Chaotic-based Security for Near Field Communication in Internet of Things devices

PRESENTER:

Colin Sokol Kuka, PhD
UNIVERSITY OF YORK
sk1759@york.ac.uk

Colin Kuka, University of York
Researcher at the University of York
Lecturer and Programme Leader Electrical and Electronic Engineering at The City of Liverpool College
Research interests:
Control and Security Wireless Power Transfer, Memristor, Artificial Intelligence, [1-2]
Algorithms in Photovoltaic Management Systems [3-5]
Near Field Communication NFC

- Easy to use
- Portable
- Key, Ticket, ...

Security?
Near Field Communication (NFC)

NFC is based on Secure Hash Algorithms (SHA-256)

Based on the “Hash function”
https://www.xorbin.com/tools/sha256-hash-calculator
New Topology of NFC

- Switch Power dissipation
- Additional circuit to control the switching time
- Security issues – based on algorithms
- Memristors

Highest Level of Encryption
New Topology of NFC

- No switches
- No Additional circuit
- Highest Level of Security – No Copy

<table>
<thead>
<tr>
<th></th>
<th>WTP (NFC)</th>
<th>M-WPT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
<td>Transmitted (Harvested)</td>
<td>Harvested</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>Oscillation</td>
<td>Chaos</td>
</tr>
<tr>
<td><strong>Distance</strong></td>
<td>Over 30 cm (10 cm)</td>
<td>10 cm</td>
</tr>
<tr>
<td><strong>Operating Frequency</strong></td>
<td>Up to 13.5 MHz</td>
<td>Up to 7 KHz</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>Timing, Switches and Data Algorithm</td>
<td>Data</td>
</tr>
<tr>
<td><strong>Receivers</strong></td>
<td>Many</td>
<td>Only one</td>
</tr>
</tbody>
</table>
Simulations

Time step of the chaotic behaviour when the receiver is disconnected (highlighted in yellow): the LC and memristor voltage $V_{LC}$ and $V_M$ in receiver and transmitter, in purple and green respectively. At the disconnection (in the 3rd graph), the receiver memristor holds its last status as shown in the 4th graph in blue.

Data transmission at 3Kbps, it is possible to notice the time of switching (highlighted in green) the chaotic behaviour in the LC, the memristor voltage and the internal status in the 4th graph.
Chaotic waveform

Synchronisation of Chaotic waveforms:

\[
\begin{align*}
\frac{dv_1}{dt} &= \frac{1}{C_1} [(v_2 - v_1)G - f(v_d)] \\
\frac{dv_2}{dt} &= \frac{1}{C_2} [(v_2 - v_1)G - i_L] \\
\frac{di_3}{dt} &= -\frac{1}{L_T} [v_2 - R_0i_3]
\end{align*}
\]

where the \( f(v_d) \) is the diode function:

\[
f(v_d) = G_bv_1 + 0.5(G_a - G_b)[|v_1 + B_p| - |v_1 - B_p|]
\]

Synchronisation of the phase portraits of a chaotic attractor: voltage in the inductor \( V_{LC} \) referred to the memristor voltage \( V_M \) in the transmitter (a) and receiver (b) coil; current in the inductor \( i_L \) referred to the memristor voltage \( V_M \) in the transmitter (c) and receiver (d) coil; the memristor voltage \( V_M \) referred to its internal voltage status \( V_0 \) in the transmitter (e) and receiver (f).
Experiments

Experiment results: a) chaotic behaviour of the voltage in the primary (yellow) and secondary (blue) coil; voltage in the primary (yellow) and secondary (blue) memristor; c) voltage in $R = 1 \Omega$ for current measure in the primary (yellow) and secondary (blue) coil; d) XY-plot of the single attractor phase portrait.

The prototype transmitter highlighted in orange, the receiver in red and the coupling transformer in blue.
IoT web application

Use of Python and use chaotic encryption for web resources.
References


