Certificate Status Information Distribution and Validation in Vehicular Networks

Carlos H. Gañán
carlos.ganan@entel.upc.edu

Advisor: José L. Muñoz Tapia
Co-advisor: Óscar Esparza
Department of Telematics Engineering (UPC)

Doctoral Dissertation Defense

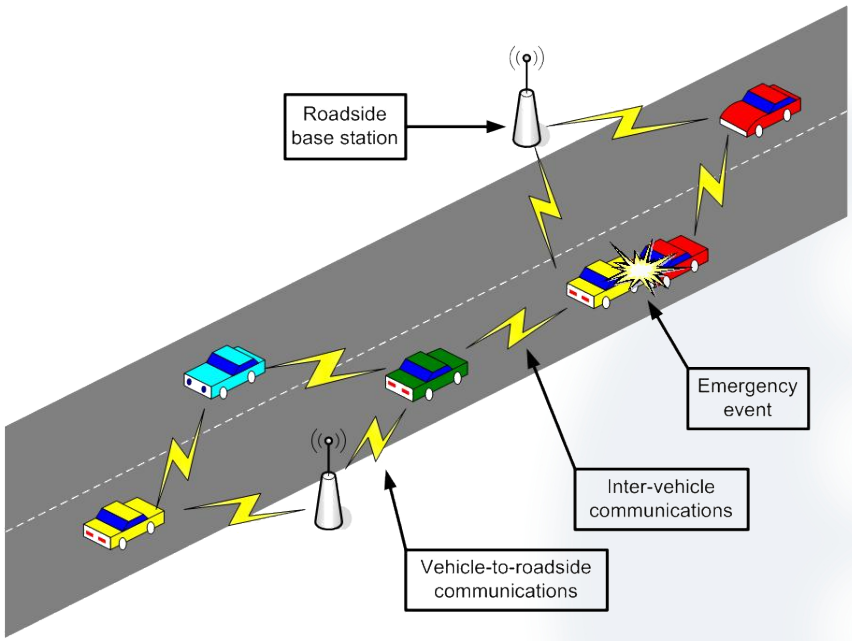
Barcelona, September 4, 2013

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Departament d'Enginyeria Telemàtica

Outline

Outline

What is VANET?



- Communication: typically over the Dedicated Short Range Communications (DSRC) (5.9 GHz).
- Example of protocol: IEEE 802.11p.
- Penetration will be progressive (over 2 decades or so).

Security Standard: 1609.2 I

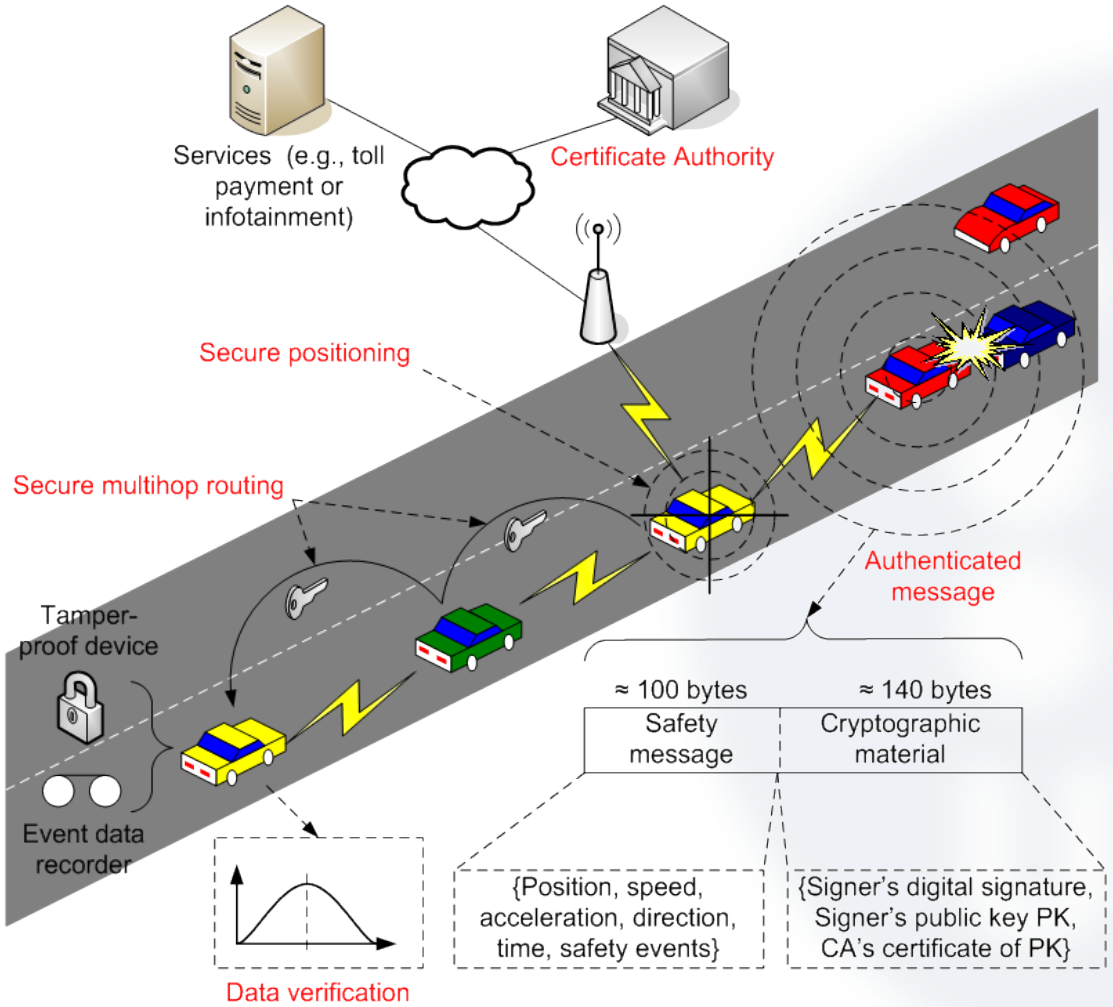
- Integrity: messages must be protected from any alteration.
- Authentication: the receiver is ensured that the sender generated a message. The receiver has evidence of the liveness of the sender.
- Access Control: establish what each node is allowed to do in the network.
- Confidentiality: the content of a message is kept secret from those nodes that are not authorized to access it.
- Availability: protocols and services should remain operational even in the presence of faults, malicious or benign.

Security Standard: 1609.2 II

Privacy and Anonymity

- Not addressed in the current version.
- For broadcast applications:
  - Ensure that that identifiers do not link to the device's real-world identity,
  - Ensure that identifiers change frequently,
  - Ensure that identifiers change at the same time.

Security Architecture



Context I

IEEE 1609.2-2013

- Based on Public Key Infrastructure
  - Trusted authority signs a copy of each OBU's public key
  - Every OBU gets a copy of the authority's public key
  - OBUs sign each message using their private key
- Authority must publicize which OBUs are no longer valid
  - Certificate Revocation Lists (CRLs) are needed for:
    - Excluding compromised, faulty or illegitimate nodes
    - Preventing the use of compromised cryptographic material
  - CRL pose a problem: How to distribute large CRLs in a reasonable time with low bandwidth utilization?

Problem Statement

- Distributing CRLs is an issue
  - Large list to distribute and keep up to date
  - Millions of vehicles removed from the road annually

Objectives

- Minimize the size of the revocation data
- Minimize communication overhead
- Fast certificate validation with minimum cryptographic overhead

Outline

Data Collection I

Issuer Name	# Revoked Certificates	Last Update	Next Update
GoDaddy	932,900	2012/02/01	2012/02/03
VeriSign	5,346	2012/02/02	2012/02/16
Comodo	2,727	2012/02/03	2012/02/06
Thawte	8,061	2012/02/01	2012/02/16

Table: Description of the collected CRLs.

Data Collection II

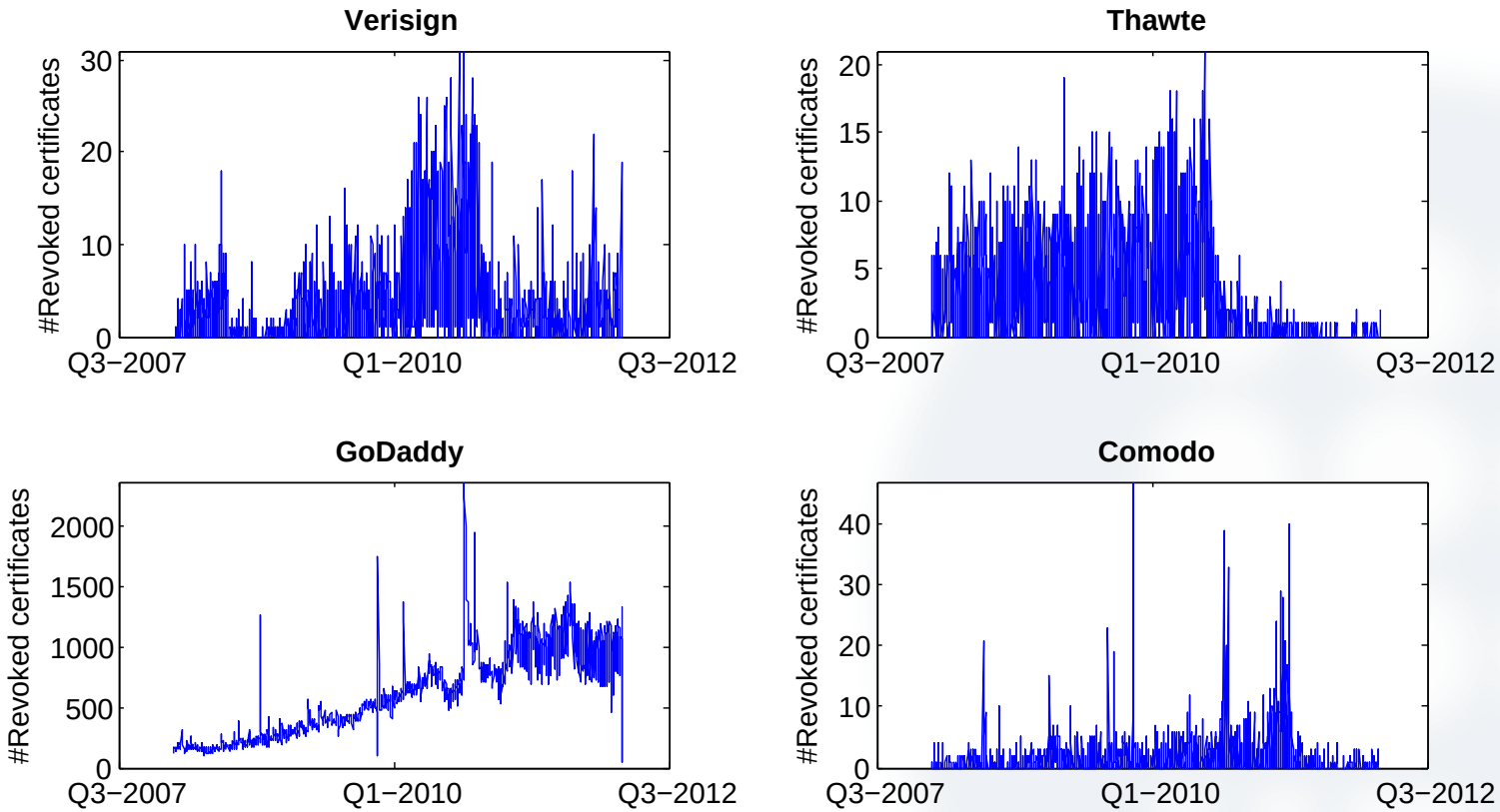


Figure: Number of daily revoked certificates evolution for each CA.

Analysis revocation data I

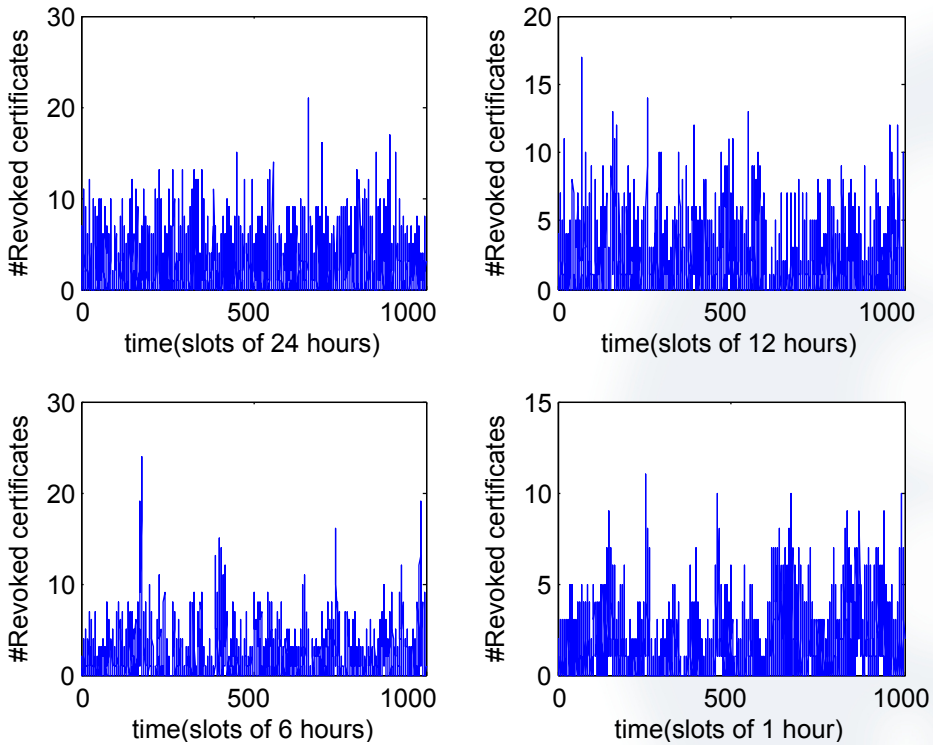


Figure: Revocation Bursts over Four Orders of Magnitude.

Analysis revocation data II

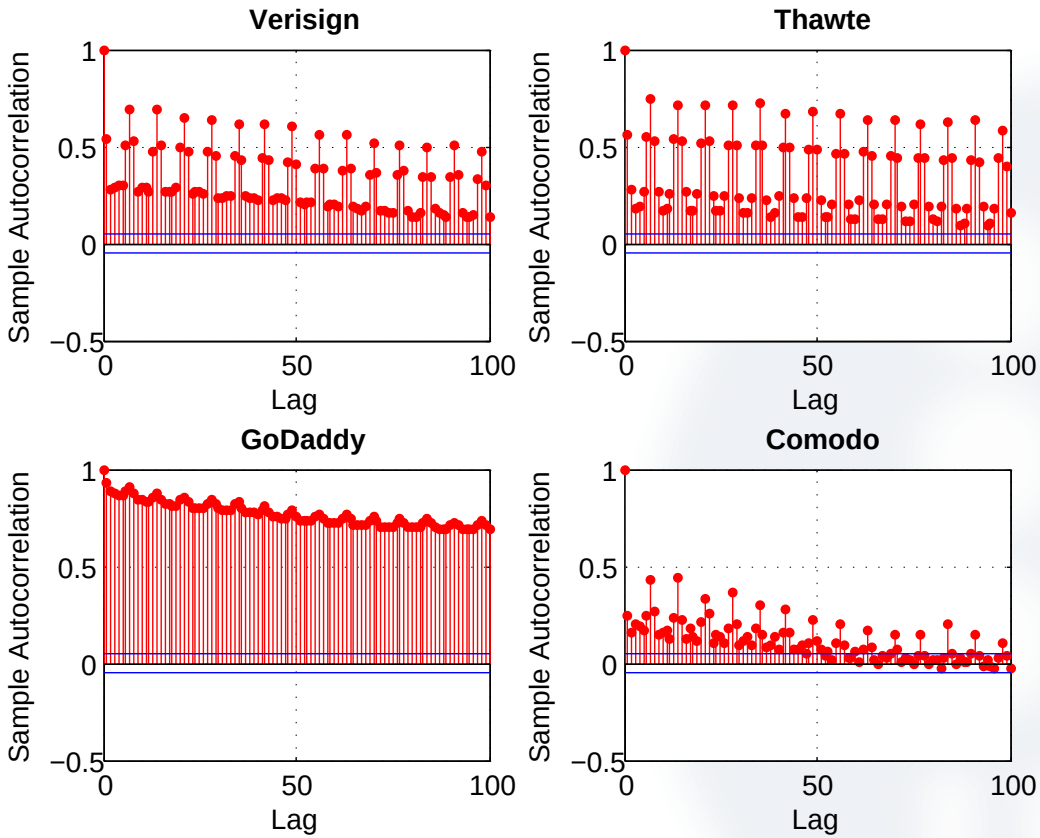


Figure: Autocorrelation function of the revocation process per CA.

Revocation process

- Current models assume that revocation follows Poisson process, i.e.:
  - when observed on a fine time scale will appear bursty,
  - when aggregated on a coarse time scale will flatten (smooth) to white noise.

Revocation Process

- A Self-Similar process:
  - when aggregated over wide range of time scales will maintain its bursty characteristic

What is Self-Similarity? I

- Self-similarity describes the phenomenon where a certain property of an object is preserved with respect to scaling in space and/or time.
- If an object is self-similar, its parts, when magnified, resemble the shape of the whole.
- In other words, self-similarity implies a "fractal-like" behavior: no matter what time scale you use to examine the data, you see similar patterns
- Implications:
  - Burstiness exists across many time scales
  - No natural length of a burst
  - Revocation data does not necessarily get "smoother" when you aggregate it (unlike Poisson traffic)

What is Self-Similarity? II

- Consider a zero-mean stationary time series $X = (X_t; t = 1, 2, 3, \ldots)$, we define the m-aggregated series $X^{(m)} = (X_k^{(m)}; k = 1, 2, 3, \ldots)$ by summing X over blocks of size m. We say X is *H*-self-similar if for all positive m, $X^{(m)}$ has the same distribution as X rescaled by m^H.
- If X is H-self-similar, it has the same autocorrelation function as the series $X^{(m)}$ for all m. This is actually distributional self-similarity.
- Degree of self-similarity is expressed as the speed of decay of series autocorrelation function using the Hurst parameter
  - For SS series with LRD, $0.5 < H < 1$
  - Degree of SS and LRD increases as $H \to 1$

Why is Self-Similarity Important?

- Current revocation data releasing policies are modeled using Poisson distributing (etc.) which does not take into account the self-similar nature of traffic.
- This leads to inaccurate modeling of the infrastructure needed to support the revocation service.

Measuring Self-similarity

- Hurst Parameter H, $0.5 < H < 1$
- Five approaches to estimate H (Based on properties of self-similar processes)
  - Variance Analysis of aggregated processes
  - Analysis of Rescaled Range (R/S) statistic for different block sizes
  - Periodogram-based analysis in the frequency domain
  - Detrended Fluctuation Analysis (DFA)
  - A Whittle Estimator

Hust Parameter Estimation

- All five tests for self-similarity were employed: $0.7 < H < 0.95$

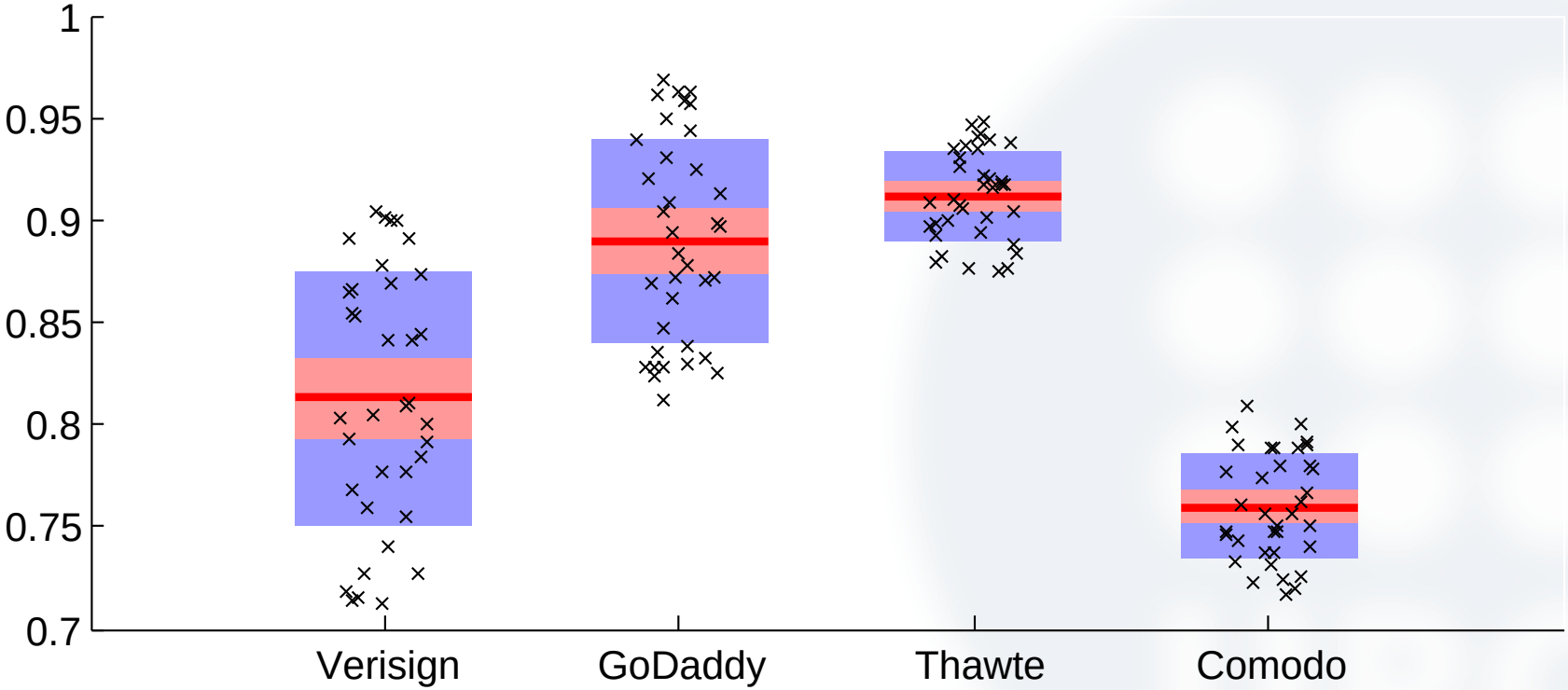


Figure: Summary plot of estimates of the Hurst parameter H for all the CAs.

Impact on CRLs

- $Size_{CRL} = 51 + 4.5 \cdot r \cdot L_c$ (bytes)

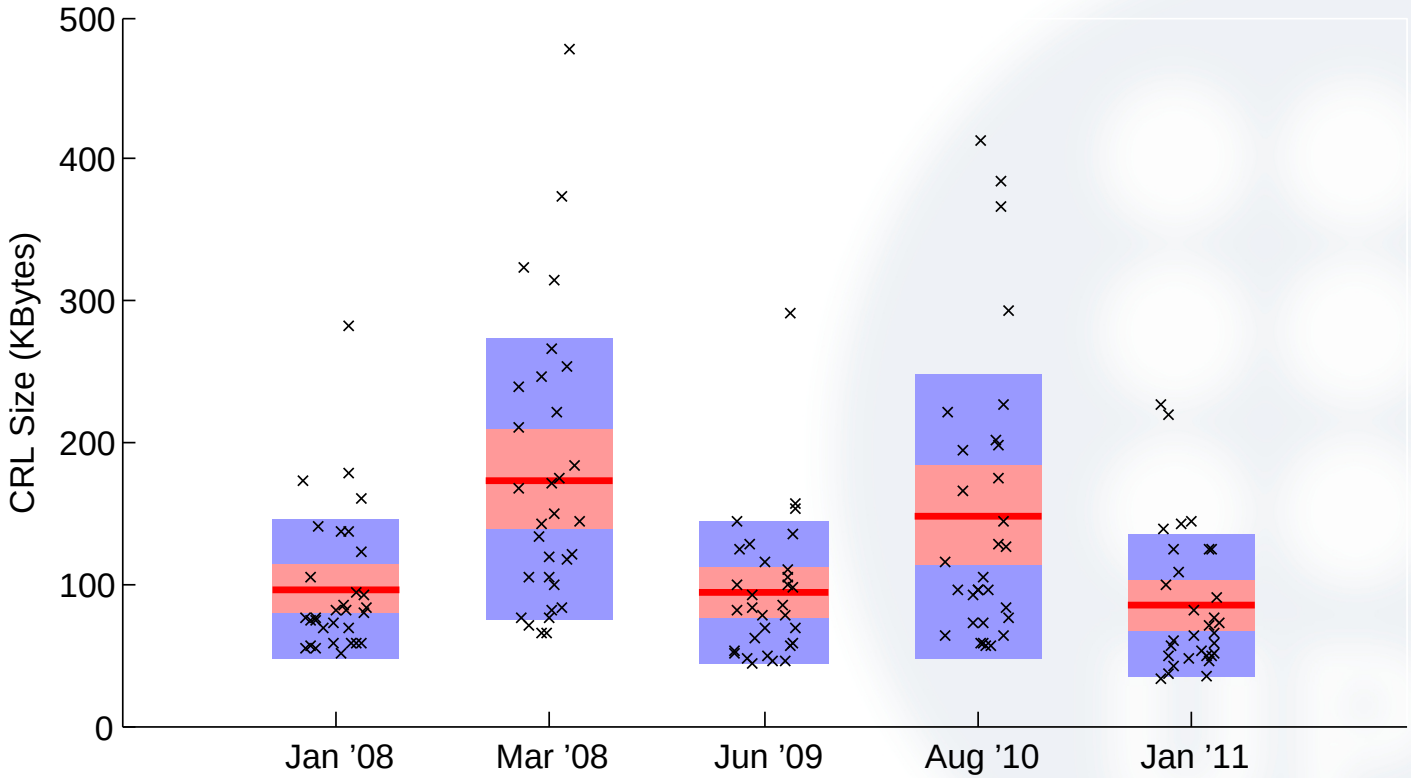


Figure: Estimated daily size of Verisign's CRL.

Impact on delta-CRLs

$$B = \frac{Nve^{-vt}((51 + 4.5rL_c)e^{-(w+\frac{I}{O}-I)v} + (51 + 9rw))}{(O-1)1 - e^{vI/O} + 1}$$

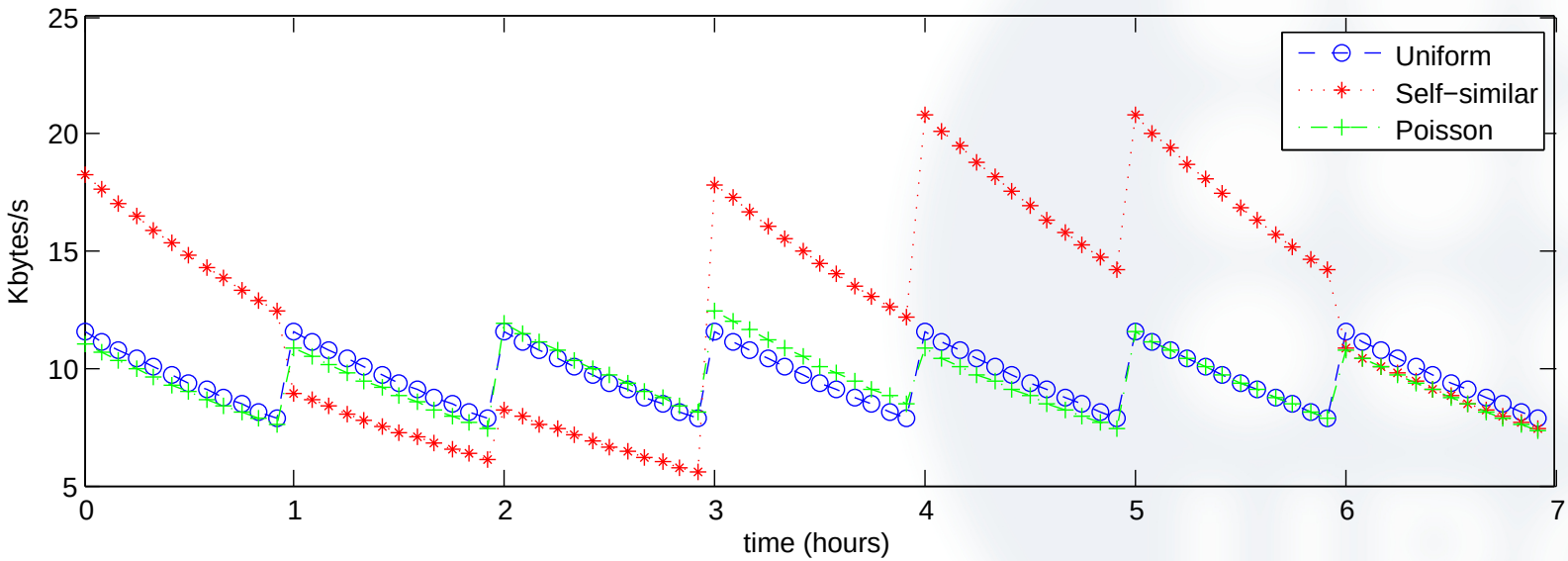


Figure: Delta-CRL BW consumption.

Revocation process model I

- Based on an autoregressive fractionally integrated moving average (ARFIMA) process

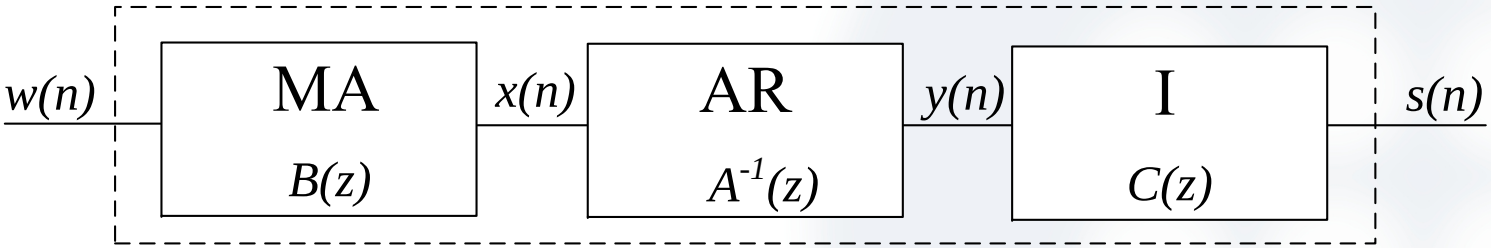


Figure: Components of an ARFIMA process.

Revocation process model II

$$w(n) \boxed{\frac{b_0 + b_1 z^{-1} + b_2 z^{-2} \ldots + b_q z^{-q}}{(1 + a_1 z^{-1} + a_2 z^{-2} \ldots + a_p z^{-p})(1 - z^{-1})^d}} s(n)$$

$$\begin{aligned} A(z) = {} & 1 - 0.6467z^{-1} + 0.02693z^{-2} + 0.09085z^{-3} + 0.09753z^{-4} + 0.1218z^{-5} + 0.1991z^{-6} \\ & - 0.804z^{-7} + 0.6906z^{-8} + 0.03223z^{-9} - 0.04807z^{-10} - 0.007471z^{-11} - 0.0759z^{-12} \\ & - 0.08934z^{-13} - 0.07605z^{-14} - 0.006487z^{-15} - 0.02565z^{-16} - 0.01994z^{-17} - 0.04003z^{-18} \\ & - 0.05007z^{-19} - 0.01331z^{-20} - 0.07361z^{-21} - 0.001947z^{-22} - 0.02836z^{-23} - 0.01824z^{-24} \\ & - 0.03693z^{-25} + 0.007019z^{-26} - 0.07691z^{-27} - 0.01872z^{-28} - 0.03821z^{-29}, \end{aligned} \quad (1)$$

$$\begin{aligned} B(z) = {} & 1 - 0.6454z^{-1} + 0.005554z^{-2} + 0.1113z^{-3} + 0.1317z^{-4} + 0.1032z^{-5} + 0.2802z^{-6} \\ & - 0.6652z^{-7} + 0.6688z^{-8}, \end{aligned} \quad (2)$$

$$C(z) = (1 - z^{-1})^{-0.3}. \quad (3)$$

Synthetic Revocation trace generator I

- Concatenation of a zero memory non-linear function (ZMNL) to the ARFIMA filter

$$g(s(n)) = max\left(0, \left\lceil \mu_r - \mu_r \frac{\sigma_r}{\sigma_s} \cdot ln\left(\frac{1}{\sqrt{2\pi\ \sigma_s^2}} \int_{-\infty}^{s(n)} e^{-\frac{x}{2\ \sigma_s^2}}\, dx\right)\right\rceil\right)$$

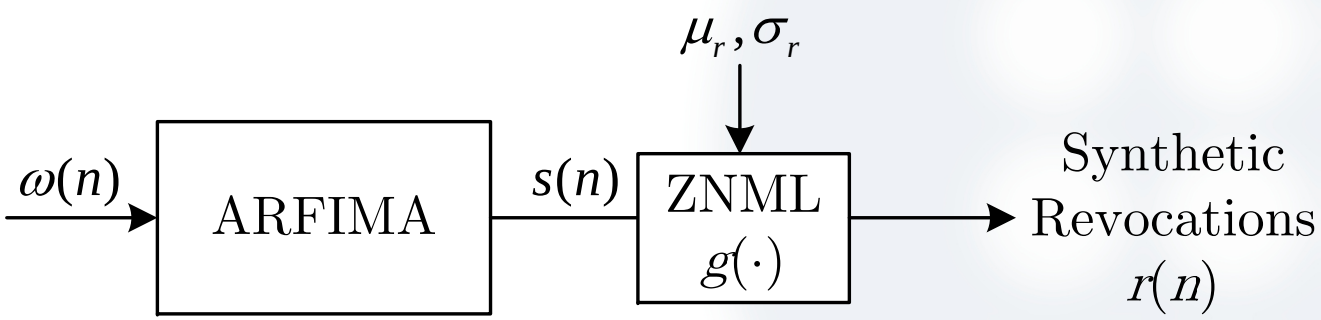
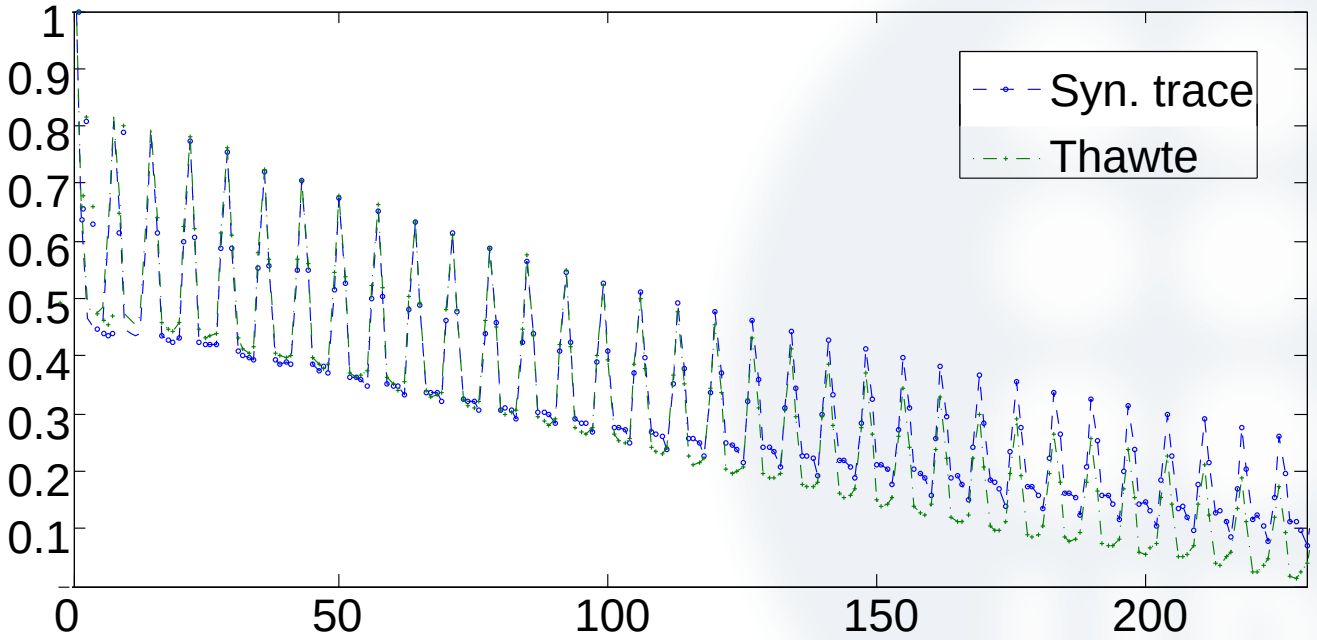


Figure: Synthetic Revocation trace generator.

Quality of the traces

- Correlation Structure



Conclusions

- Established that revocation data self-similar, i.e., burstiness at all time-scales, confirming scale-invariance of distribution.
- Poisson distribution is not able to capture the bursty pattern
- Traditional revocation mechanisms, such as CRLs or delta-CRLs, do not take into account self-similarity:
  - These bursts increase the maximum peak bandwidth required to provide the revocation data timely.

Publications

Carlos Gañán, Jorge Mata-Diaz, Jose L. Munoz, Juan Hernandez-Serrano, Oscar Esparza, and Juanjo Alins.
A Modeling of Certificate Revocation and Its Application to Synthesis of Revocation Traces.
IEEE Transactions on Information Forensics and Security, 7(6):1673–1686, December 2012.

Carlos Gañán, Jorge Mata-Díaz, Jose L. Muñoz, Oscar Esparza, and Juanjo Alins.
On the Self-similarity Nature of the Revocation Data.
In Dieter Gollmann and FelixC. Freiling, editors, *Information Security*, volume 7483 of *Lecture Notes in Computer Science*, pages 387–400, Passau, 2012. Springer Berlin Heidelberg.

Outline

Challenges & Constraints

- Scalability
  - Large number of revoked certificates
  - Large number of equipped vehicles that need the revocation information
- Communication between RSUs and vehicles
  - Non-pervasive
  - Short contact times
  - Bandwidth constrained

Problem Statement

- Distributing CRLs is an issue
  - Large list to distribute and keep up to date
  - Millions of vehicles removed from the road annually
- OBUs cannot download the CRL as frequently as users do in wired network
  - Trade-off between the frehsness of the revocation information and the updating frequency.
  - Vehicles will be taking some risk while operating with cached CRLs.
- CRLs are issued periodically.
- *Time-stamps* are a typical way of ensuring freshness.
- However, during the validity of the CRL, the new revoked certificates are unknown to the users.
- The set of unknown revoked certificates could be specially large in VANET.

Objectives

- There exists a risk inherent in the vehicular PKI, as total security is unachievable
- That risk cannot be avoided but controlled

Risk Aware Revocation mechanism for VANET

- Certification Authorities can estimate the risk of operating in the VANET
- Users should set recency requirements that will determine how recent a CRL should be.
- More strict recency requirements have lower risk, but they have higher communication costs
- Because risk is application-dependent, different applications and users have different recency requirements

Probability of using an unknown revoked certificate I

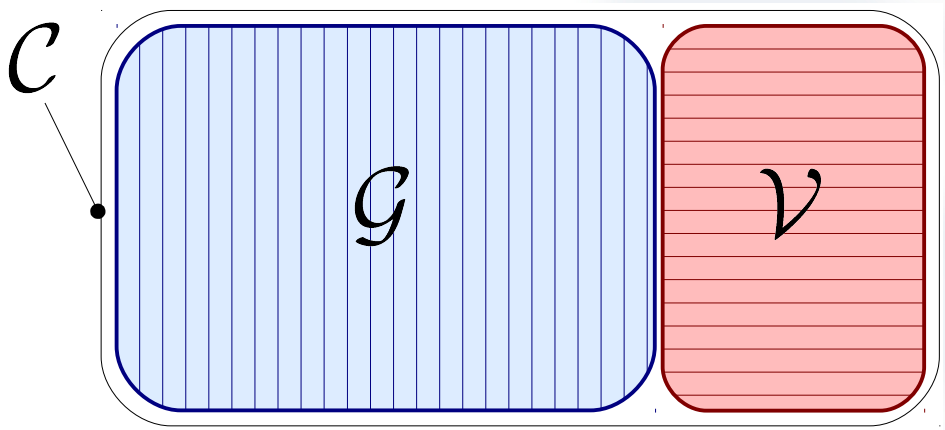
Assumptions

- Certificate queries arrive following a Poisson law
- Expiration time is homogeneous for all certificates (T_c cte.)
- Certificate revocation events are independent from the certification process.
- The percentage of revoked certificates (p) remains roughly constant during consecutive CRL updates.

Probability of using an unknown revoked certificate II

Notation

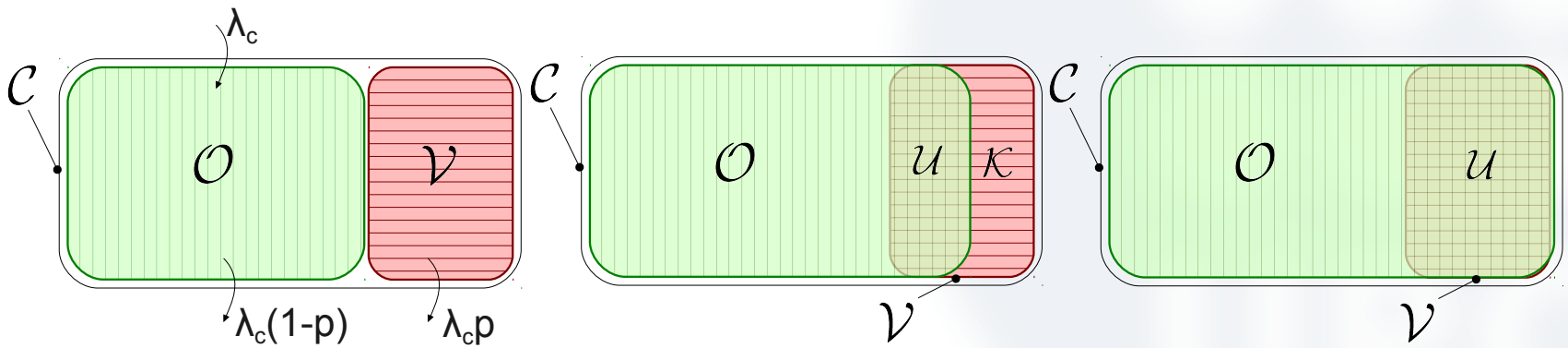
- Let $\mathcal{C}$ be the set of *non-expired certificates*
- Let $\mathcal{V}$ be the set of *revoked non-expired certificates*
- Let $\mathcal{G}$ be the set of *non-expired certificates* that have not been revoked



Probability of using an unknown revoked certificate III

Notation

- Let $\mathcal{O}$ be the set of *non-expired certificates* for which the latest status known by a user is *non-revoked*.
- Let $\mathcal{U}$ be the *unknown revoked operative certificates*
- Let $\mathcal{K}$ be the set of *non-expired certificates* for which the latest status known by a user is *revoked*.



(a) $t = t_0 = thisUpdate$ (b) $t < T_c$ (c) $t \geq T_c$

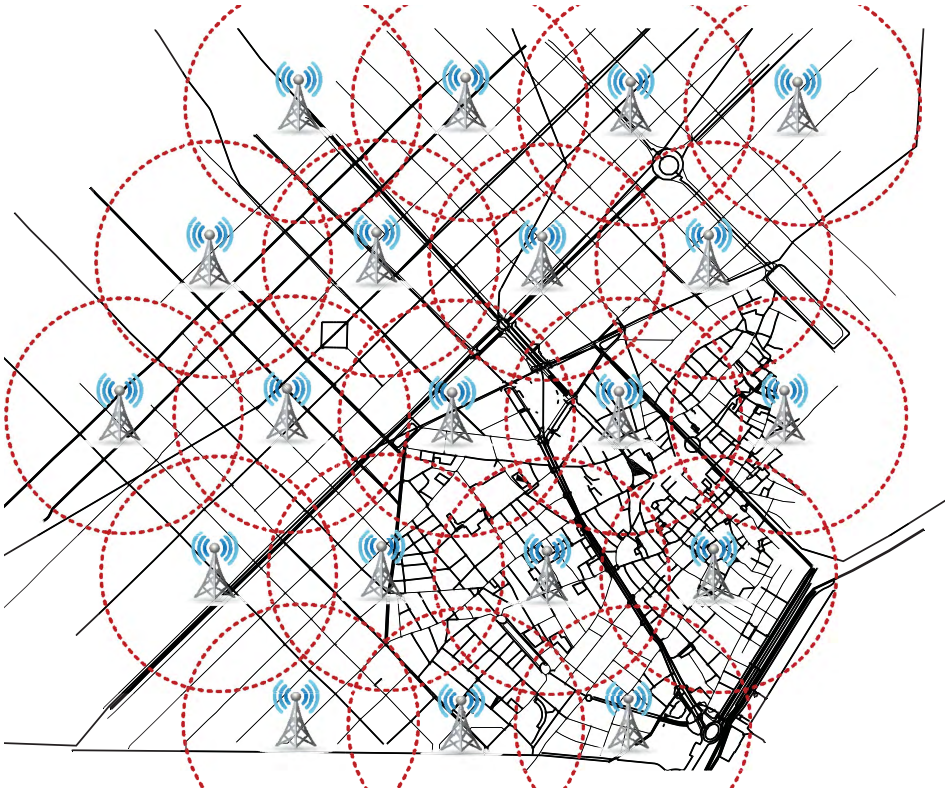
Probability of using an unknown revoked certificate IV

Using group theory we can calculate the probability of considering a certificate as a valid one when the real status known by the CA is revoked at time t

Probability of considering a certificate as a valid wrongly

$$\rho(t) = Prob(Cert \in \mathcal{U}) = \frac{E[\mathcal{U}(t)]}{E[\mathcal{O}(t)]} = \frac{p(t-t_0)}{(1-p)T_c + p(t-t_0)}$$

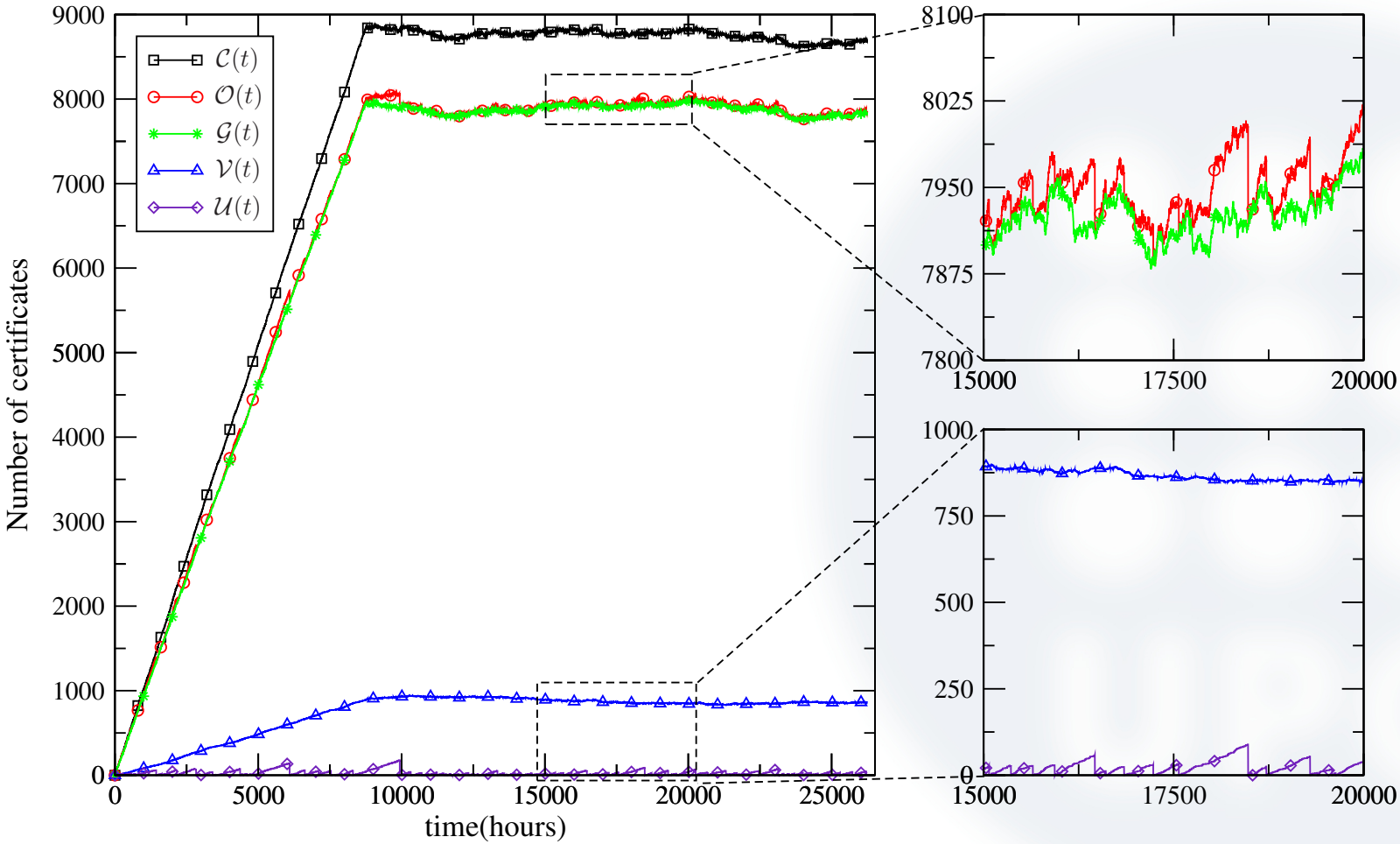
Simulation



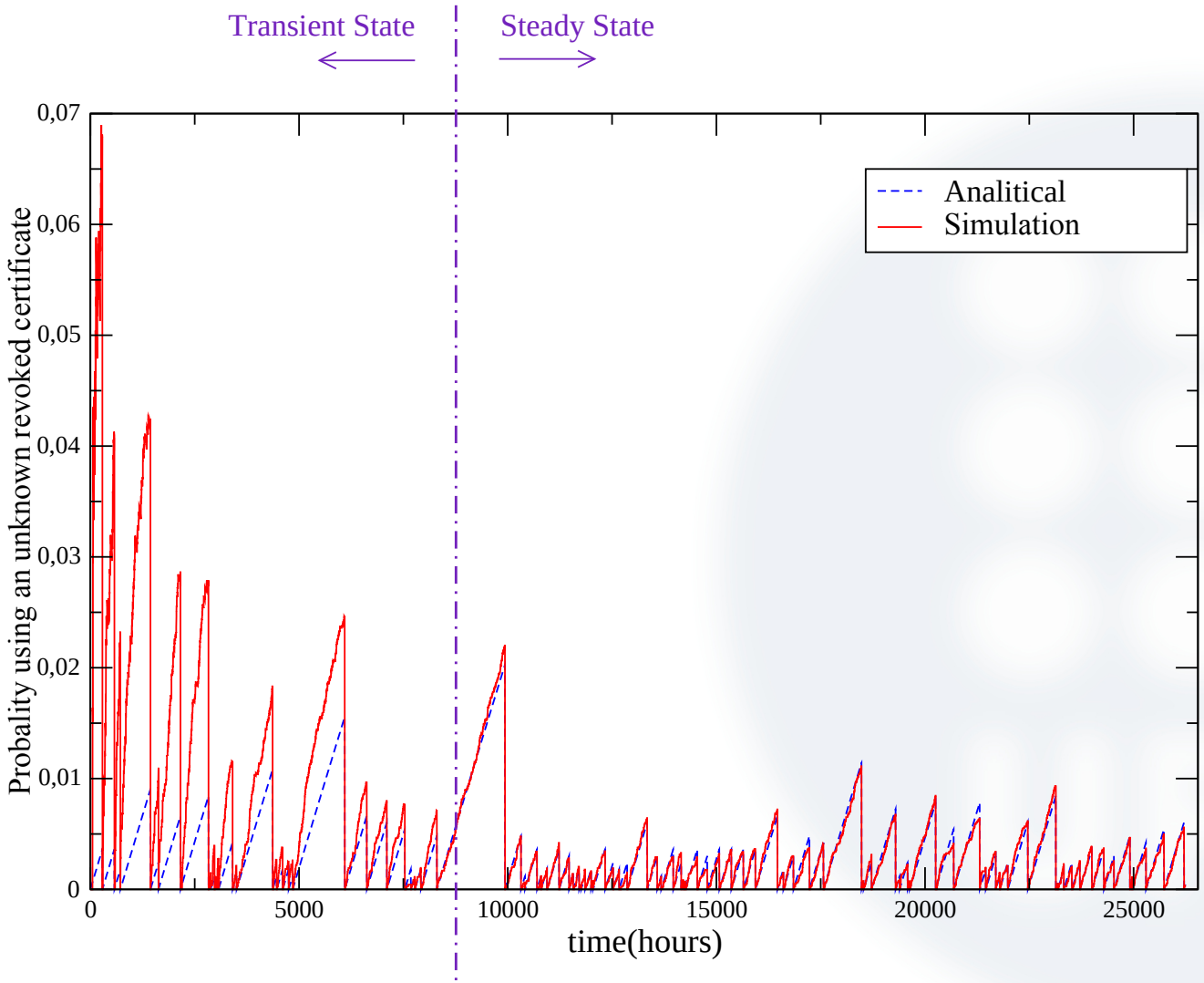
Parameter	Value
Speed	{20,30,40} m/s
Max. Acceleration	5 m/s
Max. Deceleration	3 m/s
Channel bandwidth	10 MHz
OBU receiver sensitivity	-82.0dBm
Transmission power	28.8dBm
MAC	IEEE 802.11p
Propagation model	Nakagami
Type of antenna	Omnidirectional

Table: Car Profile.

Results I


$\mathcal{C}(t)$
$\mathcal{O}(t)$
$\mathcal{G}(t)$
$\mathcal{V}(t)$
$\mathcal{U}(t)$
Number of certificates
time(hours)
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
0
5000
10000
15000
20000
25000
7800
7875
7950
8025
8100
15000
17500
20000
0
250
500
750
1000
15000
17500
20000

Results II


Transient State
Steady State
Analitical
Simulation
Probality using an unknown revoked certificate
time(hours)
0
0,01
0,02
0,03
0,04
0,05
0,06
0,07
0
5000
10000
15000
20000
25000

Risk Assessment Model for PKI

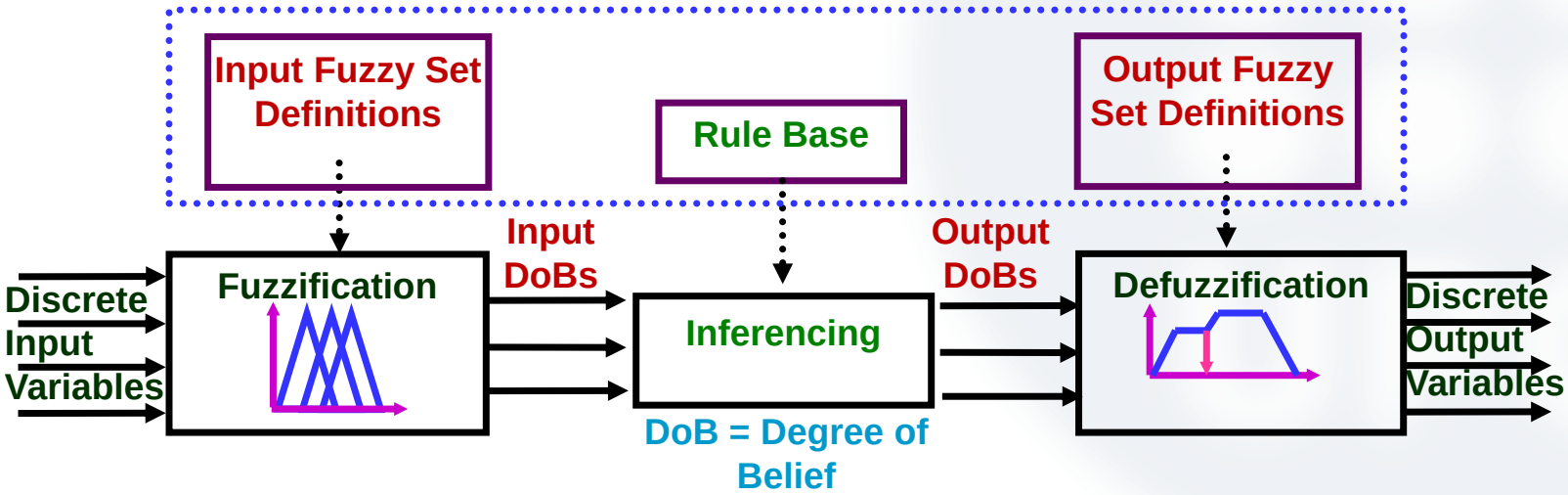
- Risk can be defined as the combination of the probability of an event and its consequences (ISO/IEC Guide 73).

Key Risk Factors

1. **Number of revoked certificates (*NumRev*)**: as users have cached CRLs which include the list of revoked certificates and their revoked date, users can know the number of revoked certificates per day;
2. **Revocation categories (*RevCat*)**: CRLs can also include the revocation cause of each certificate;
3. **Age of the CRL (CRL_{age})**: using also the information contained in the CRL; users can calculate the time elapsed since the issuance of the CRL.

Fuzzy Expert System

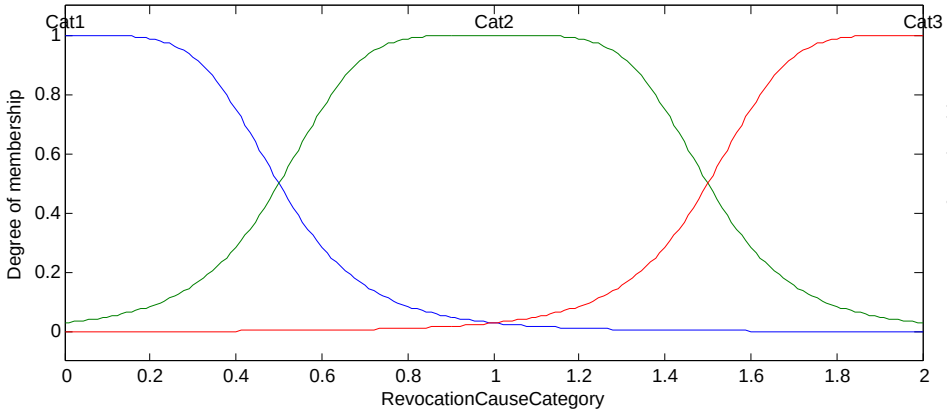
- Approximating uncertain problems
  - Measured data or Expert knowledge
- Decision-making based on logical rules
  - Rule base: Set of fuzzy rules - Expression of IF A THEN B
  - Database: Membership functions
  - Inference: Conclusion from facts & rules
  - Defuzzification: Extraction of a crisp value

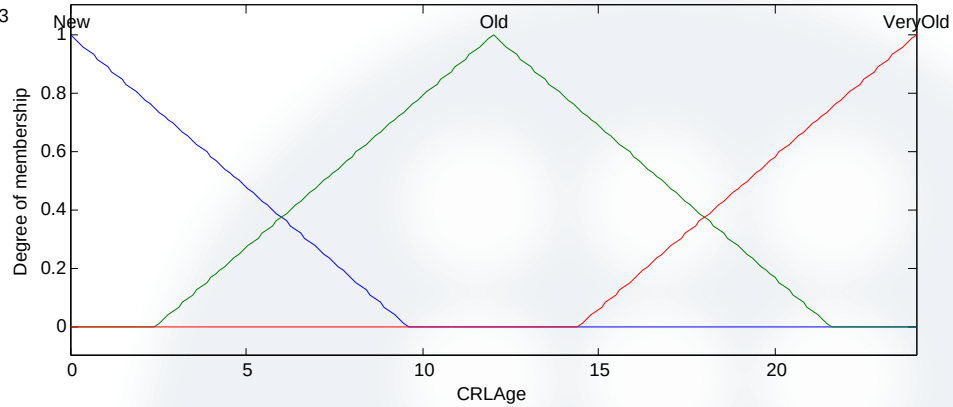


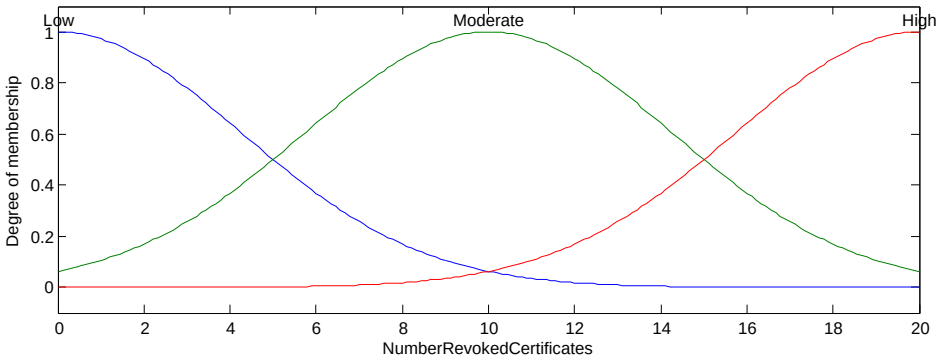
Revocation causes categorization

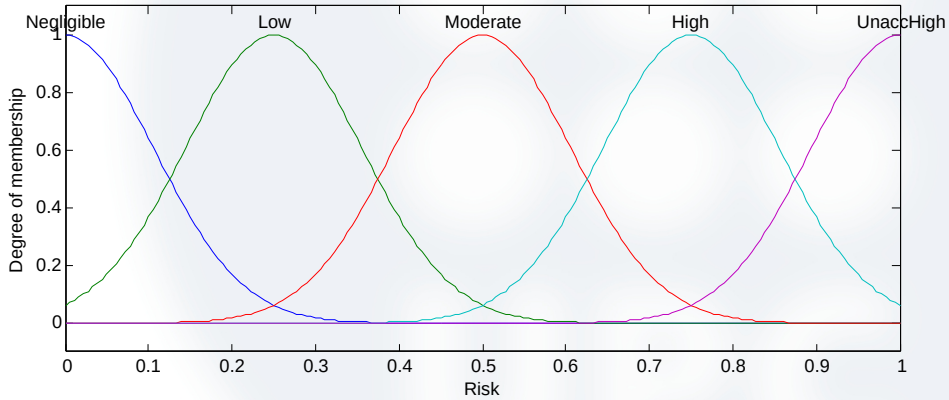
Code	Text Code	w_i	Description
(1)	`keyCompromise`	9	Private key has been compromised
(2)	`cACompromise`	10	Certificate authority has been compromised
(3)	`affiliationChanged`	1	Subject's name or other information has changed.
(4)	`superseded`	1	Certificate has been superseded
(5)	`cessationOfOperation`	2	Certificate is no longer needed.
(6)	`certificateHold`	3	Certificate has been put on hold.
(7)	`removeFromCRL`	0	Certificate was previously on hold and should be removed from the CRL.
(8)	`privilegeWithdrawn`	5	Privileges granted to the subject of the certificate have been withdrawn
(9)	`aACompromise`	10	Attribute authority has been compromised

Fuzzification membership functions









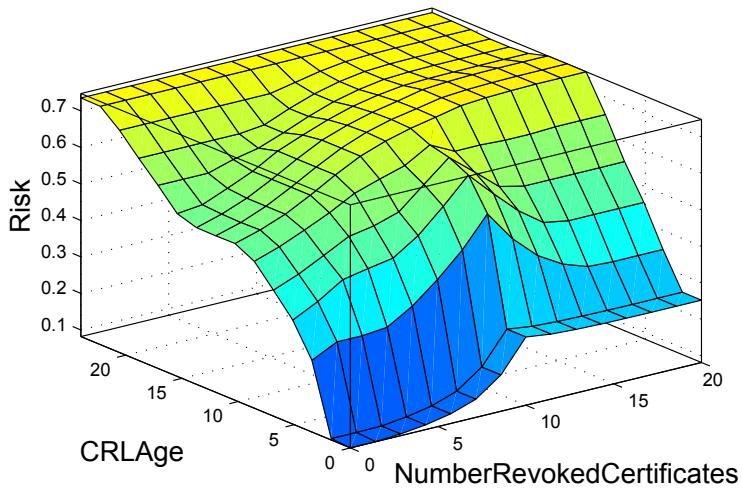
Rules for the Fuzzy Logic System

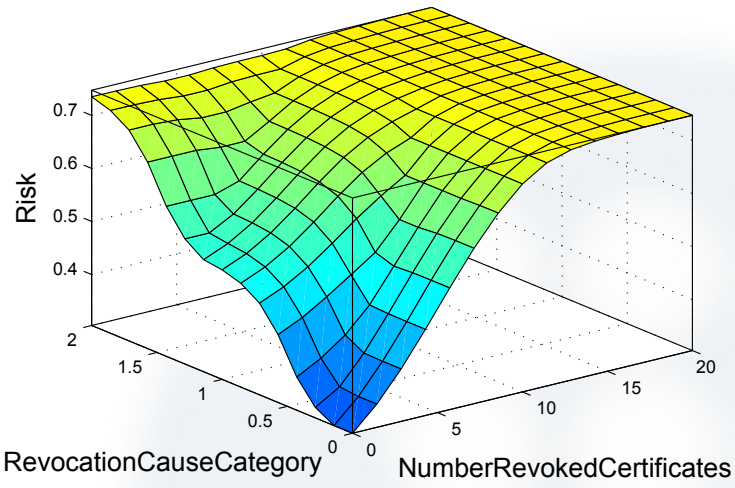
R_1: If (*NumRev* is Low) and (CRL_{age} is New) then (Risk is Negligible)
R_2: If (*NumRev* is High) and (CRL_{age} is New) then (Risk is Low)
R_3: If (*NumRev* is Low) and (CRL_{age} is Old) and (*RevCat* is Cat1) then (Risk is Low)
R_4: If (*NumRev* is Low) and (CRL_{age} is Old) and (*RevCat* is Cat2) then (Risk is Moderate)
R_4: If (*NumRev* is Low) and (CRL_{age} is Old) and (*RevCat* is Cat3)then (Risk is High)
R_6: If (*NumRev* is Moderate) and (CRL_{age} is Old) then (Risk is High)
R_7: If (*NumRev* is High) and (CRL_{age} is Old) then (Risk is High)
R_8: If (CRL_{age} is VeryOld) and (*RevCat* is Cat3) then (Risk is UnaccHigh)
R_9: If (CRL_{age} is VeryOld) and (*RevCat* is Catl) then (Risk is Moderate)
R_{10}: If (CRL_{age} is VeryOld) and (*RevCat* is Cat2) then (Risk is High)
R_{11}: If (*NumRev* is Moderate) and (CRL_{age} is New) then (Risk is Low)

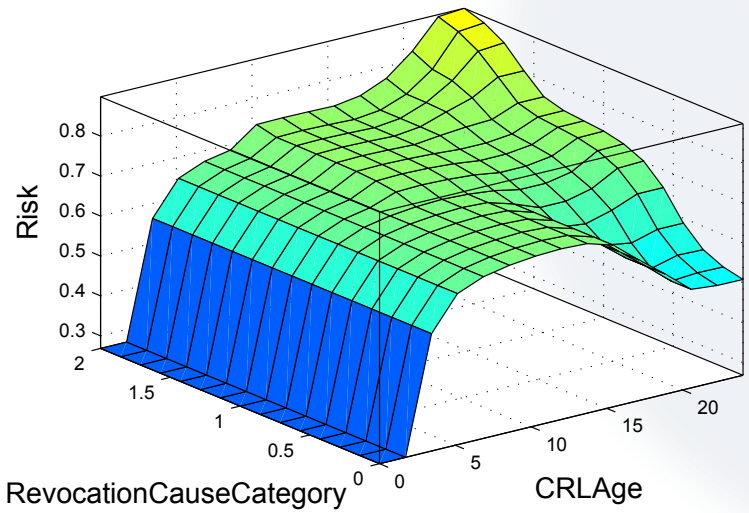
Defuzzification

- At the end of inference, the output fuzzy set is determined, but cannot be directly used to provide the operator with precise information or control an actuator.
- Centroid of area (COA) method used to convert the fuzzy output of the inference engine to crisp using membership functions analogous to the ones used by the fuzzifier.

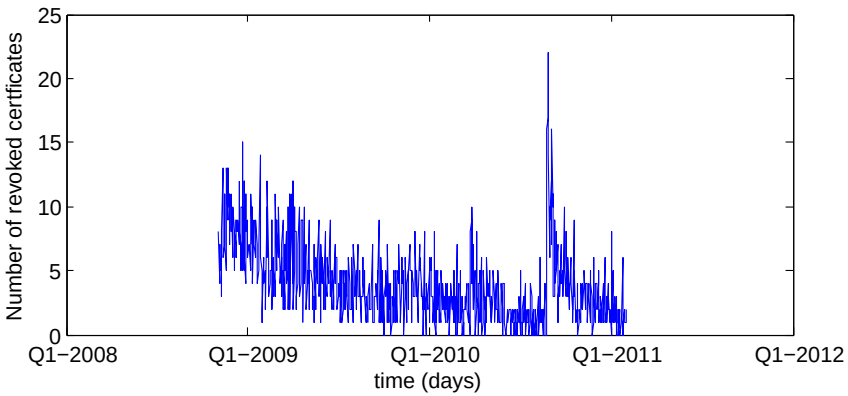
Results

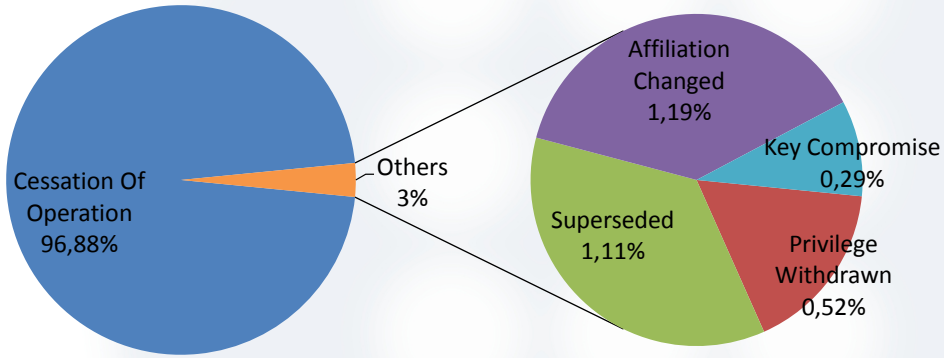

Risk
0.7
0.6
0.5
0.4
0.3
0.2
0.1
20
15
10
5
0
CRLAge
0
5
10
15
20
NumberRevokedCertificates


Risk
0.7
0.6
0.5
0.4
2
1.5
1
0.5
0
RevocationCauseCategory
0
5
10
15
20
NumberRevokedCertificates


Risk
0.8
0.7
0.6
0.5
0.4
0.3
2
1.5
1
0.5
0
RevocationCauseCategory
0
5
10
15
20
CRLAge

Case Study: GoDaddy I





Case Study: GoDaddy II

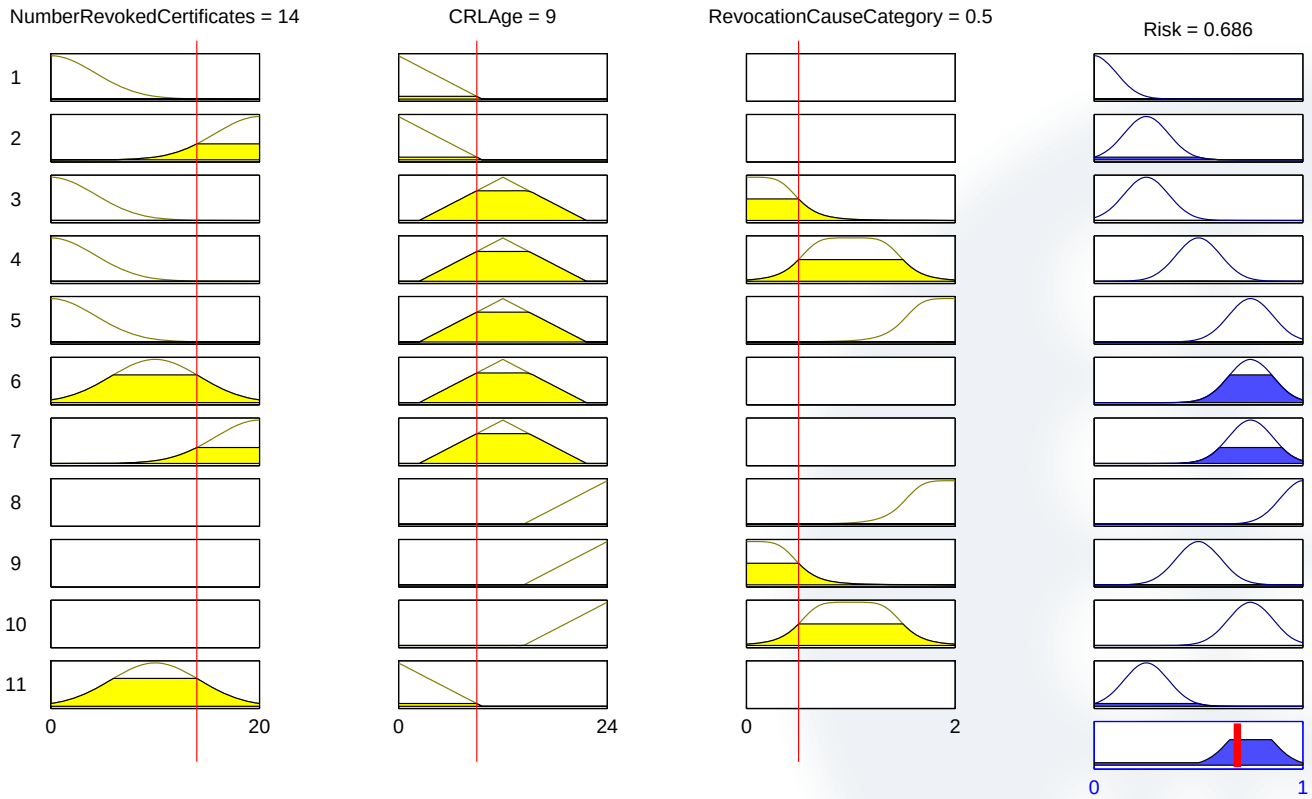


Figure: Risk output Mandani(Jan 24 09:25:44 2009 GMT)

Case Study: GoDaddy III

Day	#Revoked Cert	CRL Age	Rev Cat	Risk
24/01/2009	14	9 hours	Cat 1	0.686
22/04/2009	1	12 hours	Cat 2	0.523
21/05/2009	5	8 hours	Cat 2	0.567
18/05/2009	6	1 hour	Cat 3	0.112
25/08/2010	16	2 hours	Cat 2	0.253
27/08/2010	20	12 hours	Cat 2	0.748
16/09/2010	1	18 hours	Cat 1	0.424
28/09/2010	10	22 hours	Cat 3	0.892
22/10/2010	1	0.5 hours	Cat 1	0.0824
08/11/2010	5	10 hours	Cat 1	0.500

Table: Risk analysis score for ten days.

Conclusions

- Vehicular PKI has an inherent risk associated to the revocation mechanism
- We have developed a systematic methodology to build a fuzzy system that models risk and assists the user in the decision making process related to certificate revocation.
- OBUs can balance the risk and the cost of downloading fresh CSI.

Publications

Carlos Gañán, JoseL. Muñoz, Oscar Esparza, Jorge Mata-Díaz, and Juanjo Alins.
Risk-based decision making for Public Key Infrastructure using fuzzy logic.
International Journal of Innovative Computing, Information and Control (IJICIC), 8(11):7925–7942, 2012.

Jose L. Muñoz, Oscar Esparza, Carlos Gañán, and Javier Parra-Arnau.
PKIX certificate status in hybrid MANETs.
In *Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks*, volume 5746 of *Lecture Notes in Computer Science*, pages 153–166. Springer Berlin Heidelberg, 2009.

Outline

Revocation Service Requirements

1. *Low computational cost*: The computations performed internally by each entity (CA, RSU, and OBU) should be simple and fast.
2. *Low communication overhead*: CA-to-RSU communication (update authentication information) and RSU-to-OBU communication (answer authentication information) should be as small as possible.
3. *Security*: the authenticity of the answers given by a RSU should be verifiable.

CRL in VANETs

- Problems with CRLs in VANETs
  - Communication with infrastructure at irregular intervals
  - Varying contact times with infrastructure
  - Number of CRLs limited to storage space in OBU
  - Time to search the certificate in CRLs
  - Operating time of malicious node = avg. CRL update interval
- Expected CRL size

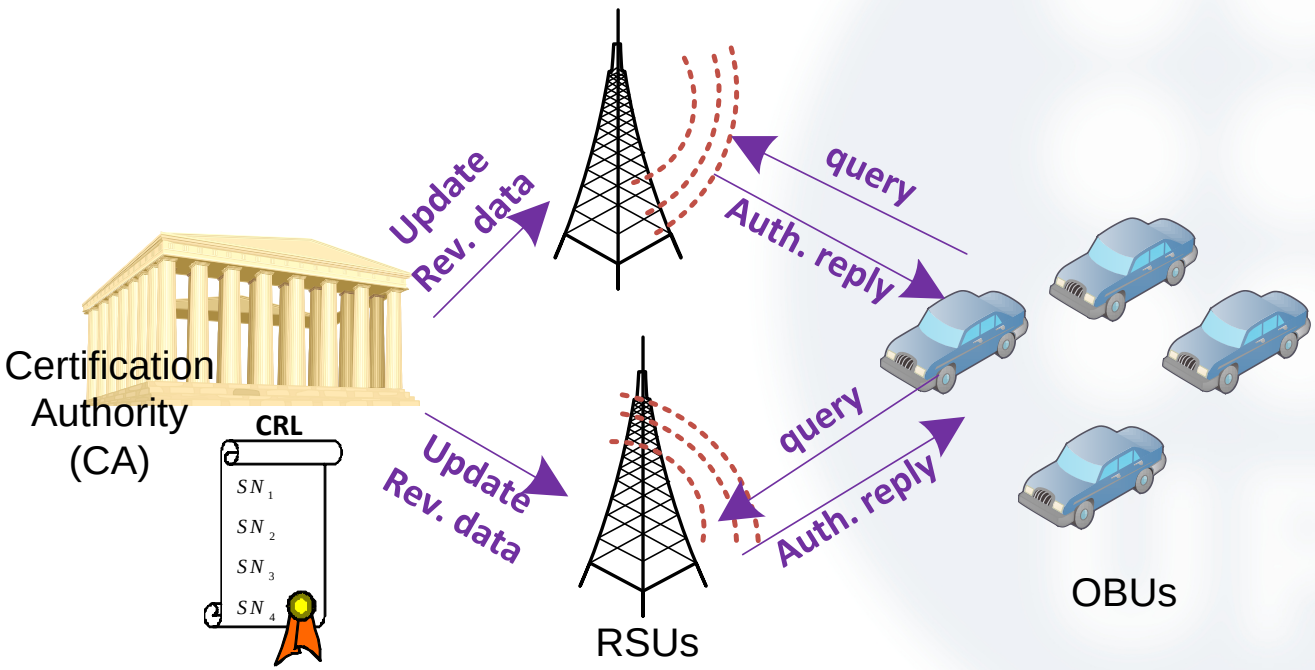
$$CRL_{size} = N_{veh} \cdot \rho \cdot \bar{s} \cdot T_c \cdot s_e$$

N_{veh}	Total number of vehicles
ρ	Percentage of certificates revoked
T_c	Validity period of a certificate
$\bar{s}$	Mean number of pseudonyms of a vehicle
s_e	CRL entry size per revoked certificate

- In Spain, $N_{veh} \approx 31,3 \cdot 10^6 \rightarrow CRL_{size} = 89,75$ GB.

Authenticated Data Structures

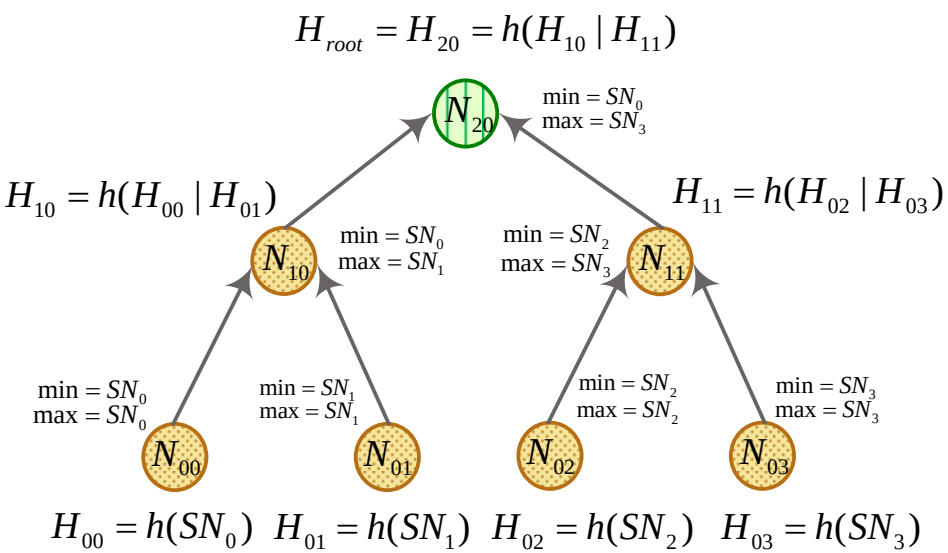
- Data structure representing a set of elements (i.e., revoked certificates) supporting authenticated membership queries and update operations



Authenticated Data Structures

- Three proposal based on the used of Merkle Hash trees:
  - COACH,
  - EvCOACH: suitable for networks with low revocation rates,
  - BECSI: suitable for networks with high revocation rates.
- Merkle Hash trees:
  - Use to prove existence of an element in a set. For instance, prove that a given certificate exists in the set $\mathcal{R} = \{SN_1, SN_5, SN_{40}, SN_{89}\}$
  - Constructed as binary tree where leaves are hash value of corresponding element.
  - Non leaf & Leaf nodes
  - Root of the MHT is digitally signed using public key signature scheme (RSA/ DSA)

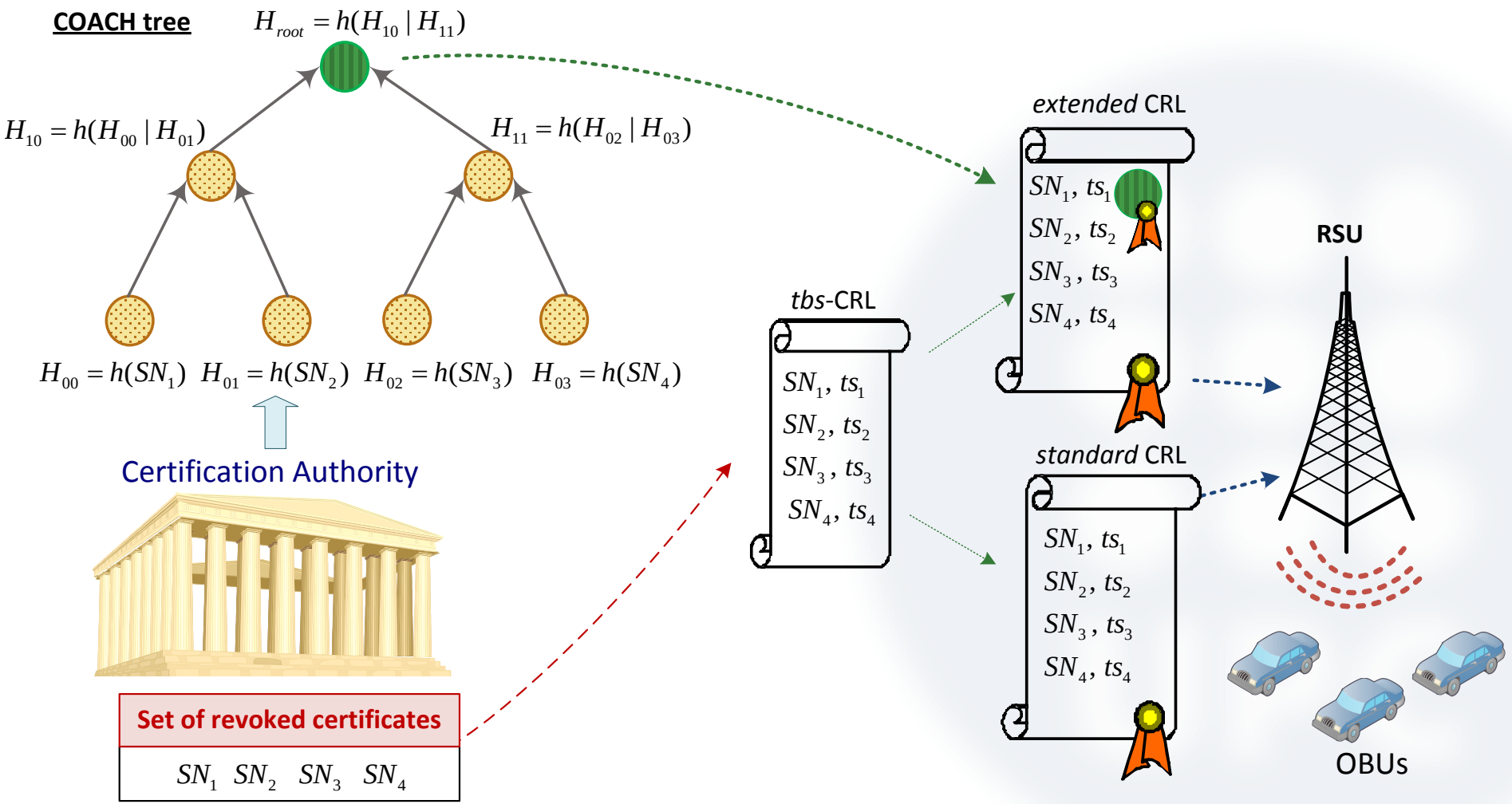
Sample COACH Tree



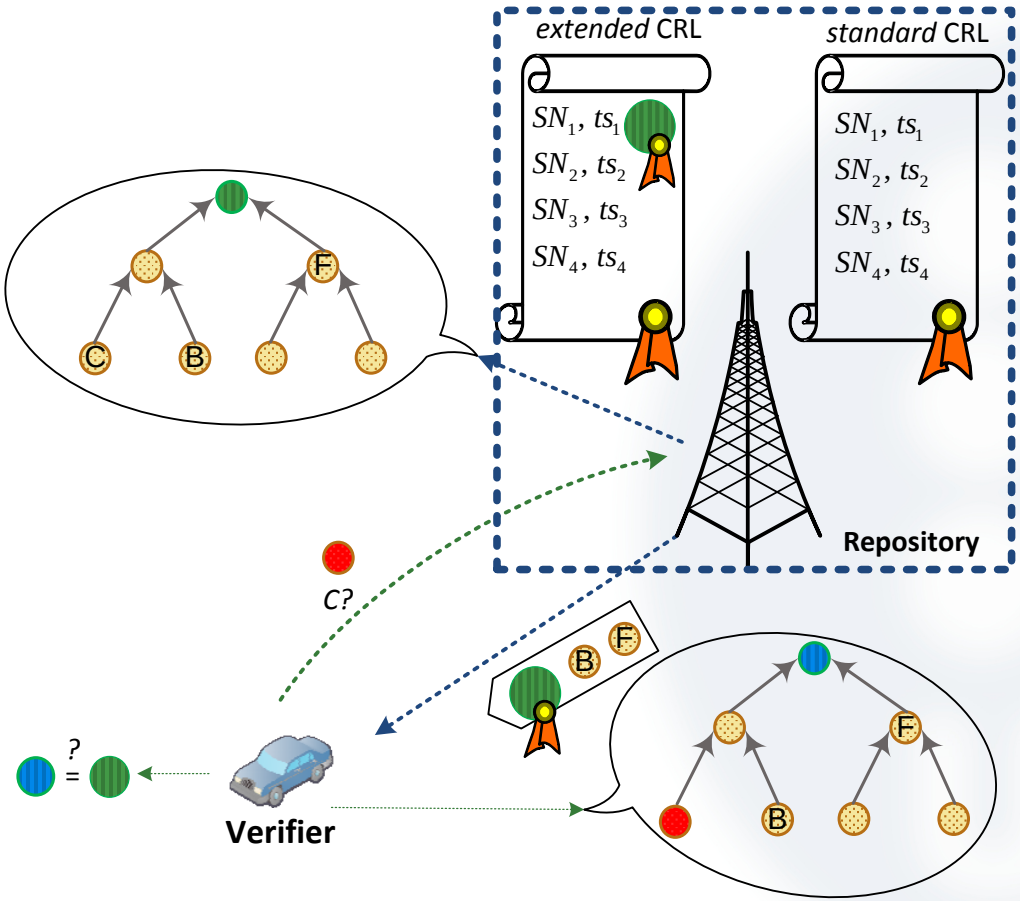
- For any node in the tree, we use the term Path to mean a sequence of nodes representing siblings of all direct ancestors of that node, i.e., the set of cryptographic values necessary to compute H_{root} from the leaf SN_j.
- The $\mathcal{D}$igest be the concatenation of the certification authority distinguished number DN_{CA}, the root hash H_{root} and the validity period of the CRL.

$$\mathcal{D}igest = \{DN_{CA}, H_{root}, Val.Period\}_{SIG_{CA}}$$

System Initialization

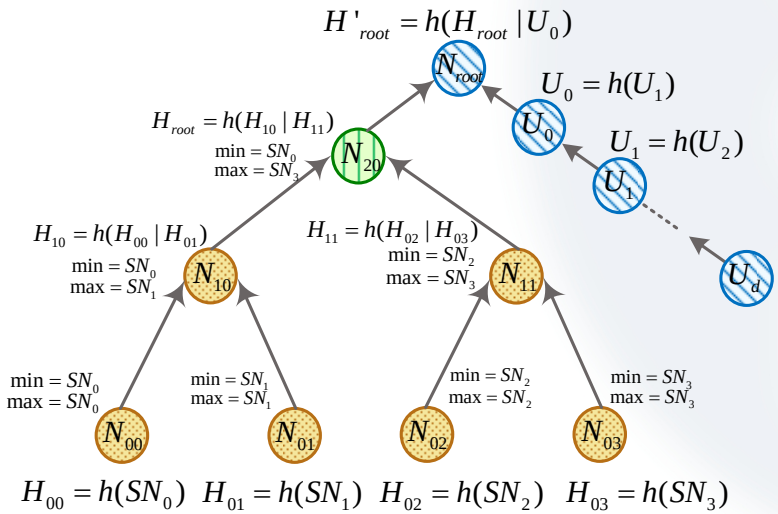


Certificate status checking I



Evergreen COACH (EvCOACH)

- Relatively few revocations per CSI validity period.
  - Same revocation information in several consecutive CRLs.
- EvCOACH prevents end-entities from downloading a new CRL whose information is already known.
- Extend the validity of a previous CRL by periodically disclosing successive values of the hash chain.
  - Embedded hash chain in the *extended-CRL*



BECSI I

- Relatively many revocations per CSI validity period.
- CSI freshness improvement by combining the use of delta-CRLs with MHTs.

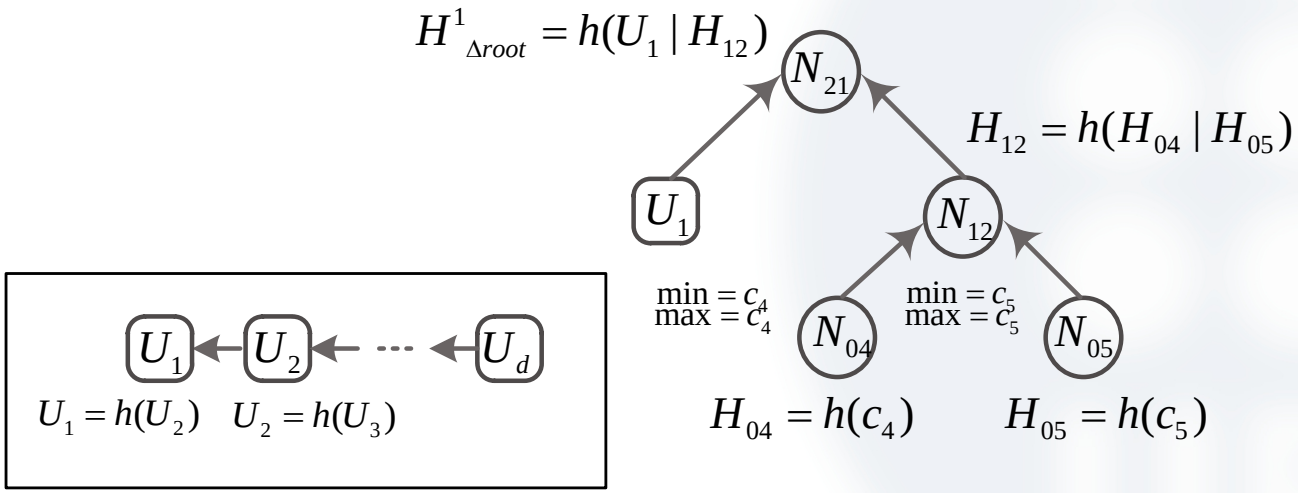


Figure: Sample BECSI Δ-tree.

BECSI II

$$\mathcal{D}\text{igest}_{\Delta_i} = \{DN_{CA}, H^i_{\Delta root}, ValidityPeriod\}_{SIG_{CA}}.$$

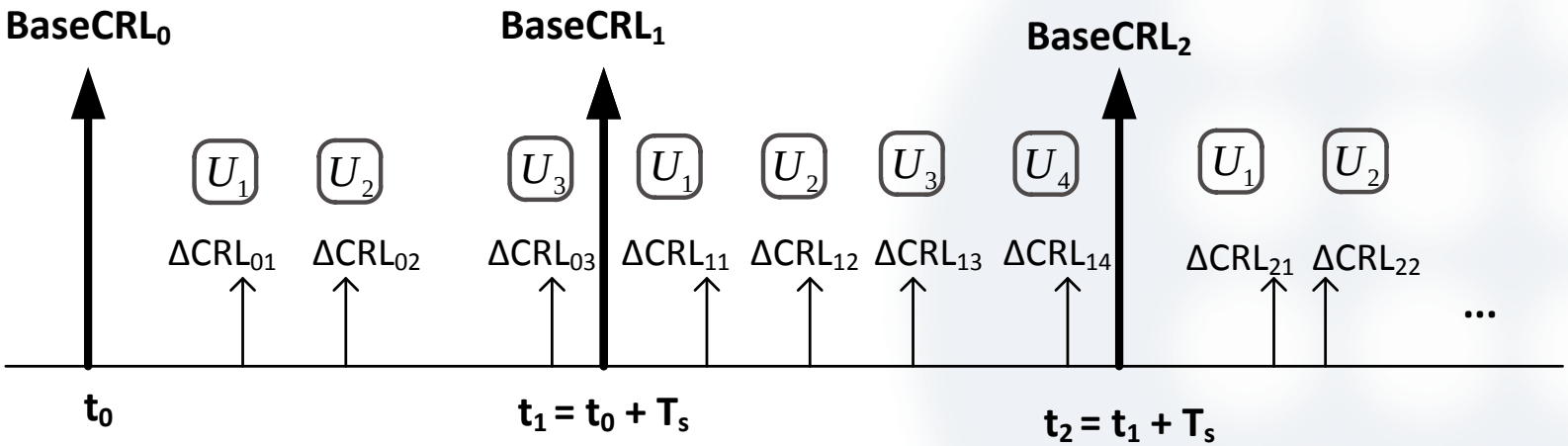


Figure: Delta-CRLs Issuance Scheduling.

BECSI III

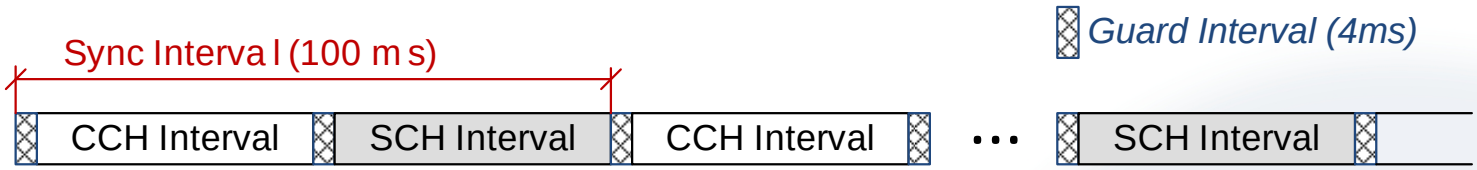


Figure: CCH/SCH timing.

$$CA \rightarrow RSUs : M = [U_i, TimeStamp]_{Sign_{CA}}$$

- 64 bytes for the ECDSA-256 CA's signature.
- 4 bytes for the timestamp representing seconds UTC since the epoch ('1970-01-01 00:00:00' UTC).
- 4 bytes for representing the U_i value.

Communication Overhead I

Mechanism	Request size	Response size
CRL	73 bytes	145 Mbytes
COACH	73 bytes	710 bytes
EvCOACH	73 bytes	725 bytes*
BECSI	73 bytes	840 bytes*
ADOPT	66 bytes	586 bytes

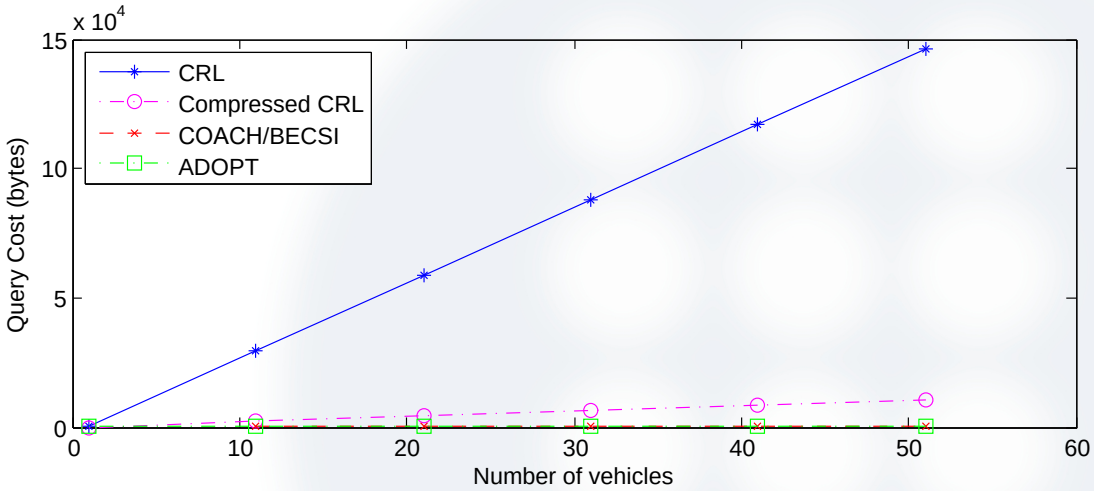


Figure: Response size vs number of vehicles.

Communication Overhead II

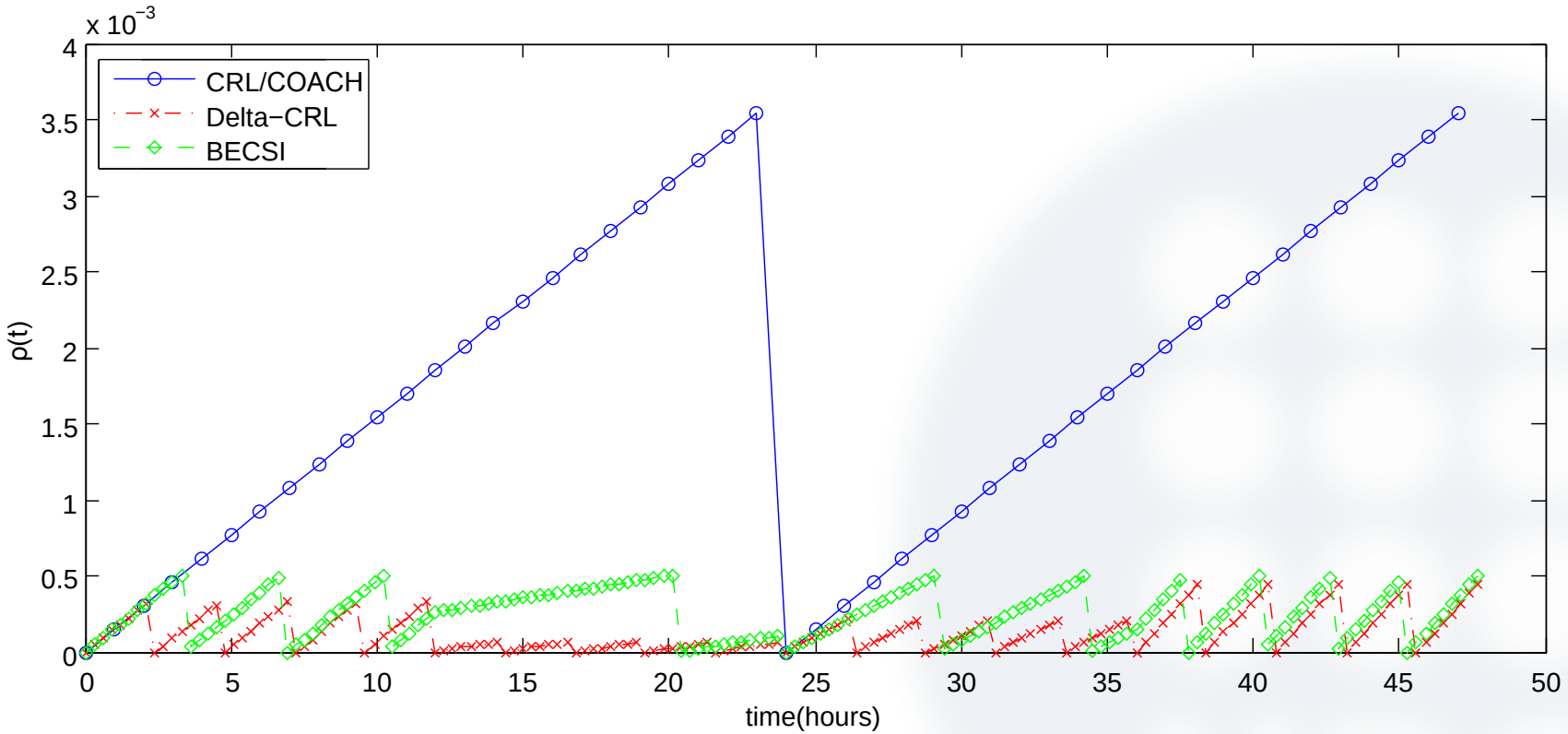


Figure: $\rho(t)$ for different revocation mechanisms.

Computational Cost

Mechanism	Verification delay
CRL	$4\,T_{mul}$
COACH	$k(\,T_{hash}(log_2 N + 1) + 4\,T_{mul})$
EvCOACH	$k(\,T_{hash}(log_2 N + i + 2) + 4\,T_{mul})$
BECSI	$k(\,T_{hash}(log_2 N + 1) + \alpha\,T_{hash}(log_2 \Delta n + 1) + 4\,T_{mul})$
ADOPT	$k(4\,T_{mul})$

Table: Computational cost of validating k certificates per revocation mechanism.

Simulation I

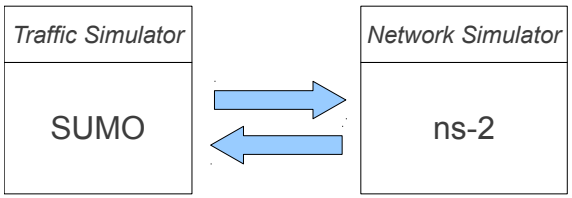


Figure: Simulation Architecture.

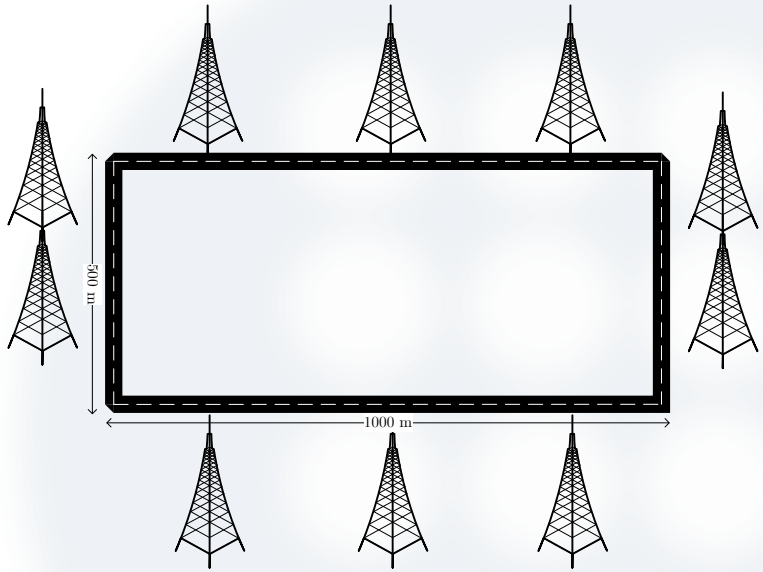


Figure: Reference Scenario.

Simulation II

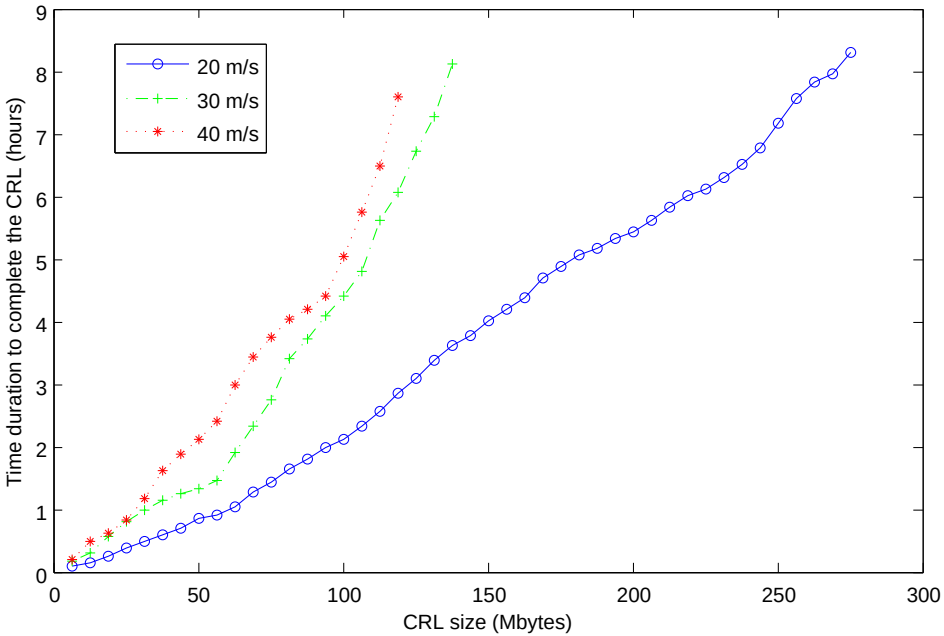


Figure: Mean time to download a CRL for a 12-vehicle scenario.

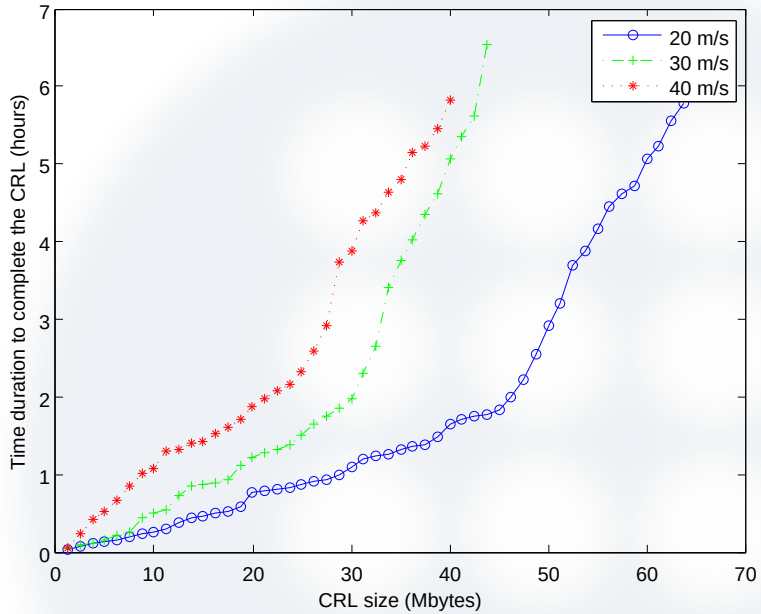


Figure: Mean time to download a CRL for a 24-vehicle scenario.

Simulation III

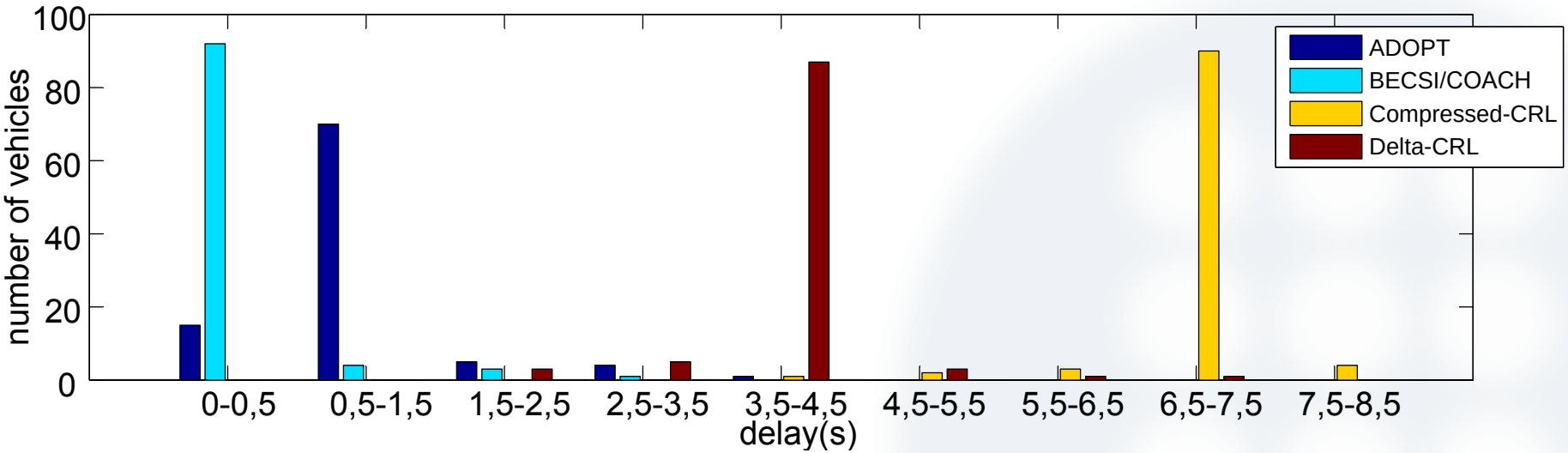


Figure: Histogram plot of time delay of the vehicles that receive the CSI depending on the revocation mechanism.

Conclusions

- Traditional way of issuing CRLs do not fit well in a VANET where huge number of nodes are involved and where several pseudonym certificates are assigned in addition to vehicle identity certificates.
- RSUs and repository vehicles can build an efficient structure based on an authenticated hash tree to respond to status checking requests inside the VANET, saving time and bandwidth
- Allocating a small bandwidth is enough to ensure that vehicles receive certificate status responses within few seconds.

Publications

Carlos Gañán, Jose L. Muñoz, Oscar Esparza, Jorge Mata-Díaz, Juan Hernández-Serrano, and Juanjo Alins.
COACH: COllaborative certificate stAtus CHecking mechanism for VANETs.
Journal of Network and Computer Applications, 36(5):1337 – 1351, 2013.

Carlos Gañan, Jose L Muñoz, Oscar Esparza, Jonathan Loo, Jorge Mata-Díaz, and Juanjo Alins.
BECSI : Bandwidth Efficient Certificate Status Information distribution mechanism for VANETs.
Mobile Information Systems, pages 1–31, 2013.
(in press).

Carlos Gañán, JoseL. Muñoz, Oscar Esparza, Jorge Mata-Díaz, and Juanjo Alins.
Toward Revocation Data Handling Efficiency in VANETs.
In Alexey Vinel, Rashid Mehmood, Marion Berbineau, CristinaRico Garcia, Chung-Ming Huang, and Naveen Chilamkurti, editors, *Communication Technologies for Vehicles*, volume 7266 of *Lecture Notes in Computer Science*, pages 80–90, Vilnius, 2012. Springer Berlin Heidelberg.

Outline

Context

- Certifications authorities provide different quality of the revocation service:
  - Take advantage of trust – biggest strength!
  - Manage risk
  - Customer loyalty

Objectives

- Modeling the impact of the revocation service on the certificates prices
  - Oligopoly of certificate providers
  - Different levels of security
  - Different warranty quantities
  - Diametrical revocation service

Demand for certificates I

- Model of the certificate market with profit-maximizing certification authorities and a continuum of network users.
- Each user faces an individual risk of operating with another user whose certificate has been revoked.
- CA will bear the liability cost due to any damage that may occur between the revocation of a certificate and the release of the CRL.
- CAs have to take into account this liability cost when establishing their price strategy.

Demand for certificates II

- Oligopoly of A CAs, indexed by $i = 1, \cdots, A-1$
- Each user has an initial wealth $w > 0$
- Let (P_i, C_i, t_i, s_i) be a certificate contract offered by CA_i which specifies the price P_i to be paid by a user and the level of coverage C_i paid to the user if an attack takes place and she operates with a revoked certificate.
- Let t_i represent the CRL updating interval, and s_i represent the security level.

Supply of certificates

- Oligopoly of CAs competing for users by offering certificates and CRLs.
- The level of service quality is mainly shown by the CRL updating interval and the security level
- CAs compete by quoting a certificate price which has associated a particular quality of service, we have Bertrand competition.

Equilibrium Certificate Providers

- Goal: Finding the prices at which CAs obtain their maximum profit.
- Recall that these certificates differ in the QoS so that $\forall i, j; i \neq j, t_i \neq t_j$ and $s_i \neq s_j$.
- Users will intend to maximize their utility, i.e.:

$$\theta^* = \arg\max_{\theta} \quad U(P_i, C_i).$$

- CAs will intend to minimize their costs.
  - Fixed Cost: release of a new CRL
  - Variable Costs: number of certificates contained in the CRL and certificate type
- We can calculate the gain function G_i of any CA_i:

$$G_i = \theta^* P_i - Q(s_i, t_i),$$

  where the gain function captures the overall profits of CA_i for a given certificate product characterized by (P_i, C_i).
- The price of each CA P_i^* and the corresponding coverage C_i^*.

$$P_i^* : \frac{\partial G_i}{\partial P_i} = 0, \quad C_i^* : \frac{\partial G_i}{\partial C_i} = 0.$$

Game Equilibrium I

- Asssume that the CA indexed by $i = 1$ offers better quality than the second CA in both QoS parameters, i.e., $t_1 < t_2$ and $s_1 > s_2$.
- the value of θ^* at which a user has no obvious trend between the certificates offered by different CAs:

$$\theta^* = \frac{\alpha_1 \left(P_1 - P_2 + \pi C_1(1 + RC_1 - R\pi C_1) - \pi C_2(1 - RC_2 + R\pi C_2)\right)}{\pi \alpha_2 K}$$

- So the market demand of CA_2 is θ^*, and the demand of CA_1 is $1 - \theta^*$.
- We obtain the certificate price and the coverage in the equilibrium :

$$P_1^* = \frac{2\pi\,\alpha_2 K}{3\alpha_1} \qquad P_2^* = \frac{\pi\,\alpha_2 K}{3\alpha_1}, \qquad C_1^* = C_2^* = \frac{1}{2R\left(-1+\pi\right)}.$$

Game Equilibrium II

From these results we can conclude that:

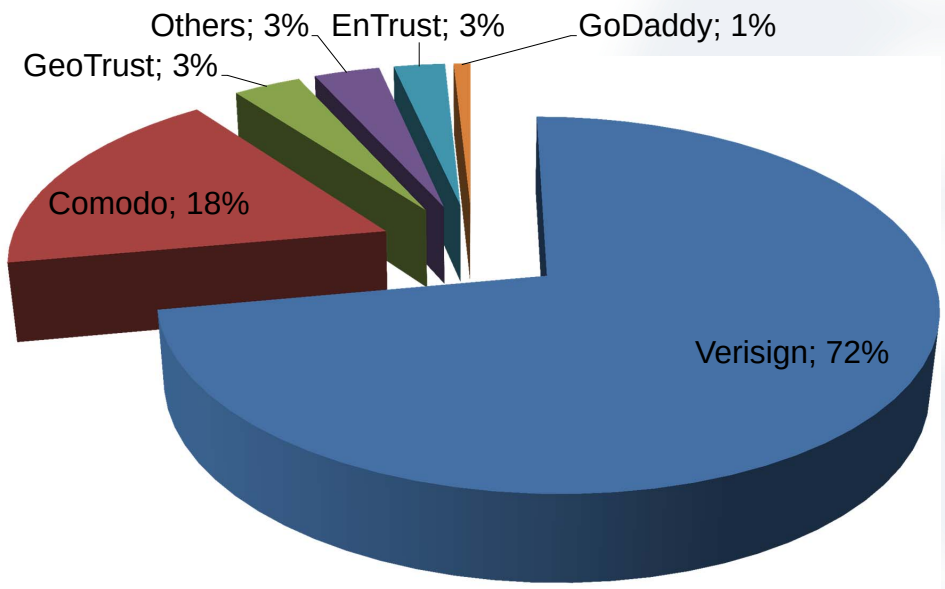
- In the equilibrium, when both CAs achieve their maximum gain, CA_1 obtains a higher price than CA_2. This is mainly due to the fact that when both CAs have associated the same probability of an attack, as the QoS of the first CA is better so that CA_1 can set a higher price per certificate.
- In the equilibrium, the coverage that each CA should establish is the same and is inversely proportional to the risk-aversion and the probability of operating with a revoked certificate.

SSL Certificate market I

SSL Provider	Product Name	Price/Year($)	Warranty($)	Assurance	Mean Issuing time	Mean CRL lifetime
COMODO	EnterpriseSSL Platinum	311.80	1,000,000	High	Under 1 hour	4 days
COMODO	InstantSSL Pro	169.80	100,000	High	Under 1 hour	4 days
Verisign	Secure Site Pro Cert	826.67	2,500,000	High	2-3 days	15 days
Verisign	Managed PKI for SSL Std	234.00	100,000	High	2-3 days	15 days
GeoTrust	QuickSSL Premium	118.00	100,000	Low	Immediate	10 days
GeoTrust	True BusinessID	159.20	100,000	High	2 days	10 days
Go Daddy	Standard SSL	42.99	10,000	Low	Immediate	1 day
Go Daddy	Standard Wildcard	179.99	10,000	Low	Immediate	1 day
Entrust	Advantage SSL Certificates	167.00	10,000	High	2 days	1 week
Entrust	Standard SSL Certificates	132.00	10,000	High	2 days	1 week
Thawte	SSL 123	129.80	-	Low	Immediate	1 month
Thawte	SGC Super cert	599.80	-	High	2 days	1 month

SSL Certificate market II

Regarding the market share, the CA which leads the SSL Certificate market is VeriSign. Note that according to these data, a monopolistic assumption or even a duopoly between Verisign and Comodo will be reasonable as they hoard most of the market.



Determinant factors for the certficate prices I

- Multivariate regression analysis explaining the yearly price of SSL certificates.
- General regression investigates and models the relationship between a response (Certificate price) and predictors (Warranty, issuing interval and CRL lifetime).
- We determine how the certificate price changes as a particular predictor variable changes.

$$Price/Year(\$) = 98 + 0.00022\ W - 0.55\ \overline{I_{time}} + 8.6\ \frac{1}{\overline{CRL_{Lf}}},$$

$$Price/Year(\$) = 20 + 0.00022\ W - 0.55\ \overline{I_{time}} + 8.6\ \frac{1}{\overline{CRL_{Lf}}},$$

where W denotes the warranty, $\overline{I_{time}}$ is the mean issuing time, and $\overline{CRL_{Lf}}$ is the mean lifetime of the CRLs issued by the CA.

CAs Gain/Loss I

- GoDaddy competes not only in prices but also in QoS to gain market share.
- As our model shows, the reaction of GoDaddy to compete in the oligopoly is to offer better quality of service.
- GoDaddy is the CA that issues CRLs more often. Using this CRL releasing policy, users increase their utility and, at the same time, the probability of operating with a revoked certificate is also reduced. However, the variable costs increase due to this way of issuing CRLs.
- Note that VeriSign, the leading CA, is the one who is offering the worst QoS, both in terms of CRL lifetime and time to issue a new certificate.
- Providers that are offering better QoS (i.e. GoDaddy or Comodo) are having gains, while providers that have the worst QoS with similar prices are having loses (i.e. Verisign).
- Depending on the QoS, prices and revocation probability each provider suffers gains or losses

SSL Provider	9 Month Gain/Loss
Verisign	-3.38%
Comodo	2.15%
GeoTrust	-0.17%
Others	0.71%
EnTrust	0.07%
GoDaddy	0.51%

Conclusions

- The market of certificate providers can be described as an oligopoly where oligarchs compete not only in price but also in quality of service.
- We have modeled this oligopoly using a game theoretic approach to find the prices in the equilibrium.
- We have been able to capture the QoS of the products offered by a CA, by means of the timeliness of the revocation mechanism and the security level.

Publications

Carlos Gañán, Jose L. Muñoz, Oscar Esparza, Jorge Mata-Díaz, and Juanjo Alins.
Impact of the Revocation Service in PKI Prices.
In TatWing Chim and TszHon Yuen, editors, *Information and Communications Security*, volume 7618 of *Lecture Notes in Computer Science*, pages 22–32, Hong Kong, 2012. Springer Berlin Heidelberg.

Outline

Conclusions I

- The revocation process is statistically self-similar. The degree of self-similarity (measured in terms of the Hurst parameter H) is a function of the overall utilization of the revocation service and can be used for measuring the "burstiness" of the revocation process (i.e. the more bursts in the revocation process the higher H).
- We have presented a new metric that quantifies the confidence the recipients can have while accepting messages signed using certificates that are not present in the CRLs at the OBU. Moreover, we have developed a systematic methodology to build a fuzzy system that models risk and assists the user in the decision making process related to certificate revocation.

Conclusions II

- We have proposed novel efficient revocation mechanisms for VANETs, which substantially reduce the overhead of the certificate status checking. Thus, we decrease the vulnerability window that a misbehaving vehicle has and this results in higher safety level for VANET.
- The market of certificate providers can be described as an oligopoly where oligarchs compete not only in price but also in quality of service. We have modeled this oligopoly using a game theoretic approach to find the prices in the equilibrium. We showed that although the undercutting process in certification prices seems similar to the price setting behavior of firms in Bertrand competition there exists a crucial difference depending on the QoS of the revocation service.

Future Work

Future Work

- Analysis of the impact of the revocation service on the user's anonymity.
- Proposal of a new revocation mechanism that allows CAs controlling the risk depending on the revocation rate.

Certificate Status Information Distribution and Validation in Vehicular Networks

Carlos H. Gañán
carlos.ganan@entel.upc.edu

Advisor: José L. Muñoz Tapia
Co-advisor: Óscar Esparza
Department of Telematics Engineering (UPC)

Doctoral Dissertation Defense

Barcelona, September 4, 2013

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Departament d'Enginyeria Telemàtica

Checking status non-revoked certificate

To check revocation status, a client sends a request containing the certificate serial number, say SN_{target}, to its closest repository. If C_i is not revoked, the response consists of:

1. Two adjacent leaf nodes SN_{minor}, SN_{major} such that $SN_{minor} < SN_{target} < SN_{major}$
2. Two paths: one from SN_{minor} and one from SN_{major} to the root.
3. The $\mathcal{D}$igest.

The client must check that:

1. $SN_{major} \in \Phi$.
2. $SN_{minor} \in \Phi$.
3. $SN_{minor} < SN_{target} < SN_{major}$.
4. SN_{minor} and SN_{major} are adjacent nodes.