Distributed Key Management in Microgrids

Micro sElf-orgaNiSed mAnagement (MENSA)

Prof. Christos Xenakis

Department of Digital Systems

University of Piraeus, Greece.

Email: xenakis@unipi.gr

Vaios Bolgouras, Christoforos Ntantogian, Emmanouil Panaousis, Christos Xenakis, " Distributed Key Management in Microgrids." *IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2125-2133, March 2020.*

SealedGRID: Scalable, trusted, and interoperable platform for secured smart grid

European Commission | Horizon 2020 European Union funding for Research & Innovation

SealedGRID

Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no 777996.

https://www.sgrid.eu/

Facebook: https://www.facebook.com/SealedGRIDH2020/

Twitter: https://twitter.com/sealedgridh2020?lang=en

LinkedIn: https://www.linkedin.com/in/sealedgrid-project-98246b187/

YouTube: https://www.youtube.com/channel/UC7k6Lz_RgV9GDPYyTi8qtTA

Sealed GRID

SealedGRID: Scalable, trusted, and interoperable platform for secured smart grid

UNIVERSITY OF PIRAEUS

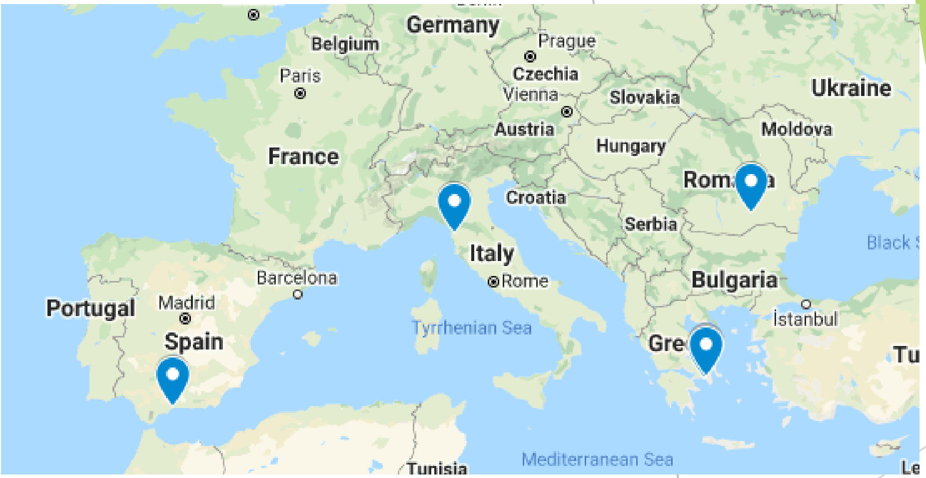
UNIVERSIDAD DE MÁLAGA

Beia CONSULT INTERNATIONAL

NEUROsoft

FOGUS INNOVATIONS & SERVICES

cnit



European Commission

Horizon 2020
European Union funding
for Research & Innovation

Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no 777996.

Smart Grid and renewable energy sources

Environmental responsibility

Diversify energy mix

Increasing demand for energy power

Multiple energy producers

Microgrids

- A microgrid is formed by **a group** of electricity ***producers*** and ***consumers***
- Typically **connected** to a **Smart Grid**
- Can operate **autonomously** in an **“islanded”** mode
- Network of **interconnected smart devices**
- Bidirectional **M2M communication**
- **Power consumption**-oriented **smart applications**

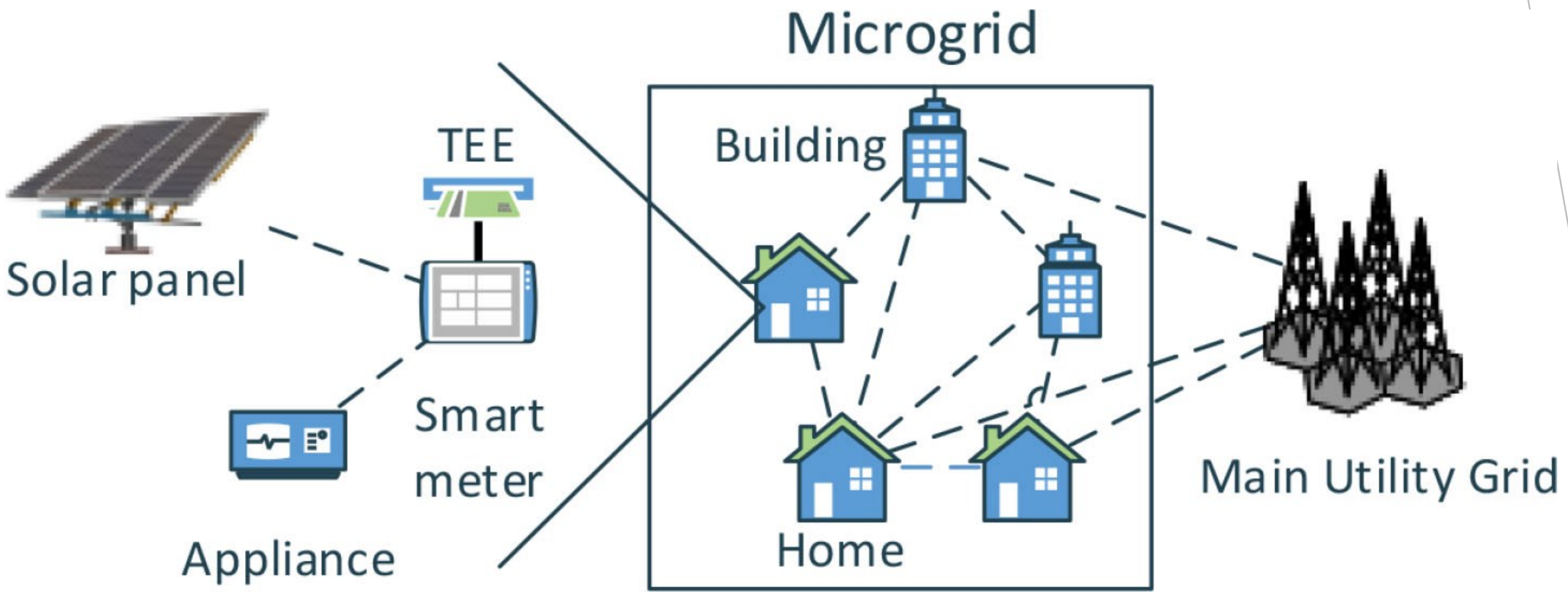
Challenges for Key Management in Microgrids

- **C1:** High **churn rate** (frequent **join** & **leave** of nodes), causes **overhead** to centralized structures & solutions
- **C2: Compromised** Certification Authority (CA)
  - **Revocation** of all issued certificates
  - **Impairment** of information exchange
- **C3: Dependability** to the CA
  - **Unable** to validate certificates if **connectivity** with the **CA is lost**
- C4: The **CA** constitutes a **single point of failure**

MENSA: Micro sElf-orgaNiSed mAnagement

- Distributed & scalable **key management** and **authentication scheme** for microgrids
- Hybrid solution utilizing **Public Key Infrastructure** and **Web of Trust** concepts
- Allows **frequent** actions of **“Join”** and/or **“Leave”** without impacting on the network’s efficiency
- **Compromised CA** does not necessarily result in performing **certificate revocation**
- Network’s operational continuity **does not depend** on the **CA’s availability**
- No **single point of failure** due to decentralized nature

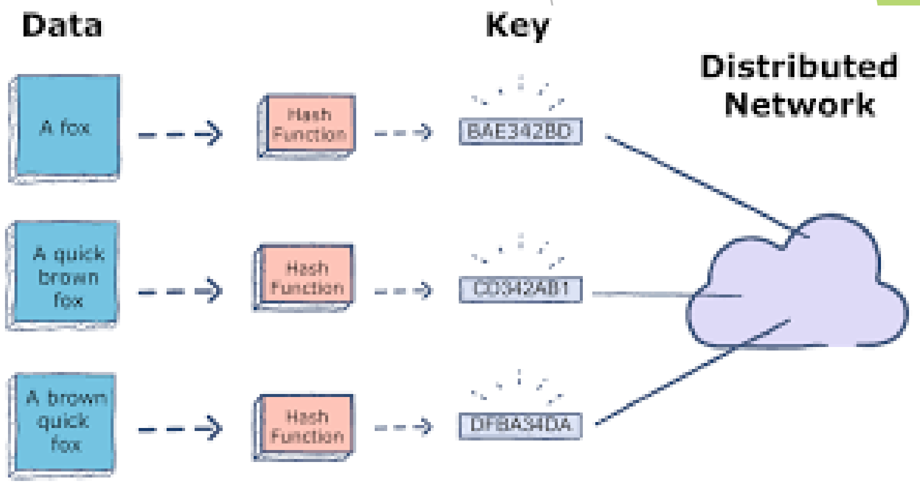
Functional Components

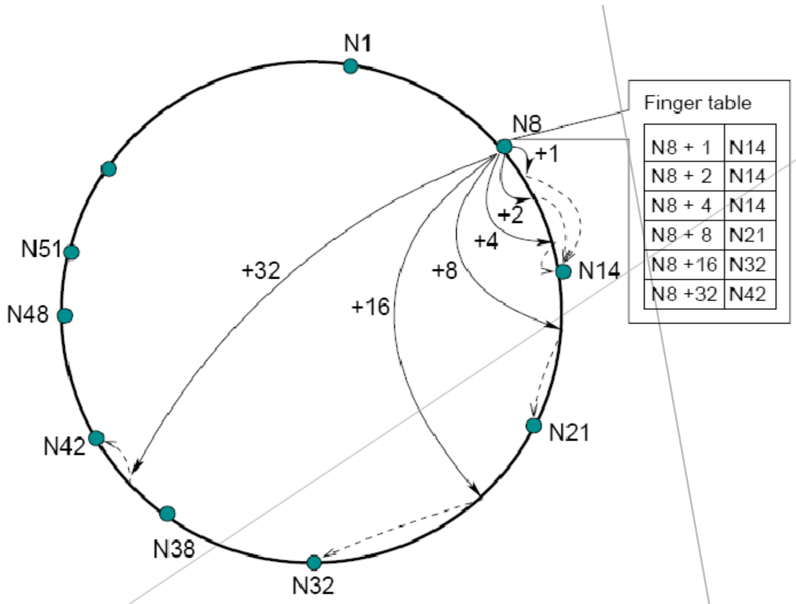


**Trusted Execution Environment resides in the smart meters*

Technical Background

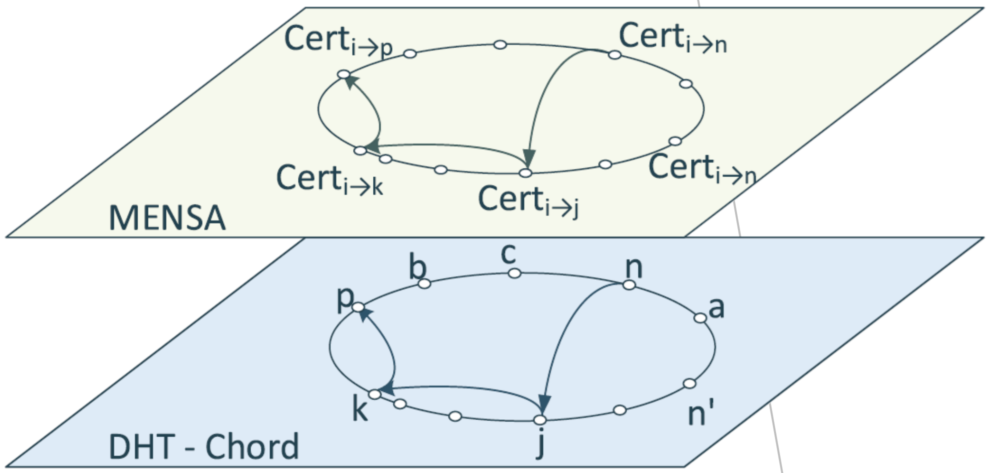
- **Distributed Hash Tables - DHT**
  - **key, value pairs** are stored in a **distributed manner** among the network participants
  - **Value** is retrieved based on its **paired key**
- **Chord Protocol**
  - Defines **key assignment** to the network
  - Provides queries to **locate the value** of a corresponding **key**
  - **“Finger Table”** defines nodes that can be communicated with

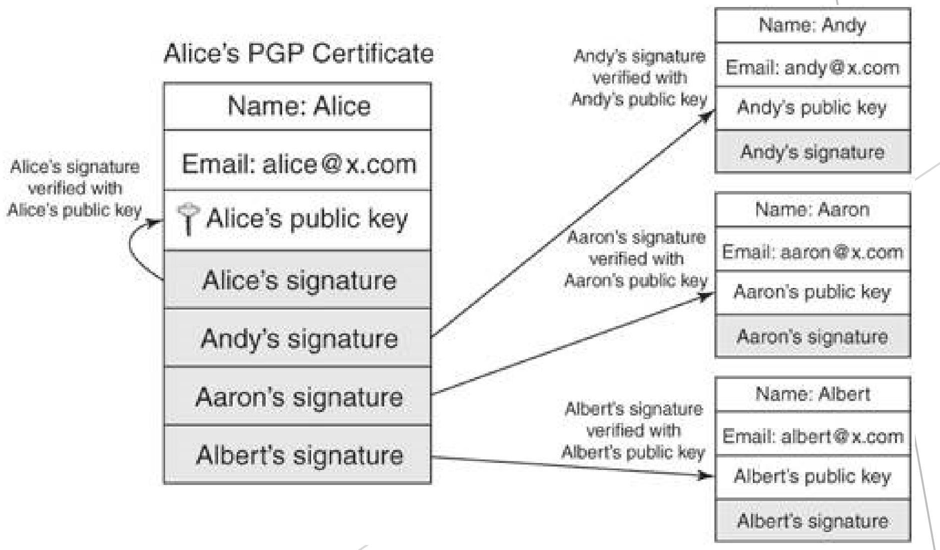




MENSA Architecture

- Each node ***n*** possesses **key pair *Pk_n/Sk_n***
- ***Pk_n/Sk_n*** follows the self-generated approach
- Overlay pair → **(*K_n* , *$Cert_n$*) as (key, value)**
  - ***$K_n = h(Pk_n + ID_{device})$***
  - ***$Cert_n$*** follows the **OpenPGP** format
- **Finger tables** contain nodes that:
  - Hold **position** defined by Chord protocol
  - Possess a **valid certificate**
- If ***a*** wants to communicate with ***b***
  - ***a*** retrieves ***b's* certificate**
  - if ***a*** trusts it or its trust path
  - ***a*** communicates with ***b***

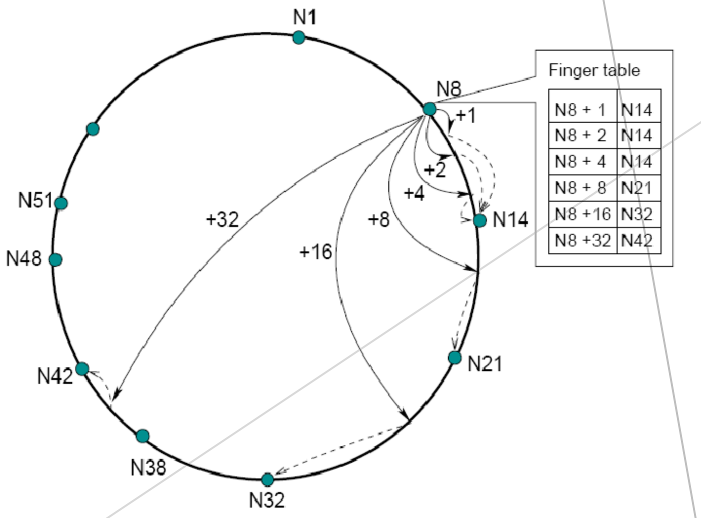




Node Join – node n

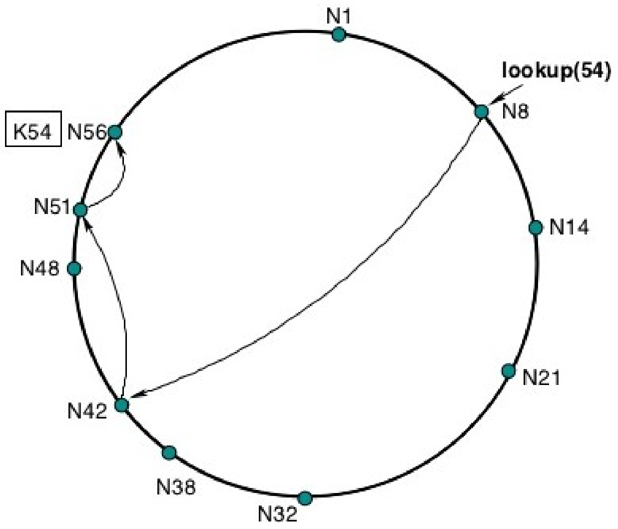
- ***n's Cert$_n$*** should be signed by <u>at least one</u> **"Introducer"** (trusted members of the structure)
- If the ***Cert$_I$*** of the **introducer is invalid**, the process **stops**
- ***n*** verifies the **validity** of the ***Certs*** assigned to the nodes ***n's* finger table** by chord
- Each node in ***n's* figure table** also checks the validity of the node ***n's Cert$_n$***
- Validation can be also performed using **remote attestation**

Function *nodeJoin(k)*
- **if** $Cert_i$ *is valid* **then**
  - **while** *next* (IP_k) *to be stored in* $fingerTable_n$ **do**
    - **if** $Cert_k$ *is signed by introducer i* **then**
      - // $Cert_k$ is trusted
      - n stores IP_k in $fingerTable_n$
    - **end**
  - **end**
- **end**



Normal Operation

- **n** accumulates signatures from **multiple endorsers**
- Operations **not affected** if an **Introducer gets compromised**, other endorsements are utilized
- Searches are executed as defined by the **Chord protocol**



Function $n.find(n')$

if n' *resides in* $n.fingerTable$ **then**

`// n' is trusted`

return success

else

send request to the next trusted node p closest to n' from node n

if n' *resides in* $p.fingerTable$ **then**

`// n' is trusted`

return success

else

send request to the next trusted node k closest to n' from node p

.

.

.

end

end

`// No trust chain was found`

return failure

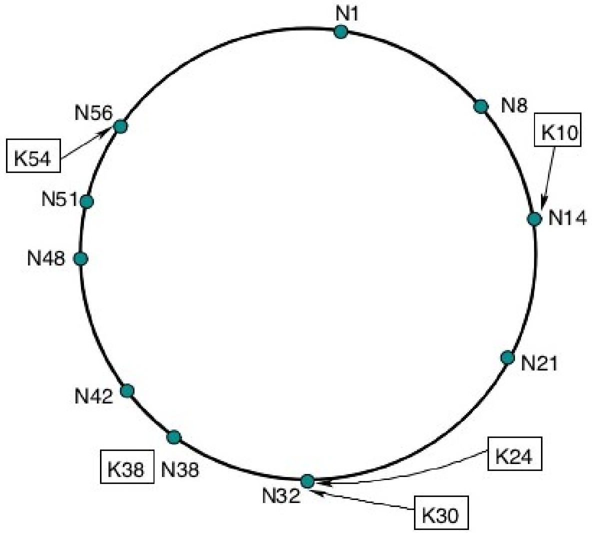
Algorithm 2: Searching for another network node.

Certificate Revocation

- There are **three ways** to revoke a **Cert** in **MENSA**
- 1st **Implicitly,** when a **Cert expires**
  - Nodes with expired **Certs** will have to get through the **verification process** again
- 2nd **Explicitly,** by the owner using a revocation Cert, ***RevC****n* (created together with *Cert**n*)
  - ***n*** sends its ***RevC****n* to the nodes that are included in **its figure table**
- 3rd **An empowered node** is able to revoke ***n's*** Cert using ***RevC****n*
  - Misbehavior can be detected using **specification-based methods + remote attestation**
  - The ***RevC****n* is sent only to the nodes that have **the leaving node** in their **finger tables**
- **Trusted Execution Environment** is used to avoid **abuse** of revocation certificates

Node Leave

- **Implicit** or **explicit** certificate revocation
- **Re-organization** of finger tables
- Affected nodes will need to check the **certificates** of the **newly** assigned nodes



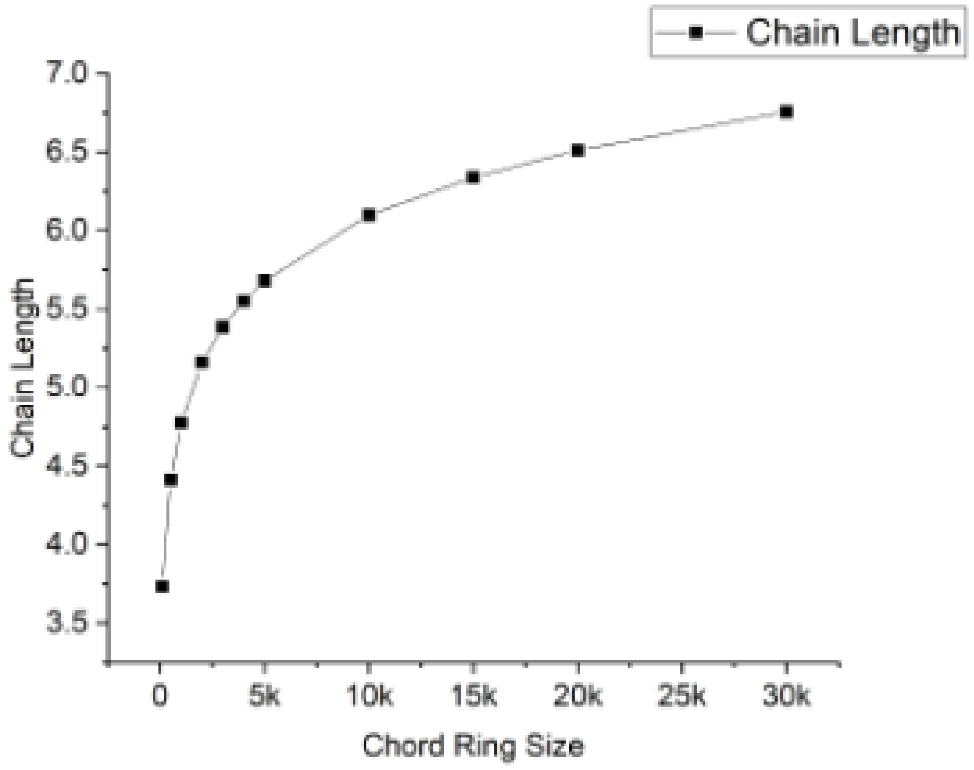
Evaluation – Node Join delay

- Scenario 1: Node **Join time delay** (0 – 30.000 nodes)
  - For 0 – 5.000 nodes the **delay is 1.55 sec**
  - While from 20.000 – 30.000 the **delay is 2.2 sec**
- The **slight decline in performance** is the byproduct of the overall **increased requests**
- **Negligible impact** of **signing** and **validation delays**
- Minimal increase in nodes saved at **finger tables** ***O(log N)***
- **MENSA is scalable**

N	fingerTable size
500	8
5,000	12
15,000	13
30,000	14
.	
.	
5,000,000	22

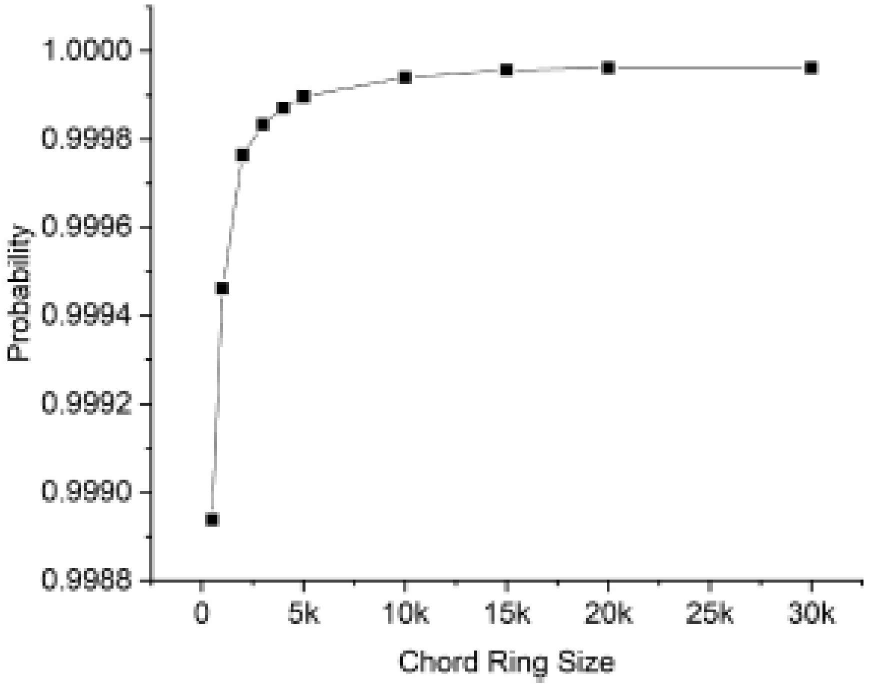
Evaluation – Chain Length

- **Scenario 2:** Ordered **list of certificates** starting from the **node initiating a look-up** operation up to the **target node**
- Mean length of the **chain of trust**
- It includes the **initiator** & the **target** node
- Chain length varies from **1 - 5 nodes**
- No **significant changes** are perceived in MENSA as the **size of the grid increases**



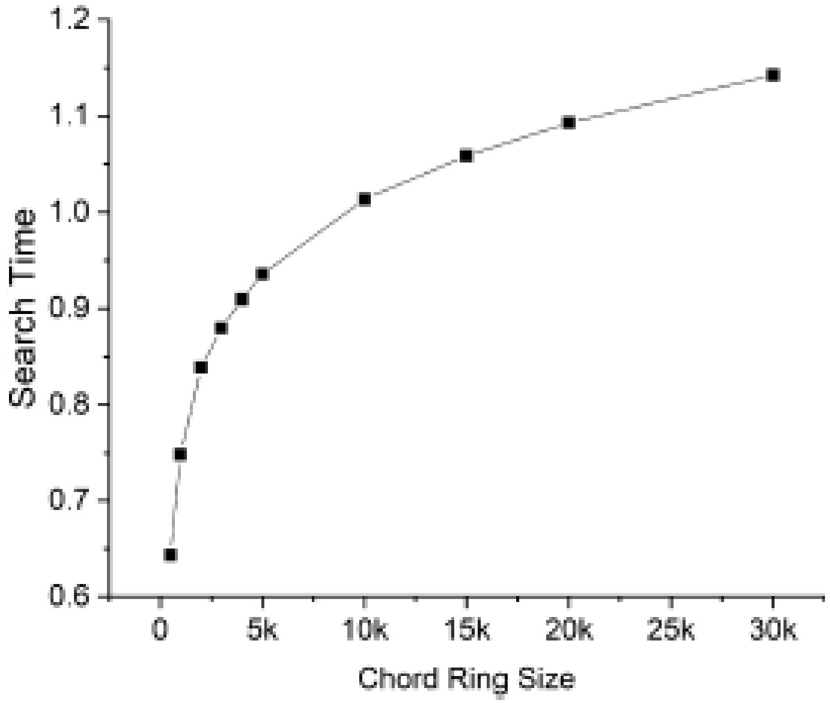
Evaluation - Probability of finding trust

- The **probability** that **two random nodes** will be able to **establish trust relationship** between them



Evaluation - Search time

- **Average time needed** for a random node to establish **trust relationships** with another random node



Conclusions

- MENSA is the **first distributed hybrid key management** and **authentication system** for microgrids
- It **eliminates** the need for **a TTP**, while ensures **high availability**
- DHT is used for **efficient discovery of trust relationships** among the microgrid nodes
- It is a **decentralized** and **flexible** solution that promotes **scalability** and **resilience**
- Paves the way toward **developing microgrids** further and it will help **realizing their full potential** in terms of scalability and performance efficiency

Thank you!

Prof. Christos Xenakis

Department of Digital Systems

University of Piraeus, Greece.

Email: xenakis@unipi.gr