

V. Mitigating the DDoS Attack

We introduce the following techniques to thwart the synchronization-based DDoS attack in VANETs.

A. Randomizing the RSU Schedule

Since periodic broadcasts allow delivery frames at a regular interval, an attacker may successfully guess the timing of subsequent broadcast attempts from the knowledge of any of the previous delivery times. In order to get rid of this problem, a deliberate randomization of the delivery time can be applied during each cycle of periodic transmission. An RSU can randomize the schedule for its periodic broadcasts by following a normal distribution with the originally scheduled broadcast time as the mean, and a predefined small delay as the standard deviation, with the intention of reducing the accuracy of attacker's jitter estimate, and thus diminishing its ability to synchronize with the RSU's transmission.

Experiment 1: Using the simulator described in Section IV, we run an experiment with a number of attackers ranging from 2 to 20 hiding in disguise of OBUs in a VANET. An RSU, and 100 OBUs in the network are transmitting 10 periodic frames per second while attackers are attempting to synchronize to the RSU's timing of periodic frame delivery. We choose six different standard deviations for this experiment: unit slot time period (16μsec.), two slot period (32μsec), four slot period (64μsec.), five slot period (80μsec.), ten slot period (160μsec.), and fifteen slot period (240μsec.).

Assuming that all the WAVE devices are working in the same AC_k, we repeat the same experiment for all four priority classes.

Results of this experiment are shown in Fig. 3. We also compare the results with the regular periodic broadcast scenario for the corresponding access categories. The changed RSU schedule achieves notable success in reducing the frame loss due to the synchronization-based DDoS attack. From the outcome of the experiment, we can also anticipate that this mitigation technique is effective mostly within the range of 4 to 5 slot times.

B. Increasing the Contention Window

As given in expression (3), an attacker's estimation of backoff period depends on the CW_k for the access category AC_k. Increasing the value of the CW_k would result in a smaller probability $p_{cw}(r, k)$ of having the same contention window with the attackers.

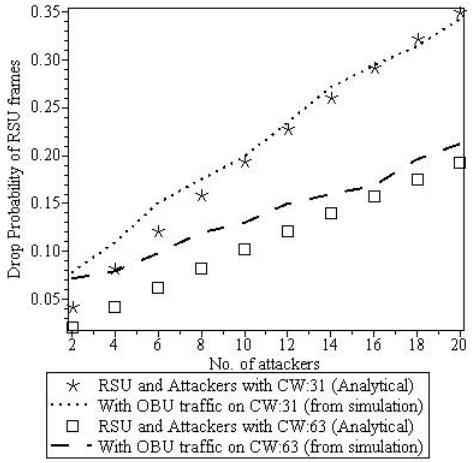


Fig. 4. Experiment 2: Packet drop probability on DDoS Attack with extended contention window size in AC3.

Experiment 2: We keep the similar set up of Experiment 1, and run the simulation with the larger contention window (CW_k) for each of the VANET entities. We use the contention window size 31 and 63 respectively to make a DDoS attack reasonably hard for the attackers.

Results are plotted in Fig. 4. The drop probability of the RSU periodic broadcasts has been reduced significantly compared to the similar experiment with AC3. Therefore, the larger the contention window we have, the more we can protect the network against a synchronization-based DDoS attack.

C. Randomization with Increasing the Contention Window

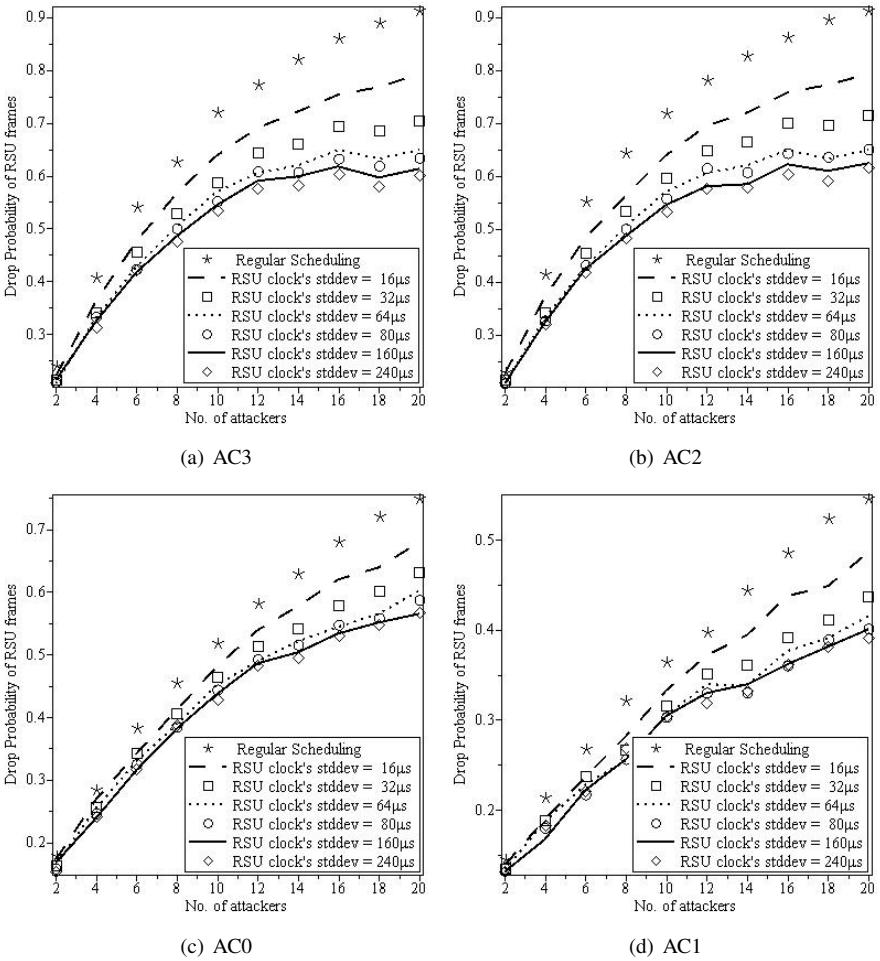
We apply the techniques of Experiment 1 and 2 simultaneously to prevent the synchronization-based DDoS attack in VANETs.

Experiment 3: In this experiment, we increase the contention window size of each VANET entity, at the same time the RSU randomizes the schedule for periodic broadcasts.

Fig. 5 reveals the outcome of the experiment. The drop probability has been reduced for each combination of contention window size and the standard deviation of the RSU's randomization of the periodic transmission.

VI. Conclusion

In this paper, we highlight a security vulnerability of VANETs where a group of malicious entities can launch a DDoS attack exploiting the IEEE 802.11p's weak EDCA credentials. EDCA allows a VANET entity to prioritize the outgoing frames by $AIFSN_k$ and contention window (CW_k). However, due to the small contention window sizes, an intelligent attacker can easily synchronize to any periodic transmission in the network. We analyze the prospect of launching such an attack, and also suggest different mitigating techniques including larger EDCA parameters for VANET entities. Our



(a) AC3 (b) AC2

(c) AC0 (d) AC1

Fig. 3. Experiment 1: Periodic message drop probability on a DDoS attack for different access categories and standard deviation values

attack model and the solutions have been well supported by mathematical analysis, as well as simulation results.

REFERENCES

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 6, pp. 2772 –2785, july 2010.

[2] S. Biswas and J. Misic, "Location-based anonymous authentication for vehicular communications," in *PIMRC 2011: Proceedings of the 22nd IEEE Symposium on Personal, Indoor, Mobile and Radio Communications*. IEEE Communication Society, 2011, pp. 1–5.

[3] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 2, pp. 559 –573, 2010.

[4] Y. Sun, R. Lu, X. Lin, X. S. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 7, pp. 3589 –3603, 2010.

[5] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, Extensible, and Efficient VANET Authentication," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 574–588, Dec. 2009.

[6] J. Isaac, S. Zeadally, and J. Camara, "Security attacks and solutions for vehicular ad hoc networks," *Communications, IET*, vol. 4, no. 7, pp. 894–903, 30 2010.

[7] D. J. Thuente, B. Newlin, and M. Acharya, "Jamming Vulnerabilities of IEEE 802.11e," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*, Orlando, FL, USA, oct. 2007, pp. 1–7.

[8] S. Biswas and J. Misic, "Prioritized WAVE-based Parking Assistance with Security and User Anonymity," *to appear in Journal of Communications, Special Issue on Security and Privacy in Communication Systems and Networks*, 2012.

[9] J. Guo, J. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," May 2007, pp. 103–108.

[10] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 88 –95, april 2008.

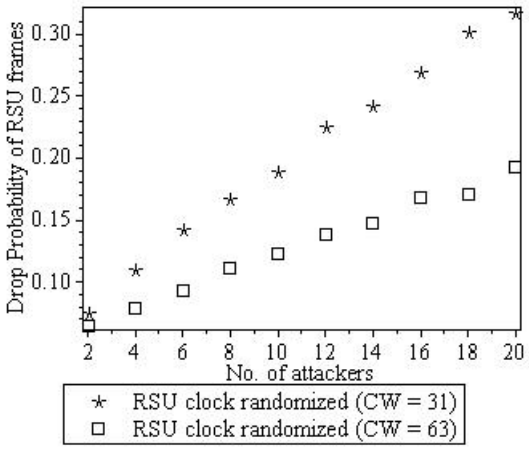
[11] "IEEE trial-use standard for wireless access in vehicular environments (wave)- multi-channel operation," IEEE, New York, NY, IEEE Std 1609.4, Nov. 2006.

[12] "IEEE trial-use standard for wireless access in vehicular environments (WAVE)- networking services," IEEE, New York, NY, IEEE Std 1609.3, Apr. 2007.

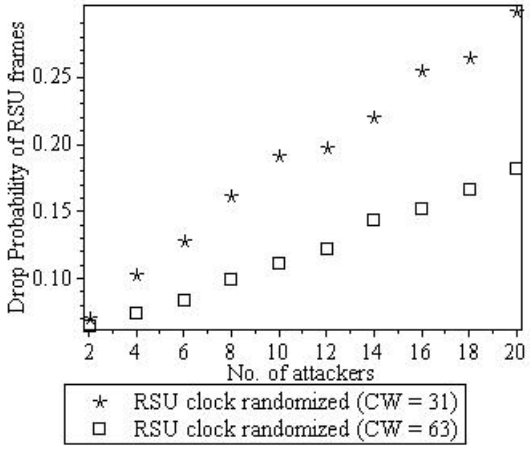
[13] "Draft amendment for wireless access in vehicular environments (WAVE)," IEEE, New York, NY, IEEE Draft 802.11p, Jul. 2007.

[14] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, "Overhaul of IEEE 802.11 modeling and simulation in ns-2," in *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, ser. MSWiM '07. New York, NY, USA: ACM, 2007, pp. 159–168.

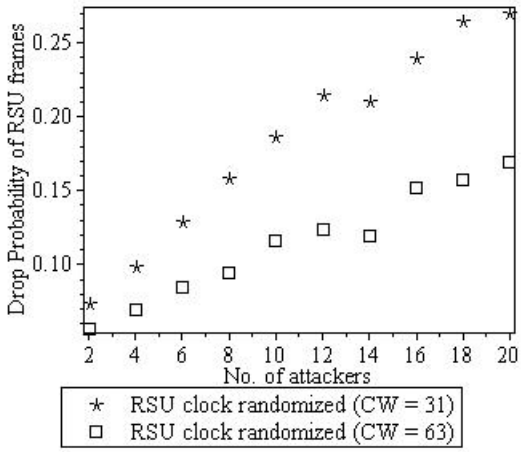
[15] "IEEE trial-use standard for wireless access in vehicular environments (WAVE)- security services for applications and management messages," IEEE, New York, NY, IEEE Std 1609.2, Jul. 2006.



(a) RSU clock randomized (standard deviation = 16μs).



(b) RSU clock randomized (standard deviation = 32μs).



(c) RSU clock randomized (standard deviation = 64μs).

Fig. 5. Experiment 3: Drop probability of periodic frames by an RSU during a DDoS attack with extended contention window size and RSU time randomized.