Quantisation feasibility and performance of RSS-based secret key extraction in VANETs

Mirko Bottarelli [1] Gregory Epiphaniou [1] Dhouha Kbaier
Ben Ismsail [1] Petros Karadimas [2]

[1]Wolverhampton Cyber Research Institute, University of Wolverhampton, UK

[2]School of Engineering, University of Glasgow, Scotland

June 2018

Cyber SA 2018

Outline

Vehicle Ad-hoc NETworks

- Decentralised **networks of vehicles' on-board-units** (OBUs) and **road-side units** (RSUs)
- Provide **Safety-related** services, **Navigation-related** information and **Infotainment**
- System security challenged by the network properties and service constraints

VANETs Security

- **Symmetric** techniques are not applicable
- Proposed **Public Key Cryptography** has drawbacks

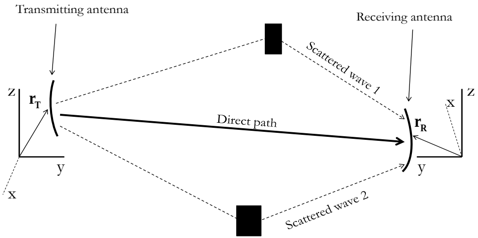
Symmetric (bits)	RSA and Diffie-Hellman (bits)	Elliptic Curve (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

NIST Recommended Key Sizes

- Physical layer imperfections can be harnessed to **unconditionally** secure wireless communications

Physical Layer Security

Multipath propagation phenomena



- **Shared** → multipath effects almost identical for both communicating parties (**Channel reciprocity**)
- **Secret** → correlation rapidly vanishes with time and distance (**Channel variability**)

The Extraction Process

Advantage distillation	Quantisation of channel characteristics
↓	
Information reconciliation	Correction of disagreements due to imperfect reciprocity
↓	
Privacy amplification	Enhancing key robustness

Aims and objectives

Aims

- Evaluation of RSS-based **Level Crossing** quantisation in VANETs

$$Q(x) = \begin{cases} 1, & \text{if } x > q_+ \\ 0, & \text{if } x < q_- \\ \text{dropped} & \text{otherwise} \end{cases}$$

Objectives

- Optimization of system parameters
- Reliability of the protocol against VANETs requirements
- Search of possible improvement directions

Evaluation metrics

- **Key entropy**

$$H = \sum_{i=0}^{N} -p_{0,i} log p_{0,i} - (1 - p_{0,i}) log(1 - p_{0,i})$$

  where $p_{0,i}$ is the probability of bit i being 0.
- **Bit Mismatch Rate** $\rightarrow$ the ratio of mismatch bits between legitimate parties to the total number of quantised bits
- **Bit Generation Rate** $\rightarrow$ the number of secret bits generated per unit time or per sample

The theoretical model

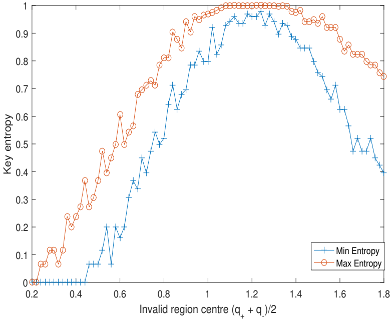
- Channel modeled as narrow-band frequency-invariant V-V channel with three-dimensional scattering

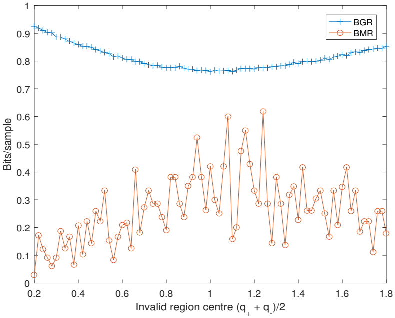
$$G_N(t) = \sum_{l=1}^{L} |\alpha_l| exp(j\phi_l) exp(j2\pi v_l t)$$

- $L = 20$ multipath components with constant magnitude $|\alpha_l|$ and random phase $\phi_l \sim U[-\pi, \pi]$
- the Doppler effect v_l adds up the contributions of transmitter, receiver and scatterers in a three-dimensional environment

The simulation 1/2

Fixed invalid region size of $q_+ - q_- = 0.4$

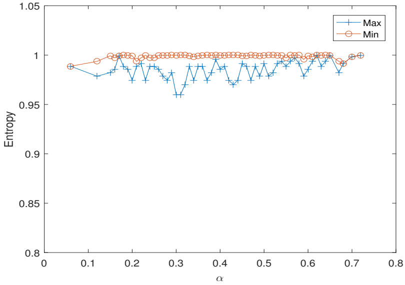


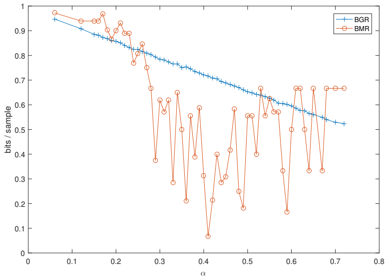


- Original LC algorithm achieves $BGR \sim 0.2$ bits/sample, whilst the improved scheme records ~ 0.76 bits/sample
- Higher results (> 0.8) achieved, sacrificing key robustness

The simulation 2/2

Thresholds computed as $q_{\pm} = mean(\underline{\hat{h}}) \pm \alpha \cdot stdev(\underline{\hat{h}})$
Parameter α determines the invalid region size.





- Optimal value $\alpha = 0.3$ achieves $BGR \sim 0.85$ bits / sample

Conclusions and future work

- Original LC algorithm generates a shared secret key in not less than two seconds, whilst improved version takes half a second
- Performances are inadequate if the constraints of safety-related applications (10Hz frequency and $< 100ms$ latency) are considered
- Possible improvements
  - probing rate adaptation
  - design of a smarter thresholds strategy to exploit the dynamic characteristics of the channel

Thank you